Network & Information Security

Sub. Code : 22620

EDITION : 2020

INCLUDES-I SCHEME PATTERN
SAMPLE PAPERS

MSBTE I SCHEME PATTERN
T. Y. DIPLOMA SEM VI (ELECTIVE-II)
COMPUTER ENGINEERING PROGRAM GROUP
(CO/CM/IF/CW)

- SIMPLIFIED & CONCEPTUAL APPROACH

SOLVED MSBTE PAPERS

- SUMMER 2015 • WINTER 2015 • SUMMER 2016 • WINTER 2016
- SUMMER 2017 • WINTER 2017 • SUMMER 2018 • WINTER 2018
- SUMMER 2019

TECHNICAL® PUBLICATIONS
SINCE 1993
An Up-Thrust for Knowledge

I. A. Dhotre
V. S. Bagad
M. S. Kalbande

SUBJECT CODE : **22620**

As per Revised Syllabus of

MSBTE - I SCHEME

T.Y. Diploma Semester - VI (Elective - II)
Computer Engineering Program Group
(CO / CM / IF / CW)

NETWORK & INFORMATION SECURITY

Iresh A. Dhotre
M.E. (Information Technology)
Ex-Faculty, Sinhgad College of Engineering
Pune

Vilas S. Bagad
M.E. (E&Tc), Microwaves
M.M.S. (Information systems)
Faculty, Institute of Telecommunication Management
Ex-Faculty, Sinhgad College of Engineering,
Pune

Maruti S. Kalbande
M.E. (Computer Science & Engineering)
H.O.D., Computer Engineering
JSPM's Jayawantrao Sawant Polytechnic,
Pune

TECHNICAL® PUBLICATIONS
SINCE 1993
An Up-Thrust for Knowledge

NETWORK & INFORMATION SECURITY

Subject Code : 22620

Third Year Diploma Semester - VI (Elective - II)
Computer Engineering Program Group (CO / CM / IF / CW)

First Edition : January 2020

Published by :

TECHNICAL PUBLICATIONS SINCE 1993 An Up-Thrust for Knowledge

Amit Residency, Office No.1, 412, Shaniwar Peth, Pune - 411030, M.S. INDIA
Ph.: +91-020-24495496/97, Telefax : +91-020-24495497
Email : sales@technicalpublications.org Website : www.technicalpublications.org

ISBN 978-93-89750-06-5

9 789389 750065

MSBTE I

PREFACE

The importance of **Network and Information Security** is well known in various engineering fields. Overwhelming response to our books on various subjects inspired us to write this book. The book is structured to cover the key aspects of the subject **Network and Information Security**.

The book uses plain, lucid language to explain fundamentals of this subject. The book provides logical method of explaining various complicated concepts and stepwise methods to explain the important topics. Each chapter is well supported with necessary illustrations, practical examples and solved problems. All chapters in this book are arranged in a proper sequence that permits each topic to build upon earlier studies. All care has been taken to make students comfortable in understanding the basic concepts of this subject.

Representative questions have been added at the end of each section to help the students in picking important points from that section.

Sample question papers are solved and included at the end of the book.

The book not only covers the entire scope of the subject but explains the philosophy of the subject. This makes the understanding of this subject more clear and makes it more interesting. The book will be very useful not only to the students but also to the subject teachers. The students have to omit nothing and possibly have to cover nothing more.

We wish to express our profound thanks to all those who helped in making this book a reality. Much needed moral support and encouragement is provided on numerous occasions by our whole family. We wish to thank the **Publisher** and the entire team of **Technical Publications** who have taken immense pain to get this book in time with quality printing.

Any suggestion for the improvement of the book will be acknowledged and well appreciated.

Authors
D. A. Dhotre
V. S. Bagad
M. S. Kalbande

Dedicated to God ....

SYLLABUS

Network and Information Security (22620)

Teaching Scheme			Credit (L+T+P)	Examination Scheme											
				Theory						Practical					
L	T	P		Paper Hrs.	ESE		PA		Total		ESE		PA		Total	
					Max	Min	Max	Min	Max	Min	Max	Min	Max	Min	Max	Min
3	-	2	5	3	70	28	30*	00	100	40	25@	10	25	10	50	20

Unit	Unit Outcomes (UOs) (in cognitive domain)	Topics and Sub-topics
Unit - I **Introduction to Computer and Information Security**	1a. Explain the importance of the given component of computer security. 1b. Explain the characteristics of the given type of threat. 1c. Explain the given type of attacks related with security. 1d. Describe the features of given type of update of operating system. 1e. Classify Information. 1f. Explain Principles of Information Security.	1.1 Foundations of Computer Security : Definition and Need of computer security, Security Basics : Confidentiality, Intergrity, Availability, Accountability, Non - Repudiation and Reliability. 1.2 Risk and Threat Analysis : Assets, Vulnerability, Threas, Risks, Counter measures. 1.3 Threat to Security : Viruses, Phases of Viruses, Types of Virus, Dealing with Viruses, Worms, Trojan Horse, Intruders, Insiders. 1.4 Type of Attacks : Active and Passive attacks, Denial of Service, DDOS, Backdoors and Trapdoors, Sniffing, Spoofing, Man in the Middle, Replay, TCP/IP, Hacking, Encryption attacks. 1.5 Operating system security : Operating system updates : Hotfix, Patch, Service Pack. 1.6 Information, Need and Importance of Information, information classification, criteria for information classification, Security, need of security, Basics principles of information security.

Unit - II **User Authentication and Access Control**	2a. Explain techniques of the given type of attack on passsword. 2b. Explain mechanism of the given type of Biometric. 2c. Apply the relevant Authentication method for the given situation with an example. 2d. Describe features of the given access control policy.	2.1 Identification and Authentication : User name and Password, Guessing password, Password attacks-Piggybacking, Shoulder surfing, Dumpster diving. 2.2 Biometrics : Finger prints, Hand prints, Retina, patterns, Voice patterns, Signature and Writing patterns, Keystrokes. 2.3 Access controls : Definition, Authentication Mechanism, principle-Authentication, Authorization, Audit, Policies : DAC, MAC, RBAC.
Unit - III **Cryptography**	3a. Encrypt/Decrypt the given text using different substitution techniques. 3b. Convert plain text to cipher text and vice versa using the given transposition technique. 3c. Convert the given message using steganography. 3d. Explain the given technique of cryptography using example.	3.1 Introduction : Plain text, Cipher text, Cryptography, Cryptanalysis, Cryptology, Encryption, Decryption. 3.2 Substitution Techniques : Caesar's cipher, Modified Caesar's Cipher, Transposition Techniques : Simple Columnar Transposition. 3.3 Steganography : Procedure 3.4 Symmetric and Asymmetric cryptography : Introduction to Symmetric encryption, DES (Data encryption Standard) algorithm, Asymmetric key cryptography : Digital Signature.
Unit - IV **Firewall and Intrusion Detection System**	4a. Compare types of firewall on the given parameter(s). 4b. Explain function of the given type of firewall configuration. 4c. Compare various IDS techniques on the given parameter(s). 4d. Describe features of the given IDS technique.	4.1 Firewall : Need of Firwall, types of firewall - Packet Filters, Stateful Packet Filters, Application Gateways, Circuit gateways. 4.2 Firewall Policies Configuration, limitations, DMZ. 4.3 Intrusion Detection System : Vulnerability Assement, Misuse detection, Anomaly Detection, Network-Based IDS, Host-Based IDS, Honeypots.

Unit - V **Network Security, Cyber Laws and Compliance Standards**	5a. Explain the given component of Kerberos authentication protocol. 5b. Explain the given IP Security protocol with modes. 5c. Explain working of the given protocol for Email security. 5d. Describe the given component of Publick Key Infrastructure. 5e. Classify the given Cyber crime. 5f. Explain the specified Cyber law. 5g. Describe compliance standards for Information Security.	5.1 Kerberos : Working, AS, TGS, SS 5.2 IP Security - Overview, Protocols - AH, ESP, Modes - transport and Tunnel. 5.3 Email security - SMTP, PEM, PGP. 5.4 Public key infrastructure (PKI) : Introduction, Certificates, Certificate authority, Registration Authority, X.509/PKIX certificate format. 5.5 Cyber Crime : Introduction, Hacking, Digital Forgery, Cyber, Stalking/Harassment, Cyber Pornography, Indentity Theft and Fraud, Cyber terrorism, Cyber Defamation. 5.6 Cyber Laws : Introduction, need Categories : Crime against Individual Government, Property. 5.7 Complaince standards : Implementing and Information Security Management System, ISO 27001, ISO 20000, BS 25999, PCI DSS, ITIL, framework, COBIT framework.

Table of Contents

Unit - I

Unit - II

Unit - III

Unit - IV

Unit - V

UNIT - I

1 Introduction to Computer and Information Security

1.1 Foundations of Computer Security

- The computing system is a collection of hardware, software, storage media, data and people that an organization uses to perform **computing** tasks.
- Computer security is the protection of computing systems and the data that they store or access.
- Computer security is important for protecting the confidentiality, integrity and availability of computer systems and their resources.
- The computing system is a collection of hardware, software, storage media, data and people that an organization uses to perform computing tasks.
- Computer security : Computer security is the protection of computing systems and the data that they store or access.
- Data security is the science and study of methods of protecting data from unauthorized disclosure and modification.
- Data and information security is about enabling collaboration while managing risk with an approach that balances availability versus the confidentiality of data.
- Network security : Measures to protect data during their transmission.
- Internet security : Measures to protect data during their transmission over a collection of interconnected networks.
- Computer security awareness helps minimize the chances of computer attacks and prevent the loss of information stored on the systems.

1.1.1 Definition and Need of Computer Security

- Basic terminology used for security purposes are as follows :

a. **Cryptography :** The art or science encompassing the principles and methods of transforming an plaintext message into one that is unintelligible and then retransforming that message back to its original form.

b. **Plaintext :** The original message.

c. **Ciphertext :** The transformed message produced as output, It depends on the plaintext and key.

d. **Cipher :** An algorithm for transforming plaintext message into one that is unintelligible by transposition and/or substitution methods.

e. **Encipher (encode) :** The process of converting plaintext to ciphertext using a cipher and a key.

f. **Decipher (decode) :** The process of converting ciphertext back into plaintext using a cipher and a key.

g. **Key :** Some critical information used by the cipher, known only to the sender and receiver.

Need of Computer Security :

- Confidentiality, integrity, non-repudiation, authenticity, and availability are the elements of security.

1.1.2 CIA Model for Security

- Security goals are as follows :
  1. Confidentially
  2. Integrity
  3. Availability

1. Confidentiality

- Confidentiality refers to limiting information access and disclosure to authorized users and preventing access by or disclosure to unauthorized ones.
- Sensitive information should be kept secret from individuals who are not authorized to see the information.

- Underpinning the goal of confidentiality are authentication methods like user-IDs and passwords that uniquely identify a data system's users, and supporting control methods that limit each identified user's access to the data system's resources.
- Confidentiality is not only applied to storage of data but also applies to the transmission of information.
- Confidentiality means that people cannot read sensitive information, either while it is on a computer or while it is traveling across a network.
- Fig. 1.1.1 shows relationship between confidentiality integrity and availability.

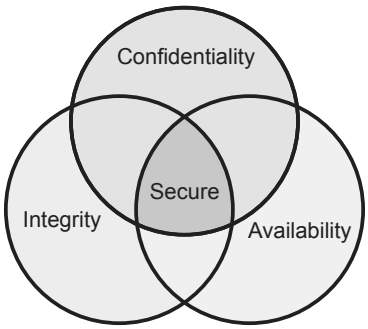


Fig. 1.1.1 Relationship between confidentiality integrity and availability

2. Integrity

- Integrity refers to the trustworthiness of information resources.
- Integrity should not be altered without detection.
- It includes the concept of "data integrity" namely, that data have not been changed inappropriately, whether by accident or deliberately malign activity.
- It also includes "origin" or "source integrity" that is, that the data actually came from the person or entity you think it did, rather than an imposter.
- Integrity ensures that information is not changed or altered in transit. Under certain attack models, an adversary may not have to power to impersonate an authenticated party or understand a confidential communication, but may have the ability to change the information being transmitted.
- On a more restrictive view, however, integrity of an information system includes only preservation without corruption of whatever was transmitted or entered into the system, right or wrong.

3. Availability

- Availability refers, to the availability of information resources. An information system that is not available when you need it is at least as bad as none at all.
- Availability means that people who are authorized to use information are not prevented from doing so. It may be much worse, depending on how reliant the organization has become on a functioning computer and communications infrastructure.
- Almost all modern organizations are highly dependent on functioning information systems. Many literally could not operate without them.
- Availability, like other aspects of security, may be affected by purely technical issues (e.g. a malfunctioning part of a computer or communications device), natural phenomena (e.g. wind or water), or human causes (accidental or deliberate).
- For example, an object or service is thought to be available if
  i. It is present in a usable form.
  ii. It has capacity enough to meet the services needs.
  iii. The service is completed an acceptable period of time.
- By combining these goals, we can construct the availability. The data item, service or system is available if
  i. There is a timely response to our request.
  ii. The service and system can be used easily.
  iii. Concurrency is controlled.
  iv. It follows the fault tolerance.
  v. Resources are allocated fairly.

1.1.3 Nonrepudiation and Reliability

- Nonrepudiation prevents either sender or receiver from denying a transmitted message. Non-repudiation is the assurance that someone cannot deny the validity of something.
- When a message is sent, the receiver can prove that the alleged sender in fact sent the message.
- When a message is received, the sender can prove that the alleged receiver in fact received the message.

- Goal : Making sending and receiving messages undeniable through unforgeable evidence.

a. Non-repudiation of origin : proof that data was sent.

b. Non-repudiation of delivery : proof that data was received.

- Main threats :

a. Sender falsely denying having sent message.

b. Recipient falsely denying having received message.

- Control :

1. digital signature - Cryptographic evidence that can be confirmed by a third party.
2. Data origin authentication and non-repudiation are similar.
3. Data origin authentication only provides proof to recipient party.
4. Non-repudiation also provides proof to third parties.

Board Questions

1. *What is CIA of security ? Describe in brief.* **MSBTE : Summer-15**
2. *Describe security principles based on CIA.* **MSBTE : Winter-15**
3. *State the need for computer security.* **MSBTE : Summer-16, Winter-17**
4. *Describe CIA security model.* **MSBTE : Summer-17**
5. *What is Computer Security and its need ?* **MSBTE : Summer-18**
6. *Explain Security Basics in detail.* **MSBTE : Summer-18**
7. *Define computer security. Explain the need of computer security.* **MSBTE : Winter-18**
8. *Explain CIA model for security.* **MSBTE : Summer-19**
9. *Describe CIA model for computer security with example.* **MSBTE : Summer-16**
10. *Descrobe the basic principles of computer security.* **MSBTE : Winter-16**

1.2 Risk and Threat

1.2.1 Risk

- The potential for loss, damage or destruction of an asset as a result of a threat exploiting vulnerability. Risk is the intersection of assets, threats and vulnerabilities.
- The formula used to determine risk is

$$\text{Risk} = \text{Asset} + \text{Threat} + \text{Vulnerability}$$

$$R = A + T + V$$

- Risk is a function of threats exploiting vulnerabilities to obtain damage or destroy assets. Thus, threats may exist, but if there are no vulnerabilities then there is little/no risk.
- Similarly, you can have vulnerability, but if you have no threat, then you have little/no risk.
- Control is used as proactive measure. Control is a action, device, procedure, or technique that removes or reduces a vulnerability.
- A threat is blocked by control of vulnerability.
- Interception, interruption, modification and fabrication are the system security threats.

1.2.2 Threat

- The term "threat" refers to the source and means of a particular type of attack.
- A threat assessment is performed to determine the best approaches to securing a system against a particular threat, or class of threat.
- Penetration testing exercises are substantially focused on assessing threat profiles, to help one develop effective countermeasures against the types of attacks represented by a given threat.
- Where risk assessments focus more on analyzing the potential and tendency of one's resources to fall prey to various attacks, threat assessments focus more on analyzing the attacker's resources.
- Analyzing threats can help one develop specific security policies to implement in line with policy priorities and understand the specific implementation needs for securing one's resources.
- Anything that can exploit vulnerability, intentionally or accidentally, and obtain, damage, or destroy an

asset. A threat is what we're trying to protect against.

- Threat refers to the source and means of a particular type of attack.
- A threat assessment is performed to determine the best approaches to securing a system against a particular threat, or class of threat.
- A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm. That is, a threat is a possible danger that might exploit vulnerability.
- Penetration testing exercises are substantially focused on assessing threat profiles, to help one develop effective countermeasures against the types of attacks represented by a given threat.
- Where risk assessments focus more on analyzing the potential and tendency of one's resources to fall prey to various attacks, threat assessments focus more on analyzing the attacker's resources.
- Analyzing threats can help one develop specific security policies to implement in line with policy priorities and understand the specific implementation needs for securing one's resources.
- Threats come in many forms, depending on their mode of attack. From viruses to trojans, spyware and bots, threats have evolved into sophisticated programs intended to harm computers.

1.2.3 Risk Management

- Risk management is process of identifying, controlling and minimizing or eliminating security risks that may affect information systems, for an acceptable cost.
- An assessment of risk and the implementation of procedures and practices designed to control the level of risk.

Risk management classifications	Remarks
Risk Identification	• Identify and Inventory Assets • Classify and prioritize assets • Identify and prioritize threats
Risk Assessment	• Identify vulnerabilities between assets and threats • Identify and quantify asset exposure
Risk Control	• Select strategy • Justify Controls • Implement and monitor controls

- Process of assessing risk, taking steps to reduce it to an acceptable level, and maintaining that level of risk.
- Five principle :

1. **Assess risk and determine needs :**
   - Recognize the importance of protecting information resource assets.
   - Develop risk assessment procedures that link IA to business needs.
   - Hold programs and managers accountable.
   - Manage risk on a continuing basis.
2. **Establish a central management focus :**
   - Designate a central group for key activities.
   - Provide independent access to senior executives to the group.
   - Designate dedicated funding and staff.
   - Periodically, enhance staff technical skills.
3. **Implement appropriate policies and related controls :**
   - Link policies to business risks.
   - Differentiate policies and guidelines.
   - Support polices via the central IA group.
4. **Promote awareness :**
   - Educate user and others on risks and related policies.
   - Use attention-getting and user-friendly techniques.
5. **Monitor and evaluate policy and control effectiveness :**
   - Monitor factor that affect risk and indicate IA effectiveness.
   - Use results to direct future efforts and hold managers accountable.
   - Be on the lookout for new monitoring tools and techniques.

1.2.4 Control Strategies and Counter Measures

- Risk control is an important part of risk management. It involves determining what to do with uncontrolled risks.
- Some questions to ask when selecting a risk control strategy are, "What is an acceptable level of risk ?" and "What should I do about the risks ?"
- Risk control is often achieved by applying safeguards. Safeguard is anything that removes a vulnerability or protects against one or more specific threats.
- Fig. 1.2.1 shows elements of risks.
- There are four basic strategies for controlling risks : avoidance, transference, mitigation, and acceptance.

1. **Avoidance :** This step involves preventing the exploitation of vulnerability. Applying safeguards that eliminate or reduce the remaining uncontrolled risks for the vulnerability. This can be accomplished through applying technical security controls and safeguards that eliminate or reduce the uncontrolled risk.

- For example, "system administrators can configure systems to use passwords where policy requires them and where the administrators are both aware of the requirement and trained to implement it"
- Avoidance is accomplished through :
  a) Application of policy.
  b) Application of training and education.
  c) Countering threats.
  d) Implementation of technical security controls and safeguards.

2. **Transference :** This step involves shifting the risk to other areas or to outside entities. Some companies transfer the risk by contracting with an outside company to provide security expertise.

- For example, the organization might decide to contract with an ISP to outsource its Web services. Risk can also be transferred by purchasing insurance. In this case, the insurance company is responsible for the risk. The organization would be reimbursed if the risk actually occurred.
- Transference may be accomplished by
  a) Rethinking how services are offered.
  b) Revising deployment models.
  c) Outsourcing to other organizations.
  d) Purchasing insurance.
  e) Implementing service contracts with providers.

3. **Mitigation :** This step involves taking a proactive approach to reduce the severity or impact should an attacker successfully exploit vulnerability.

- For example, an organization develops and implements a disaster recovery plan in the event that a system attack causes disruption to services. The disaster recovery plan would restore the organization's IT operations to their former state.
- This approach includes three types of plans :
  a) Disaster Recovery Plan (DRP)
  b) Incident Response Plan (IRP)
  c) Business Continuity Plan (BCP)
- Mitigation depends upon the ability to detect and respond to an attack as quickly as possible.

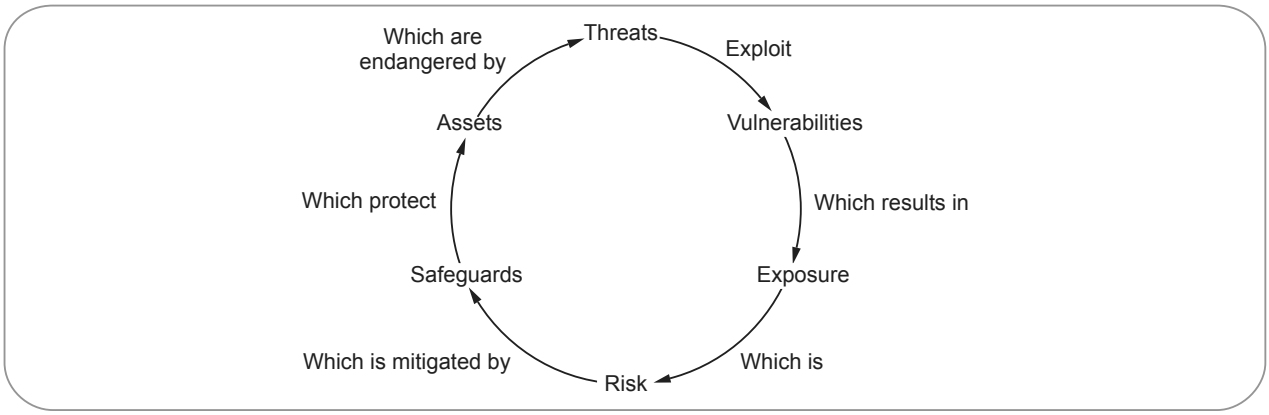


Fig. 1.2.1 Elements of risk

4. **Acceptance :** This step involves understanding the consequences and acknowledging the risk without any attempts at control or mitigation.

- It also means that management has agreed to accept the consequences and the loss if the risk is realized.
- Some risks are accepted because they simply cannot be avoided. Selecting a Risk Control Strategy are as follows :
  a) Rules of thumb on strategy selection can be applied.
  b) When a vulnerability exists.
  c) When a vulnerability can be exploited.
  d) When attacker's cost is less than potential gain.
  e) When potential loss is substantial.
- Level of threat and value of asset play major role in selection of strategy.

Board Questions

1. *What is Risk ? How it can be analyzed ? List various assets.*
   MSBTE : Summer-17
2. *Define Counter Measures in computer system and threats types at least four for computers.*
   MSBTE : Summer-18
3. *Explain risk and threat analysis w.r.t. i) Assets, ii) Threats, iii) Vulnerabilities*
   MSBTE : Summer-18, 19
4. *Describe terms regarding computer security, a) Assets b) Vulnerability c) Threats d) Risk*
   MSBTE : Winter-15

1.3 Risk Analysis

- Security risk analysis, otherwise known as risk assessment, is fundamental to the security of any organization. It is essential in ensuring that controls and expenditure are fully commensurate with the risks to which the organization is exposed.
- However, many conventional methods for performing security risk analysis are becoming more and more untenable in terms of usability, flexibility, and critically... in terms of what they produce for the user.
- Security in any system should be commensurate with its risks. However, the process to determine which security controls are appropriate and cost effective, is quite often a complex and sometimes a subjective matter.
- One of the prime functions of security risk analysis is to put this process onto a more objective basis.
- There are a number of distinct approaches to risk analysis. However, these essentially break down into two types : quantitative and qualitative.

1.3.1 Quantitative Risk Analysis

- This approach employs two fundamental elements; the probability of an event occurring and the likely loss should it occur.
- Quantitative risk analysis makes use of a single figure produced from these elements. This is called the 'Annual Loss Expectancy (ALE)' or the 'Estimated Annual Cost (EAC)'. This is calculated for an event by simply multiplying the potential loss by the probability.
- It is thus theoretically possible to rank events in order of risk (ALE) and to make decisions based upon this.
- The problems with this type of risk analysis are usually associated with the unreliability and inaccuracy of the data. Probability can rarely be precise and can, in some cases, promote complacency.
- In addition, controls and countermeasures often tackle a number of potential events and the events themselves are frequently interrelated.
- Notwithstanding the drawbacks, a number of organizations have successfully adopted quantitative risk analysis.
- Quantitative Risk Assessment Attributes.
  a) Quantified estimates of impact, threat frequency, safeguard effectiveness and cost, and probability
  b) Powerful aid to decision making
  c) Difficult to conduct

1.3.2 Qualitative Risk Analysis

- This is by far the most widely used approach to risk analysis. Probability data is not required and only estimated potential loss is used.

- Most qualitative risk analysis methodologies make use of a number of interrelated elements : THREATS, VULNERABILITIES and CONTROLS.
  1. **Threats :** These are things that can go wrong or that can 'attack' the system. Examples might include fire or fraud. Threats are ever present for every system.
  2. **Vulnerabilities :** These make a system more prone to attack by a threat or make an attack more likely to have some success or impact. For example, for fire vulnerability would be the presence of inflammable materials (e.g. paper).
  3. **Controls :** These are the countermeasures for vulnerabilities. There are four types :
     a) Deterrent controls reduce the likelihood of a deliberate attack
     b) Preventative controls protect vulnerabilities and make an attack unsuccessful or reduce its impact
     c) Corrective controls reduce the effect of an attack
     d) Detective controls discover attacks and trigger preventative or corrective controls.
- Qualitative Risk Assessment Attributes
  a) Minimally quantified estimates
  b) Exposure scale ranking estimates
  c) Easier to conduct than quantitative risk assessment

1.3.3 Qualitative vs Quantitative

	Qualitative	Quantitative
Benefits	1. Enables visibility and understanding of risk ranking. 2. Easier to reach consensus. 3. Not necessary to quantify threat frequency. 4. Not necessary to determine financial values of assets. 5. Easier to involve people who are not experts on security or computers	1. Risks are prioritized by financial impact; assets are prioritized by financial values. 2. Results facilitate management of risk by return on security investment. 3. Results can be expressed in management-specific terminology. 4. Accuracy tends to increase over time as the organization builds historic record of data while gaining experience.
Drawbacks	1. Insufficient differentiation between important risks. 2. Difficult to justify investing in control implementation because there is no basis for a cost-benefit analysis. 3. Results are dependent upon the quality of the risk management team that is created.	1. Impact values assigned to risks are based on subjective opinions of participants. 2. Process to reach credible results and consensus is very time consuming. 3. Calculations can be complex and time consuming. 4. Results are presented in monetary terms only, and they may be difficult for non-technical people to interpret. 5. Process requires expertise.

1.4 Threat to Security

- Security threat is defined as a risk that which can potentially harm computer systems and organization. The cause could be physical such as someone stealing a computer that contains vital data. The cause could also be non-physical such as a virus attack.
- The generic term for threats is malicious software or malware. Malware is software designed to cause damage to or use up the resources of a target computer.
- Threat can be divided into two categories those that need a host program, and those that are independent. Which requires host programs are essentially fragments of programs that cannot exist independently of some actual application program, utility or system program.
- Second category i.e. independent programs are self-contained programs that can be scheduled and run by the operating system.

1.4.1 Virus

- A Virus is **a block of code** that inserts copies of itself into other programs. A virus generally carries a payload, which may have nuisance value, or serious consequences. To avoid early detection, viruses may delay the performance of functions other than replication.
- Virus is one type of system threats.
- A virus is any unauthorized program that is designed to gain access to a computer system. Viruses need other programs to spread. Due to its spreading nature, a virus can cause severe damage to a system.
- Virus attacks are active type Trojan horse attacks. A macro virus is embedded in a word processing. When the recepient of an email or data file with embedded virus opens the document, the macro defined as an auto exec file, execute and immediately infects the systems. Viruses have even been found in legitimate applications software.
- Most viruses include a string of characters that acts as a marker showing that the program has been infected. When an uninfected program is found, the virus infects it by attaching a copy of itself to the end of the program and replacing the first instruction of the program with a jump to the viral code.
- Virus does not infect an already infected file in order to prevent an object file growing ever longer. This allows the virus to infect many programs without noticeably increasing disk space usage.

Precautions to prevent virus problems

1. Buying software only from respectable store.
2. Avoid uploading of free software from public domain.
3. Avoid borrowing programs for someone whose security standards are less.

Nature of virus

- Once a virus is executing, it can perform any function, such as erasing files and programs, that is allowed by the privileges of the current user.
- During its lifecycle, a typical virus goes through the following four stages.

Viruses

- A computer virus is a program that inserts itself into one or more files and then performs some action.

1.4.1.1 Phases of Viruses

During its lifecycle, virus goes through these phases

1. Dormant phase
2. Propagation phase
3. Triggering phase
4. Execution phase

- **Dormant phase :** The virus will eventually be activated by some event, such as a date, the presence of another program or file, or the capacity of the disk exceeding some limit.
- **Propagation phase :** The virus places an identical copy of itself into other programs or into certain system areas on the disk. Each infected program will now contain a clone of the virus, which will itself enter a propagation phase.
- **Triggering phase :** The virus is activated to perform the function for which it was intended.

- **Execution phase :** The function is performed. The function may be harmless, such as a message on the screen, or damaging, such as the destruction of programs and data files.

1.4.1.2 Types of Viruses

1. **Parasitic virus :** A parasitic virus attaches itself to executable files and replicates, when the infected program is executed, by finding other executable files to infect.
2. **Memory-resident virus :** Lodges in main memory as part of a resident system program. From that point on, the virus infects every program that executes.
3. **Boot sector virus :** Infects a master boot record or boot record and spreads when a system is booted from the disk containing the virus.
4. **Stealth virus :** A form of virus explicitly designed to hide itself from detection by antivirus software.
5. **Polymorphic virus :** A virus that mutates with every infection, making detection by the signature of the virus impossible.
6. **Metamorphic virus :** A metamorphic virus rewrites itself completely at each iteration, increasing the difficulty of detection. Metamorphic viruses may change their behavior as well as their appearance.

Macro Viruses

- Macro viruses are particularly threatening for a number of reasons
  1. A macro virus is platform independent virtually all of the macro viruses infect MS Word documents.
  2. Macro viruses infect documents, not executable portions of code.
  3. Macro viruses are easily spread. A very common method is by electronic mail.
- Macro viruses take advantage of a feature found in Word and other Office applications such as Microsoft Excel, namely the Macro.

E-mail Viruses

- If the recipient opens the email attachment, the Word Macro is activated. The e-mail virus sends itself to everyone on the mailing list in the user's e-mail package. The virus does local damage.
- The first rapidly spreading e-mail viruses, such as Melissa, made use of a Microsoft Word Macro embedded in an attachment.

1.4.2 Worms

- Worm is a program that replicates itself by installing copies of itself on other machines across a network.
- An e-mail virus has some of the characteristics of a worm because it propagates itself from system to system.
- Network worm programs use network connections to spread from system to system. To replicate itself, a network worm uses some sort of network vehicle. Examples include the following.
  1. Electronic mail facility.
  2. Remote execution capability
  3. Remote login capability.
- A network worm exhibits the same characteristics as a computer virus a dormant phase a propagation phase, a triggering phase and an execution phase.
- The propagation phase generally performs the following functions.
  1. Search for other systems to infect by examining host tables or similar repositories of remote system addresses.
  2. Establish a connection with a remote system.
  3. Copy itself to the remote system and cause the copy to be run.

State of Worm Technology

- Worm technology includes
  1. **Multiplatform :** Newer worms are not limited to windows machines but can attack a variety of platforms, especially the popular varieties of UNIX.
  2. **Multiexploit :** New worms penetrate systems in a variety of ways, using exploits against web servers, browsers, e-mail, file sharing.
  3. Ultrafast spreading
  4. Polymorphic
  5. Metamorphic

6. Transport vehicles
7. Zero-day exploit

1.4.3 Difference between Worm and Virus

- A virus is a piece of code that adds itself to other programs, including operating systems.
- Virus cannot run independently, host program is required to run it.
- Alters system file or any other file that is to be used in future.
- Until the user (inadvertently) activates the virus or the altered file is called, the virus is unable to do any activity.
- It needs to be carried from one computer to another.
- A ***worm*** is a program that can run by itself and can propagate a fully working version of itself to other machines.
- When a worm gains access to a computer (usually by breaking into it over the Internet) it launches a program which searches for other Internet locations, infecting them if it can.
- At no time does the worm need user assistance in order to operate its programming.

1.4.4 Trojan Horse

- Trojan horse is a virus that's disguised as a legitimate or harmless program that sometimes carries within itself the mean to allow the programs creator to secretly access the users system.
- Trojan horse attack may either be passive or active depending on the activities performed by the clandestine code.
- For example, if the clandestine code simply steals information then it is of the passive type. But if it does something more harmful like destroying or corrupting files, then it is of the active type. A variation of the Trojan horse is a program that emulates a login program.
- Many systems have mechanisms for allowing programs written by users to be used by other users. These programs can improperly use the access rights of an executing user and leak information.
- For example an intruder may wriute an editor program that works perfectly as an editor but also creates a copy of the edited file to a special area accessible to the intruder. The user is ignorant of the theft being made because the editor program performs all jobs in a perfectly normal fashion.

1.4.5 Counter Measures

1.4.5.1 Antivirus Approaches

- Viruses preventation is done by the following steps.
  1. Detection (determine and locate) virus
  2. Identification of virus.
  3. Removal of traces of virus
- Four generations of antivirus software
  1. First generation - Simple scanners
  2. Second generation - Heuristic scanners
  3. Third generation - Activity traps
  4. Fourth generation - Full featured protection

1.4.5.2 Advanced Antivirus Techniques

- Two important advanced antivirus techniques are
  1. Generic Decryption (GD) Technology.
  2. Digital Immune System.

1.4.5.3 Generic Decryption (GD) Technology

- GD technology can detect most complex polymorphic viruses with fast scanning speed. The detection is done by executing files through GD scanner. The elements of executable files are :
  i) CPU emulator
  ii) Virus signature scanner
  iii) Emulation control module

1.4.5.4 Digital Immune System

- Digital immune system is aimed to provide rapid response time so that virus can be stamped out as soon as they are introduced. Fig. 1.4.1 shows components of digital immune system.

1.4.5.5 Behavior-Blocking Software

- The behavior blocking software blocks potential malicious actions before they get chance to affect the system. The behavior monitering many include

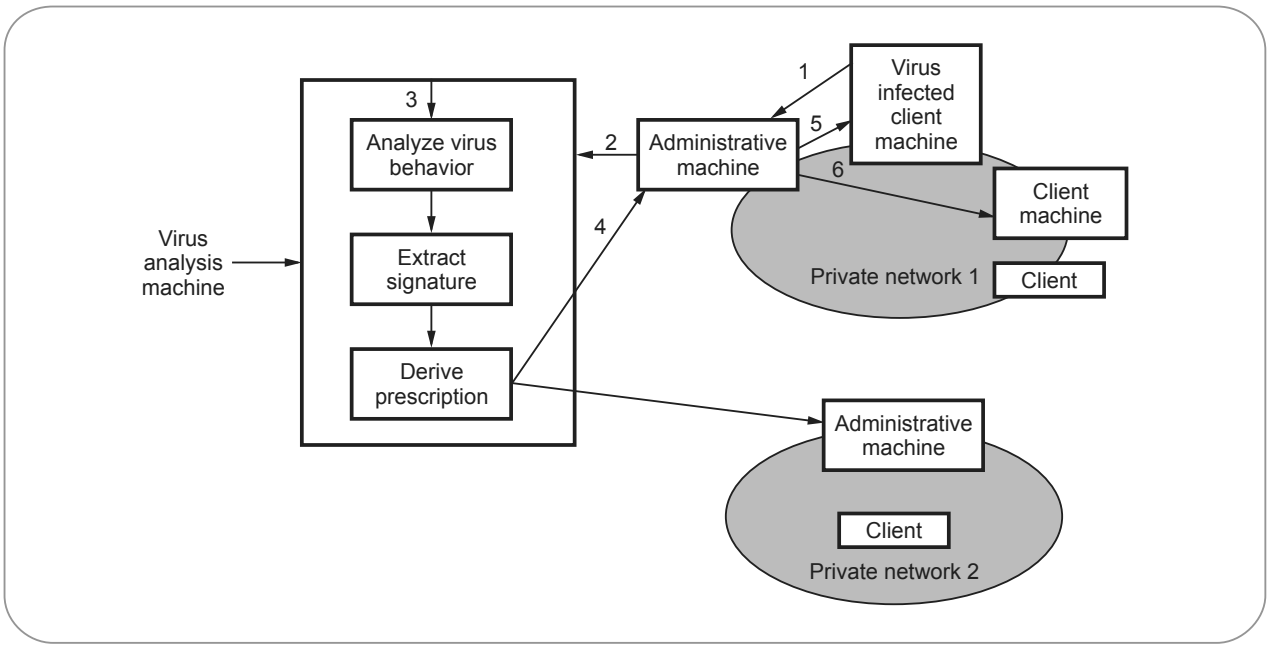


Fig. 1.4.1 Digital immune system

a) Attempt to open, view or delete/modify system files.

b) Attempt to format disk drives.

c) Modifying logic of executable file.

d) Scripting of e-mail and instant messaging clients to send executable content.

e) Initiating network communications.

- If the behavior blocker, detects program initiation is malicious, it can block the behavior and terminate the response.

1.4.6 Intruders and Insider

- An intruder is a person who attempts to gain unauthorized access to a system, to damage that system, or to disturb data on that system.
- Intrusion is the act of gaining unauthorized access to a system so as to cause loss.
- Three classes of intruders are Masquerader, Misfeasor, and Clandestine user.

1. Masquerader : An unauthorized user who penetrates a computer system's access control and gains access to user accounts.
2. Misfeasor : A legitimate user who accesses resources he is not authorized to access. Who is authorized such access but misuses his privileges.
3. Clandestine user : A user who seizes the supervisory control of the system and uses it to evade auditing and access control.

Intrusion techniques

- Objective : An intruder wants to gain access to a system.
- Access is generally protected by passwords. System maintains a file that associates a password with each authorized user.
- Password file can be protected with : **One-way encryption and access control**.

1. **One-way function :** A system stores passwords only in encrypted form. When user presents a password, the system transforms that password and compares it with the stored value.
2. **Access control :** Access to the password file is limited to very few people.

Insiders :

- An Insider threat is a malicious threat to an organization that comes from people within the

organization, such as employees, former employees, contractors or business associates, who have inside information concerning the organization's security practices, data and computer systems.

- The threat may involve fraud, the theft of confidential or commercially valuable information.
- Insiders are more dangerous than outside intruders.
- They have the access and knowledge necessary to cause immediate damage to an organization.
- Most security is designed to protect against outside intruders and thus lies at the boundary between the organization and the rest of the world.
- Besides employees, insiders also include a number of other individuals who have physical access to facilities.
- Insider attacks can be motivated by revenge or simply a feeling of entitlement. Some of the measures are taken to avoid risk :

1. Enforce least privilege, only allowing access to the resources employees need to do their job.
2. Set logs to see what users access and what commands they are entering.
3. Protect sensitive resources with strong authentication.
4. Upon termination, delete employee's computer and network access.
5. Upon termination, make a mirror image of employee's hard drive before reissuing it. That evidence might be needed if your company information turns up at a competitor.

Board Questions

1. *Describe the following attacks :*
   i) Sniffing ii) Spoofing
   MSBTE : Summer-15, 16, Winter-17
2. *Define virus. Explain atleast 5 types of viruses.*
   MSBTE : Winter-15, 17
3. *Explain worm and virus. Differentiate between worm and virus.* **MSBTE : Summer-16**
4. *Explain threat to security in detail w.r.t virus, worms, intruders, insiders.* **MSBTE : Winter-16**
5. *What is a virus ? Describe various phases of virus.* **MSBTE : Summer-17**
6. *Describe Insiders and Intruders. Who is more dangerous ?* **MSBTE : Summer-18**
7. *Differentiate between Virus and Worms.* **MSBTE : Winter-18**
8. *Describe the following terms :*
   i) Intruders ii) Insiders iii) Sniffing
   iv) Spoofing **MSBTE : Winter-18**
9. *Explain the term Intruders and Insiders.* **MSBTE : Summer-19**
10. *Define virus and logic bomb.* **MSBTE : Summer-19**

1.5 Types of Attacks

- Computer based systems have three valuable components : **Hardware, software and data**.
- Securities of these components are evaluated in terms of vulnerability, threats, attacks and control.
- An assault on system security that derives from an intelligent threat; that is, an intelligent act that is a deliberate attempt to evade security services and violate the security policy of a system.

Asset

- Asset means people, property and information.
- People may include employees and customers along with other invited persons such as contractors or guests.
- Property assets consist of both tangible and intangible items that can be assigned a value.
- Intangible assets include reputation and proprietary information. Information may include databases, software code, critical company records and many other intangible items.

Vulnerability

- Vulnerability refers to the security flaws in a system that allows an attack to be successful.
- Weaknesses or gaps in a security program that can be exploited by threats to gain unauthorized access to an asset. Vulnerability is a weakness or gap in our protection efforts.
- Vulnerability testing should be performed on an ongoing basis by the parties responsible for resolving such vulnerabilities, and helps to provide data used to identify unexpected dangers to security that need to be addressed.

- Testing for vulnerabilities is useful for maintaining ongoing security, allowing the people responsible for the security of one's resources to respond effectively to new dangers as they arise.
- **Example :** In design, implementation or procedure, that might be exploited to cause loss or harm.

Control

- Control is used as proactive measure. Control is a action, device, procedure, or technique that removes or reduces a vulnerability.
- A threat is blocked by control of vulnerability.
- Interception, interruption, modification and fabrication are the system security threats.

1.5.1 Passive Attack

- Passive attacks are those, wherein the attacker indulges in eavesdropping on, or monitoring of data transmission. A passive attack attempts to learn or make use of information from the system but does not affect system resources.
- The attacker aims to obtain information that is in transit. The term passive indicates that the attacker does not attempt to perform any modifications to the data.
- **Passive attacks** are of two types :
  1. Release of message contents
  2. Traffic analysis
- **Release of message content** is shown in Fig. 1.5.1. A telephone conversation, an electronic mail message and a transferred file may contain sensitive or confidential information we would like to prevent an opponent from learning the content of these transmissions.

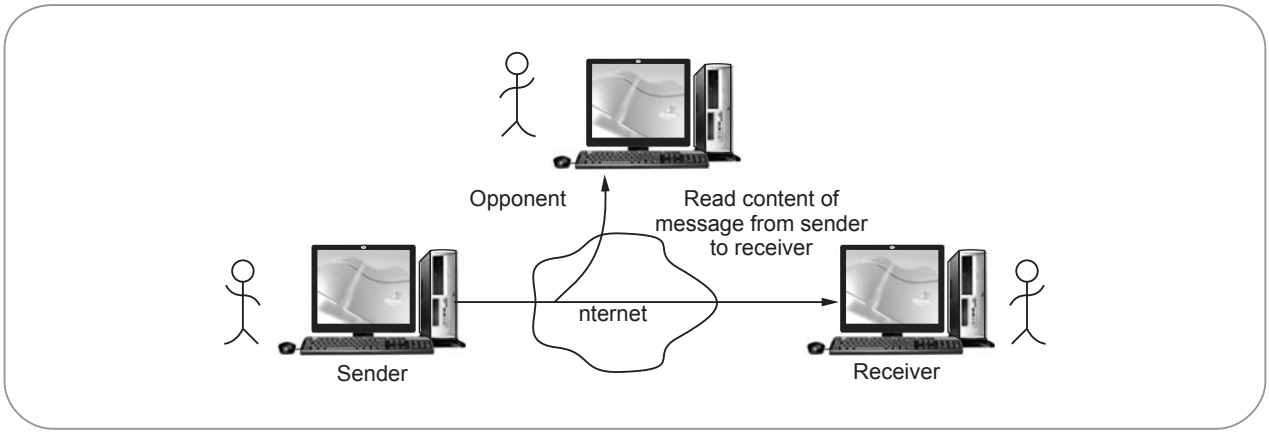


Fig. 1.5.1 Release of message contents

- **Traffic analysis :** Mask the contents of message so that opponents could not extract the information from the message. Encryption is used for masking Fig. 1.5.2 shows the traffic analysis.
- Passive attacks are very difficult to detect because they do not involve any alternation of data. It is feasible to prevent the success of attack, usually by means of encryption.

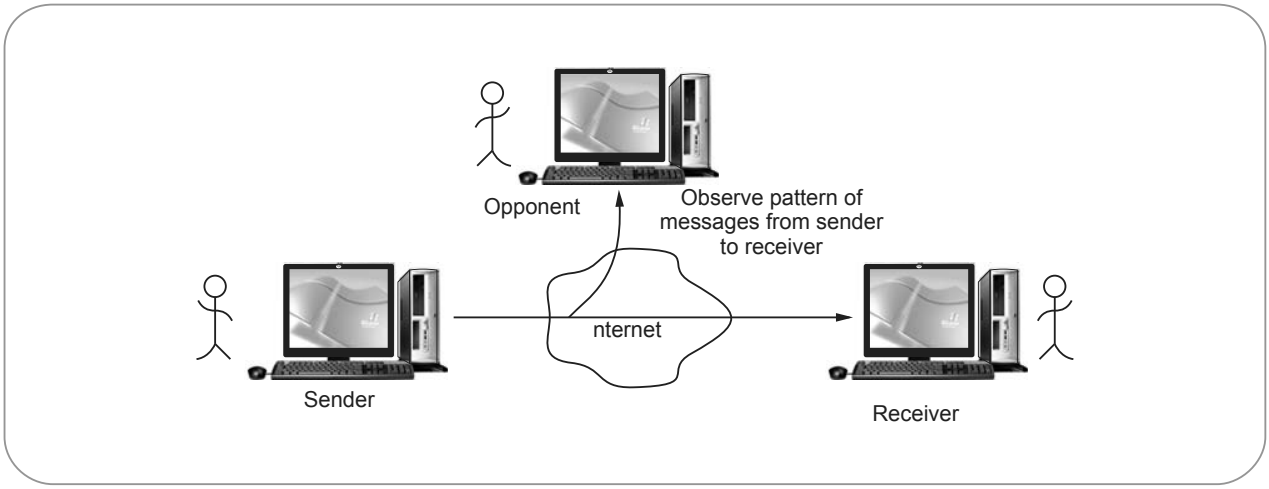


Fig. 1.5.2 Traffic analysis

1.5.2 Active Attack

- Active attacks involve some modification of the data stream or the creation of a false stream. These attacks can not be prevented easily.
- Active attacks can be subdivided into four types :
  1. Masquerade
  2. Replay
  3. Modification of message
  4. Denial of service

1. Masquerade

- It takes place when one entity pretends to be a different entity. Fig. 1.5.3 shows masquerade.

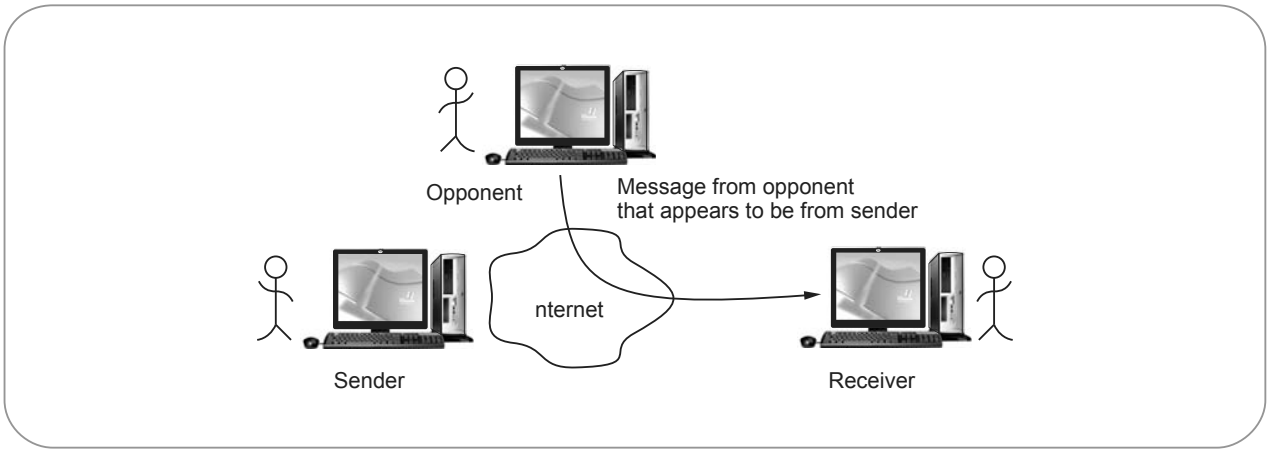


Fig. 1.5.3 Masquerade

- **For example :** Authentication sequences can be captured and replayed after a valid authentication sequence has taken place, thus enabling an authorized entity with few privileges to obtain extra privileges by impersonating an entity that has those privileges.
- **Interruption** attacks are called as masquerade attacks.

2. Replay

- It involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect.
- Fig. 1.5.4 shows replay attack.

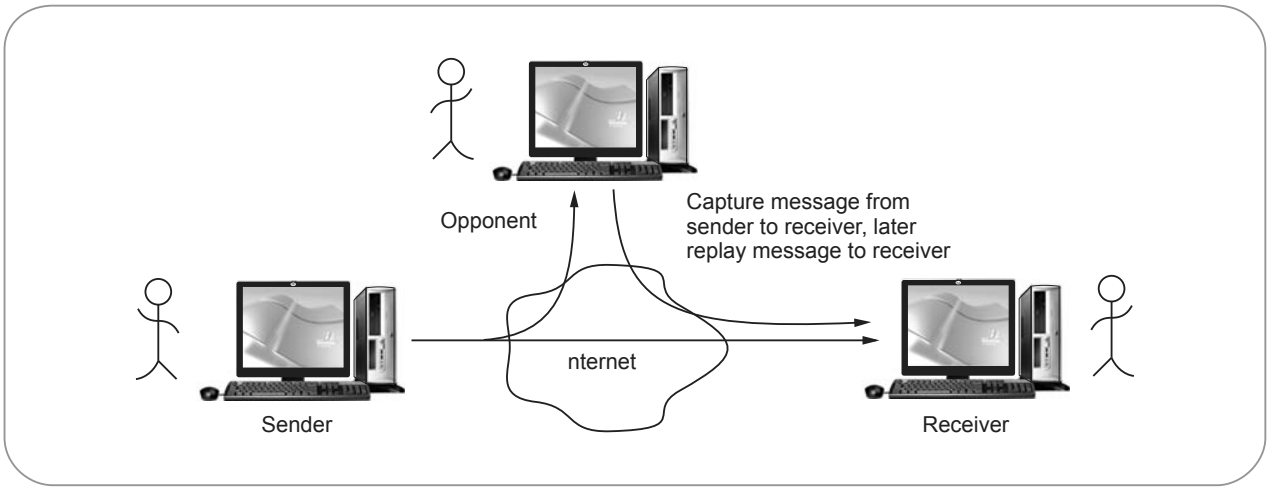


Fig. 1.5.4 Replay

3. Modification of message

- It involves some change to the original message. It produces an unauthorized effect. Fig. 1.5.5 shows the modification of message.

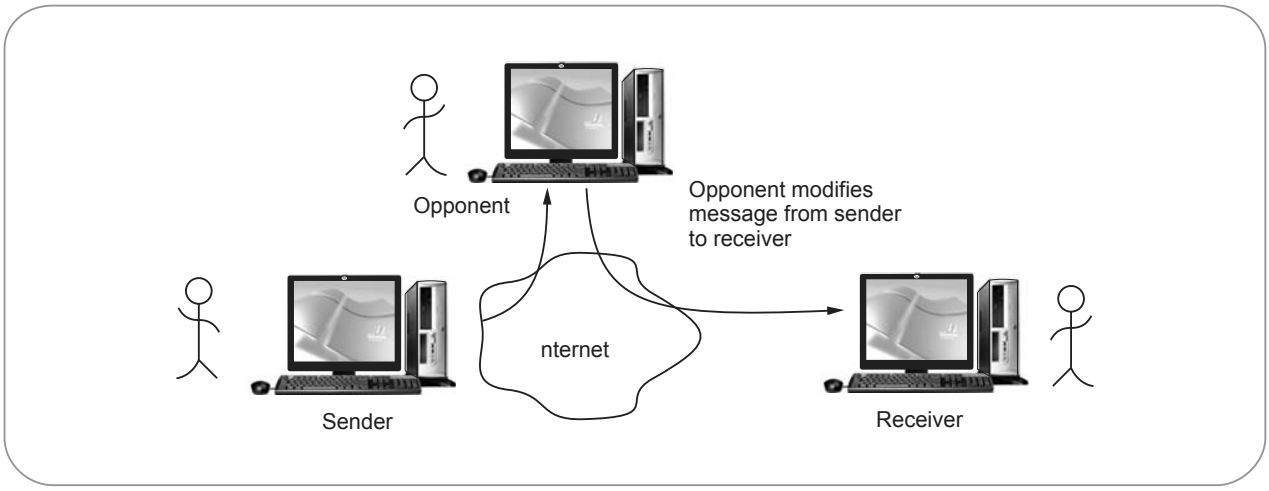


Fig. 1.5.5 Modification of message

- For example, a message meaning "Allow Rupali Dhotre to read confidential file accounts " is modified to mean "Allow Mahesh Awati to read confidential file accounts".

4. Denial of service

- Fabrication causes Denial Of Service (DOS) attacks.
- DOS prevents the normal use or management of communications facilities.
- Another form of service denial is the disruption of an entire network, either by disabling the network or by overloading it with messages so as to degrade performance.
- Fig. 1.5.6 shows denial of service attack.

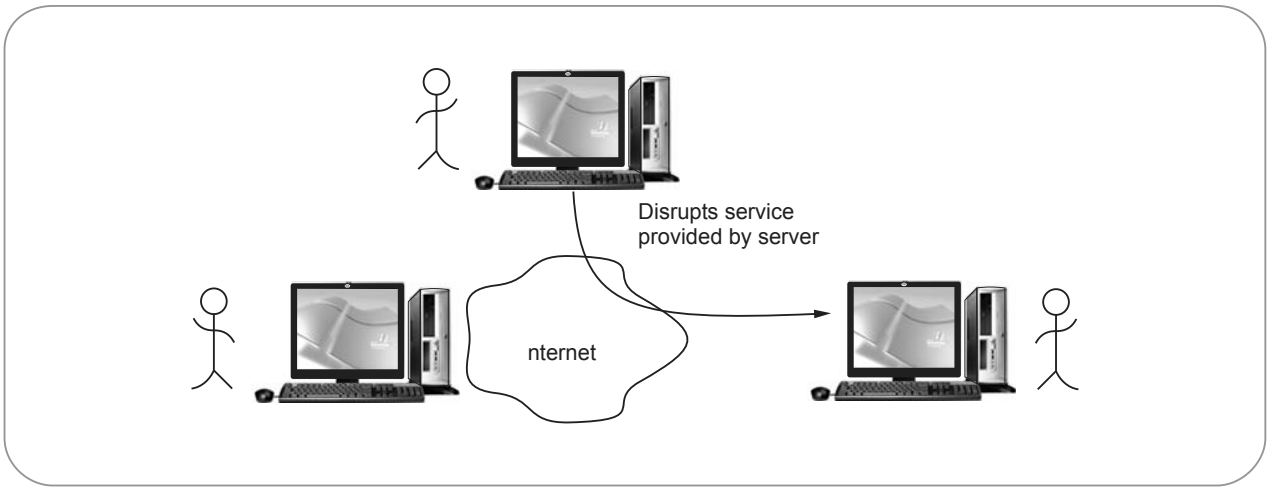


Fig. 1.5.6 Denial of service

- It is difficult to prevent active attack because of the wide variety of potential physical, software and network vulnerabilities.
- The first type of DOS attacks were single source attacks, meaning that a single system was used to attack another system and cause something on that system to fail. SYN flood is the most widely used DOS attack.
- Fig. 1.5.7 shows the SYN flood DOS attack.

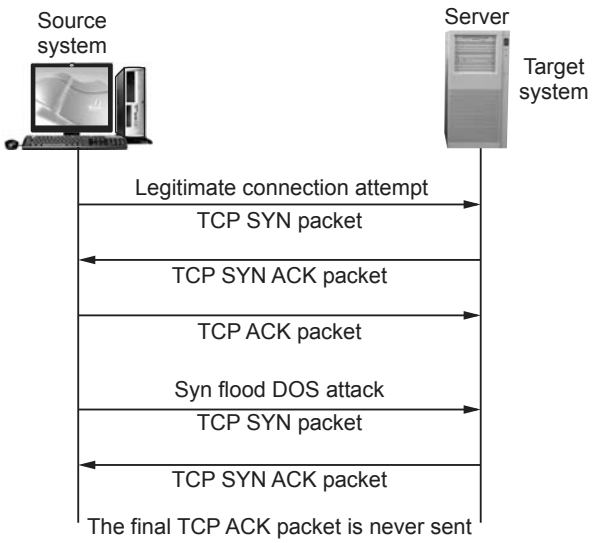


Fig. 1.5.7 SYN flood DOS attack

- Source system sends a large number of TCP SYN packets to the target system. The SYN packets are used to begin a new TCP connection.
- When the target receives a SYN packet, it replies with TCP SYN ACK packet, which acknowledges the SYN packet and sends connection setup information back to the source of the SYN.
- The target also places the new connection information into a pending connection buffer.
- For a real TCP connection, the source would send a final TCP ACK packet when it receives the SYN ACK.
- However, for this attack, the source ignores the SYN ACK and continues to send SYN packets. Eventually, the target's pending connection buffer fills up and it can no longer respond to new connection requests.

1.5.3 Difference between Passive and Active Attack

Sr. No.	Passive attacks	Active attacks
1.	Passive attacks are in the nature of eavesdropping on, or monitoring of, transmissions.	Active attacks involve some modification of the data stream or the creation of a false stream.
2.	**Types :** Release of message contents and traffic analysis	**Types :** Masquerade, replay, modification of message and denial of service.
3.	Very difficult to detect.	Easy to detect.
4.	The emphasis in dealing with passive attacks is on prevention rather than detection.	It is quite difficult to prevent active attacks absolutely.

5.	It does not affect the system.	It affects the system.

1.5.4 Man-in-the-Middle Attack

- In cryptography, a **Man-In-The-Middle (MITM) attack** is an attack in which an attacker is able to read, insert and modify at will, meassages between two parties without either party knowing that the link between them has been compromised.
- The attacker must be able to observe and intercept messages going between the two victims. The MITM attack can work against public-key cryptography and is also particularly applicable to the original Diffie-Hellman key exchange protocol, when used without authentication.
- The MITM attack may include one or more of
  1. Eavesdropping, including traffic analysis and possibly a known-plaintext attack.
  2. Chosen ciphertext attack, depending on what the receiver does with a message that it decrypts.
  3. Substitution attack
  4. Replay attacks
  5. Denial of service attack. The attacker may for instance jam all communications before attacking one of the parties. The defense is for both parties to periodically send authenticated status messages and to treat their disappearance with paranoia.
- MITM is typically used to refer to active manipulation of the meassages, rather than passively eavesdropping.

Example of a successful MITM attack against public-key encryption

- Suppose Alice wishes to communicate with Bob and that Mallory wishes to eavesdrop on the conversation, or possibly deliver a false message to Bob. To get started. Alice must ask Bob for his public key. If Bob sends his public key to Alice, but Mallory is able to intercept it, a man-in-the-middle attack can begin.
- Mallory can simply send Alice a public key for which she has the private, matching, key. Alice, believing this public key to be Bob's, then encrypts her message with Mallory's key and sends the enciphered message back to Bob.
- Mallory again intercepts, deciphers the message, keeps a copy, and reenciphers it using the public key Bob originally sent to Alice. When Bob receives the newly enciphered message, he will believe it came from Alice.
- This example shows the need for Alice and Bob to have some way to ensure that they are truly using the correct public keys of each other. Otherwise, such attacks are generally possible in principle, against any message sent using public-key technology.

Defenses against the attack

- The possibility of a man-in-the-middle attack remains a serious security problem even for many public-key based cryptosystems. Various defenses against MITM attacks use authentication techniques that are based on :
  1. Public keys
  2. Stronger mutual authentication
  3. Secret keys (high information entropy secrets)
  4. Passwords (low information entropy secrets)
  5. Other criteria, such as voice recognition or other biometrics
- The integrity of public keys must generally be assured in some manner, but need not be secret, whereas passwords and shared secret keys have the additional secrecy requirement. Public keys can be verified by a Certificate Authority, whose public key is distributed through a secure channel.

1.5.5 DDOS

- A distributed denial-of-service (DDoS) attack is a malicious attempt to disrupt normal traffic of a targeted server, service or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic.
- DDoS attacks achieve effectiveness by utilizing multiple compromised computer systems as sources of attack traffic. Exploited machines can include computers and other networked resources such as IoT devices.

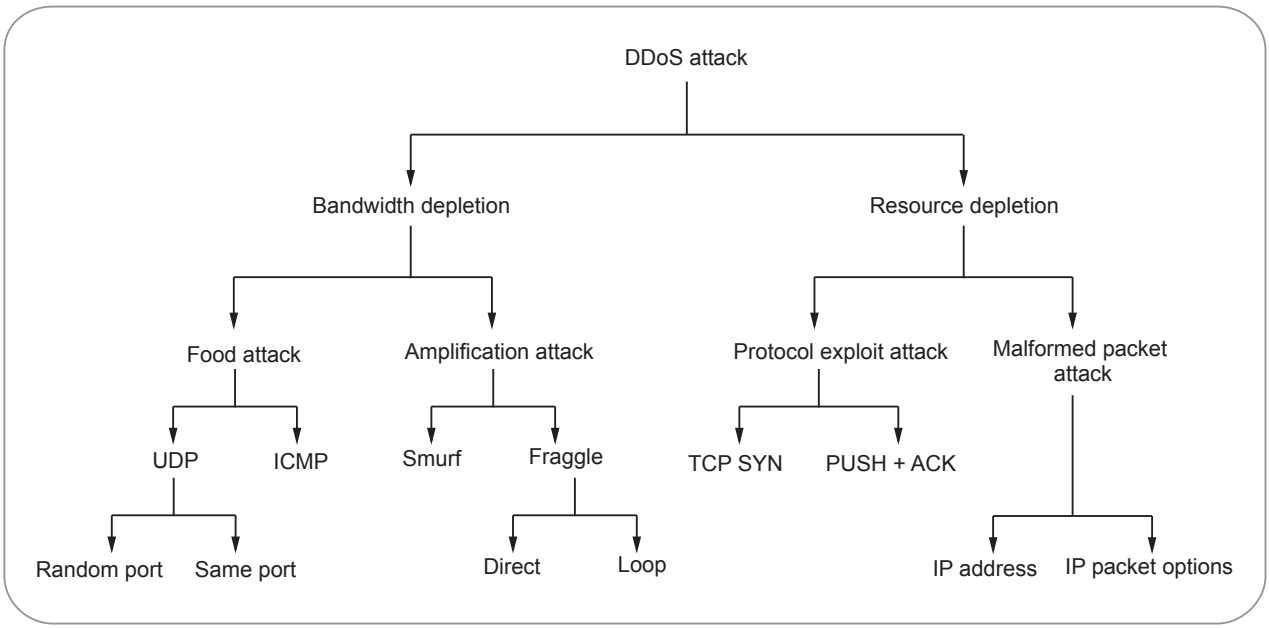


Fig. 1.5.8 DDoS attack taxonomy

- From a high level, a DDoS attack is like a traffic jam clogging up with highway, preventing regular traffic from arriving at its desired destination.
- In a DDoS attack, an attacker may use your computer to attack another computer. By taking advantage of security vulnerabilities or weaknesses, an attacker could take control of your computer.
- He or she could then force your computer to send huge amounts of data to a website or send spam to particular email addresses. The attack is "distributed" because the attacker is using multiple computers, including yours, to launch the denial-of-service attack.
- A denial of service attack is an attack with the purpose of preventing legitimate users from using a specified network resource such as a website, web service, or computer system.
- A distributed denial of service attack is a coordinated attack on the availability of services of a given target system or network that is launched indirectly through many compromised computing systems. The services under attack are those of the "primary victim", while the compromised systems used to launch the attack are often called the "secondary victims."
- The use of secondary victims in a DDoS attack provides the attacker with the ability to wage a much larger and more disruptive attack while remaining anonymous since the secondary victims actually perform the attack making it more difficult for network forensics to track down the real attacker.
- Fig. 1.5.8 shows DDoS attack taxonomy.
- There are two main classes of DDoS attacks :
  1. Bandwidth depletion
  2. Resource depletion attacks.
- A *bandwidth depletion attack* is designed to flood the victim network with unwanted traffic that prevents legitimate traffic from reaching the primary victim.
- A *resource depletion attack* is an attack that is designed to tie up the resources of a victim system making the victim unable to process legitimate requests for service.

1.5.6 Trap Door

- Secret undocumented entry point into a program used to grant access without normal methods of access authentication.
- Trap doors have been used legitimately for many years by programmers to debug and test programs.

- Trap door can be caused by a flow in the system design or they can be installed there by a system programmer for future use. Trap door including backdoor passwords are unspecified and non documented entry points to the system. A clever trap door could be included in a compiler.
- The compiler could generate standard object code as well as a trap door regardless of the source code being compiled. Trap door may also be a incorporated into the system by a destructive virus or by a Trojan horse program.
- Trap door is one type of program threat.
- Trap door is code that recognizes some special sequence of input or is triggered by being run from a certain user ID or by an unlikely sequence of events.
- It is difficult to implement operating system controls for trap doors. Security measures must focus on the program development and software update activities.

1.5.7 TCP SYN Flooding

- The TCP SYN flooding is the most commonly-used attack.

TCP SYN Flooding

- It consists of a stream of spoofed TCP SYN packets directed to a listening TCP port of the victim.
- Not only the Web servers but also any systems connected to the Internet providing TCP-based network services, such as FTP servers or Mail servers, are susceptible to the TCP SYN flooding attacks.
- The SYN flooding attacks exploit the TCP's three-way handshake mechanism and its limitation in maintaining half-open connections. When a server receives a SYN request, it returns a SYN/ACK packet to the client.
- If a SYN request is spoofed, the victim server will never receive the final ACK packet to complete the three-way handshake.
- Flooding spoofed SYN requests can easily exhaust the victim server's backlog queue, causing all the incoming SYN requests to be dropped.
- The stateless and destination-based nature of Internet routing infrastructure cannot differentiate a legitimate SYN from a spoofed one, and TCP does not offer strong authentication on SYN packets.
- Therefore, under SYN flooding attacks, the victim server cannot single out, and respond only to, legitimate connection requests while ignoring the spoofed.
- To counter SYN flooding attacks, several defence mechanisms have been proposed, such as Syn cache, Syn cookies, SynDefender, Syn proxying, and Synkill.
- All of these defence mechanisms are installed at the firewall of the victim server or inside the victim server, thereby providing no hints about the sources of the SYN flooding. They have to rely on the expensive IP traceback to locate the flooding sources. Because the defence line is at, or close to, the victim, the network resources are also wasted by transmitting the flooding packets.
- The key feature of Flooding Detection System (FDS) is to utilize the inherent TCP SYN-FIN pair'sbehaviour for SYN flooding detection.
- The SYN/FIN packets delimit the beginning (SYN) and end (FIN) of each TCP connection. As shown in Fig. 1.5.9 that is borrowed from, under the normal condition, one appearance of a SYN packet results in the eventual return of a FIN packet.
- Although we can distinguish SYNs from SYN/ACK packets, we have no means to discriminate active FINs from passive FINs since each end host behind a leaf router may be either a client or a server. Therefore, the SYN-FIN pairs refer to the pairs of (SYN, FIN) and (SYN/ACK, FIN).
- The "SYN" packets are generalized to include the pure SYN and SYN/ACK packets. While the RST packet violates the SYN-FIN pair, for any RST that is generated to abort a TCP connection, we can still get a SYN-RST pair.
- Large-scale packet classification mechanisms have been proposed, making it possible to distinguish TCP control packets at routers at a very high speed.

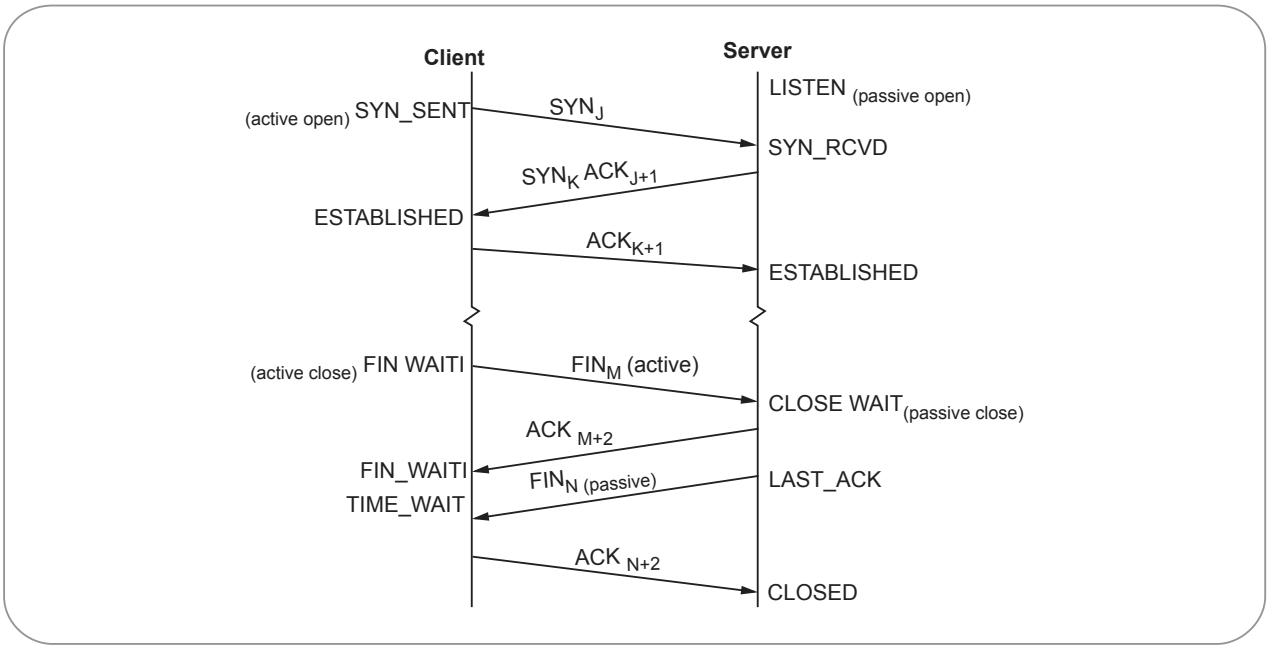


Fig. 1.5.9 TCP states corresponding to normal connection establishment and teardown

1.5.8 Sniffing

- Packet sniffing involves capturing, decoding, inspecting and interpreting the information inside a network packet on a TCP/IP network. Tools like Wireshark, Ettercap or NetworkMiner give anybody the ability to sniff network traffic.
- Most of the Internet runs in plain text, which means that most of the information you look at is viewable by someone with a packet sniffer.
- Network sniffing is a network layer attack consisting of capturing packets from the network transmitted by other computers and reading the data content in search of sensitive information like passwords, session tokens and confidential information.
- Sniffers are programs that allow a host to capture any network packet illicitly. Specially, if the sniffers are active because active sniffer can alter or block network traffic while passive sniffer can only monitor network traffic.
- There are two ways to sniff network traffic :

1. Host running a sniffer sets its NIC in promiscuous mode. If any host's NIC is running in promiscuous mode, it will receive all packets either those packets targeted to it or not.
2. ARP cache poisoning is also used for sniffing. This way of sniffing is effective in an environment, which is not broadcast in nature. ARP cache poisoning depends on local ARP cache maintained by each host of network. This cache contains IP with corresponding MAC addresses of recently accessed hosts.

- There are two ways to detect a sniffer : host-based and network-based.

1. Host-based detection : Small utilities can used to detect if the NIC is running in a promiscuous mode on any host in a network.
2. Network-based detection : Anti-sniffer software can be run to detect the presence of specific signature packets.

Protection from sniffers :

1. Disabling promiscuous mode on network interfaces results in shutting down most sniffer software.
2. Anti-sniffing tools can be used to detect the network interface mode.
3. IPSec encryption can be used for token-based packet security in the network infrastructure.

1.5.9 Spoofing

ARP Spoofing :

- ARP Spoofing is a type of attack in which a malicious actor sends falsified ARP messages over a local area network. This results in the linking of an attacker's MAC address with the IP address of a legitimate computer or server on the network.
- Once the attacker's MAC address is connected to an authentic IP address the attacker will begin receiving any data that is intended for that IP address.
- Session hijacking attacks can use ARP spoofing to steal session IDs, granting attacker's access to private systems and data. Fig. 1.5.10 shows ARP spoofing.
- In the ARP poisoning attack, attacker sends an ARP reply to victim's ARP request for a server. The attacker claims to be that server, tying his own MAC address to that of an IP address owned by another device.
- The bogus ARP message then also adds an entry to the switch's ARP table. When a message arrives for the device as shown in the given diagram MAC B bogus ARP entry diverts to it MAC C.
- If a legitimate MAC address entry exists in the ARP table for that IP address, it will be overwritten by the MAC address from the attacker's forged ARP reply.
- After the attacker's MAC address is injected into a poisoned ARP table, any traffic sent to that IP address will actually be routed to the attacker's hardware instead of the real owner of the IP.
- Use cryptographic network protocols : Transport Layer Security (TLS), Secure Shell (SSH), HTTP Secure (HTTPS), and other secure communications protocols bolster ARP spoofing attack prevention by encrypting data prior to transmission and authenticating data when it is received.

IP Spoofing

- IP spoofing, also known as IP address forgery, is a hijacking technique in which the attacker masquerades as a trusted host to conceal his identity, hijack browsers, or gain access to a network.

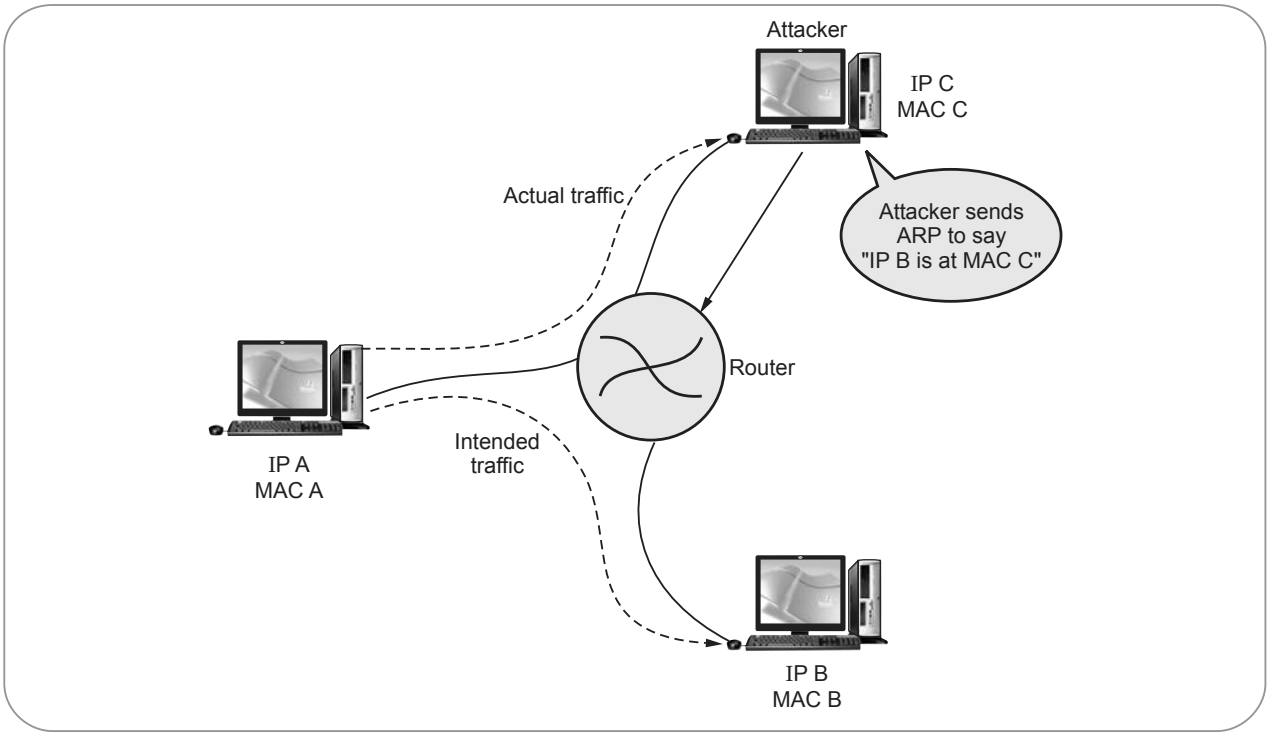


Fig. 1.5.10 ARP spoofing

- The hijacker obtains the IP address of a legitimate host and alters packet headers so that the legitimate host appears to be the source.
- When IP spoofing is used to hijack a browser, a visitor who types in the URL of a legitimate site is taken to a fraudulent Web page created by the hijacker.
- IP routing is hop by hop. Every IP packet is routed separately. The route of IP packet is decided by all the routers the packet goes through.
- IP address spoofing is possible because routers only require inspection of the destination IP address in the packet to make routing decisions.
- The source IP address is not required by routers and an invalid source IP address will not affect the delivery of packets. That address is only used by the destination machine when it responds back to the source.
- IP Spoofing Steps :

1. Selecting the victim (target host).
2. Identify a host that the target "trust".
3. Disable the trusted host, sampled the target's TCP sequence.
4. The trusted host is impersonated and the ISN forged.
5. Connection attempt to a service that only requires address-based authentication.
6. If successfully connected, executes a simple command to leave a backdoor.

- How to prevent Spoofing Attacks

1. Avoid using the source address authentication. Implement system wide cryptographic authentication function.
2. Disable all the r* commands, remove all .rhosts files and empty out the /etc/hosts.equiv file. This will force all users to use other means of remote access.
3. Configure the network to reject packets from the net that claim to originate from a local address.
4. If you allow outside connections from trusted hosts, enable encryption sessions at the router.

1.5.10 Hacking

- Hacking in simple terms means an illegal intrusion into a computer system and/or network. Government websites are the hot target of the hackers due to the press coverage; it receives. Hackers enjoy the media coverage.
- Hacking refers to an array of activities which are done to intrude some one else's personal information space so as to use it for malicious, unwanted purposes.
- Hacking is a term used to refer to activities aimed at exploiting security flaws to obtain critical information for gaining access to secured networks.
- Hacking refers to an array of activities which are done to intrude some one else's personal information space so as to use it for malicious, unwanted purposes.
- Hacking is a term used to refer to activities aimed at exploiting security flaws to obtain critical information for gaining access to secured networks.
- **White Hat hackers** are also known as Ethical Hackers. They never intent to harm a system, rather they try to find out weaknesses in a computer or a network system as a part of penetration testing and vulnerability assessments.
- **Black Hat hackers,** also known as crackers, are those who hack in order to gain unauthorized access to a system and harm its operations or steal sensitive information.
- Black Hat hacking is always illegal because of its bad intent which includes stealing corporate data, violating privacy, damaging the system, blocking network communication, etc.
- **Grey hat hackers** are a blend of both black hat and white hat hackers. They act without malicious intent but for their fun, they exploit a security weakness in a computer system or network without the owner's permission or knowledge.

1.5.11 Encryption Attacks

Types of Attacks on Encrypted Messages

Sr. No.	Type of attack	Known to cryptanalyst
1.	Ciphertext only	1. Encryption algorithm 2. Ciphertext
2.	Known plaintext	1. Encryption algorithm 2. Ciphertext 3. One or more plaintext ciphertext pairs formed with the secret key
3.	Chosen plaintext	1. Encryption algorithm 2. Ciphertext 3. Plaintext message chosen by cryptanalyst, together with its corresponding decrypted plaintext generated with the secret key.
4.	Chosen ciphertext	1. Encryption algorithm 2. Ciphertext 3. Purported ciphertext chosen by cryptanalyst, together with its corresponding decrypted plaintext generated with the secret key.
5.	Chosen text	1. Encryption algorithm 2. Ciphertext 3. Plaintext message chosen by cryptanalyst, together with its corresponding ciphertext generated with the secret key. 4. Purported ciphertext chosen by cryptanalyst, together with its corresponding decrypted plaintext generated with the secret key.

Board Questions

1. *Explain following terms w.r.t. security :*
   i) Intruders ii) Insiders **MSBTE : Summer-15**
2. *Explain following attacks : i) Man in Middle Attack and ii) Denial of Service Attack. Also suggest ways to aviod them.* **MSBTE : Summer-15**
3. *Define attack. Explain steps in attack.* **MSBTE : Winter-15**
4. *Explain DOS and DDOS with neat diagram.* **MSBTE : Summer-16, Winter-17**
5. *List types of attacks. Explain backdoors and trapdoors attack.* **MSBTE : Winter-16, 17**
6. *With neat sketches explain the following :*
   i) SYN flood attack
   ii) Man-in-the middle attack. **MSBTE : Winter-16**
7. *Describe packet sniffing and packet spoofing attacks.* **MSBTE : Winter-16**
8. *State the types of attacks and describe Active and Passive attack with atleast one example each.* **MSBTE : Summer-15, 17**
9. *Explain any four attacks on Computer System Security.* **MSBTE : Winter-17**
10. *Explain active attack and passive attack with suitable example.* **MSBTE : Winter-18**
11. *Explain Man-In-Middle attack with help of diagram.* **MSBTE : Winter-18**
12. *Explain Man-in-the middle and TCP/IP Hacking attacks.* **MSBTE : Summer-19**
13. *Explain the concept of hacking.* **MSBTE : Summer-19**
14. *Explain sniffing and spoofing attacks.* **MSBTE : Summer-19**
15. *Describe the following terms :*
    i) Sniffing ii) Spoofing
    iii) Man-in-the middle iv) TCP/IPHijack
    MSBTE : Summer-17

1.6 Operating System Security

- Operating system security is the process of ensuring OS integrity, confidentiality and availability. OS security refers to specified steps or measures used to protect the OS from threats, viruses, worms, malware or remote hacker intrusions.
- A patch is a program that makes changes to software installed on a computer. Software

companies issue patches to fix bugs in their programs, address security problems, or add functionality.

- A patch is a software update comprised code inserted (or patched) into the code of an executable program. Typically, a patch is installed into an existing software program. Patches are often temporary fixes between full releases of a software package.
- Patches may do any of the following :
  a) Fix a software bug
  b) Install new drivers
  c) Address new security vulnerabilities
  d) Address software stability issues
  e) Upgrade the software
- A hotfix is a single, cumulative package that includes one or more files that are used to address a problem in a software product (i.e. a software bug).
- Hotfixes are Microsoft's version of patches. Microsoft bundles hotfixes into service packs for easier installation. To keep your Windows computer secure, keep your operating system up to date with the latest security patches and service packs.
- Service Pack : Large Update that fixes many outstanding issues, normally includes all Patches, Hotfixes, Maintenance releases that predate the service pack.
- A service pack (SP) is a Windows update, often combining previously released updates, that helps make Windows more reliable. Service packs, which are provided free of charge on this page, can include security and performance improvements and support for new types of hardware.

Board Question

1. *Describe any **two** terms :*
   i) Application patches ii) Hotfix iii) Upgrades

MSBTE : Winter-18

1.7 Information

- Information is a service that supports decision making within organizations. Information is changed time to time. Managing information through the process becomes an exercise in knowing when to formalize, rationalize and eventually discard information.
- Information is essential to any business. Organizations have the challenge to efficiently manage information, throughout its lifecycle, related to its business value.
- Information Lifecycle Management (ILM) is a process for managing information through its lifecycle, from conception until disposal, in a manner that optimizes storage and access at the lowest cost.
- The goal of any Information Lifecycle Management strategy is to ensure data is continuously reassessed throughout its entire lifecycle while keeping storage management costs under control.
- Information Lifecycle Management (ILM) is a process for managing information through its lifecycle, from conception until disposal, in a manner that optimizes storage and access at the lowest cost.
- ILM is an organization-wide process, encompassing all of the people and processes contributing to an organization's data flows.
- Function of information security :
  1. Protects the organization 's ability to function.
  2. Enables the safe operation of applications implemented on the organization 's IT systems.
  3. Protects the data the organization collects and uses.
  4. Safeguards the technology assets in use at the organization.
- **Information Security** is not all about securing information from unauthorized access.
- Information Security is basically the practice of preventing unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction of information. Information can be physical or electrical one.
- **Need of Security :** The information security is important in the organization because it can protect the confidential information, enables the organization function, also enables the safe operation of application implemented on the

organization's Information Technology system, and information is an asset for an organization.

Importance of Information Classification :

1. The main reason for classifying is that not all information have the same level of importance to an organization.
2. Some data are more valuable to the people who make strategic decisions because they aid them in making long-range or short-range business direction decisions.
3. Some data such as trade secrets, formulae and new product information are so valuable that their loss could create a significant problem for the enterprise in the market.
4. Thus it is obvious that information classification provides a higher, enterprise-level benefit.
5. Classification of information is used to prevent the unauthorized disclosure and the resultant failure of confidentiality.

- **Criteria for Information Classification :**

1. Value : It is the most commonly used criteria for classifying data in private sector. If the Information is valuable to an organization it needs to be classified.
2. Age : The classification of the information may be lowered if the information value decreases over the time.
3. Useful Life : If the information has been made available to new information, important changes to the information can be often considered.
4. Personal association : If the information is personally associated with specific individual or is addressed by a privacy law then it may need to be classified.

- Basic principle of security : Principle which is a core requirement of information security for the safe utilization, flow and storage of information is the CIA triad. CIA stands for confidentiality, integrity and availability and these are the three main objectives of information security.

❑❑❑

Notes

UNIT - II

2 User Authentication and Access Control

2.1 Identification and Authentication

- When you open email account, it asks user name and password. The first step is called identification (user name) and next step is called authentication (password).
- Authentication is the process of making sure that the credentials provided by someone are valid and therefore the identity of the principal (person, organization, machine, etc.) can be reasonably established with trust from both parties.
- Authentication techniques are used to verify identity. The authentication of authorized users prevents unauthorized users from gaining access to corporate information systems.
- Authentication method is of validating the identity of user, service or application. The use of authentication mechanisms can also prevent authorized users from accessing information that they are not authorized to view.
- **Entity authentication** is a technique designed to let one party prove the identity of another party. An entity can be a person, a process, a client, or a server. The entity whose identity needs to be proved is called the claimant; the party that tries to prove the identity of the claimant is called the verifier.
- The simplest and oldest method of entity authentication is the password-based authentication, where the password is something that the claimant knows.
- Password is a front-line protection against the unauthorized access (intruder) to the system. A password authenticates the identifier (ID) and provides security to the system. Therefore, almost all systems are password protected.

2.1.1 Password Vulnerability

- Passwords are extremely common. Passwords can often be guessed. Use of mechanisms to keep passwords secret does not guarantee that the system security cannot be broken.
- It only says that it is difficult to obtain passwords. The intruder can always use a trial and error method. A test of only a limited set of potential strings tends to reveal most passwords because there is a strong tendency for people to choose relatively short and simple passwords that they can remember.
- Some techniques that may be used to make the task of guessing a password difficult are as follows

  1. Longer passwords.
  2. Salting the password table.
  3. System assistance in password selection.

- The length of a password determines the ease with which a password can be found by exhaustion. For example, 3-digit password provides 1000 variations whereas four-digit passwords provides 10,000 variations.
- Second method is the system assistance. A password can be either system generated or user selected. User selected passwords are often easy to guess. A system can be designed to assist users in using passwords that are difficult to guess.

2.1.2 Encrypted Passwords

- Instead of storing the names and passwords in plain text form, they are encrypted and stored in cipher text form in the table.
- In this case, instead of directly using a user specified name and password for table lookup, they are first encrypted and then the results are used for table lookup.

- If the stored encoded password is seen, it cannot be loaded, so the password cannot be determined. The password file does not need to be kept secret.

2.1.3 One-time Passwords

- Set of paired passwords solve the problem of password sniffing.
- When a session begins, the system randomly selects and presents one part of a password pair; user must supply the other part.
- In this, user is challenged and must respond with the correct answer to that challenge. In this method, the password is different in each instance.
- One-time passwords are among the only ways to prevent improper authentication due to password exposure. Commercial implementations of one-time password system such as secure ID, use hardware calculators.

2.1.4 Criteria for Password Selection

- There are four basic techniques passwords selection strategies :
  a) User education : Tell the importance of hard-to-guess passwords to the users and provide guidelines for selecting strong password.
  b) Computer generated password : Computer generated passwords are random in nature so difficult for user to remember it and may note down somewhere.
  c) Reactive password checking : The system periodically runs its own password cracker program to find out guessable passwords. If the system finds any such password, the system cancels it and notifies the user.
  d) Proactive password checking : It is a most promising approach to improve password security. In this scheme, a user is allowed to select his own password, if password is allowable then allow or reject it.

2.1.5 Password Management

- In most cases, intruders need to acquire protected information, most often passwords. Password security is a big problem on any system : Hackers may take over someone's user account and use it in a major attack inside that system or against a totally different system; liability may involve the careless user.
- The system protects the user passwords in two ways
  1) Keeps them "encrypted" on the disk; in fact, one keeps on the disk hashes of the password : In this way, nobody can attack the system by trying to "decrypt" the password file.
  2) The file with the user personal information should be public so that when the user initiates login, the login process can check his data.
  3) The password file should be "hidden" : */etc/passwd, /etc/shadow* in Linux.
- To break the password file, the attacker essentially has to "guess" the password of a user, hash it and then compare it with the entry in the password file.
- In UNIX, the 8 characters of the password are converted to a 56-bit string that serves as key for (modified with 12-bit "salt"value) DES. It start with 64 bits all 0 and iterate DES encryption 25 times: the result will be the hash of the password and will be stored in the file.
- The salt prevents duplicate passwords from showing in the password file. Fig. 5.10.1 shows loading a new password.

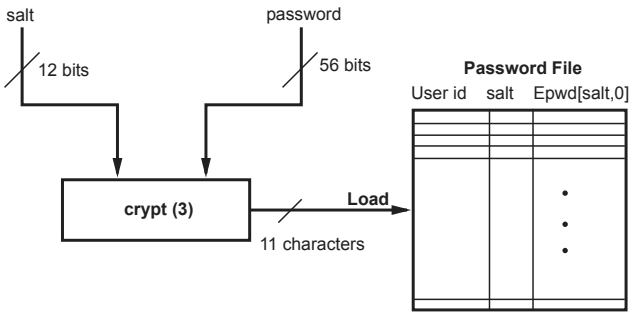


Fig. 2.1.1 Loading a new password

- Ciphertext password is stored in the table together with Salt. UNIX passwords were kept in a publicly readable file, *etc/passwords*. Now they are kept in a "shadow" directory and only visible to "root".

- The salt serves three purposes :
  1) Prevents duplicate passwords from being visible in the password file. //Even if two users choose the same password, their ciphertexts will differ//
  2) Effectively increases the length of the password by two chars. //Makes password guessing difficult//
  3) Prevents the use of hardware implementations of DES.

Board Questions

1. *Give characteristics of good password.*
   MSBTE : Summer-15, Marks 4
2. *Explain what are components of good password and four password selection stratgies.*
   MSBTE : Winter-15, Marks 8
3. *Describe different password selection criteria.*
   MSBTE : Summer-16, 19, Winter-17, Marks 4
4. *What is a password ? Describe various policies for password selection.* **MSBTE : Summer-17, Marks 8**
5. *Explain criteria for password selection.*
   MSBTE : Summer-18, Marks 4

2.2 Password Attacks

2.2.1 Piggybacking

- Piggybacking also called tailgating, is when an unauthorized person physically follows an authorized person into a restricted corporate area or system.
- It is the simple process of following closely behind a person who has just used their own access card or PIN to gain physical access to a room or building.
- In security, piggybacking refers to when a person tags along with another person who is authorized to gain entry into a restricted area, or pass a certain checkpoint.
- Another method involves a person asking an employee to "borrow" his or her laptop for a few minutes, during which the criminal is able to quickly install malicious software.
- Piggybacking on Internet access is the practice of establishing a wireless Internet connection by using another subscriber's wireless Internet access service without the subscriber's explicit permission or knowledge.
- The act may be legal or illegal, authorized or unauthorized, depending on the circumstances. However, the term more often has the connotation of being an illegal or unauthorized act.
- To describe the act of an unauthorized person who follows someone to a restricted area without the consent of the authorized person, the term tailgating is also used.
- "Tailgating" implies without consent, while "piggybacking" usually implies consent of the authorized person.
- Piggybacking is the tactic of closely following a person who has just used an access card or PIN to gain physical access to a room or building.
- Piggybacking on Internet access is the practice of establishing a wireless Internet connection by using another subscriber's wireless Internet access service without the subscriber's explicit permission or knowledge.
- It is a legally and ethically controversial practice, with laws that vary by jurisdiction around the world. While completely outlawed or regulated in some places, it is permitted in others.
- The process of sending data along with the acknowledgment is called piggybacking. Piggybacking is distinct from war driving, which involves only the logging or mapping of the existence of access points.
- Piggybacking is sometimes referred to as "Wi-Fi squatting."

2.2.2 Shoulder Surfing

- Shoulder surfing refers to using direct observation techniques, such as looking over someone's shoulder, to get information. It is commonly used to obtain passwords, PINs, security codes, and similar data.
- Shoulder surfing is particularly effective in crowded places because it is relatively easy to observe someone as they :

a. Fill out a form

b. Enter their PIN at an automated teller machine or a POS terminal

c. Use a telephone card at a public payphone

d. Enter a password at a cybercafe, public and university libraries, or airport kiosks

e. Enter a code for a rented locker in a public place such as a swimming pool or airport

f. Public transport is a particular area of concern

- Shoulder surfing can also be done long distance with the aid of binoculars or other vision-enhancing devices.
- To prevent shoulder surfing, experts recommend that you shield paperwork or your keypad from view by using your body or cupping your hand.

2.2.3 Dumpster Diving

- Dumpster diving" means searching trash for useful information. The trash may be in a public dumpster or in a restricted area requiring unauthorized entry. Dumpster diving depends on a human weakness: the lack of security knowledge.
- Many things can be found dumpster diving (e.g., CDs, DVDs, hard drives, company directories, and so forth).
- Probably the most famous example of dumpster diving was performed by Jerry Schneider in southern California. While in high school in 1968, Jerry found documentation regarding Pacific Telephone's automated equipment ordering and delivery system, which he used to order equipment and have delivered to dead drops.
- Jerry accumulated hundreds of thousands of dollars' worth of telephone equipment and established Creative Systems Enterprises to sell it; some of it was sold back to Pacific Telephone.
- Jerry was arrested in 1972, and started a security company in 1973.
- Dumpster diving is an interesting attack that produces an immense amount of information on an organization, firm, individual, or entity.
- You can learn a lot about a person or company from the trash they throw away. It's also extremely surprising how much personal and private information is thrown out for those to find.
- Generally, most dumpsters and trash receptacles do not come with locks, this would make it nearly impossible for regular trash collection services to dispose of it properly; however, other solutions are available to secure your trash.
- To prevent dumpster divers from learning anything valuable from your trash, experts recommend that your company establish a disposal policy where all paper, including print-outs, is shredded in a cross-cut shredder before being recycled, all storage media is erased, and all staff is educated about the danger of untracked trash.

Board Questions

1. *What is meant by Dumpster diving ? How it is used for attacking ? Give the ways to avoid /prevent this.* **MSBTE : Summer-15, Marks 4**
2. *Describe in brief : Piggybacking* **MSBTE : Summer-15, 18, Marks 4**
3. *Explain piggybacking.* **MSBTE : Winter-15, Marks 4**
4. *Describe piggybacking and shoulder surfing.* **MSBTE : Winter-16, 18, Marks 4**
5. *What is should surfing ? How it can be prevented ?* **MSBTE : Summer-17, Marks 4**
6. *What is piggybadking ? How it can be prevented ?* **MSBTE : Summer-17, Marks 4**
7. *Describe dumpster diving with its prevention mechanism.* **MSBTE : Winter-17, Marks 4**
8. *What is dumpster diving ? State preventative measures to avoid dumpster diving.* **MSBTE : Winter-18, Marks 6**
9. *Explain piggybacking and shoulder surfing.* **MSBTE : Summer-19, Marks 4**

2.3 Biometric

- Fig. 2.3.1 shows basic block diagram of a biometric system.
- Biometric devices consist of a reader or scanning device, software that converts the scanned information into digital form, and wherever the data is to be analyzed, a database that stores the biometric data for comparison with previous records.

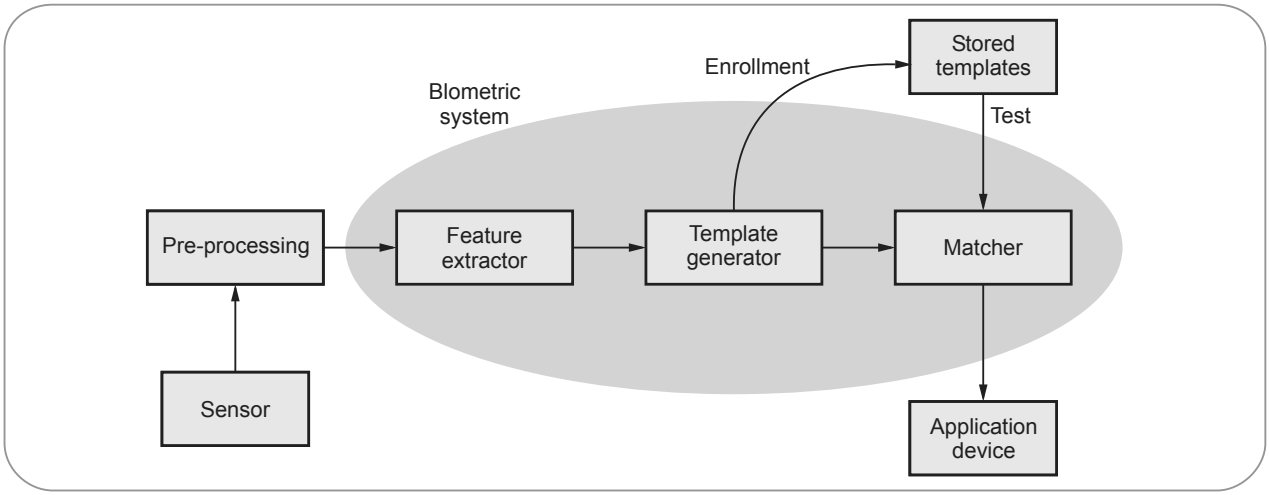


Fig. 2.3.1 Block diagram of biometric system

- When converting the biometric input, the software identifies specific points of data as match points. The match points are processed using an algorithm into a value that can be compared with biometric data scanned when a user tries to gain access.

Verification vs. identification

- Depending on the application context, a biometric system can operate either in verification or identification mode.
- In verification mode the system performs a one-to-one comparison of a captured biometric with a specific template stored in a biometric database in order to verify the individual is the person they claim to be.
- 'Positive recognition' is a common use of verification mode, where the aim is to prevent multiple people from using same identity.
- In identification mode the system performs a one-to-many comparison against a biometric database in attempt to establish the identity of an unknown individual. The system will succeed in identifying the individual if the comparison of the biometric sample to a template in the database falls within a previously set threshold.
- Identification mode can be used either for 'positive recognition' or for 'negative recognition' of the person where the system establishes whether the person is who she denies to be.
- Biometric identification systems can be grouped based on the main physical characteristic that lends itself to biometric identification.

1. Fingerprint identification : Fingerprint ridges are formed in the womb; you have fingerprints by the fourth month of fetal development. Once formed, fingerprint ridges are like a picture on the surface of a balloon. As the person ages, the fingers do get larger. However, the relationship between the ridges stays the same, just like the picture on a balloon is still recognizable as the balloon is inflated.
2. Hand geometry : Hand geometry is the measurement and comparison of the different physical characteristics of the hand. Although hand geometry does not have the same degree of permanence or individuality as some other characteristics, it is still a popular means of biometric authentication.
3. Palm vein authentication : This system uses an infrared beam to penetrate the users hand as it is waved over the system; the veins within the plam of the user are returned as black lines. Palm vein authentication has a high level of authentication accuracy due to the complexity of vein patterns of the palm. Because the palm vein patterns are internal to the body, this would be a difficult system to counterfeit. Also, the system is contactless and therefore hygienic for use in public areas.

4. Retina scan : A retina scan provides an analysis of the capillary blood vessels located in the back of the eye; the pattern remains the same throughout life. A scan uses a low intensity light to take an image of the pattern formed by the blood vessels. Retina scans were first suggested in the 1930's.
5. Iris scan : An iris scan provides an analysis of the rings, furrows and freckles in the colored ring that surrounds the pupil of the eye. More than 200 points are used for comparison.
6. Face recognition : Facial characteristics are depends on the size and shape of facial characteristics, and their relationship to each other. Although this method is the one that human beings have always used with each other, it is not easy to automate it. Typically, this method uses relative distances between common landmarks on the face to generate a unique "faceprint".
7. Signature : Although the way you sign your name does change over time, and can be consciously changed to some extent, it provides a basic means of identification.
8. Voice analysis : The analysis of the pitch, tone, cadence and frequency of a person's voice.

Advantages :

- Biometric identification can provide extremely accurate, secured access to information; fingerprints, retinal and iris scan produce absolutely unique data sets when do properly.
- Current methods like password verification have many problems (people write them down, they forget them, they make up easy-to-hack passwords).
- Automated biometric identification can be done very rapidly and uniformly, with a minimum of training.
- Your identity can be verified without resort to documents that may be stolen, lost or altered.

Board Questions

1. *List any four bometrics methods used for idenfitication. List any four advantages of biometrics.* **MSBTE : Summer-15, Marks 4**
2. *Describe the process of biometric authentication with neat labelled diagram for fingerprint.* **MSBTE : Winter-15, Marks 4**
3. *Explain use of biometrics in computer security. List various biometrics used for computer security.* **MSBTE : Winter-16, Marks 4**
4. *Describe biometric security mechanism with suitable diagram.* **MSBTE : Summer-17, Marks 8**
5. *What is the importance of biometrics in computer security ? Describe finer prints registration and verification process.* **MSBTE : Summer-16, Winter-17**
6. *Explain working of fingerprint mechanism and its limitations.* **MSBTE : Summer-18, Marks 8**
7. *Enlist types of biometrics. Explain any one biometrics type in detail.* **MSBTE : Winter-18, Marks 4**
8. *State any four advantages of biometrics.* **MSBTE : Winter-18, Marks 4**
9. *Enlist types of Biometrics. Explain any one Biometrics type in detail.* **MSBTE : Winter-18, Marks 4**
10. *Explain fingerprint and retina pattern in biometric.* **MSBTE : Summer-19, Marks 4**

2.4 Access Controls

- Access control is an important tool of security to protect data and other resources.
- The access control mechanism refers to prevention of unauthorized use of a resource.
- Access control is a security term used to refer to a set of policies for restricting access to information, tools, and physical locations. Typically access control falls under the domain of physical access control or information access control.
- Access control includes :
  1. Authentication of users
  2. Authorization of their privileges
  3. Auditing to monitor and record user actions
- Access Control List (ACL) is a set of rules that define security policy. These ACLs contain one or more Access Control Entries (ACEs), which are the actual rule definitions themselves.
- These rules can restrict access by specific user, time of day, IP address, function (department,

management level, etc.), or specific system from which a logon or access attempt is being made.

- Three types of access controls system are :
  1. Discretionary access control
  2. Mandatory access control
  3. Role-based access control

2.4.1 Authentication Mechanism

- Access is the ability of a subject to interest with an object.
- Authentication deals with verifying the identity of a subject. It is ability to specify, control and limit the access to the host system or application, which prevents unauthorized use to access or modify data or resources.
- Authentication method is of validating the identity of user, service or application. The use of authentication mechanisms can also prevent authorized users from accessing information that they are not authorized to view.
- In authentication :
  a. A Brute force attack is an automated process of trial and error used to guess a person's user name, password, credit-card number of cryptographic key.
  b. Insufficient authentication occurs when a website permits an attacker to access sensitive content or functionality without having to properly authenticate.
  c. Weak password recovery validation is when a website permits an attacker to illegally obtain, change or recover another user's password.

2.4.2 Discretionary Access Control (DAC)

- When user set an access control mechanism to allow or deny access to an object (system resource), such a mechanism is a Discretionary Access Control (DAC).
- The Discretionary Access Control is also called as an Identity-Based Access Control (IBAC).
- DAC policy is a means of assigning access rights based on rules specified by users.
- The DAC policies include the file permissions model implemented by nearly all operating systems.
- In Unix, for example, a directory listing might yield "... rw, xr-xr-x ... file.txt", meaning that the owner of file.txt may read, write, or execute it, and that other users may read or execute the file but not write it.
- The set of access rights in this example is {read, write, execute}, and the operating system mediates all requests to perform any of these actions. Users may change the permissions on files they own, making this a discretionary policy.
- Discretionary Access Control List (DACL) determines which users and groups can access the object (system resource) for operations. It consists of a list of Access Control Entries (ACEs).

Drawbacks of DAC

1. It relies on decisions by the end user to set the proper level of security. As a result, incorrect permissions might be granted to a subject or permissions might be given to an unauthorized subject.
2. The subject's permissions will be inherited by any programs that the subject executes.

2.4.3 Mandatory Access Control (MAC)

- When a system mechanism controls access to an object and an individual user cannot alter that access, then such a control is called as Mandatory Access Control (MAC).
- Mandatory Access Control (MAC) is also called as rule-based access control.
- Mandatory access control is a more restrictive scheme that does not allow users to define permissions on files, regardless of ownership. Instead, security decisions are made by a central policy administrator.
- Each security rule consists of a subject, which represents the party attempting to gain access, an object, referring to the resource being accessed, and a series of permissions that define the extent to which that resource can be accessed.
- MAC has two key elements : Labels and Levels
  1. Labels : In a system using MAC, every entity is an object (laptops, files, projects, etc.) and is assigned a classification label. These labels represent the relative importance of the object, such as confidential, secret, and top secret. Subjects (users, processes, etc.) are assigned a privilege label (sometimes called a clearance).

2. Levels : A hierarchy based on the labels is also used, both for objects and subjects. Top secret has a higher level than secret, which has a higher level than confidential.

- Major implementations of MAC are :
  1. Lattice model : Security levels for objects and subjects are ordered as a lattice.
  2. Bell-LaPadula confidentiality model : Advanced version of the lattice model.

2.4.4 Role-Based Access Control (RBAC)

- A user is an entity that wishes to access resources of the organization to perform a task. Usually, users are actual human users, but a user can also be a machine or application.
- A role is defined as a collection of users with similar functions and responsibilities in the organization. Examples of roles in a university may include "student," "alum," "faculty," "dean," "staff," and "contractor."
- In general, a user may have multiple roles.
  a) Roles and their functions are often specified in the written documents of the organization.
  b) The assignment of users to roles follows resolutions by the organization, such as employment actions (e.g. hiring and resignation) and academic actions (e.g., admission and graduation).
- Role-Based Access Control (RBAC) is a method of regulating access to computer or network resources based on the roles of individual users within an enterprise.
- In RBAC, the rights and permissions are assigned to roles instead of individual users.
- RBAC is also called as Non-Discretionary Access Control (NDAC).
- This added layer of abstraction permits easier and more flexible administration and enforcement of access controls.
- The RBAC framework provides administrators with the capability to regulate who can perform what actions, when, from where, in what order, and in some cases under what relational circumstances.
- RBAC is important because it provides customers a greater degree of control over cloud resource utilization with the added layer of system security.
- RBAC should be implemented in the following situations :
  1. In an effort to minimize downtime and accidental changes to the cloud resources, the account owner would like to restrict access to the accounts to only a few people.
  2. In an effort to synchronize cloud product access to the functions of an employee's job, the account owner would like to grant access to employees based on the nature of their position.
  3. In an effort to help prevent unauthorized access to cloud products through the sharing of admin credentials, the account owner would like each user of the cloud accounts to have their own credentials.

2.4.5 Difference between DAC and RBAC

1. DAC is based on personal permissions, while RBAC is based on group-level permissions.
2. DAC is set by the data owner, while RBAC by the system owner/s.
3. DAC definitions are typically attached to the data/resource, whereas RBAC is usually defined in two places : in code/configuration/metadata and on the user object.
4. DAC is administered "on the resource", whereas RBAC roles are centrally administered.
5. DAC should be seen as enumerating "who has access to my data", and RBAC defines "what can this user do".
6. The definition of permissions per role is typically static in RBAC, and users are only granted roles; in DAC the permissions per resource are often changed at runtime.

Board Questions

1. *What is meant by access control. Describe : i) DAC ii) MAC iii) RBAC*
   MSBTE : Summer-15, Winter-18, Marks 4
2. *What is access control ? Explain DAC, MAC and RBAC access control model.*
   MSBTE : Winter-16, Marks 8
3. *Describe access control policies in detail.*
   MSBTE : Summer-18, Marks 8

❑❑❑

UNIT - III

3 Cryptography

3.1 Introduction

1. **Plaintext :** It is the data to be protected during transmission.
2. **Encryption Algorithm :** It is a mathematical process that produces a cipher-text for any given plaintext and encryption key. It is a cryptographic algorithm that takes plaintext and an encryption key as input and produces a cipher-text.
3. **Cipher-text :** It is the scrambled version of the plaintext produced by the encryption algorithm using a specific the encryption key.
   The cipher-text is not guarded. It flows on public channel. It can be intercepted or compromised by anyone who has access to the communication channel.
4. **Decryption Algorithm :** It is a mathematical process, that produces a unique plaintext for any given cipher-text and decryption key. It is a cryptographic algorithm that takes a cipher-text and a decryption key as input, and outputs a plaintext. The decryption algorithm essentially reverses the encryption algorithm and is thus closely related to it.
7. **Encryption Key :** It is a value that is known to the sender. The sender inputs the encryption key into the encryption algorithm along with the plaintext in order to compute the cipher-text.
8. **Decryption Key :** It is a value that is known to the receiver. The decryption key is related to the encryption key, but is not always identical to it. The receiver inputs the decryption key into the decryption algorithm along with the cipher-text in order to compute the plaintext.

3.1.1 Cryptography and Cryptanalysis

Cryptography :

1. The original intelligible message, referred to as plaintext is converted into random nonsense, referred to as ciphertext. The science and art of manipulating messages to make them secure is called **cryptography.**
2. Cryptography is the art of achieving security by encoding message to make them non-readble.
3. Characteristics of cryptography
   1. The type of operations used for transforming plaintext to ciphertext.
   2. The number of keys used.
   3. The way in which the plaintext is processed.

Cryptanalysis :

- The process of trying to break any cipher text message to obtain the original plain text message itself is called as cryptanalysis.
- Cryptanalysis is the breaking of codes. The person attempting a cryptanalysis is called as a cryptanalyst.
- Brute force attack : The attacker tries every possible key on a piece of cipher text until an intelligible translation into plaintext is obtained.
- The goal of a cryptanalyst is to find some weakness or insecurity in a cryptographic scheme to prevent obtaining plaintext without keys.
- There are at least five main sections that best describe the types of attacks within cryptanalysis.
  1. Ciphertext-only attacks, where you just have access to the ciphertext. This type is rather hard to implement in more recent cryptosystems, since they are better protected.

2. Known-plaintext attacks, where you have access to the ciphertext and a plaintext-ciphertext pair.
3. Chosen-plaintext attacks, where you may choose a plaintext and learn its ciphertext in regards to how it was encrypted.
4. Chosen-ciphertext attacks, the same as the previous one except that here you may pick ciphertexts and find out the appropriate plaintexts.
5. Chosen-text attacks, where you have access to the plaintext and ciphertext, where the purpose of it is to find out the key.

Cryptology :

- Cryptology is the art and science that deals with both cryptography and cryptanalysis.
- Today we need cryptology because of the everyday use of computers and the Internet. It is important for businesses to be able to protect the information in their computers.
- If you decide to buy a CD from Amazon.com/flipkart.com using your credit card, it is important that no one but Amazon has the ability to read the file where your credit card number is stored. Electronic fund transfers have made privacy a great concern.

Board Questions

1. *Define Encryption and Descryption with reference to computer security.* **MSBTE : Summer-15, Marks 4**
2. *Define the following term.*
   A) Crytograph B) Cryptology C) Cryptanalysis D) Cipher text **MSBTE : Summer-16, Winter-18, Marks 4**
3. *Explain the terms : Cryptography, Cryptanalysis and Cryptology.* **MSBTE : Winter-16, 17, Marks 4**

3.2 Substitution Techniques

- A substitution cipher changes characters in the plaintext to produce to ciphertext. A substitution technique is one in which the letters of plaintext are replaced by other letters or by numbers or symbols.
- If the plaintext is viewed as a sequence of bits, then substitution involves replacing plaintext bit patterns with ciphertext bit patterns.

3.2.1 Caesar Cipher

- Caesar cipher is a special case of substitution techniques wherein each alphabet in a message is replaced by an alphabet three places down the line.
- Caesar cipher is susceptible to a statistical ciphertext only attack.
- For example,

Plaintext	hellow world
Ciphertext	KHOOR ZRUOG

- List of all possible combination of letters.

Plain	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s
Cipher	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V

Plain	t	u	v	w	x	y	z
Cipher	W	X	Y	Z	A	B	C

- Numerical equivalent to each letter is given below.

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

- The algorithm can be expressed as follows. For each plaintext letter P, substitute the ciphertext letter C :

$$C = E(3, P) = (P + 3) \bmod 26$$

- A shift may be of any amount, so that the general Caesar algorithm is

$$C = E(K, P) = (P + K) \bmod 26$$

where K = Values from 1 to 25

- The decryption algorithm is simply

$$P = D(K, C) = (C - K) \bmod 26$$

- If it is known that a given ciphertext is a Caesar cipher, then a brute force cryptanalysis is easily performed : Simply try all the 25 possible keys.
- **Demerits :**
  1. The encryption and decryption algorithms are known.
  2. There are only 25 keys to try.
  3. The language of the plaintext is known and easily recognizable.

3.2.2 Monoalphabetic Cipher

- Monoalphabetic cipher substitutes one letter of the alphabet with another letter of the alphabet. However, rather than substituting according to a regular pattern, any letter can be substituted for any other letter, as long as each letter has a unique substitute left and vice versa.

Plaintext	a	b	c	d	e	f	g	h	i	j	k	l	m
Ciphertext	m	n	b	v	c	x	z	a	s	d	f	g	h

Plaintext	n	o	p	q	r	s	t	u	v	w	x	y	z
Ciphertext	j	k	l	p	o	i	u	y	t	r	e	w	q

For example

Plaintext message : hello how are you

Ciphertext message : acggk akr moc wky

- Monoalphabetic ciphers are easy to break because they reflect the frequency data of the original alphabet.

Homophonic substitution cipher

- It provides multiple substitutes for a single letter. For example, A can be replaced by D, H, P, R ; B can be replaced by E, Q, S, T etc.

3.2.3 Playfair Cipher

- The playfair algorithm is based on the use of a 5 × 5 matrix of letters constructed using a keyword.
- **For example :** Monarchy is the keyword.

M	O	N	A	R
C	H	Y	B	D
E	F	G	I/J	K
L	P	O	S	T
U	V	W	X	Z

- The matrix is constructed by filling in the letters of the keyword from left to right and from top to bottom and then filling in the remainder of the matrix with the remaining letters in alphabetic order.
- The letters I and J count as one letter.

3.2.4 Hill Cipher

- The encryption algorithm takes m successive plaintext letters and substitutor for them m ciphertext letters.
- The substitution is determined by m linear equations in which each character is assigned a numerical value (a = 0, b = 1, c = 2, ... z = 25), the system can be described as follows :

$$C_1 = (K_{11} P_1 + K_{12} P_2 + K_{13} P_3) \bmod 26$$

$$C_2 = (K_{21} P_1 + K_{22} P_2 + K_{23} P_3) \bmod 26$$

$$C_3 = (K_{31} P_1 + K_{32} P_2 + K_{33} P_3) \bmod 26$$

- This can be expressed in term of column vectors and matrices :

$$\begin{pmatrix} C_1 \\ C_2 \\ C_3 \end{pmatrix} = \begin{pmatrix} K_{11} & K_{12} & K_{13} \\ K_{21} & K_{22} & K_{23} \\ K_{31} & K_{32} & K_{33} \end{pmatrix} \begin{pmatrix} P_1 \\ P_2 \\ P_3 \end{pmatrix} \bmod 26$$

or $C = KP \bmod 26$

Where C and P are column vectors of length 3, representing the plaintext and ciphertext.

- K is a 3 × 3 matrix, representing the encrypting key.
- **For example :**

Plaintext = Paymoremoney

$$\text{Key (K)} = \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix}$$

The first three letters of the plaintext are represented by the vector.

$$C = KP \bmod 26$$

$$= \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix} \begin{pmatrix} 15 \\ 0 \\ 24 \end{pmatrix} \bmod 26$$

$$= \begin{pmatrix} 375 \\ 819 \\ 486 \end{pmatrix} \bmod 26 = \begin{pmatrix} 11 \\ 13 \\ 18 \end{pmatrix} = \text{LNS}$$

For plaintext pay, ciphertext is LNS.

The entire ciphertext is **LNSHDLEWMTRW**

- Decryption requires using the inverse of the matrix K.
- The general terms in Hill cipher is

$$\text{Cipher } C = E(K, P) = KP \bmod 26$$

$$\text{Plaintext } P = D(K, P) = K^{-1} C \bmod 26$$

$$= K^{-1} KP = P$$

Advantages

1. It completely hides single letter frequency.
2. Hill cipher is strong against a ciphertext only attack.
3. By using larger matrix, more frequency information hiding is possible.

Disadvantage

1. Easily broken with a known plaintext attack.

3.2.5 Polyalphabetic Substitution

- In polyalphabetic substitution, each occurrence of a character can have a different substitute. The relationship between a character in the plaintext to a character in the ciphertext is one to many.
- An example of polyalphabetic substitution is the **Vigenere cipher.**
- The Vigenere cipher chooses a sequence of keys, represented by a string. The key letters are applied to successive plaintext characters, and when the end of the key is reached, the key start over.

• Fig. 3.2.1 shows a tableall or table to implement this cipher efficiently,

		Plaintext																									
		a	**b**	**c**	**d**	**e**	**f**	**g**	**h**	**i**	**j**	**k**	**l**	**m**	**n**	**o**	**p**	**q**	**r**	**s**	**t**	**u**	**v**	**w**	**x**	**y**	**z**
Key	**a**	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	b	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
	c	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
	d	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
	e	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
	f	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
	g	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
	h	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
	i	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
	j	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
	k	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
	l	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
	m	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
	n	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
	o	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
	p	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
	q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
	r	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	N	N	O	P	Q
	s	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
	t	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
	u	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
	v	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
	w	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
	x	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
	y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
	z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Fig. 3.2.1

• **For example :** Let the message be THE BOY HAS THE BAG and let the key be VIG.

Key = VIG VIG VIG VIG VIG

Plaintext = THE BOY HAS THE BAG

Ciphertext = OPKWWECIYOPKWIM

• The strength of this cipher is that there are multiple ciphertext letters for each plaintext letter, one for each unique letter of the keyword.

3.2.6 One Time Pad

• The key string is chosen at random and at least as long as the message, so it does not repeat.

- Each new message requires a new key of the same length as the new message. It produces random output that bears no statistical relationship to the plaintext.
- **Vernam cipher** uses a one time pad, which is discarded after a single use, and therefore is suitable only for short messages.
- **For example :**

Plaintext :	c	o	m	e	t	o	d	a	y
	2	14	12	4	19	14	3	0	24
Key	N	C	B	T	Z	Q	A	R	X
	13	2	1	19	25	16	0	17	23
Total	15	16	13	23	44	30	3	17	47
Subtract 26 if > 25	15	16	13	23	18	04	3	17	21
Ciphertext	P	Q	N	X	S	E	D	R	V

- The one time pad offers complete security but, in practice, has two fundamental difficulties.
  1. There is the practical problem of making large quantities of random keys.
  2. Key distribution and protection is also major problem with one time pad.
  3. Only possible attack to such a cipher is a brute force attack.

3.2.7 Feistel Cipher

- Fig. 3.2.2 shows the classical Feistel network. The inputs to the encryption algorithm are a plaintext block of length 2w bits and a key K. The plaintext block is divided into two halves i.e. Left (L_0) and Right (R_0).

(See Fig. 3.2.2 on next page)

Parameters and design features

Following parameters are considered :

1. Block size
2. Key size
3. Number of rounds
4. Subkey generation algorithms
5. Round function
6. Fast software encryption / decryption.
7. Ease of analysis

1. Security depends upon the block size. Larger **block size** gives greater security but encryption / decryption speed is reduced normal. Block size is 64-bit and AES uses 128-bit block size.
2. Greater security is achieved by using longer **key size**. Because of longer key size, again speed of algorithm decreases. Key sizes of 64 bits or less are now widely considered to be inadequate and 128 bits have become a common size.
3. **Number of rounds** are 16 in most of the algorithm. In Feistel cipher, single round offers insufficient security and multiple rounds offer greater security.
4. In **subkey generation algorithm**, greater complexity leads to greater difficulty of cryptanalysis.
5. **Round function** is again greater complexity for greater resistance to cryptanalysis.
6. **Fast software encryption / decryption** : The speed of execution of the algorithm becomes a concern.
7. **Ease of analysis** : There is great benefit in making the algorithm easy to analysis.

Decryption algorithm

- Use the ciphertext as input to the algorithm, but use the subkeys K_i in reverse order.
- The output of the first round of the decryption process is equal to a 32 bit swap of the input to the 16^{th} round of the encryption process.
- Consider the encryption process :

$$LE_{16} = RE_{15}$$

$$RE_{16} = LE_{15} \times F(RE_{15}, K_{16})$$

- On the decryption side

$$LD_1 = RD_0 = LE_{16} = RE_{15}$$

$$RD_1 = LD_0 \times F(RD_0, K_{16})$$

$$= RE_{16} \times F(RE_{15}, K_{16})$$

$$= [(LE_{15} \times F(RE_{15}, K_{16})] \times F(RE_{15}, K_{16})$$

$\therefore$ We have $LD_1 = RE_{15}$ and $RD_1 = LE_{15}$

- For the i^{th} iteration of the encryption algorithm,

$$LE_i = RE_{i-1}$$

$$RE_i = LE_{i-1} \times F(RE_{i-1}, K_i)$$

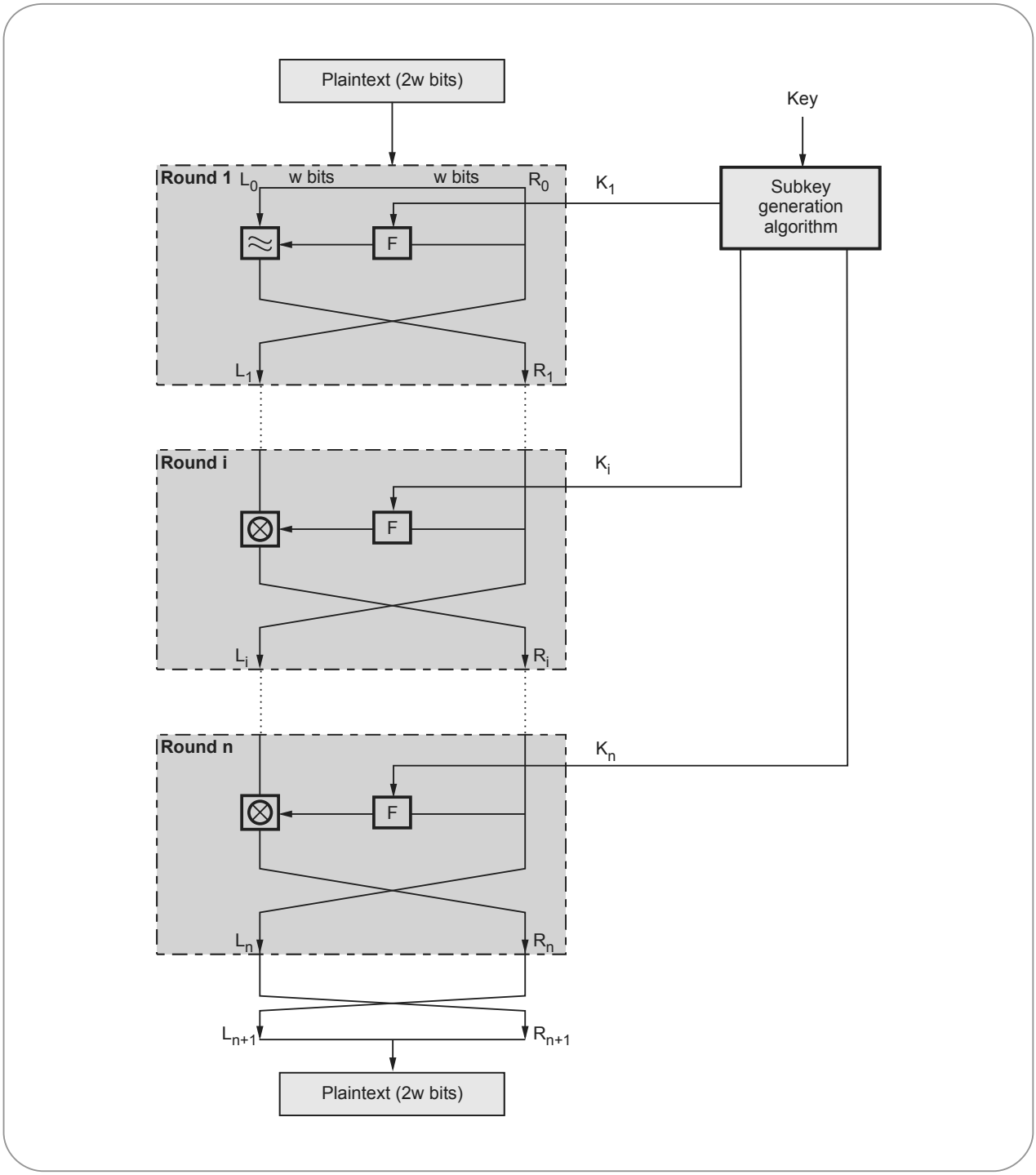


Fig. 3.2.2 Classical feistel network

Finally, the output of the last round of the decryption process is $RE_0 \| LE_0$. A 32 bit swap recovers the original plaintext, demonstrating the validity of the Feistel decryption process.

3.2.8 Comparison between Monoalphabetic and Polyalphabetic Cipher

Sr. No.	Monoalphabetic cipher	Polyalphabetic cipher
1.	Once a key is chosen, each alphabetic character of a plaintext is mapped onto a **unique** alphabetic character of a ciphertext.	Each alphabetic character of a plaintext can be mapped onto "**m**" alphabetic characters of a ciphertext.
2.	The relationship between a character in the plaintext and the characters in the ciphertext is one-to-one.	The relationship between a character in the plaintext and the characters in the ciphertext is one-to-many.
3.	A stream cipher is a monoalphabetic cipher if the value of *k*i does not depend on the position of the plaintext character in the plaintext stream	A stream cipher is a polyalphabetic cipher if the value of *k*i does depend on the position of the plaintext character in the plaintext stream.
4.	Monoalphabetic cipher includes additive, multiplicative, affine and monoalphabetic substitution cipher.	Polyalphabetic cipher includes autokey, Playfair, Vigenere, Hill, one-time pad, rotor , and Enigma cipher.

Ex. 3.2.1 *Encrypt the message "PAY" using Hill cipher with the following key matrix and show the decryption to get the original plain text.*

$$K = \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix}$$

Sol. :

$$K = \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix}$$

The letters PAY of the plaintext are represented by the vector :

$$\begin{pmatrix} 15 \\ 0 \\ 24 \end{pmatrix} \begin{pmatrix} 15 \\ 0 \\ 24 \end{pmatrix} = \begin{pmatrix} 375 \\ 819 \\ 486 \end{pmatrix} \bmod 26 = \begin{pmatrix} 11 \\ 13 \\ 18 \end{pmatrix} = \text{LNS}$$

Ciphertext = LNS

Ex. 3.2.2 : *Convert "COMPUTER SECUIRTY" using Caesar cipher* **MSBTE : Winter-16, Marks 2**

Sol. : Caesar cipher involves replacing each letter of the alphabet with the letter standing 3 places further down the alphabet.

Plain text : COMPUTER SECUIRTY

Cipher Text : FRPSXWHU VHFXLUWB

Board Questions

1. *Define caesar cipher. Write its algorithm and convert "COMPUTER SECURITY" using caesar cipher.* **MSBTE : Winter-16, Marks 4**
2. *What is One Time Pad (OTP) security mechanism ?* **MSBTE : Summer-17, Marks 4**
3. *Explain one time pad technique.* **MSBTE : Summer-18, Marks 4**
4. *What are the techniques for transforming plain text to cipher text ? Explain any one in detail.* **MSBTE : Summer-18, Marks 4**
5. *Explain the terms :*
   i) Cryptography ii) Cryptanalysis
   iii) Cryptology iv) Cipher text. **MSBTE : Summer-19, Marks 4**
6. *Explain Caesar's cipher substitution technique with example.* **MSBTE : Summer-19, Marks 4**

3.3 Transposition Techniques

- A transposition cipher rearranges the characters in the plaintext to form the ciphertext. The letters are not changed.
- The rail fence cipher is composed by writing the plaintext in two rows, proceeding down, then across and reading the ciphertext across, then down.
- For example, to encipher the message "meet me after this party" with a rail fence of depth 2, we write the following :

m e m a t r h s a t

e t e f e t i p r y

- The ciphertext is
  MEMATRHSATETEFETIPRY
- Attacking a transposition cipher requires rearrangement of the letters of the ciphertext.
- A pure transposition cipher is easily recognized because it has the same letter frequencies as the original plaintext.

Plaintext : The book is suitable for self study.

Key : 5 6 4 1 3 2

Key :	5	6	4	1	3	2
Plaintext:	t	h	e	b	o	o
	k	i	s	s	u	i
	t	a	b	l	e	f
	o	r	s	e	l	f
	s	t	u	d	y	

Ciphertext : BSLEDOIFFOUELYESBSUTKTOSHIART.

3.3.1 Comparison of Substitution and Transposition Ciphers

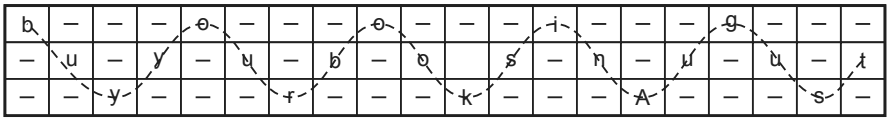
	Substitution ciphers	Transposition ciphers
Definition	Each letter or group of letters of the plaintext are replaced by some other letter of group of letters, to obtain the ciphertext.	Letters of the plaintext are permuted in some form.
Example	Hill cipher, one time pad	Rail fence cipher
Strength	1.Exhaustive search is infeasible. 2.Through to be unbreakable by many back then.	1.Reduce redundancies in plaintext. 2.Transposition cipher can be made more secure by performing more than one stage of transposition.
Drawback	1.Brute force attack is easy	1.The ciphertext has the same letter frequency as the original plaintext. 2.Guessing the number of columns and some probable words in the plaintext holds the key.

3.3.2 Rail Fence Cipher

- The Rail Fence Cipher is a transposition cipher. It rearranges the plaintext letters by drawing them in a way that they form a shape of the rails of an imaginary fence.
- To encrypt the message, the letters should be written in a zigzag pattern, going downwards and upwards between the levels of the top and bottom imaginary rails. The shape that is formed by the letters is similar to the shape of the top edge of the rail fence.
- Next, all the letters should be read off and concatenated, to produce one line of ciphertext. The letters should be read in rows, usually from the top row down to the bottom one.
- The secret key is the number of levels in the rail. It is also a number of rows of letters that are created during encryption. This number cannot be very big, so the number of possible keys is quite limited.

- Suppose we want to encrypt the message "buy your books in August" using a rail fence cipher with encryption key 3.

a) Arrange the plaintext characters in an array with 3 rows (the key determines the number of rows), forming a zig-zag pattern :



b) Then concatenate the non-empty characters from the rows to obtain the ciphertext: BOOIGUYUBOSNUUTYRKAS

Ex. 3.3.1 *Solve the following example using rail fence technique. "COMPUTER SECURITY IS IMPORTANT"*

MSBTE : Summer -19, Marks 4

Sol. : Plain text : COMPUTER SECURITY IS IMPORTANT

Arrange the plaintext characters in an array with 3 rows

C	-	-	-	U	-	-	-	S	-	-	-	R	-	-	-	I	-	-	-	P	-	-	-	A	-	-
-	O	-	P	-	T	-	R	-	E		U	-	I	-	Y	-	S	-	M	-	O	-	T	-	N	-
-	-	M	-	-	-	E	-	-	-	C	-	-	-	T	-	-	-	I	-	-	-	R	-	-	-	T

Ciphertext : CUSRIPAOPTREUIYSMOTNMECTIRT

Ex. 3.3.2 *Decipher a message : "TSACT SGCEB HISRM SELNV ISEEE AVITP" using a Rail fence using 10 Columns & 3 rails & retrieve original massage.*

MSBTE : Summer-18, Marks 4

Sol. : The number of columns in rail fence cipher remains equal to the length of plaintext message. Hence, rail matrix can be constructed accordingly.

T	S	A	C	T	S	G	C	E	B
H	I	S	R	M	S	E	L	V	N
I	S	E	E	E	A	V	I	T	P

Original Message : THIS IS A SECRET MESSAGE VCLIEVT BNP

Ex. 3.3.3 *Convert plain text to cipher text using Rail Fence technique "COMPUTER ENGINEERING".*

MSBTE : Winter-17, Marks 4

Sol. :

Plain text = COMPUTER ENGINEERING

Step 1 : Write down Plain text as sequence of diagonal.

C	-	-	-	U	-	-	-	E	-	-	-	N	-	-	-	I	-	-
-	O	-	P	-	T	-	R	-	N		I	-	E	-	R	-	N	-
-	-	M	-	-	-	E	-	-	-	G	-	-	-	E	-	-	-	G

Ciphertext : CUENIOPTRNIERNMEGEG

Ex. 3.3.4 *Convert plain text into cipher text by using simple columnas techniques of the following sentence: 'ALL IS WELL FOR YOUR EXAM'* **MSBTE : Summer-17, Marks 4**

Sol. : Consider the six columns. Therefore, we write the message in the rectangle row-by-row :

Column 1	Column 2	Column 3	Column 4	Column 5	Column 6
A	L	L	I	S	W
E	L	L	F	O	R
Y	O	U	R	E	X
A	M				

- Now let us decide the order of columns at some random order, say 5, 2,4,1,6,3. Then read the text in the order of these columns.

  Ciphertext = SOELLOMIFRAEYAWRXLLU

Ex. 3.3.5 *Convert plain text to cipher text using Rail Fence technique "COMPUTER SECUIRTY"* **MSBTE : Winter-16, Marks 4**

Sol. :

Plain text : COMPUTER SECURITY

Arrange the plaintext characters in an array with 3 rows

C	-	-	-	U	-	-	-	S	-	-	-	R	-	-	-
-	O	-	P	-	T	-	R	-	E		U	-	I	-	Y
-	-	M	-	-	-	E	-	-	-	C	-	-	-	T	-

Ciphertext : CUSROPTREUIYMECT

Ex. 3.3.6 *Encrypt "Computer Security Technology" using rail fence technique.* **MSBTE : Summer-16, Marks 4**

Sol. : Plain text : Computer Security Technology

Arrange the plaintext characters in an array with 3 rows

C	-	-	-	u	-	-	-	S	-	-	-	r	-	-	-	T	-	-	-	n	-	-	-	g	-
-	o	-	p	-	t	-	r	-	e		u	-	i	-	y	-	e	-	h	-	o	-	o	-	y
-	-	m	-	-	-	e	-	-	-	c	-	-	-	t	-	-	-	c	-	-	-	l	-	-	-

Ciphertext : CuSrtngoptreuiyehooymectc 1

Board Questions

1. *Explain rail fence transposition technique.* **MSBTE : Winter-15, Marks 4**
2. *Explain simple columnar transposition technique with algorithm and example.* **MSBTE : Summer-16, Marks 4**
3. *Explain rail fence technique with algorithm. Encrypt "Computer Security Technology" using rail fence technique.* **MSBTE : Summer-16, Marks 8**
4. *Distinguish between substitution cipher and transposition cipher.* **MSBTE : Winter-16, Marks 3**
5. *Explain simple columnar transposition technique with algorithm and example.* **MSBTE : Winter-17, Marks 4**
6. *Consider plain text "Network security", encrypt it with help of Rail fence technique, also write the algorithm.* **MSBTE : Winter-18, Marks 4**

7. Explain the rail fence techniques and simple columnar transposition technique. Solve the following example using rail fence technique "COMPUTER SECURITY IS IMPORTANT".

MSBTE : Summer-19, Marks 8

3.4 Steganography

- Steganography is derived from the Greek for covered writing and essentially means "to hide in plain sight".
- As defined as it is the art and science of communicating in such a way that the presence of a message cannot be detected.
- Simple steganographic techniques have been in use for hundreds of years, but with the increasing use of files in an electronic format new technique for information hiding have become possible.
- The other major area of steganography is copyright marking, where the message to be inserted is used to assert copyright over a document. This can be further divided into watermarking and fingerprinting.
- Steganography provides a means of secret communication which cannot be removed without significantly altering the data in which it is embedded. The embedded data will be confidential unless an attacker can find a way to detect it.
- Computer Steganography is based on two principles.
  1. The first one is that the files containing digitized images or sound can be altered to a certain extend without loosing their functionality.
  2. The other principle deals with the human inability to distinguish minor changes in image color or sound quality, which is especially easy to make use of in objects that contain redundant information, be it 16-bit sound, 8-bit or even better 24-bit image. The value of the least significant bit of the pixel color won't result in any perceivable change of that color.

Process :

- Fig. 3.4.1 shows a simple process in steganography. In this example, a secret image is being embedded inside a cover image to produce the stego-image.

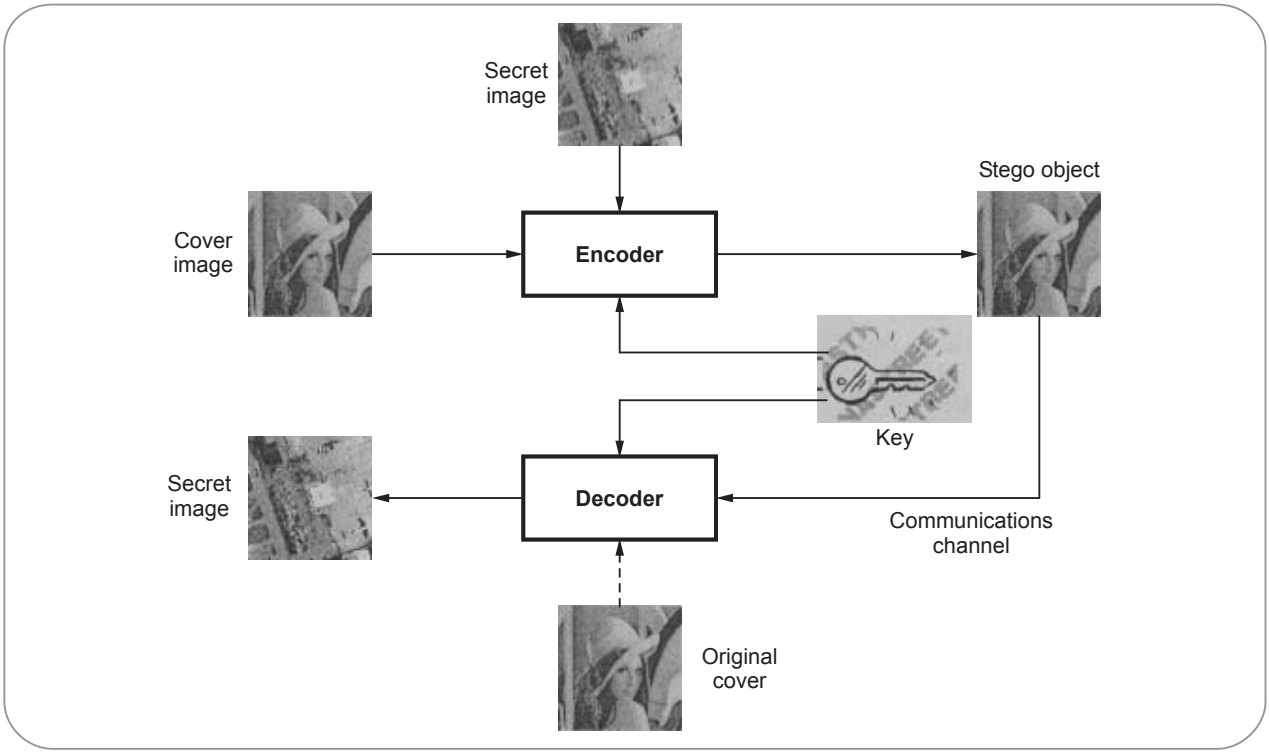


Fig. 3.4.1 Process in steganography

- The data to be concealed is compressed and hidden within another file.
- The first step is to find a file which will be used to hide the message (also called a carrier or a container.)
- The next step is to embed the message one wants to hide within the carrier using a steganographic technique.
- Two different techniques commonly used for embedding are :
  a) Replace the least significant bit of each byte in the [carrier] with a single bit for the hidden message.
  b) Select certain bytes in which to embed the message using a random number generator ; resampling the bytes to pixel mapping to preserve color scheme, in the case of an image...; hiding information in the coefficients of the discrete cosine, fractal or wavelet transform of an image ; and applying mimic functions that adapt bit pattern to a given statistical distribution."

3.4.1 Difference between Cryptography and Steganography

Sr. No.	Cryptography	Steganography
1.	It is a technique to convert the secret message into other than human readable form.	It is a technique to hide the existence of the communication.
2.	It is a kind of known communication.	It is a kind of hidden communication.
3.	Cryptography alters the overall structure of the data.	Steganography does not alters the overall structure of the data.
4.	The final result obtained is known as cipher text.	The final result obtained is known as stego media.
5.	Once it has been discovered no one can easily get the secret data.	Once it has been discovered anyone can get the secret data.

Board Questions

1. *What is meant by steganography ? Describe its importance ?* **MSBTE : Summer-15, Marks 4**
2. *Explain the term steganography with example.* **MSBTE : Summer-16, Winter-17, Marks 4**
3. *What is steganography ? What are its applications ?* **MSBTE : Summer-17, Marks 4**
4. *Define the following terms steganography.* **MSBTE : Winter-18, Marks 1**
5. *Explain stenography technique.* **MSBTE : Summer-19, Marks 4**

3.5 Symmetric Cryptography

- A symmetric encryption model has five ingredients : Plaintext, Encryption algorithm, Secret key, Ciphertext and Decryption algorithm.
- Fig. 3.5.1 (see fig. on next page) shows the conventional encryption model.
- **Plaintext** is the original message or data that is fed into the algorithm as input.
- **Encryption algorithm** performs various substitutions and transformations on the plaintext.
- **Secret key** is a value independent of the plaintext and of the algorithm. The exact substitutions and transformations performed by the algorithm depend on the key.
- **Ciphertext** is the scrambled message produced as output. It depends on the plaintext and the secret key.
- **Decryption algorithm** takes the ciphertext and the secret key and produces the original plaintext.
- The encryption process where same keys are used for encrypting and decrypting the information is known as Symmetric Key Encryption.
- The study of symmetric crypto-systems is referred to as symmetric cryptography. Symmetric crypto-systems are also sometimes referred to as secret key crypto-systems.
- A few well-known examples of symmetric key encryption methods are - Digital Encryption Standard (DES), Triple-DES (3DES), IDEA, and BLOWFISH.

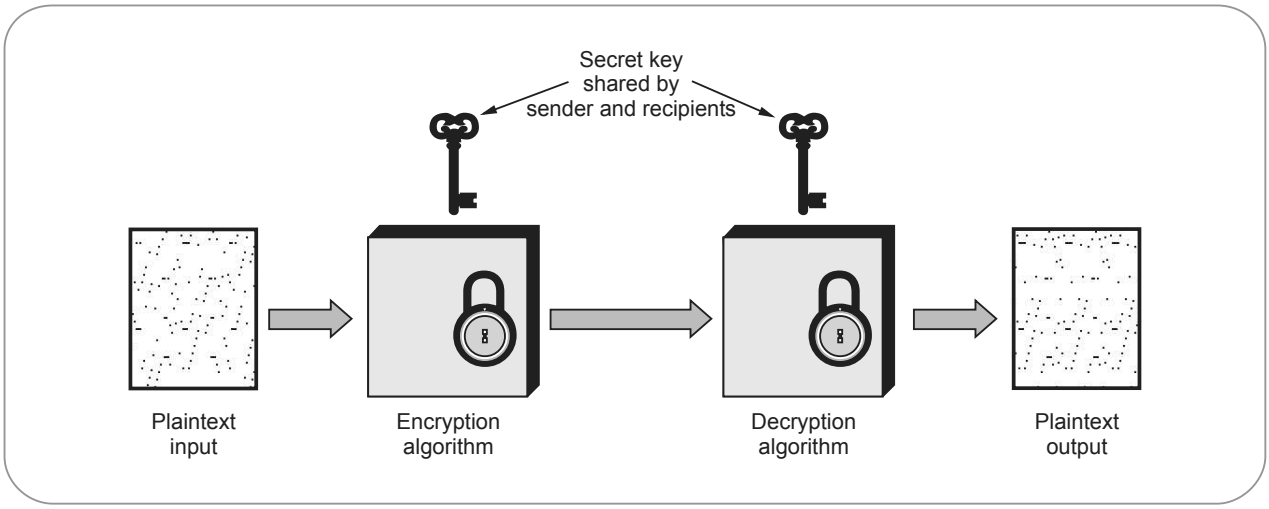


Fig. 3.5.1 Conventional encryption model

3.5.1 Advantages of Symmetric Cryptography

1. High rates of data throughput.
2. Keys for symmetric-key ciphers are relatively short.
3. Symmetric-key ciphers can be used as primitives to construct various cryptographic mechanisms (i.e. pseudorandom number generators).
4. Symmetric-key ciphers can be composed to produce stronger ciphers.
5. Symmetric-key encryption is perceived to have an extensive history.

3.5.2 Disadvantages of Symmetric Cryptography

1. Key must remain secret at both ends.
2. In large networks, there are many keys pairs to be managed
3. Sound cryptographic practices dictates that the key be changed frequently
4. Digital signature mechanisms arising from symmetric-key encryption typically require either large keys or the use of third trusted parties.

Board Questions

1. *Explain model of security with block diagram.* **MSBTE : Winter-15, Marks 6**
2. *Describe model for security with the help of diagram.* **MSBTE : Winter-16, Marks 6**
3. *Describe with the neat diagram model for security.* **MSBTE : Summer-17, Marks 6**

3.6 Simple Data Encryption Standard

- Takes an 8-bit block plaintext, a 10-bit key and produces an 8-bit block of cipher-text.
- Decryption takes the 8-bit block of cipher-text, the same 10-bit key and produces the original 8-bit block of plaintext.
- It was designed as a test block cipher for learning about modern cryptanalytic techniques such as linear cryptanalysis, differential cryptanalysis and linear-differential cryptanalysis.
- The same key is used for encryption and decryption. Though, the schedule of addressing the key bits is altered so that the decryption is the reverse of encryption.
- An input block to be encrypted is subjected to an initial permutation IP. Then, it is applied to two rounds of key-dependent computation. Finally, it is applied to a permutation which is the inverse of the initial permutation.

$$\text{plaintext} = b_1 b_2 b_3 b_4 b_5 b_6 b_7 b_8$$

$$\text{key} = k_1 k_2 k_3 k_4 k_5 k_6 k_7 k_8 k_9 k_{10}$$

Subkey generation

- First, produce two subkeys K_1 and K_2:

$$K_1 = P8(LS_1(P10(\text{key})))$$

$$K_2 = P8(LS_2(LS_1(P10(\text{key}))))$$

where P8, P10, LS_1 and LS_2 are bit substitution operators.

- For example, P10 takes 10 bits and returns the same 10 **bits in a different order :**

$$P10(k_1k_2k_3k_4k_5k_6k_7k_8k_9k_{10}) = k_3k_5k_2k_7k_4k_{10}k_1k_9k_8k_6$$

It's convenient to write such bit substitution operators in this notation :

P10 : (10 bits to 10 bits)

3	5	2	7	4	10	1	9	8	6

P8 : (10 bits to 8 bits)

6	3	7	4	8	5	10	9

LS_1 ("left shift 1 bit" on 5 bit words) : 10 bits to 10 bits

2	3	4	5	1	7	8	9	10	6

LS_2 ("left shift 2 bit" on 5 bit words) : 10 bits to 10 bits

3	4	5	1	2	8	9	10	6	7

Encryption

- The plain text is split into 8-bit blocks; each block is encrypted separately. Given a plaintext block, the cipher text is defined using the two subkeys K_1 and K_2, as follows:

$$\text{Ciphertext} = IP^{-1}(f_{K_2}(SW(f_{K_1}(IP(\text{plaintext})))))$$

where :

Initial Permutation (IP) : 8 bits to 8 bits

2	6	3	1	4	8	5	7

IP^{-1} (8 bits to 8 bits)

4	1	3	5	7	2	8	6

Switch (SW) : 8 bits to 8 bits

5	6	7	8	1	2	3	4

and $f_K( )$ is computed as follows.

We write exclusive-or (XOR) as +.

$$f_K(L, R) = (L + F_K(R), R)$$

$$F_K(R) = P4 (S0(lhs(EP(R)+K)) , S1(rhs(EP(R)+K)))$$

4 bits to 8 bits

4	1	2	3	2	3	4	1

P4 (4 bits to 4 bits)

2	4	3	1

lhs (8 bits to 4 bits)

1	2	3	4

rhs (8 bits to 4 bits)

5	6	7	8

$S0(b_1 b_2 b_3 b_4)$ = The $[b_1 b_4, b_2 b_3]$ cell from the "S-box" S0 below, and similarly for S1.

S0

	0	1	2	3
0	1	0	3	2
1	3	2	1	0
2	0	2	1	3
3	3	1	0	3

S1

	0	1	2	3
0	0	1	2	3
1	2	0	1	3
2	3	0	1	0
3	1	1	0	3

- **Algorithm :**

The block of 12 bits is written in the form $L_0 R_0$, where L_0 consists of the first 6 bits and R_0 consists of the last 6 bits. The i^{th} round of the algorithm transforms an input $L_{i-1} R_{i-1}$ to the output $L_i R_i$ using an 8-bit K_i derived from K.

- Fig. 3.6.1 shows one round of a Feistel system.

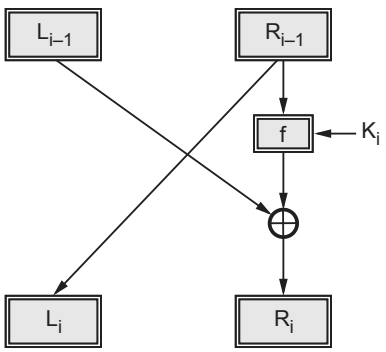


Fig. 3.6.1 One round of a Feistel system

- The output for the i^{th} round is found as follows :

$$L_i = R_{i-1} \text{ and } R_i = L_{i-1} \oplus f(R_{i-1}, K_i)$$

- This operation is performed for a certain number of rounds, say n, and produces $L_n R_n$.
- The ciphertext will be $R_n L_n$.
- Encryption and decryption are done the same way except the keys are selected in the reverse order.
- The keys for encryption will be K_1, K_2. ..... K_n and for decryption will be K_n, ...K_{n-1} ..... K_1.
- **Function $f(R_{i-1}, K_i)$:** The function $f(R_{i-1}, K_i)$, depicted in the Fig. 3.6.2 below, is described in following steps.

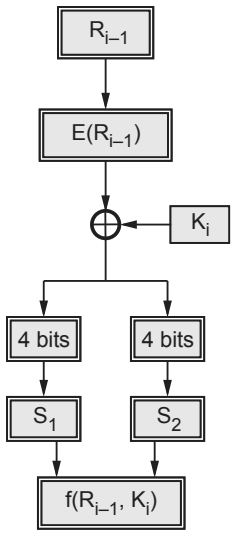


Fig. 3.6.2 The Function $f(R_{i-1}, K_i)$

1. The 6-bits are expanded using the following expansion function. The expansion function takes 6-bit input and produces an 8-bit output. This output is the input for the two S-boxes.

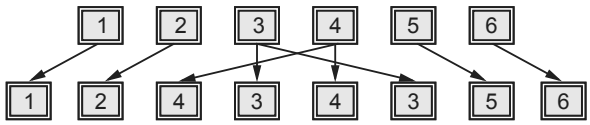


Fig. 3.6.3 The expansion function, $E(R_{i-1})$

2. The 8-bit output from the previous step is Exclusive-ORed with the key K_i
3. The 8-bit output is divided into two blocks. The first block consists of the first 4 bits and the last four bits make the second block. The first block is the input for the first S-box (S1) and the second block is the input for the second S-box (S2).

4. The S-boxes take 4-bits as input and produce 3-bits of output. The first bit of the input is used to select the row from the S-box, 0 for the first row and 1 for the second row. The last 3 bits are used to select the column.
5. The output from the S-boxes is combined to form a single block of 6-bits. These 6 bits will be the output of the function $f(R_{i-1}, K_i)$.

Example : Let the output from the expander function be 11010010.

Solution : 1101 will be the input for the S1 box and 0010 will be the input for the S2 box. The output from the S1 box will be 111, the first of the input is 1 so select the second row and 101 will select the 6^{th} column. Similarly the output from the S2 box will be 110. In above example we have the S1 output 111 and S2 output 110. So the output for the function

$f(R_{i-1}, K_i)$ will be 111110, the S1 output followed by the S2 output.

3.7 Data Encryption Standard

- DES Encryption standard (DES) is **a symmetric key block cipher** published by the National Institute of Standards and Technology (NIST).
- It encrypts data in 64-bit block.
- DES is symmetric key algorithm : The same algorithm and key is used for both encryption and decryption.
- Key size is 56-bit.
- The encryption process is made of two permutations i.e. P-boxes, which is called initial and final permutation.
- DES uses both transposition and substitution and for that reason is sometimes referred to as a **product cipher**. Its input, output and key are each 64-bits long. The sets of 64-bits are referred to as **blocks**.
- The cipher consists of 16 rounds or iterations. Each rounds uses a separate key of 48-bits.
- Fig. 3.7.1 shows DES encryption algorithm. First, the 64-bit plaintext passes through an Initial Permutation (IP) that rearranges the bits to produce the permuted input. (See Fig. 3.7.1 on next page.)
- Then there is a phase consisting of 16 rounds of the same function, which involves both permutation and substitution functions.
- The output of the sixteenth round consists of 64-bits that are a function of the input plaintext and the key.
- The left and right halves of the output are swapped to produce the pre-output. At last, the pre-output is passed through a permutation (IP^{-1}) that is the inverse of the initial permutation function, to produce the 64-bit ciphertext.

Initial permutation

- Table shows the initial permutation and its inverse. The input to a table consist of 64-bits numbered from 1 to 64.
- The 64 entries in the permutation table contain a permutation of the numbers from 1 to 64. Each entry in the permutation table indicates the positon of a numbered input bit in the output, which also consists of 64-bits.

Initial Permutation (IP) table

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	2.1	13	5
63	55	47	39	31	23	15	7

Inverse Initial Permutation (IP^{-1})

40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

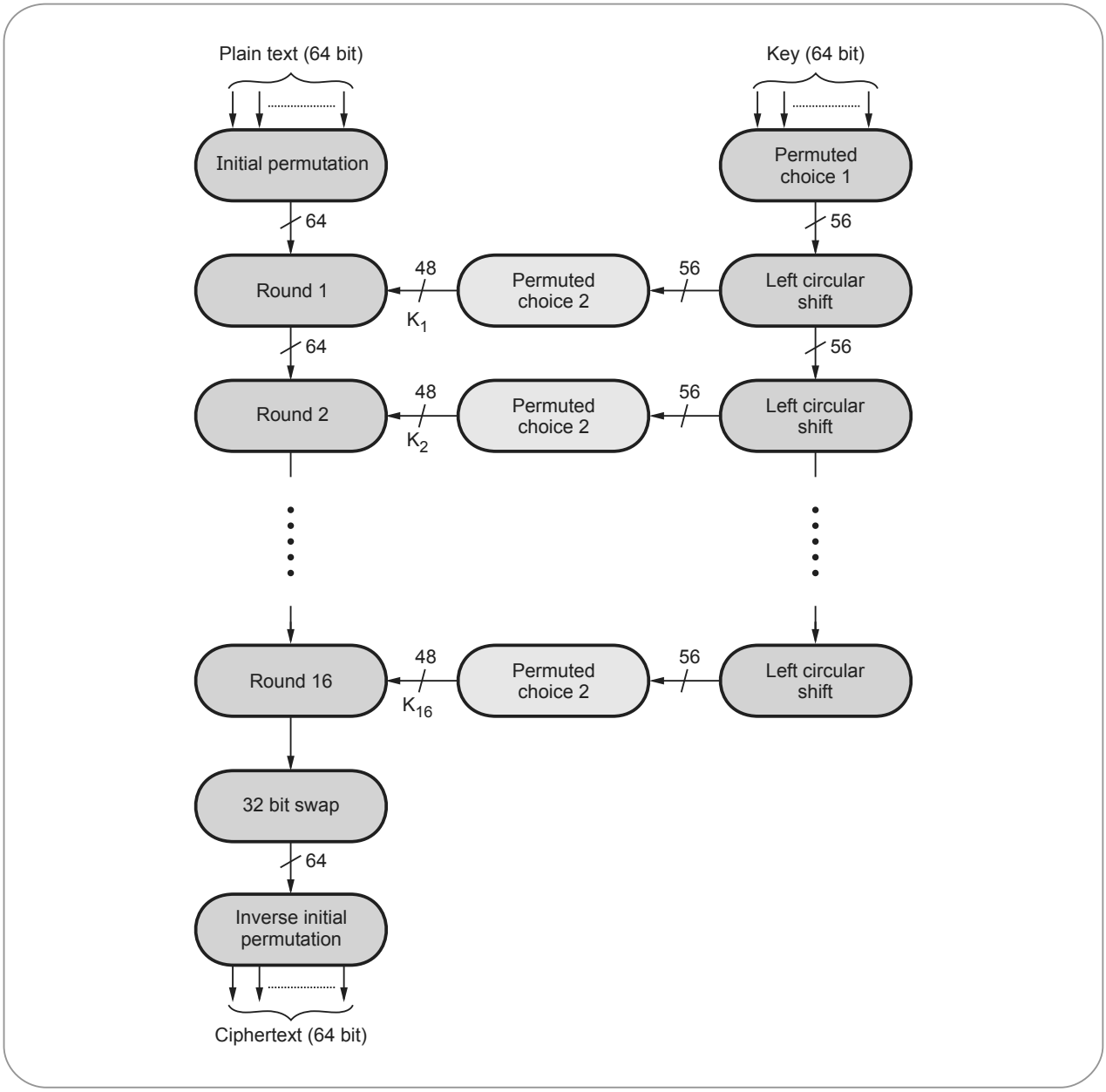


Fig. 3.7.1 DES encryption algorithm

3.7.1 Details of Single Round

- Fig. 3.7.2 shows single round of DES algorithm. The left and right halves of each 64-bit intermediate value are treated as separate 32-bit quantities, labeled L and R.
- The overall processing at each round can be summarised in the following formulae :

$$L_i = R_{i-1}$$

$$R_i = L_{i-1} \text{ X F } (R_{i-1}; K_i)$$

- The left output (L_i) is simply copy of the right input (R_{i-1}). The right output (R_i) is the XOR of left input (L_{i-1}) and right input (R_{i-1}) and key for this stage is K_i. In this stage, the substitution and permutation both functions are used.
- Fig. 3.7.3 shows role of S-boxes in the function F. It consists of set of eight S-boxes, each of which accepts 6 bits as input and produces 4 bits as output.
- The 48 bit input block is divided into 8 subblocks and each subblock is given to a S-box. The S-box transforms the 6 bit input into a 4 bit output.

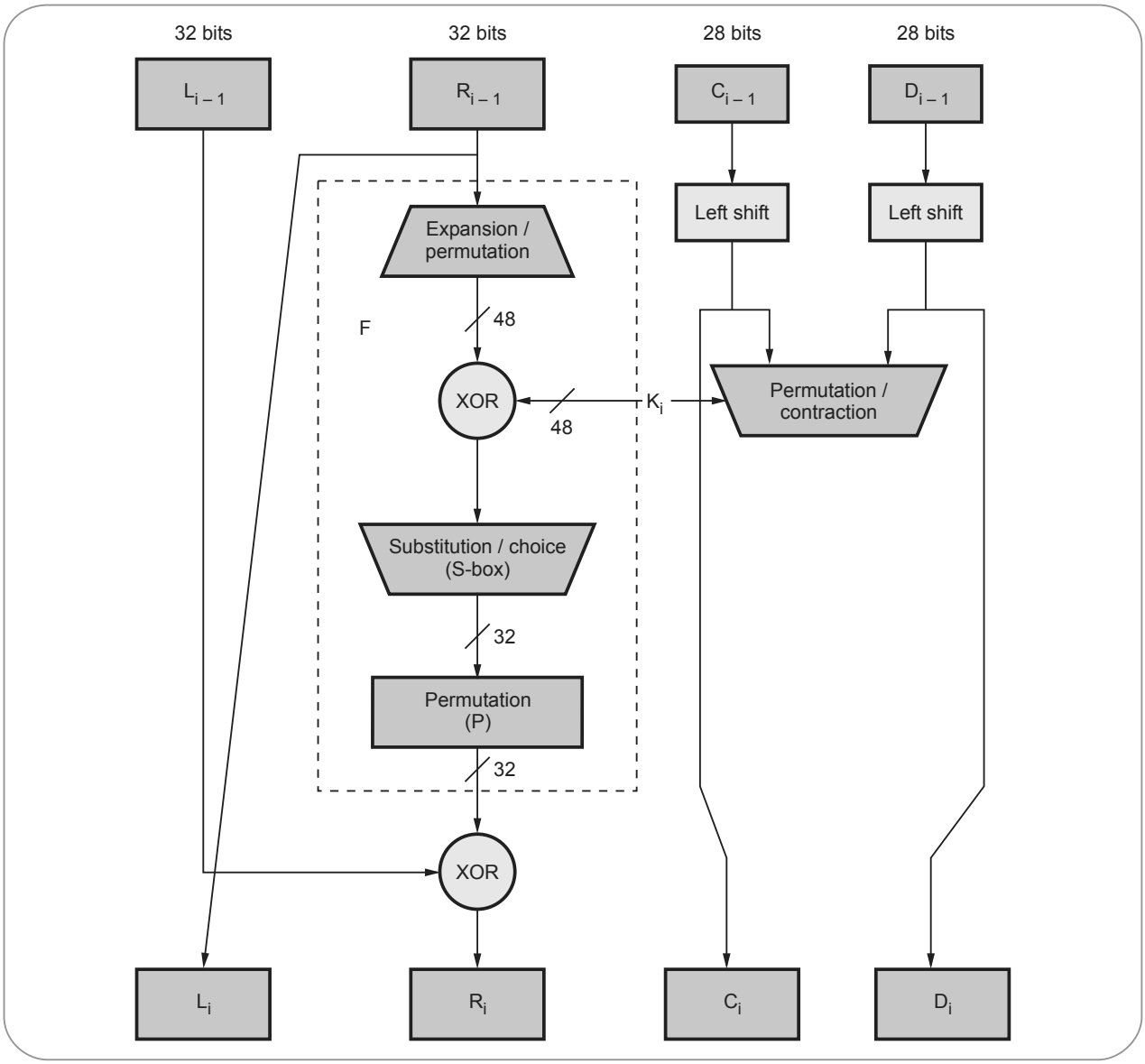


Fig. 3.7.2 Single round of DES algorithm

- First and last bits of the input to box S_i form a 2-bit binary number to select one of four substitutions defined by the four rows in the table for S_i. Two bits can store any decimal number between 0 and 3. This specifies the row number. The middle four bits select one of the sixteen columns.
- Following table gives the S-box value for DES

S_1	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

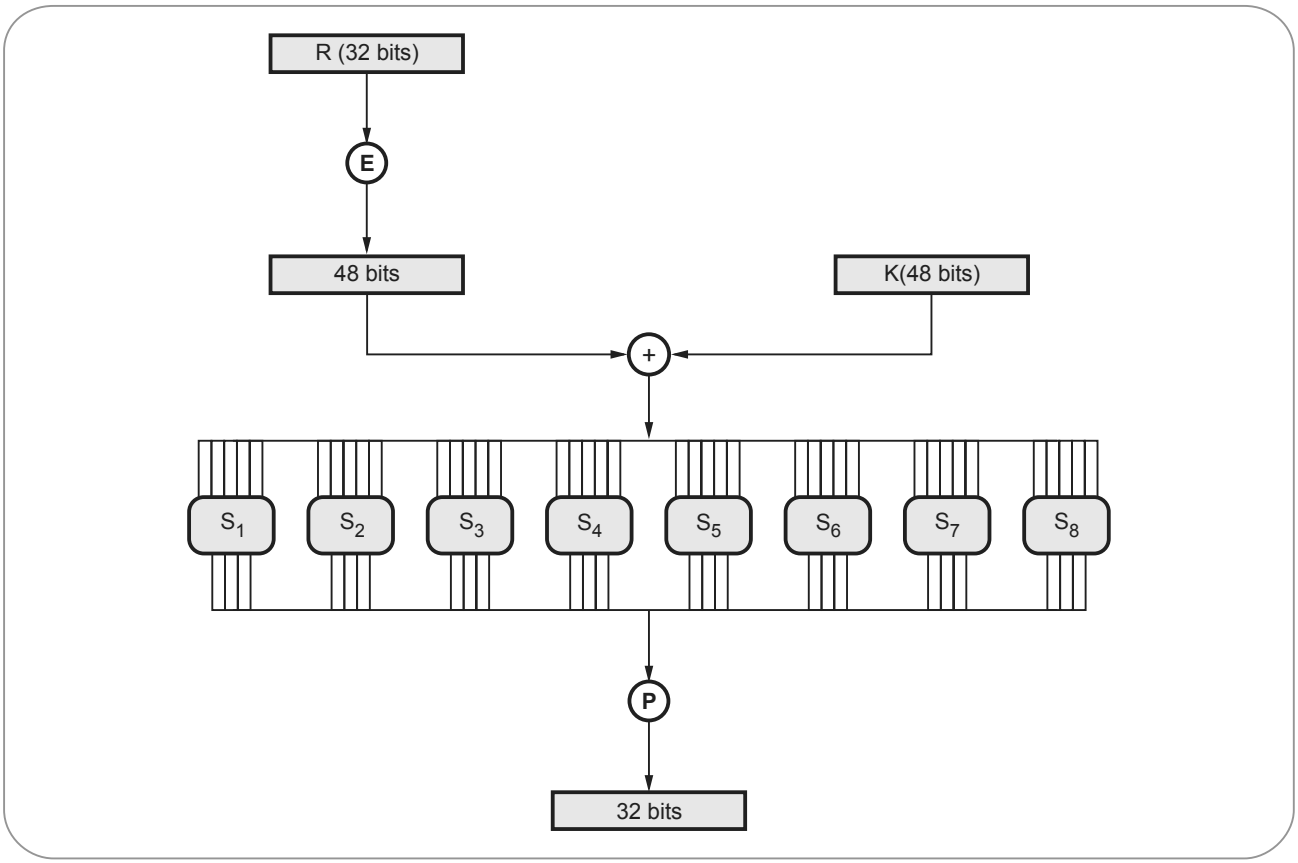


Fig. 3.7.3 S-boxes in the function (F)

S_2																
	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9

S_3																
	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
	13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
	13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12

S_4																
	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
	3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14

S_5																
	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
	11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3

S_6																
	12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
	9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
	4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13

S_7																
	4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
	13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
	1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
	6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12

S_8	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

- Fig. 3.7.4 shows the selection of an entry in a S-box based n the 6-bit input. For example, in S_2, for input 101101, the row is 11 and the column is 0110. The value in row 3, column 6 which select row 3 and column 6 of S_2 box. The output is 4.

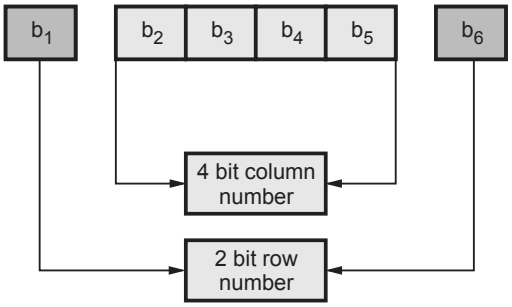


Fig. 3.7.4 Selecting entry in S-box

3.7.2 Key Generation

- 64-bit key is used as input to the algorithm. The initial 64-bit key is transformed into a 56-bit key by discarding every 8^{th} bit of the initial key.
- From 56-bit key, a different 48-bit subkey is generated during each round using a process called as key transformation.
- The resulting 56-bit key is then treated as two 28-bit quantities, labeled C_0 and D_0. At each round, C_{i-1} and D_{i-1} are separately subjected to a circular left shift, or rotation, of 1 or 2-bits.
- These shifted values serve as input to the next round. They also serve as input to Permuted choice Two, which produces a 48-bit output that serves as input to the function $F(R_{i-1}, K_i)$.

3.7.3 DES Encryption

- A block to be enciphered is subjected to an initial permutation IP, then to a complex key-dependent computation and finally to a permutation which is inverse of the initial permutation IP.
- The key-dependent computation can be simply defined in terms of a function *f*, called the cipher function, and a function KS, called the key schedule.

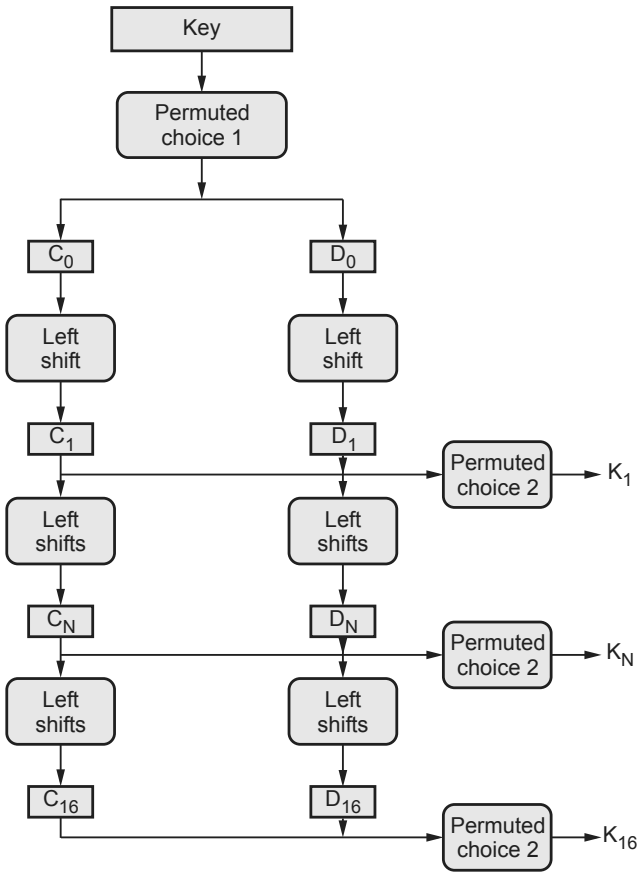


Fig. 3.7.5 Key generation techniques

- Given two blocks L and R of bits, LR denotes the block consisting of the bits of L followed by the bits of R.

1. **Initial permutation :** The 64-bits of the input block to be enciphered are first subjected to the permutation, called the initial permutation.
2. **Key dependent computation :** The computation which uses the permuted input block as its input to produce the pre-output block consists. Cipher function *f* which operates on two blocks, one of 32-bits and one of 48-bits, and produces a block of 32-bits. Let the 64 bits of the input block in an iteration consist of a 32-bit block L followed by a 32-bit block R. Using the notation defined in the introduction the input block is then LR. Let K be a block of 48 bits chosen from the 64-bit key. Then the output L' R' of an iteration with input LR is defined by :

$$\left.\begin{aligned} L' &= R \\ R' &= L \,(+)\, f(R, K) \end{aligned}\right\} \quad \ldots (3.7.1)$$

where (+) denotes bit-by-bit addition modulo 2.

As before, let the permuted input block be LR. Finally, let L_0 and R_0 be respectively L and R and let L_n and R_n be respectively L' and R' of equation (3.7.1) hence L and R are respectively L_{n-1} and R_{n-1} and K is K_n i.e. when *n* is in the range from 1 to 16,

$$\text{Then } L_n = R_{n-1}$$

$$R_n = L_{n-1} (+) f(R_{n-1}, K_n)T$$

The pre-output block is then $R_{16}L_{16}$.

3. **Key schedule :** Key generation techniques is shown in the Fig. 3.7.5 (see fig. on previous page)

The input of the first iteration of the calculation is the permuted input block. If L' R' is the output of the 16^{th} iteration then R'L' is the pre-output block. At each iteration a different block K of key bits is chosen from the 64-bit key designated by KEY. Let KS be a function which takes a integer *n* in the range from 1 to 16 and a 64-bit block KEY as input and yields as output a 48-bit block K_n which is a permuted selection of bits from KEY i.e.

$$K_n = KS(n, KEY)$$

with K_n determined by the bits in 48 distinct bit positions of KEY. KS is called the key schedule.

3.7.4 DES Decryption

- The permutation IP^{-1} applied to the pre-output block is the inverse of the initial permutation IP applied to the input. Consequently, to decipher it is only necessary to apply the very same algorithm to an enciphered message block, taking care that at each iteration of the computation the same block of key bits K is used during decipherment as was used during the encipherment of the block only in a reverse order.
- For the decipherment calculation with $R_{10}L_{10}$ as the permuted input, K_{10} is used in the first iteration, K_{10} in the second, and so on, with K, used in the 16^{th} iteration.

3.7.5 DES Weak Keys

- With many block ciphers there are some keys that should be avoided, because of reduced cipher complexity.
- These keys are such that the same sub-key is generated in more than one round, and they include :
  1. **Weak keys :** The same sub-key is generated for every round and DES has 4 weak keys.
  2. **Semi-weak keys :** Only two sub-keys are generated on alternate rounds and DES has 12 of these (in 6 pairs).
  3. **Demi-semi weak keys :** Have four sub-keys generated.
- None of these cause a problem since they are a tiny fraction of all available keys however they MUST be avoided by any key generation program.

3.7.6 Advantages of DES

1. As 56-bit keys are used there are 70 quadrillion possible key values and hence a specific key cannot be identified easily.
2. As the length of the key is increased the security provided by the algorithm also increases.
3. The security of the DES algorithm resides in the key.

3.7.7 Disadvantages of DES

1. As it is a symmetric algorithm both sender and receiver must have same key, there is a possibility that the key is intercepted.
2. The design of S boxes makes it susceptible to linear cryptanalysis attack.
3. It is susceptible to differential cryptanalysis attack and brute force attack taking advantage of which DES crackers have been designed.
4. It has certain weak keys which generate the same key for all cycles of the algorithm like when all key bits are either 0s or 1s or if one half of the key bits are 0s or 1s. They are 0000000 0000000, 0000000 ffffffff, ffffffff 0000000, ffffffff ffffffff.
5. Some initial keys produce only two subkeys while some produce only four. They are called possible weak keys.

Possible techniques for improving DES

- Multiple enciphering with DES
- Extending DES to 128-bit data paths and 112-bit keys

• Extending the key expansion calculation.

3.7.8 Block Cipher Design Principles

The criteria for the **S-boxes** are as follows :

1. No output bit of any S-box should be too close a linear function of the input bits.
2. Each row of an S-box should include all 16 possible output bit combinations.
3. If two inputs to an S-box differ in exactly one bit, the outputs must differ in at least two bits.
4. If two inputs to an S-box differ in the two middle bits exactly, the outputs must differ in at least two bits.
5. If two inputs to an S-box differ in their first two bits and are identical in their last two bits, the two outputs must not be the same.
6. For any non zero 6-bit difference betwen inputs, no more than 8 of the 32 pairs of inputs exhibiting that difference may result in the same output difference.

Criteria for **permutation P** are as follows.

1. The four output bits from each S-box at round i are distributed so that two of them affect middle bits of round (i + 1) and the other two affect end bits.
2. The four output bits from each S-box affect six different S-boxes on the next round, and no two affect the same S-box.
3. For two S-boxes j, k, if an output bit from S_j affects a middlle bits of S_{tock} on the next round, then an output bit from S_k cannot affect a middle bit of S_j.

3.7.9 Double DES

• Using two encryption stages and two keys.

A) The plain text to ciphertext is as follows,

$C = E_{K_2}(E_{K_1}(P))$ where k1 and k2 are the key.

B) Ciphertext to plain text is as follows,

$P = D_{K_1}(D_{K_2}(C))$

• Double DES suffers from Meet-in-the-Middle Attack.

• Meet-in-the-Middle Attack is as follows,

1. Assume $C = E_{K_2}(E_{K_1}(P))$
2. Given the plaintext P and ciphertext C
3. Encrypt P using all possible keys K_1
4. Decrypt C using all possible keys K_2

Fig. 3.7.6 (see fig. on next page) shows the meet-in-the-middle attack for double DES.

3.7.10 Triple DES

• Triple DES is simply another mode of DES operation. It takes three 64-bit keys, for an overall key length of 192 bits.

• The procedure for encryption is exactly the same as regular DES, but it is repeated three times. Hence the name triple DES.

• Triple DES uses 2 or 3 keys.

• The data is encrypted with the first key (K_1), decrypted with the second key (K_2), and finally encrypted again with the third key (K_3).

• Triple DES with three keys is used quite extensively in many products including PGP and S/MIME.

• Brute force search impossible on Triple DES.

• Meet-in-middle attacks need 256 Plaintext-Ciphertext pairs per key.

• Cipher text is produced as $C = E_{K_3}[D_{K_2}[E_{K_1}[P]]]$.

• Fig. 3.7.7 shows the 3DES method with three key.

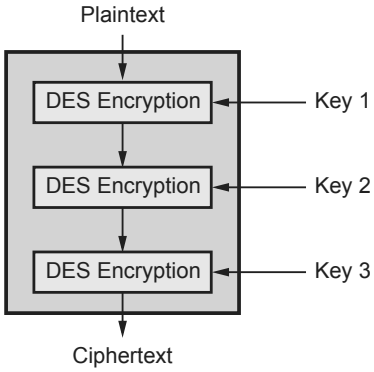


Fig. 3.7.7 3DES with three key method

• Triple DES runs three times slower than standard DES, but is much more secure if used properly.

• The procedure for decrypting something is the same as the procedure for encryption, except it is executed in reverse.

• Like DES, data is encrypted and decrypted in 64-bit chunks.

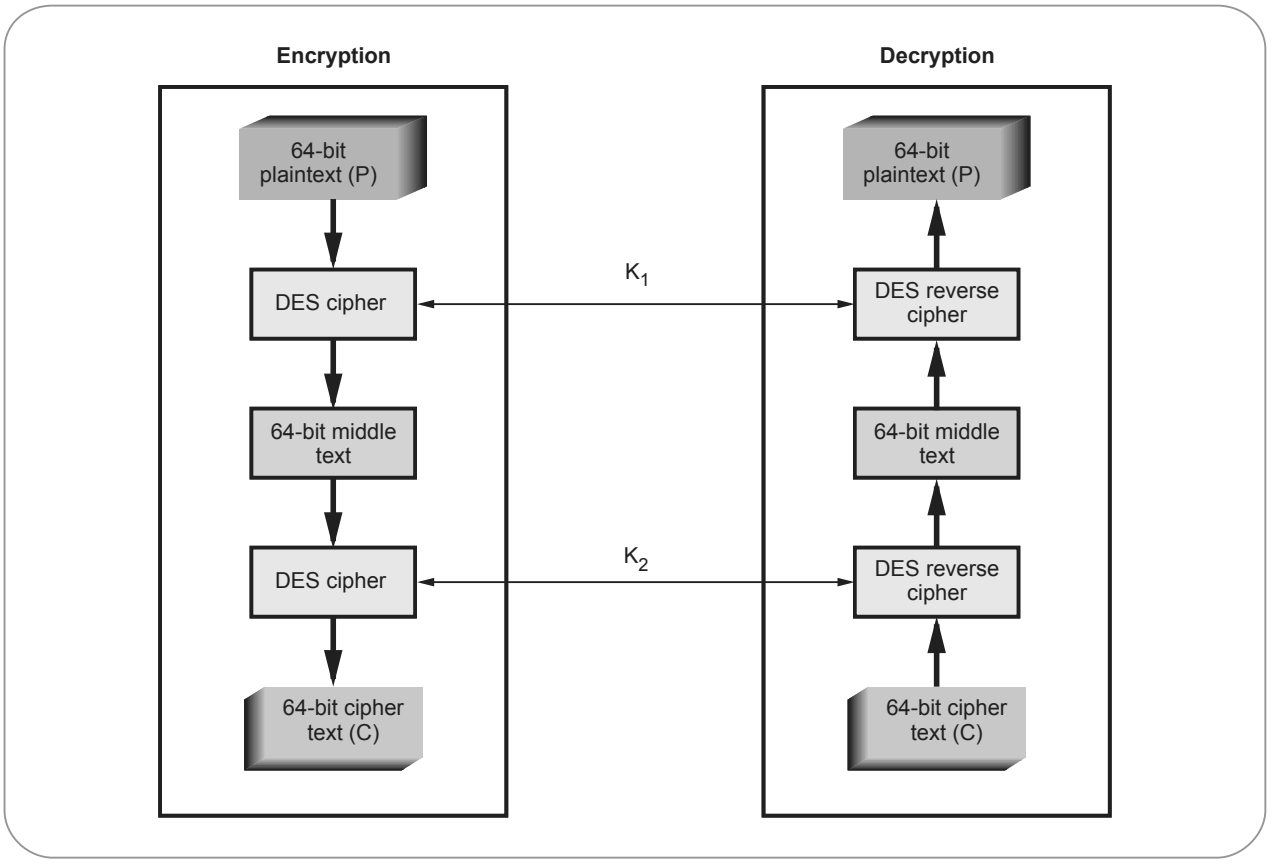


Fig. 3.7.6 Meet-in-the-middle attack for double DES

- There are some weak keys that one should be aware of : If all three keys, the first and second keys, or the second and third keys are the same, then the encryption procedure is essentially the same as standard DES. This situation is to be avoided because it is the same as using a really slow version of regular DES.
- The input key for DES is 64-bits long; the actual key used by DES is only 56-bits in length.
- The least significant (right-most) bit in each byte is a parity bit, and should be set so that there are always an odd number of 1s in every byte.
- These parity bits are ignored, so only the seven most significant bits of each byte are used, resulting in a key length of 56-bits.
- This means that the effective key strength for Triple DES is actually 168-bits because each of the three keys contains 8 parity bits that are not used during the encryption process.

Board Questions

1. *Describe DES Algorithm with suitable diagram.*
   MSBTE : Summer-17, Marks 8
2. *What is DES algorithm ? Explain each step in detail with help of diagram.*
   MSBTE : Winter-18, Marks 8

3.8 Linear and Difference Cryptanalysis

- Instead of looking for isolated points at which a block cipher behaves like something simpler, it involves trying to create a simpler approximation to the block cipher as a whole. It is an attack that can be applied to an iterated cipher.
- We want to find a probability linear relationship between a subset of plaintext bits and a subset of data bits preceding the last round. This relation behaves in a non-random fashion.
- The attacker has a lot of plaintext-chiphertext pairs known plaintext attack.
- For each candidate subkey, we partially decrypt the cipher and check if the relation holds. If the relation

holds then increment its corresponding counter. At the end, the candidate key that counts furthest form 1/2 is the most likely subkey.

- The attack has no practical implication, requires too many pairs. The key size remains the main attack point.

3.8.1 Difference Cryptanalysis

- The main difference from linear attack is that differential attack involves comparing the XOR of two inputs to the XOR of the corresponding outputs.
- Differential attack is a **choosen-plaintext attack.**
- This is a chosen plaintext attack, assumes than an attacker knows (plaintext, ciphertext) pairs.
- Difference $\Delta_P = P_1 \oplus P_2$, $\Delta_C = C_1 \oplus C_2$
- Distribution of Δ_C's given Δ_P may reveal information about the key (certain key bits).
- After finding several bits, use brute-force for the rest of the bits to find the key.
- Surprisingly ... DES was resistant to differential cryptanalysis.
- At the time DES was designed, the authors knew about differential cryptanalysis. S-boxes were designed to resist differential cryptanalysis.
- Against 8-round DES, attack requires 2^{38} known plaintext-ciphertext pairs.
- Against 16-round DES, attack required 2^{47} chosen plaintexts.
- Differential cryptanalysis not effective against DES !!!

3.8.2 Difference between Differential and Linear Cryptanalysis

- Important distinction between the two methods is that differential cryptanalysis works with blocks of bits while linear cryptanalysis typically works with a single bit. The bias of the linear approximation has a sign. Thus given two approximations with the same input and output masks and equal probability but opposite signs, the resulting approximation will have zero bias, due to the cancellation of the two approximations by each other. Linear cryptanalysis is a known plaintext attack in which the attacker studies the linear approximations of parity bits of the plaintext, cipher text and the secrete key.
- Differential cryptanalysis is a general form of cryptanalysis applicable primarily to block ciphers, but also to stream ciphers and cryptographic hash functions. Linear cryptanalysis is a general form of cryptanalysis based on finding affine approximations to the action of a cipher.
- Attacks have been developed for block ciphers and stream ciphers. Linear cryptanalysis is one of the two most widely used attacks on block ciphers. Differential cryptanalysis is usually a chosen plaintext attack, meaning that the attacker must be able to obtain encrypted cipher-texts for some set of plaintexts of his choosing.

3.9 Asymmetric Key Cryptography

- Diffie and Hellman proposed a new type of cryptography that distinguished between encryption and decryption keys. One of the keys would be publicly known; the other would be kept private by its owner.
- These algorithms have the following important **characteristic.**
  1. It must be computationally easy to encipher or decipher a message given the appropriate key.
  2. It must be computationally infeasible to derive the private key from the public key.
  3. It must be computationally infeasible to determine the private key from a chosen plaintext attack.
- A public key encryption scheme has six ingredients. Fig. 3.9.1 shows public key cryptography.

(See Fig. 3.9.1 on next page)

1. **Plaintext :** It is input to algorithm and in a readable message or data.
2. **Encryption algorithm :** It performs various transformations on the plaintext.
3. **Public and private keys :** One key is used for encryption and other is used for decryption.
4. **Ciphertext :** This is the scrambled message produced as output. It depends on the plaintext and the key.

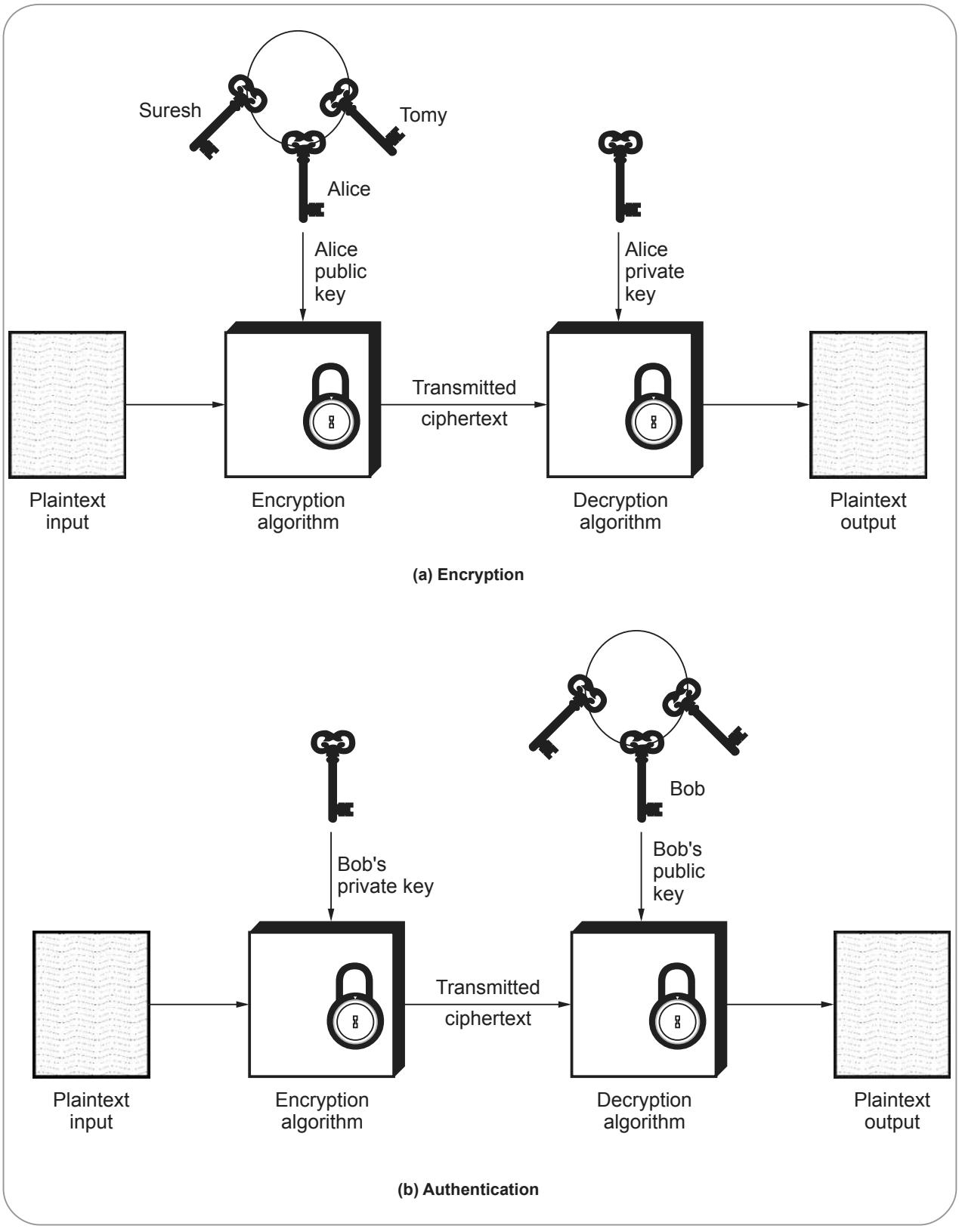


Fig. 3.9.1 Public key cryptography

5. **Decryption algorithm :** This algorithm accepts the ciphertext and the matching key and produces the original plaintext.

- The essential steps are the following :

1. Each user generates a pair of keys to be used for the encryption and decryption of messages.
2. Each user places one of the two keys in a public register. This is the public key. The companion key is kept private.
3. If Bob wishes to send a confidential message to Alice, Bob encrypts the message using Alice's public key.
4. Alice decrypts the message using her private key.

- The public key is accessed to all participants and private key is generated locally by each participant.
- System controls its private key. At any time, a system can change its private key. Fig. 3.9.2 (refer fig. on 3-28 page no) shows the process of public key algorithm.
- A message from source which is in a plaintext, $X = (X_1, X_2, \ldots X_m)$. The message is intended for destination which generates a related pair of keys a public key KU_b, and a private key KR_b.
- Private key is secret key and known only to Y_1. With the message X and encryption key KU_b as input, X_1 forms the ciphertext.

$$Y = (Y_1, Y_2, Y_3 \ldots . Y_n)$$

$$Y = E_{KU_b}(X)$$

- The intended receiver, in possession of the matching private key is able to invert the transformation.

$$X = D_{KR_b}(Y)$$

- An opponent, observing Y and having access to public key (KU_b), but not having access to private key (KR_b), must attempt to recover X. It is assumed that the opponent does have knowledge of the encryption (E) and decryption algorithms (D).
- Public key cryptography requires each user to have two keys : A public key used by anyone for encrypting messages to be sent to that user and a private key, which the user needs for decrypting messages.

Requirements for public key cryptography

1. It is computationally easy for a party B to generate a pair.
2. It is computationally easy for a sender A, to generate the corresponding ciphertext :

$$C = E(PU_b, M)$$

3. It is computationally easy for the receiver B to decrypt the resulting ciphertext using the private key to recover the original message :

$$M = D(PR_b, C) = D[PR_b, E(PU_b, M)]$$

4. It is computationally infeasible for an adversary, knowing the public key (PU_b) to determine the private key PR_b.

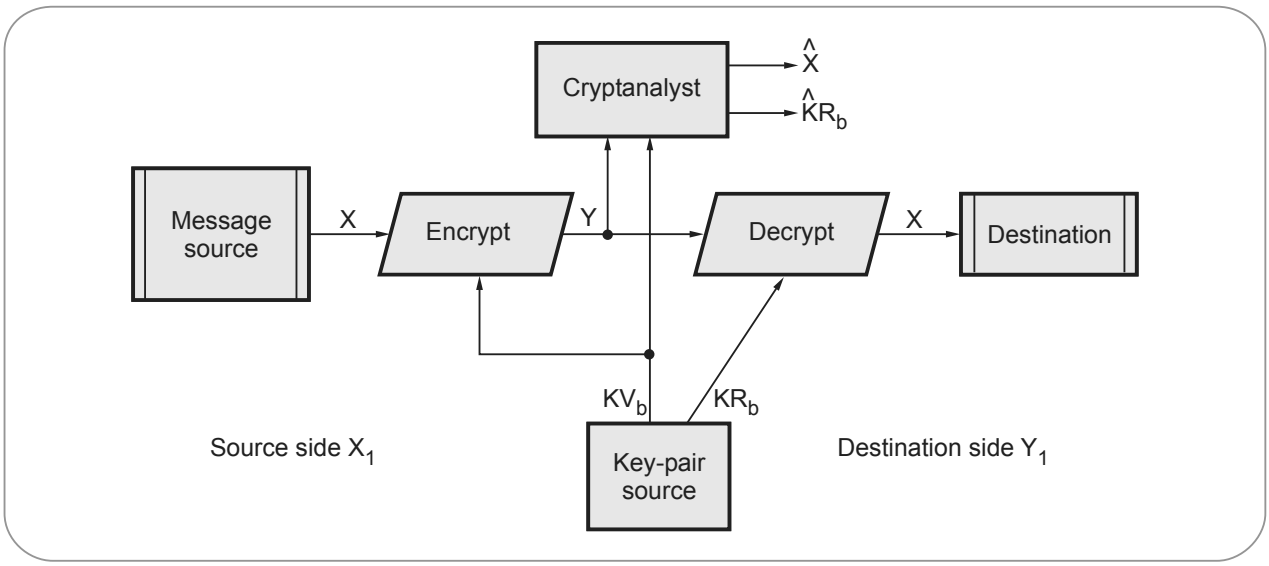


Fig. 3.9.2 Public key cryptosystem secrecy

5. It is computationally infeasible for an adversary, knowing the public key (PU_b) and a ciphertext (C) to recover the original message (M).

3.9.1 Advantages and Disadvantages

- **Advantages of public key algorithm**
  1. Only the private key must be kept secret.
  2. The administration of keys on a network requires the presence of only a functional trusted TTP as opposed to an unconditionally trusted TTP.
  3. A private/public key pair remains unchanged for considerable long periods of time.
  4. There are many relatively efficient digital signature mechanisms as a result of asymmetric-key schemes.
  5. In a large network the number of keys necessary may be considerably smaller than in the symmetric-key scenario.
- **Disadvantages of public key algorithm**
  1. Slower throughput rates than the best known symmetric-key schemes.
  2. Large key size.
  3. No asymmetric-key scheme has been proven to be secure.
  4. Lack of extensive history.

3.9.2 Comparison between Public Key and Private Key Algorithm

Sr. No.	Symmetric key cryptography	Asymmetric key cryptography
1.	Same key is used for encryption and decryption.	One key for encryption and other key for decryption.
2.	Very fast.	Slower.
3.	Key exchange is big problem.	Key exchange is not a problem.
4.	Also called **secret key** encryption.	Also called **public key** encryption.
5.	The key must be kept secret.	One of the two keys must be kept secret.
6.	The sender and receiver must share the algorithm and the key.	The sender and receiver must each have one of the matched pair of keys.
7.	Size of the resulting encrypted text is usually same as or less than the original clear text size.	Size of the resulting encrypted text is more than the original clear text size.
8.	Cannot be used for digital signatures.	Can be used for digital signature.

Board Questions

1. *Compare symmetric and asymmetric key crytography* **MSBTE : Winter-15, Marks 4**
2. *Distinguish between symmetric and asymmetric key cryphotography.* **MSBTE : Summer-16, Marks 4**
3. *Distinguish between symmetric and asymmetric cryptography (any 4 points).* **MSBTE : Winter16, Marks 4**
4. *Describe symmetric and asymmetric key cryptography.* **MSBTE : Summer-17, Marks 4**
5. *Compare symmetric and asymmetric key cryptography.* **MSBTE : Winter-17, Marks 3**

3.10 Digital Signature

- A digital signature is an authentication mechanism that enables the creator of a message to attach a code that acts as a signature. The signature is formed by taking the hash of the message and encrypting the message with the creator's private key.

Requirements

- Message authentication protects two parties who exchange messages from any third party. However, it does not protect the two parties against each other.
- In situations where there is not complete trust between sender and receiver, something more than authentication is needed. The most attractive solution to this problem is the digital signature. The digital signature is analogous to the handwritten signature.

- It must have the following properties
  1. It must verify the author and the date and time of the signature.
  2. It must to authenticate the contents at the time of the signature.
  3. It must be verifiable by third parties, to resolve disputes.
- The digital signature function includes the authentication function. On the basis of these properties, we can formulate the following requirements for a digital signature.
- Must be a bit pattern depending on the message being signed.
- Signature must use some information unique to the sender to prevent forgery and denial.
- Computationally easy to produce a signature.
- Computationally easy to recognize and verify the signature.
- Computationally infeasible to forge a digital signature.
  a) either by constructing a new message for an existing digital signature.
  b) or by constructing a fraudulent digital signature for given message.
- Practical to retain a copy of the digital signature in storage

Two general schemes for digital signatures

1) Direct 2) Arbitrated

3.10.1 Arbitrated Digital Signatures

Every signed message from A to B goes to an arbiter BB (Big Brother) that everybody trusts.

- BB checks the signature and the timestamp, origin, content, etc.
- BB dates the message and sends it to B with an indication that it has been verified and it is legitimate.

e.g. Every user shares a secret key with the arbiter

- A sends to BB in an encrypted form the plaintext P together with B's id, a timestamp and a random number RA.
- BB decrypts the message and thus makes sure it comes from A; it also checks the timestamp to protect against replays.
- BB then sends B the message P, A's id, the timestamp and the random number RA; he also sends a message encrypted with his own private key (that nobody knows) containing A's id, timestamp t and the plaintext P (or a hash).
- B cannot check the signature but trusts it because it comes from BB-he knows that because the entire communication was encrypted with KB.
- B will not accept the messages or messages containing the same RA to protect against replay.
- In case of dispute, B will show the signature he got from BB (only B may have produced it) and BB will decrypt it.

3.10.2 Direct Digital Signature

- This involves only the communicating parties and it is based on public keys.
- The sender knows the public key of the receiver.
- Digital signature : encrypt the entire message (or just a hash code of the message) with the sender's private key.
- If confidentiality is required : apply the receiver's public key or encrypt using a shared secret key.
- In case of a dispute the receiver B will produce the plaintext P and the signature E(KRA, P) - the judge will apply KUA and decrypt P and check the match : B does not know KRA and cannot have produced the signature himself.

Weaknesses

- The scheme only works as long as KRA remains secret : If it is disclosed (or A discloses it herself), then the argument of the judge does not hold : anybody can produce the signature.
- **Attack :** To deny the signature right after signing, simply claim that the private key has been lost-similar to claims of credit card misuse.

  i.e. If A changes her public-private keys (she can do that often) the judge will apply the wrong public key to check the signature.

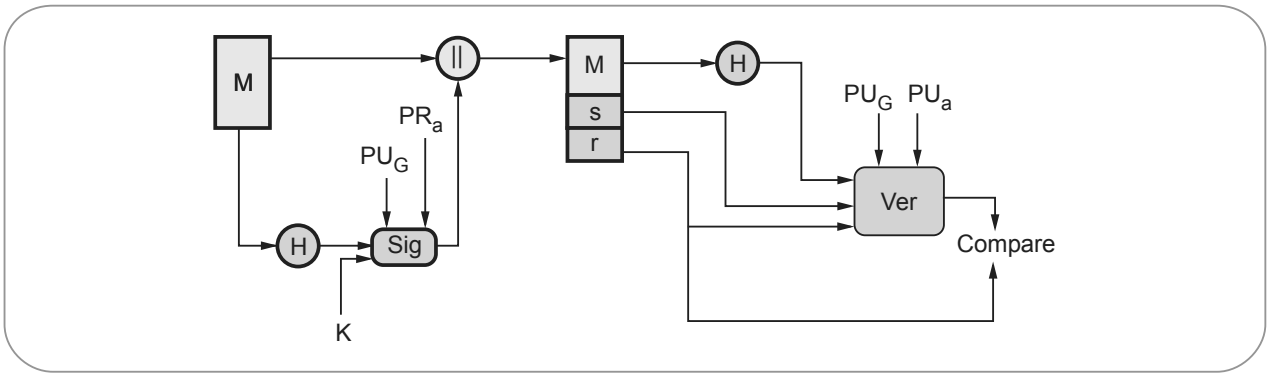


Fig. 3.10.1 DSS approach

- **Attack :** To deny the signature change your public-private key pair-this should not work if a PKI is used because they may keep trace of old public keys.

  i.e. A should protect her private key even after she changes the key.
- **Attack :** Eve could get hold of an old private key and sign a document with an old timestamp.

3.10.3 Digital Signature Standard

- The Digital Signature Standard (DSS) makes use of the Secure Hash Algorithm (SHA) and presents a new digital signature technique, the Digital Signature Algorithm (DSA). DSS cannot be used for encryption or key exchange. Fig. 3.10.1 shows the DSS approach.
- It uses a hash function. The hash code is provided as input to a signature function along with a random number K generated for this particular signature.
- The signature function also depends on the sender's private key (PR$_a$) and a set of parameters known to a group of communicating principles.
- The result is a signature consisting of two components, labeled s and r.
- At the receiving end, the hash code of the incoming message is generated. This plus the signature is input to a verification function.
- Fig. 3.10.2 shows the RSA approach. In the RSA approach, the message to be signed is input to a hash function that producs a secure hash code of fixed length. This hash code is then encrypted using the sender's private key to form the signature. Both the message and the signature are then transmitted.
- The recipient takes the message and produces a hash code. The recipient also decrypts the signature using the sender's public key. If the calculated hash code matches the decrypted signature, the signature is accepted as valid.

3.10.4 Digital Signature Algorithm

- There are three parameters that are public and can be common to a group of users. **Prime number q** is chosen and it is **160-bit**. A **prime number p** is selected with a length between **512** and **1024 bits** such that q divides (P – 1).

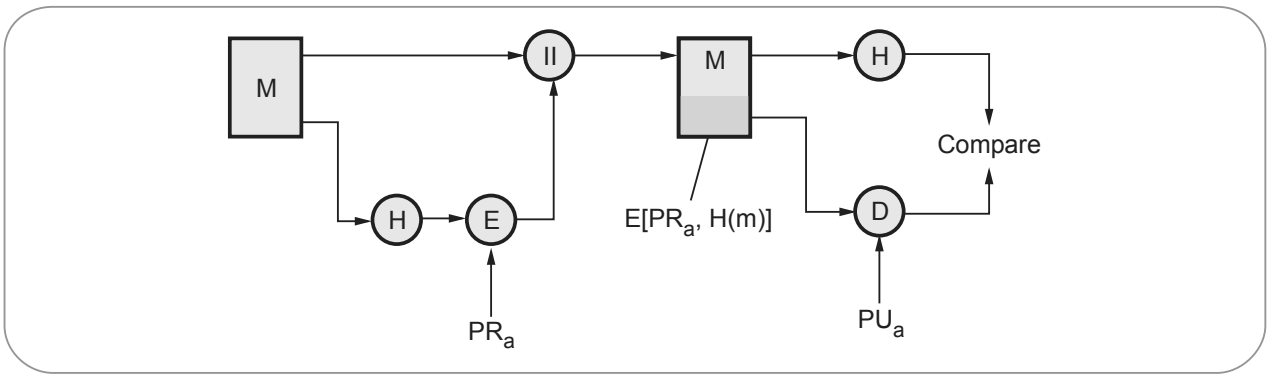


Fig. 3.10.2 RSA approach

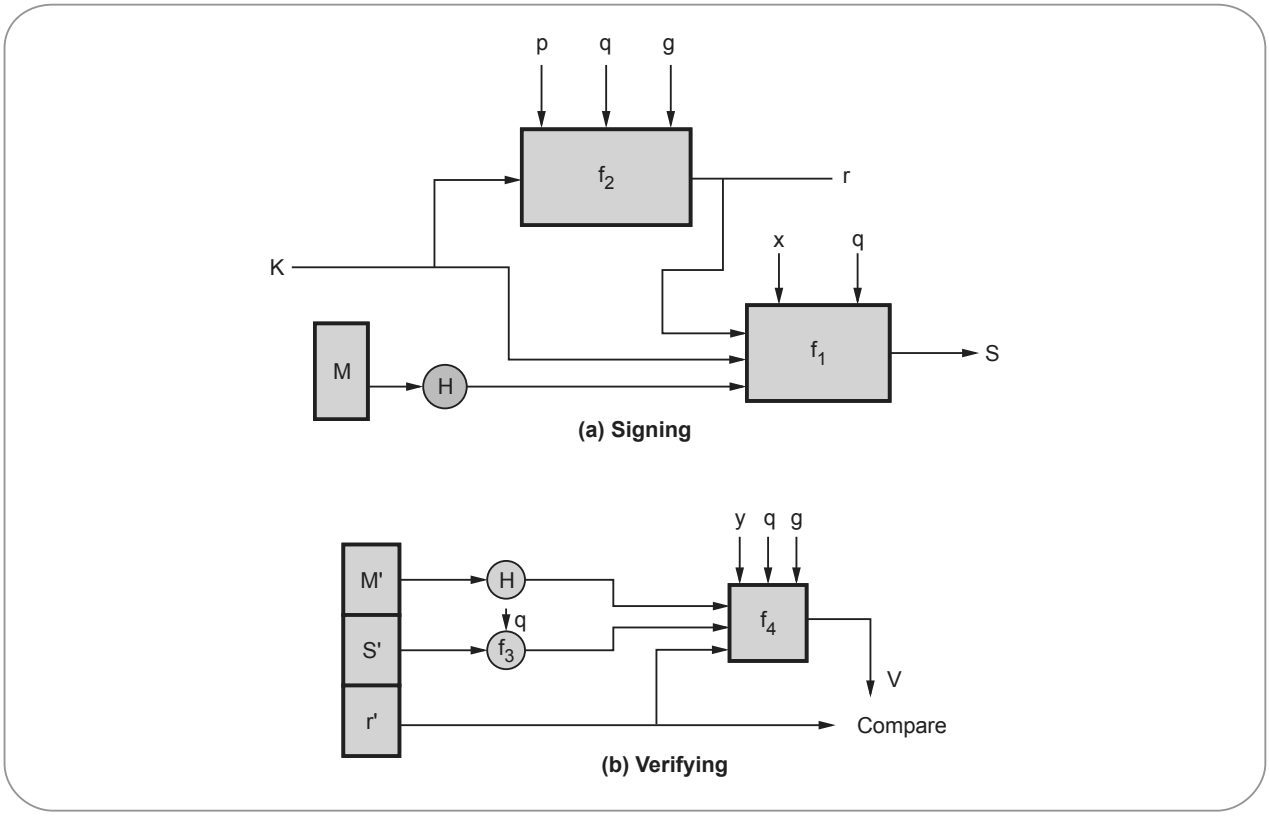


Fig. 3.10.3 Signing and verifying

- g is chosen to be of the form $h^{(P-1)/q}$ mod p where h is an integer between 1 and (P – 1)
- With these number, user selects a private key and generate a public key. The private key x must be a number from 1 to (q – 1) and should be chosen randomly or pseudorandomly.
- The public key is calculated from the private key as $y = g^x$ mod p.
- To create a signature, a user calculates two quantities, **rands**, that are functions of

  i) Public key components (p, q, g)

  ii) User's private key (x)

  iii) Hash code of the message H(M)

  iv) An additional integer (K)
- **At the receiving end**, verification is performed. The receiver generates a quantity V that is a function of the public key components, the sender's public key and the hash code of the incoming message. If this quantity matches the r components of the signature, then the signature is validated.
- Fig. 3.10.3 shows the functions of signing and verifying.

Board Question

1. *Describe digital signature mechanism with neat diagram.* **MSBTE : Summer-18, Winter-18, Marks 8**

❑❑❑

Notes

UNIT - IV

4 Firewall and Intrusion Detection System

4.1 Firewall : Need and Types of Firewall

4.1.1 Functions & Need of Firewall

1. **Access control -** Firewall filters incoming and outgoing packets.
2. **Address/Port translation -** National Address Translation (NAT) can establish a connection with external machines on internet. This is often done by firewalls.
3. **Logging -** The firewall can log all anomalous packets which are useful for analyzing intrusion, worms, DDoS attacks.
4. **Authentication -** Firewalls perform authentication of external machines attempting to establish connection with machine.

4.1.1.1 Policies and Access Control Lists

- Access control is an important tool of security to protect data and other resources.
- High level policies are translated into a set of rules that comprise an access control list.
- The policies can be permissive or restrictive. The access control mechanism refers to prevention of unauthorized use of a resource.
- **Permissive policies** are based on permitting all packets except those that are explicitly forbidden.
- **Restrictive policies** are based on dropping all packets except those that are explicitly permitted.

4.1.1.2 ACLs and Capabilities Lists

- Access control List (ACL) is a set of rules that define security policy. These ACLs contain one or more access control entries (ACEs), which are the actual rule definitions themselves.
- These rules can restrict access by specific user, time of day, IP address, function (department, management level, etc.), or specific system from which a logon or access attempt is being made.

4.1.2 Firewalls

- Information systems in an organization have changed vary rapidly over the years from centralized data processing, LANs, WANs and Internet connectivity.
- The Internet connectivity is essential for the organization enabling access to outside world. Also it is a threat to the organization if not secured from intrusions (unauthorized access/users).
- A firewall is inserted between the Internet and LAN for security purpose. The firewall protects the LAN from Internet-based attacks and also provides security and audits.
- A firewall may be a hardware or a software program running on a secure host computer. A firewall is placed at junction or gateway between the two networks.
- A firewall must have at least two network interfaces one for the network it is intended to protect and one for the network and other for the network it is exposed to. A firewall placed between a private or corporate network and a public network (Internet) is shown in Fig. 4.1.1.
- The term firewall comes from the fact that by segmenting a network into different physical subnetwork, they limit the damage that could spread from one subnet to other just like firedoors or firewalls.

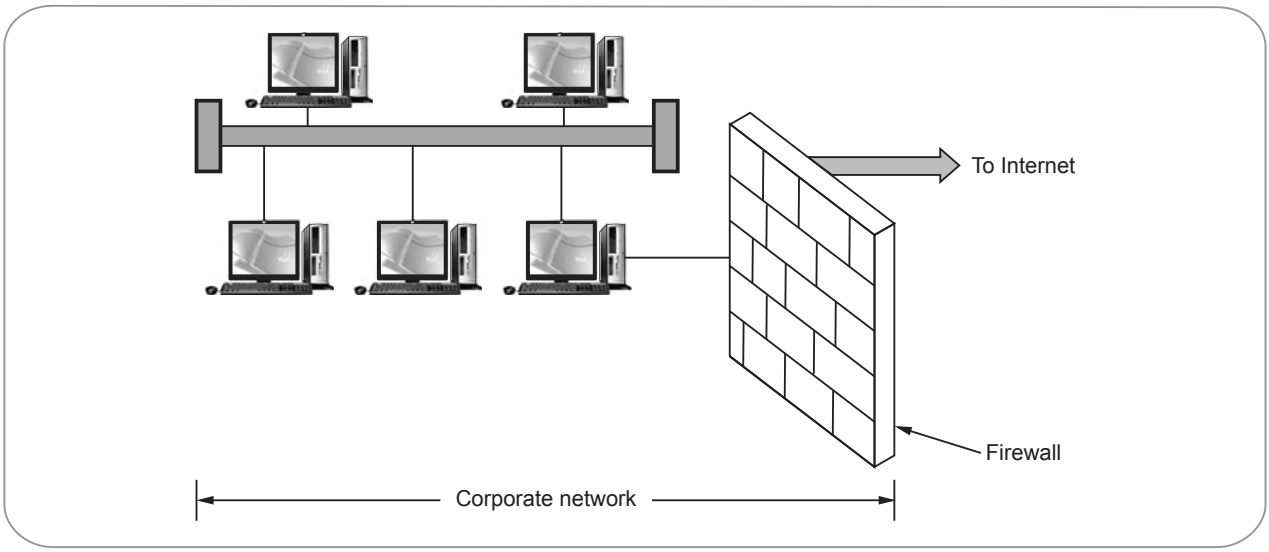


Fig. 4.1.1 Firewall

Capabilites of firewall

- A firewall examines all traffic routed between the two networks to see if it meets the certain criteria. If it does, it is routed between the networks, otherwise it is stopped.
- A firewall filters both inbound and outbound traffic. It can also manage public access to private networked resources such as host applications. It can be used to log all attempts to enter the private network and trigger alarms when hostile or unauthorized entry is attempted.
- Firewalls can filter packets based on their source and destination addresses and port numbers. This known as **address filtering**.
- Firewalls can also filter specific types of network called **protocol filtering** because the decision to forward or reject traffic is dependent upon the protocol used. For example, HTTP, FTP, Telnet.
- Firewalls can also filter traffic by packet attribute or state.

Limitations of firewall

- A firewall cannot prevent individual users with modems from dialing into or out of the network, by passing the firewall altogether.
- Employee misconduct or carelessness cannot be controlled by firewalls.
- Policies involving the use and misuse of passwords and user accounts must be strictly enforced. These are management issues that should be raised during the planning of any security policy but that cannot be solved with firewalls alone.

Firewall technology

- Firewall technology generally falls into one of the two categories. Network level and application level.

1. Network level

This guards the entire network from unauthorised intrusion. An example of this technology is packet filtering, which simply reviews all information coming into a network and rejects the data that does not meet a predefined set of criteria.

2. Application level

This technology controls access on an application by application basis. For example, proxy servers can be set up to permit access to some application, such as HTTP, while blocking access to others, such as FTP.

Design goals

- Firewalls are very effective means for network based security threats. The design goals for firewall are as under

1. All the traffic must pass through firewall both from inside to outside and outside to inside.

2. Only authorized traffic defined by local security is allowed to pass.
3. Firewall itself is immune to penetration.

- Generally four techniques are used to control access and enforce the security policy, these techniques are -

1. Service control
2. Direction control
3. User control
4. Behavior control.

1. Service control

- Service control determines the types of Internet services that are allowed to access both inbound and outbound traffic.
- The firewall may filter the traffic on the basis of IP address and TCP port number. The firewall provide proxy software to receive and interpret each service request before passing it on.

2. Direction control

- Direction control determines the direction in which particular service requests may be initiated and is allowed to flow through the firewall.

3. User control

- User control gives access to a service according to which user is attempting to access it. This feature is usually applied for local user inside the firewall perimeter.

4. Behavior control

- Behavior control allows to control the use of any particular service. For example, the firewall may filter e-mails to eliminate spam.

4.1.3 Types of Firewall

- Commonly used firewalls from threats of security are

1. Packet filtering router
2. Application level gateways
3. Circuit level gateways.

4.1.3.1 Packet Filtering Router

- Packet filtering firewalls work at the network level of the OSI model, or the IP layer of TCP/IP. They are usually part of a router. A router is a device that receives packets from one network and forwards them to another network.
- In a packet filtering firewall each packet is compared to a set of criteria before it is forwarded. Depending on the packet and the criteria, the firewall can drop the packet, forward it or send a message to the originator. Rules can include source and destination IP address, source and destination port number and protocol used.
- The advantage of packet filtering firewalls is their low cost and low impact on network performance. Most routers support packet filtering. Even if other firewalls are used, implementing packet filtering at the router level affords an initial degree of security at a low network layer. This type of firewall only works at the network layer however and does not support sophisticated rule based models. Network Address Translation (NAT) routers offer the advantages of packet filtering firewalls but can also hide the IP addresses of computers behind the firewall, and offer a level of circuit based filtering.
- Packet filtering router applies rule to each incoming and outgoing IP packet, according forward or discards it. Fig. 4.1.2 shows packet filtering router.

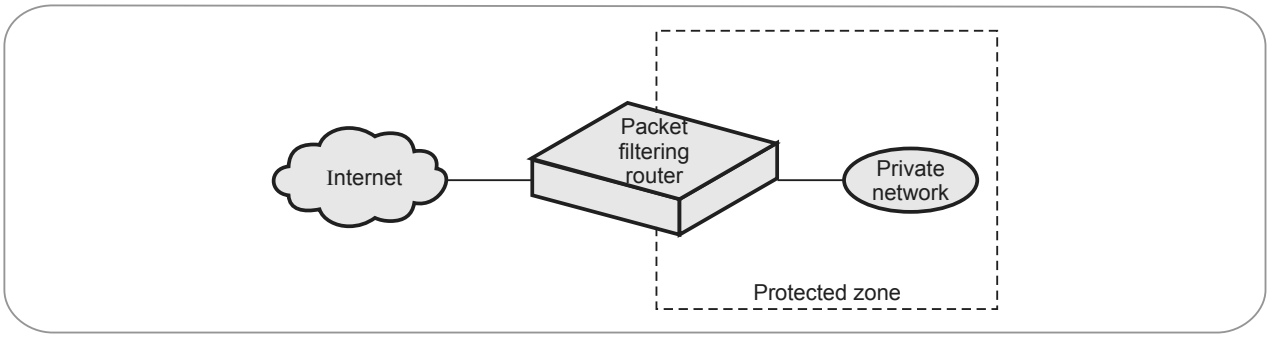


Fig. 4.1.2 Packet filtering router

- Filtering rules are based on information contained in the network packet such as
  i. Source IP address
  ii. Destination IP address
  iii. Source and destination transport level address.
  iv. IP field.
  v. Interface
- Attackers can try and break the security of the packet filter by using following techniques.
  i. IP address spoofing
  ii. Source routing attacks
  iii. Tiny fragment attacks
- Packet filtering provides a useful level of security at low cost. The type of router used in packet filtering is a screening router.

Screening router

- Each packet has two parts : The data that is part of the document and a header. If the packet is an envelope, then the data is the letter inside the envelope and the header is the address information on the outside.
- Here packet filter to refer to the technology or the process that is taking place and the screening router to refer to the thing that's doing it.
- Screening router can be a commercial router or a host-based router with some kind of packet filtering capability. Typical screening routers have the ability to block traffic between networks or specific hosts, on an IP port level. Some firewalls consist of nothing more than a screening router between a private network and the Internet.
- Screening routers operate by comparing the header information with a table of rules set by the network administrator to determine whether or not to send the packet on to its destination. If there is a rule that does not allow the packet to be sent on, the router simply discards it.

Working of packet filters

- Packet filters work by dropping packets based on their source and destination addresses or ports. Configuring a packet filter is a three step process. First of course, one must know what should and what should not be permitted. Next, the allowable types of packets must be specified, in terms of lofical expression on packet fileds. Finally the expression should be rewritten in whatever syntax your vendor supports.
- In general, for each packet, the router applies the rules sequentially, starting with the first one, until the packet fits or until it runs out of rules.
- For examples a router has 3 rules in its table.
- **Rule 1 :** Don't allow packets from a particular host, called TROUBLEHOST.
- **Rule 2 :** Let in connections into out mail gateway (using SMTP), located at port 25 on out host.
- **Rule 3 :** Block everything else.
- When a packet arrives at the screening router, the process works like this
  1. The packet filter extracts the information it needs from the packet header. In this example, it uses the local and external host identification and the local and external port numbers.
  2. The packet filter compares that information with the rules in the table.
  3. If the packet is from TROUBLEHOST, no matter what its destination, discard it.
  4. If the packet makes it past the first rule i.e. it's not from TROUBLEHOST, check to see if it's intended for port 25 on out SMTP-Mail host. If it is, send it on ; otherwise, discard it.
  5. If neither of the first two rules apply, the packet is rejected by rule three.
- Every packet has a set of headers containing certain information. The information is
  a) IP source address.
  b) IP destination address.
  c) Protocol (whether the packet is a TCP, UDP or ICMP packet).
  d) TCP or UDP source port.
  e) TCP or UDP destination port.
  f) TCP ack flag.

1. Inspection module

- If the header information listed above doesn't give you enough elements for setting up rules, you can

use a packet filter that has an inspection module. An inspection module looks at more of the header information ; some can even look at the application data itself.

- For example, by inspecting the application data, the module can deny packets the contain certain application commands, such as the FTP put command or the SNMP set command.

2. State evaluation

- The header of a TCP packet contains an indicator called the ACK flag. When the ACK flag is set, it means that the incoming packet is a response to an earlier outgoing packet.
- If the flag is not set, the packet is not a response to an earlier outgoing packet, and therefore is suspect.
- It's common to set a screen rule to allow incoming packets that have the ACK flag set and reject those that don't.
- UDP doesn't use an ACK flag or any other similar indicator, so there's no way for the screening router to know whether an incoming packet was sent in response to an outgoing packet. The only safe thing to do in that situation is to reject the packet.
- That's where state evaluation comes in a screening router that has the state evaluation capability, "remembers" the original outgoing packet for a certain length of time (set by system administrator).

Advantages of packet filters

1. Low impact on network performance.
2. Packet filters are normally transparent to user.
3. Relatively inexpensive price.

Disadvantages of packet filtering firewall

1. They are vulnerable to attacks aimed at protocol higher than the network layer protocol.
2. They cannot hide the network topology.
3. Packet filtering firewall can not support all Internet applications.
4. These firewalls have very limited auditing capabilities.
5. Sometimes user level authentication do not supported by packet filtering firewall.

4.1.3.2 Application Level Gateways

- Application level gateways, also called proxies, are similar to circuit level gateways except that they are application specific. They can filter packets at the application layer of the OSI model.
- Incoming or outgoing packets cannot access services for which there is no proxy.
- In plain terms, an application level gateway that is configured to be a web proxy will not allow any FTP, gopher, Telnet or other traffic through.
- Because they examine packets at application layer, they can filter application specific commands such as http:post and get, etc. This cannot be accomplished with either packet filtering firewalls or circuit level neither of which know anything about the application level information.
- Application level gateways can also be used to log user activity and logins. They offer a high level of security, but have a significant impact on network performance. This is because of context switches that slow down network access dramatically. They are not transparent to end users and require manual configuration of each client computer. Fig. 4.1.3 shows application level gateway.

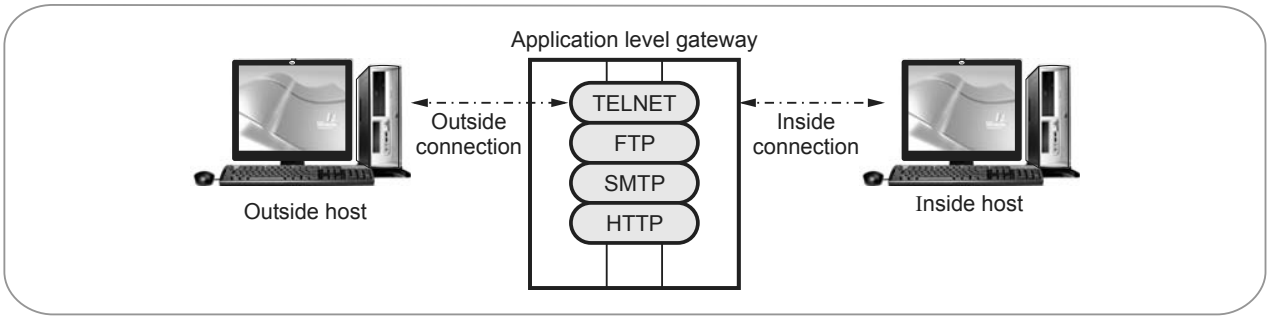


Fig. 4.1.3 Application gateway

Advantages

1. Application gateway provides high level of security than packet filters.
2. Easy to configure.
3. They can hide the private network topology.
4. It support user level authentication.
5. Capability to examine the all traffic in detail.

Disadvantages

1. High impact on network performance.
2. Slower in operation because of processing overheads.
3. Not transparent to users.

4.1.3.3 Circuit Level Gateways

- Circuit level gateways work at the session layer of the OSI model, or the TCP layer of TCP/IP. They monitor TCP handshaking between packets to determine whether a requested session is legitimate. Information passed to remote computer through a circuit level gateway appears to have originated from the gateway. This is useful for hiding information about protected networks.
- Circuit level gateways are relatively inexpensive and have the advantage of hiding information about the private network they protect. On the other hand, they do not filter individual packets.
- The circuit level gateway does not permit end-to-end TCP connection but two TCP connections are set-up. A typical use of circuit level gateway is in situations when system administrator trusts the internal users.

4.1.3.4 Comparison between Packet Filter and Proxies

Sr. No.	Packet filter	Proxy (Application level)
1.	Works at network layer of OSI and IP layer of TCP.	Works at application layer of OSI, TCP layer of TCP.
2.	Low impact on network performance.	High impact on network performance.
3.	Low level of security as compare to proxi.	High level of security.
4.	Packet filtering is not effective with the FTP protocol.	FTP and Telnet are allowed into the protected subnet.
5.	Simple level of security and faster than proxy firewall.	Capability to examine the traffic in detail, so slower than packet filtering.
6.	Normally transparent to the users.	Not transparent to the users.
7.	Difficult to configure as compare to proxy.	Easier to configure than packet filtering.
8.	They cannot hide the private network topology.	They can hide the private network topology.

4.1.4 Limitations of Firewall

- Limitations of Firewalls are :
  1. Firewall do not protect against inside threats.
  2. Packet filter firewall does not provide any content based filtering.

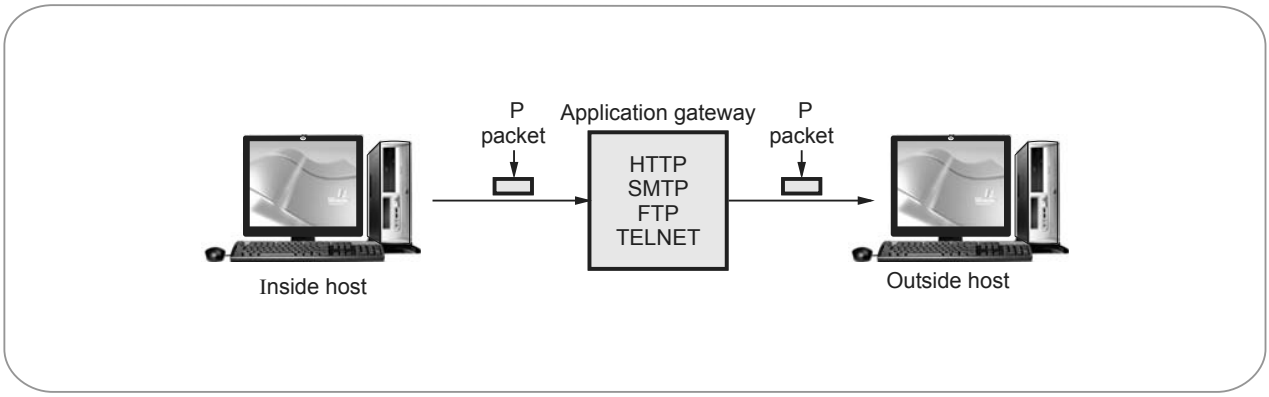


Fig. 4.1.4 Circuit gateway

3. Protocol tunneling, i.e. sending data from one protocol to another protocol which negates the purpose of firewall.
4. Encrypted traffic cannot be examine and filter.

Board Questions

1. *What is the application of firewall ? How it works ? Enlists its limitations.*
   MSBTE : Summer-15, Marks 4
2. *Explain need for firewall and explain one of the type of firewall with diagram.*
   MSBTE: Winter-15, 17, Marks 8
3. *Explain characteristics, working, design principle and limitation of firewall.*
   MSBTE : Summer-16, Marks 8
4. *List types of firewall. Explain packet filter firewall with diagram.* **MSBTE : Summer-17, 18, Marks 4**
5. *Describe packet filter router firewall with neat diagram.* **MSBTE : Summer-18, Marks 4**
6. *State any four limitations of firewall.*
   MSBTE : Winter-18, Marks 4

4.2 Firewall Location

1. DMZ network (Demilitarized Zone)
2. Virtual Private Network (VPN)
3. Distributed firewall

- A firewall is positioned to provide a protective barrier between an external, potentially untrusted source of traffic and an internal network.

4.2.1 DMZ

- Connections from the internal and the external network to the DMZ are permitted, while connections from the DMZ are only permitted to the external network, hosts in the DMZ may not connect to the internal network.
- This allows the DMZ's hosts to provide services to both the internal and external network while protecting the internal network in case intruders compromise a host in the DMZ. The DMZ is typically used for connecting servers that need to be accessible from the outside world, such as e-mail, web and DNS servers.
- Fig. 4.2.1 shows DMZ network.
- Traffic from the Internet is filtered, but some of it is allowed to reach systems in the DMZ i.e. like web servers and mail servers. If an attacker succeeds in breaking into a system in your DMZ, they won't gain access to your internal network as traffic coming from the DMZ is filtered before being allowed into the internal network.
- To create a DMZ, you can use two firewalls. Our illustration shows an outer firewall that separates the DMZ from the Internet and an inner firewall that separates the DMZ from the internal network. The outer firewall controls the traffic from the Internet to the DMZ. The inner firewall controls traffic from the DMZ to the internal network.
- The external firewall provides a measure of access control and protection for the DMZ systems consistent with their need for external connectivity. The external firewall also provides a basic level of protection for the remainder of the enterprise network.

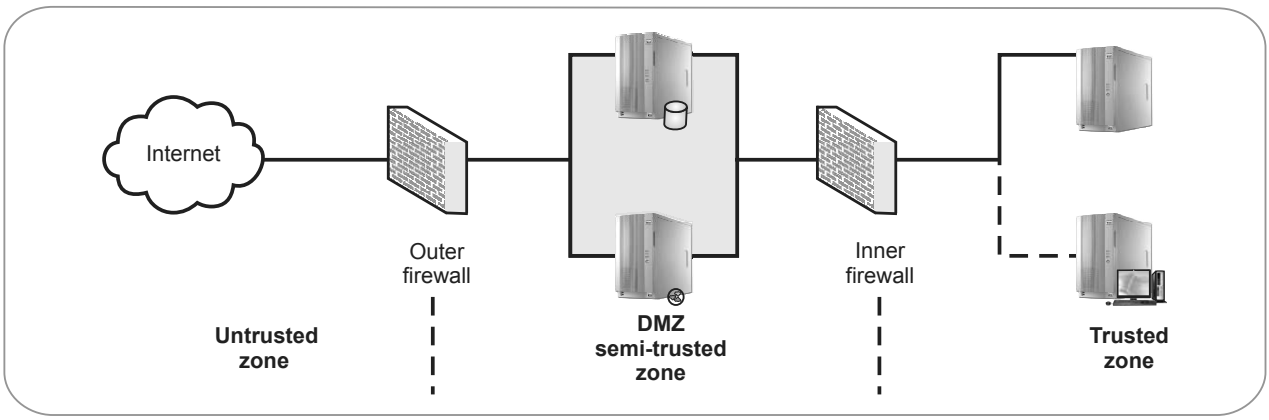


Fig. 4.2.1 DMZ network

- Internal firewalls serve three purposes :
  i. The internal firewall adds more stringent filtering capability, compared to the external firewall, in order to protect enterprise servers and workstations from external attack.
  ii. The internal firewall provides two-way protection with respect to the DMZ.
  iii. Multiple internal firewalls can be used to protect portions of the internal network from each other.

4.2.2 Virtual Private Networks (VPN)

- Virtual Private Networks (VPN) provide an encrypted connection between a user's distributed sites over a public network (e.g., the Internet). By contrast, a private network uses dedicated circuits and possibly encryption.
- Use of a public network exposes corporate traffic to eavesdropping and provides an entry point for unauthorized users. To counter this problem, a VPN is needed.
- VPN uses encryption and authentication in the lower protocol layers to provide a secure connection through an otherwise insecure network, typically the Internet. VPNs are generally cheaper than real private networks using private lines but rely on having the same encryption and authentication system at both ends. The encryption may be performed by firewall software or possibly by routers. The most common protocol mechanism used for this purpose is at the IP level and is known as IPsec.

3. Distributed Firewall

- A distributed firewall configuration involves stand-alone firewall devices plus host based firewalls working together under a central administrative control. Security policy is defined centrally and enforcement of policy is done by network endpoint(s).
- Administrators can configure host resident firewalls on hundreds of servers and workstations as well as configure personal firewalls on local and remote user systems.
- Tools let the network administrator set policies and monitor security across the entire network. These firewalls protect against internal attacks and provide protection tailored to specific machines and applications. Stand-alone firewalls provide global protection, including internal firewalls and an external firewall.

4.2.3 Firewall Configuration

- Firewall configuration are of three types :
  1. Screened host, single homed bastion host
  2. Screened host, dual homed bastion host
  3. Screened subnet.

1. Screened host, single homed bastion host

- In this system, firewall consists of two systems : A packet filtering router and a bastion host.
- The router is configured so that,
  1. For traffic from the Internet, only IP packets destined for the bastion host are allowed in.
  2. For traffic from the internal network, only IP packets from the bastion host allowed out.
- Fig. 4.2.2 shows screened host, single homed bastion host.

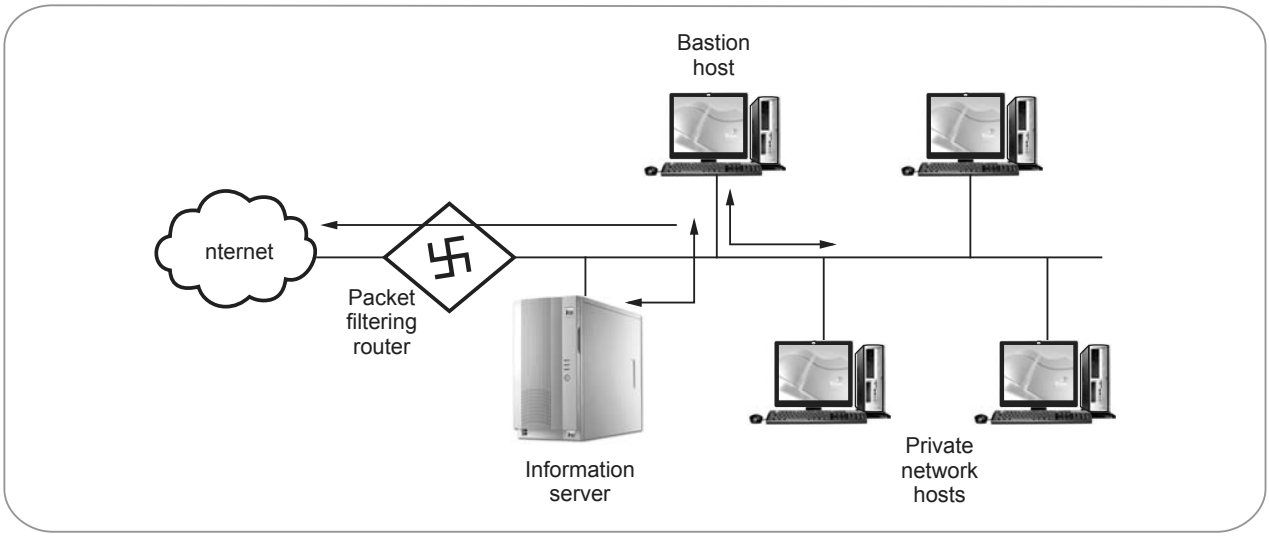


Fig. 4.2.2 Screened host, single homed bastion host

- The bastion host performs authentication and proxy functions.
- This configuration affords flexibility in providing direct internet access.

2. Screened host, dual homed bastion

- Fig. 4.2.3 shows dual homed bastion.

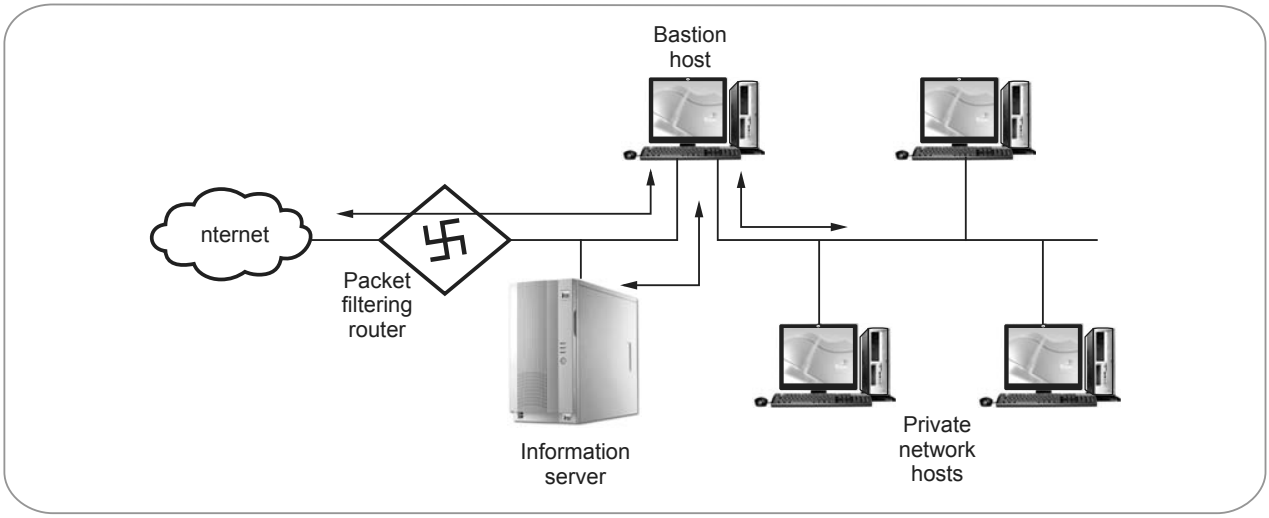


Fig. 4.2.3 Dual homed bastion

- This configuration prevents a security breach. The advantages of dual layers of security that were present in the previous configuration are present as well.
- An information server or other hosts can be allowed direct communication with the router if this is in accord with the security policy.

3. Screened subnet

- Fig. 4.2.4 shows screened subnet
- This configuration creates an isolated subnetwork which may consists of simply the bastion host but may also include one or more information servers and modems for dial-up capability.

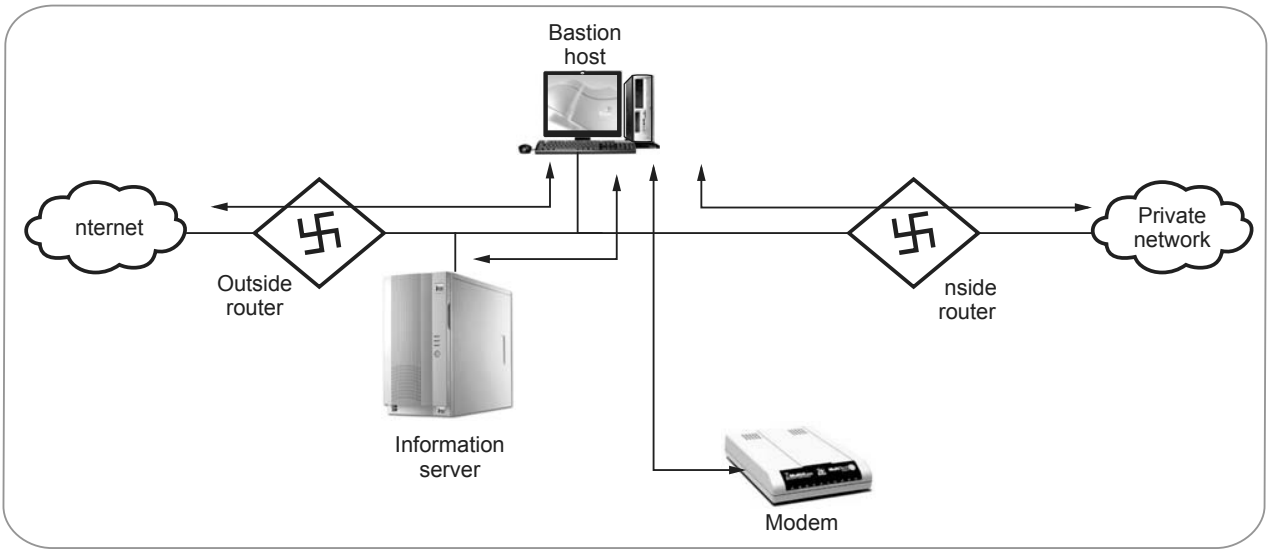


Fig. 4.2.4 Screened subnet

Advantages

1. There are now three levels of defense to thwart intruders.
2. Internal network is invisible to the Internet.
3. The systems on the inside network cannot construct direct routes to the internet.

Board Questions

1. *Describe DMZ with suitable diagram.* **MSBTE : Summer-17, Marks 4**
2. *Describe term DMZ* **MSBTE : Winter-15, Mark 1**

4.3 Intrusion Detection System (IDS)

- ***Intrusion*** is the act of gaining unauthorized access to a system so as to cause loss.
- ***Intrusion detection*** is the act of detecting unwanted traffic on a network or a device.
- Intrusion Detection Systems (IDSs) attempt to identify attacks by comparing collected data to predefined signatures known to be malicious or to a model of legal behavior.
- Intrusion detection systems are software or hardware systems that automate the process of monitoring the events occurring in a computer system or network, analyzing them for signs of security problems.

Functions of intrusion detection systems

1. Monitoring and analysis of user and system activity
2. Auditing of system configurations and vulnerabilities
3. Assessing the integrity of critical system and data files
4. Recognition of activity patterns reflecting known attacks
5. Statistical analysis for abnormal activity patterns

Benefits of intrusion detection

1. Improving integrity of other parts of the information security infrastructure
2. Improved system monitoring
3. Tracing user activity from the point of entry to point of exit or impact
4. Recognizing and reporting alterations to data files
5. Spotting errors of system configuration and sometimes correcting them
6. Recognizing specific types of attack and alerting appropriate staff for defensive responses
7. Keeping system management personnel up to date on recent corrections to programs

8. Allowing non-expert staff to contribute to system security
9. Providing guidelines in establishing information security policies

Process model

- Many IDSs can be described in terms of following functional components :

1. Information sources : The different sources of event information used to determine whether an intrusion has taken place. These sources can be drawn from different levels of the system, with network, host, and application monitoring most common.

2. Analysis : The part of intrusion detection systems that actually organizes and makes sense of the events derived from the information sources, deciding when those events indicate that intrusions are occurring or have already taken place. The most common analysis approaches are misuse detection and anomaly detection.

3. Response : The set of actions that the system takes once it detects intrusions. These are typically grouped into active and passive measures, with active measures involving some automated intervention on the part of the system, and passive measures involving reporting IDS findings to humans, who are then expected to take action based on those reports.

4.3.1 Infrastructure of IDS

- Fig. 4.3.1 shows IDS.

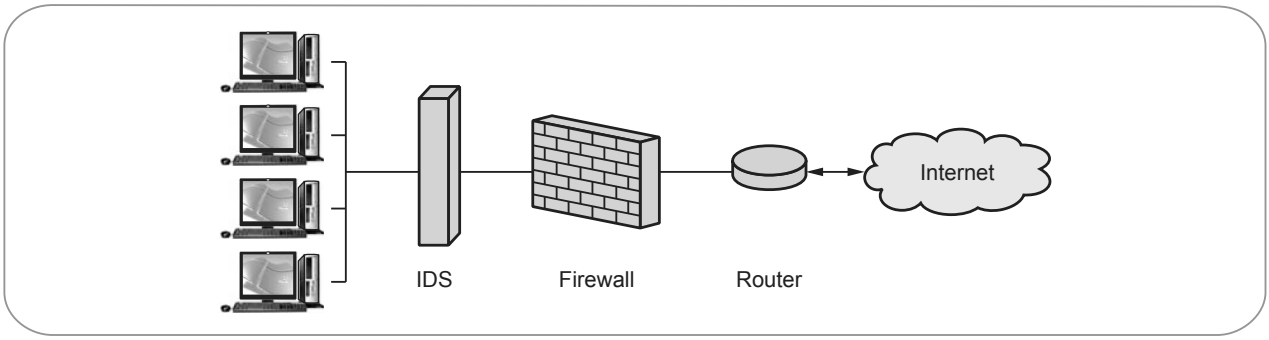


Fig. 4.3.1 IDS

- IDS monitors both inbound and outbound activities for possible intrusions. A firewall monitors all outbound traffic to a network and detects possible attacks. It cannot detect any malicious activities originated within the network.
- But, IDS on the other hand, monitors both the inbound and outbound traffic of the network to detect intrusions. In can even detect malicious activities if generated from the system.
- An IDS can detect intrusions by monitoring network traffic and compare it against established baseline. The baseline comprises of bandwidth, protocols, ports and devices used in the network. It alerts the administrator if at any time any traffic is detected which is significantly different from the baseline.
- IDS can also monitor the signatures of all inbound and outbound network traffic and compare them against a database of signatures of malicious threats. If a new threat remains undetected, the database of signatures is updated, so that the threat can be detected in future.

4.3.2 Classification of IDS

• The classification of intrusion detection system is based on following factors :

1. Location
2. Functionality
3. Deployment Approach
4. Detection Mechanism

Classification	Types	Advantages	Disadvantages
Location	Host based network intrusion detection	1. HIDS can protect off the LAN. 2. HIDS is versatile. 3. Requires lesser training than NIDS. 4. HIDS does not requires land bandwidth.	1. Data collection occurs on a per-host basis 2. Writing to log or reporting activity will generate extra load for network
	Network intrusion detection system	1. Adaptable to cross platform environment. 2. NIDS is centrally managed.	1. Requires more training. 2. Uses up LAN bandwidth. 3. Failure rate is higher
Functionality	Intrusion detection system	-	-
	Intrusion prevention system	-	-
	Intrusion detection and prevention system	-	-
Deployment approach	Single host	1. A single NIDS can monitor a wide subnet 2. The impact on the system is very little, it is a passive device which just listens	1. It is difficult to process all packets in a busy network.
	Multiple host (distributed agents	1. The problem of processing all packets by single NIDS which was present in single host NIDS is solved.	1. It is harder to manage and must be configured for each different host. 2. It's hard to coordinate between NIDS agents
Detection mechanism	Signature based	1. If attack signatures are clearly defined then it has low false positive. 2. Easy to use.	1. Requires specific knowledge of intrusion behavior and collect data before the intrusion could be out of date. 2. Difficult to detect unknown attacks.
	Anomaly based intrusion detection system	1. It has the ability to detect unknown attacks.	1. Defining the rule set for intrusion detection is difficult. 2. Efficiency of system depends on the fitness of the rules and its testing on the testing datasets

4.3.3 Host-Based IDS

- Host based monitors system logs for evidence of malicious or suspicious application activity in real time.
- It requires small programs or agents to be installed on individual systems to be monitored. The agents supervise the OS and write data to log files and activate alarm.
- Host-based IDSs operate on information collected from within an individual computer system.
- This allows host-based IDSs to analyze activities with great reliability and precision, determining exactly which processes and users are involved in a particular attack on the operating system.
- Host-based IDSs normally utilize information sources of two types, operating system audit trails, and system logs.
- Operating system audit trails are usually generated at the innermost (kernel) level of the operating system, and are therefore more detailed and better protected than system logs.
- System logs are much less obtuse and much smaller than audit trails, and are furthermore far easier to comprehend.

Advantages

1. With their ability to monitor events local to a host, can detect attacks that cannot be seen by network-based IDS.
2. It can often operate in an environment in which network traffic is encrypted.
3. When host-based IDSs operate on OS audit trails; they can help detect Trojan horse or other attacks that involve software integrity breaches.

Disadvantages

1. Host-based IDSs are harder to manage, as information must be configured and managed for every host monitored.
2. Since at least the information sources for host-based IDSs reside on the host targeted by attacks, the IDS may be attacked and disabled as part of the attack.
3. Host-based IDSs are not well suited for detecting network scans or other such surveillance that targets an entire network.
4. Host-based IDSs can be disabled by certain denial-of-service attacks.
5. When host-based IDSs use OS audit trails as an information source, the amount of information can be immense, requiring additional local storage on the system.

4.3.4 Network Based IDS

- A Network Intrusion Detection System (NIDS) is tries to detect malicious activity such as denial of service attacks; port scans or even attempts to crack into computers by network security monitoring of network traffic.
- Network intrusion detection systems are placed at a strategic point or points within the network to monitor traffic to and from all devices on the network.
- The majority of commercial intrusion detection systems are network based.
- These IDSs detect attacks by capturing and analyzing network packets.
- Listening on a network segment or switch, one network-based IDS can monitor the network traffic affecting multiple hosts that are connected to the network segment, thereby protecting those hosts.
- Network-based IDSs often consist of a set of single-purpose sensors or hosts placed at various points in a network.
- These units monitor network traffic, performing local analysis of that traffic and reporting attacks to a central management console.
- As the sensors are limited to running the IDS, they can be more easily secured against attack.
- Many of these sensors are designed to run in stealth mode, in order to make it more difficult for an attacker to determine their presence and location.

Advantages of network-based IDSs

1. A few well-placed network-based IDSs can monitor a large network.
2. The deployment of network-based IDSs has little impact upon an existing network.
3. It can be made very secure against attack.

Disadvantages of network-based IDSs

1. Network-based IDSs may have difficulty processing all packets in a large or busy network.
2. Network-based IDSs cannot analyze encrypted information.
3. Most network-based IDSs cannot tell whether or not an attack was successful
4. Some network-based IDSs have problems dealing with network-based attacks that involve fragmenting packets.

Board Questions

1. *With the help of neat diagram describe host based intrusion detection system.* **MSBTE : Summer-15, Marks 4**
2. *With neat sketch explain the working of network Based IDS.* **MSBTE : Summer-15, Marks 8**
3. *Describe term IDS* **MSBTE : Winter-15, Mark 1**
4. *Explain in detail intrusion detection systems.* **MSBTE : Winter-15, Marks 8**
5. *Describe Host based IDS with its advantages and disadvantages.* **MSBTE : Winter-17, Summer-16, Marks 4**
6. *What is intrusion detection system ? Explain host based IDS.* **MSBTE : Winter-16, 17, Marks 4**
7. *Describe with suitable diagram Intrusion Detection System.* **MSBTE : Summer-17, Marks 8**

4.4 Vulnerability Detection

- The term "vulnerability" refers to the security flaws in a system that allows an attack to be successful.
- Vulnerability testing should be performed on an ongoing basis by the parties responsible for resolving such vulnerabilities, and helps to provide data used to identify unexpected dangers to security that need to be addressed.
- Such vulnerabilities are not particular to technology - they can also apply to social factors such as individual authentication and authorization policies.
- Testing for vulnerabilities is useful for maintaining ongoing security, allowing the people responsible for the security of one's resources to respond effectively to new dangers as they arise. It is also invaluable for policy and technology development, and as part of a technology selection process; selecting the right technology early on can ensure significant savings in time, money, and other business costs further down the line.
- Understanding the proper use of such terms is important not only to sound like you know what you're talking about, nor even just to facilitate communication. It also helps develop and employ good policies.

❑❑❑

UNIT - V

5 Network Security, Cyber Laws and Compliance Standards

5.1 Kerberos

Kerberos is an **authentication protocol**. It provides a way to authenticate clients to services to each other through a trusted third party.

- Kerberos makes the assumption that the connection between a client and service is insecure. Passwords are encrypted to prevent others from reading them. Clients only have to authenticate once during a pre-defined lifetime.
- Kerberos was designed and developed at MIT by Project Athena. Currently, Kerberos is upto Version 5. Version 4 being the first version to be released outside of MIT.
- Kerberos has been adopted by several private companies as well as added to several operating systems.
- Its creation was inspired by client-server model replacing time-sharing model. Kerberos is a network authentication protocol designed to allow users, clients and servers, authenticate themselves to each other.
- This **mutual authentication** is done using **secret-key cryptography** with parties proving to each other their identity across an insecure network connection.
- Communication between the client and the server can be secure after the client and server have used Kerberos to prove their identity.
- From this point on, subsequent communication between the two can be encrypted to assure privacy and data integrity.

Requirement of Kerberos

- Kerberos client/server authentication requirements are :
  1. **Security :** That Kerberos is strong enough to stop potential eavesdroppers from finding it to be a weak link.
  2. **Reliability :** That Kerberos is highly reliable employing a distributed server architecture where one server is able to back up another. This means that Kerberos systems are fail safe, meaning graceful degradation, if it happens.
  3. **Transparency :** That user is not aware that authentication is taking place beyond providing passwords.
  4. **Scalability :** Kerberos systems accept and support new clients and servers.

     To meet these requirements, Kerberos designers proposed a third-party trusted authentication service to arbitrate between the client and server in their mutual authentication.

5.1.1 Kerberos Terminology

- Kerberos has its own terminology to define various aspects of the service.
  1. **Authentication Server (AS) :** A server that issues tickets for a desired service which are in turn given to users for access to the service.
  2. **Client :** An entity on the network that can receive a ticket from Kerberos.
  3. **Credentials :** A temporary set of electronic credentials that verify the identity of a client for a particular service. It also called a ticket.
  4. **Credential cache or ticket file :** A file which contains the keys for encrypting communications between a user and various network services.
  5. **Crypt hash :** A one-way hash used to authenticate users.
  6. **Key :** Data used when encrypting or decrypting other data.
  7. **Key Distribution Center (KDC) :** A service that issue Kerberos tickets and which usually run on

the same host as the Ticket-Granting Server (TGS).

8. **Realm :** A network that uses Kerberos composed of one or more servers called KDCs and a potentially large number of clients.
9. **Ticket-Granting Server (TGS) :** A server that issues tickets for a desired service which are in turn given to users for access to the service. The TGS usually runs on the same host as the KDC.
10. **Ticket-Granting Ticket (TGT) :** A special ticket that allows the client to obtain additional tickets without applying for them from the KDC.

5.1.2 Working of Kerberos

- The authentication service, or AS, receivers the request by the client and verifies that the client is indeed the computer it claims to be.
- This is usually just a simple database lookup of the user's ID.

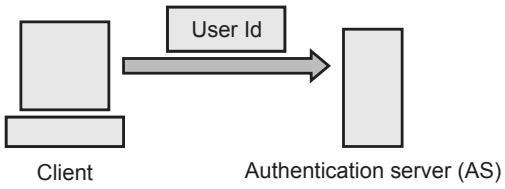


Fig. 5.1.1

- Upon verification, a timestamp is created. This puts the current time in a user session, along with an expiration date. The default expiration date of a timestamp is 8 hours.
- The encryption key is then created. The timestamp ensures that when 8 hours is up, the encryption key is useless.
- The key is sent back to the client in the form of a ticket-granting ticket, or TGT. This is a simple ticket that is issued by the authentication service. It is used for authentication the client for future reference.

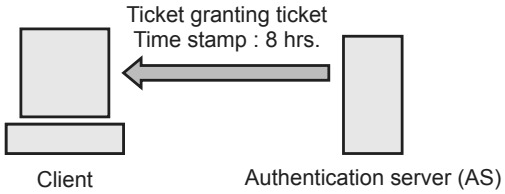


Fig. 5.1.2

- The client submits the ticket-granting ticket to the ticket-granting server, or TGS, to get authenticated.

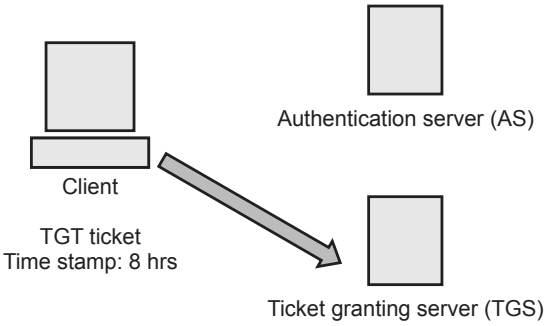


Fig. 5.1.3

- The TGS creates an encrypted key with a timestamp, and grants the client a service ticket.

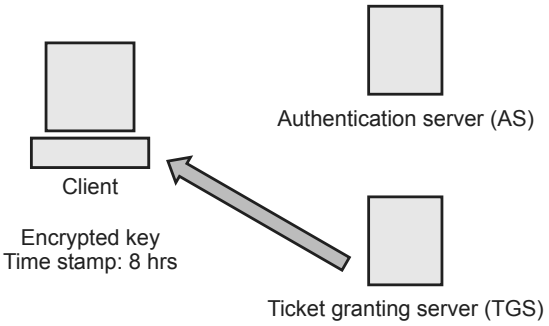


Fig. 5.1.4

- The client decrypts the ticket, tells the TGS it has done so, and then sends its own encrypted key to the service.

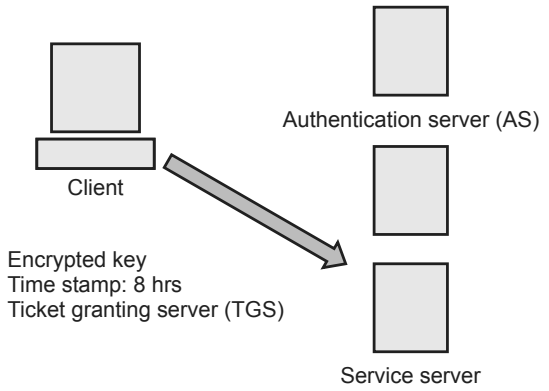


Fig. 5.1.5

- The service decrypts the key, and makes sure the timestamp is still valid. If it is, the service contacts the key distribution center to receive a session that is returned to the client.

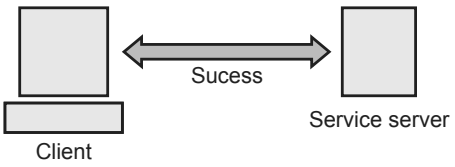


Fig. 5.1.6

- The client decrypts the ticket. If the keys are still valid, communication is initiated between client and server.

Board Questions

1. *Explain the concecpt of Kerberos.*
   MSBTE : Winter-15, Marks 4
2. *Describe the concept of kerberos.*
   MSBTE : Summer-16, Marks 4
3. *What is Kerberos ? Explain with diagram different servers involved in Kerberos.*
   MSBTE : Winter-16, Marks 4
4. *Describe 'Kerberos' protocol with suitable diagram.* **MSBTE : Summer-17, Marks 4**
5. *Explain the concept of Kerberos.*
   MSBTE : Winter-17, Marks 4
6. *Explain the kerberos with help of suitable diagram.*
   MSBTE : Winter-18, Marks 4

5.2 IP Security

- Different application specific security mechanisms are developed such as electronic mail (PAG, S/MIME), client/server (Kerberos), web access (secure sockets layer). An IP level security can ensure secure networking not only for applications with security mechanisms but also for many security ignorant applications.
- IP Security (IPSec) is the capability that can be added to present versions of Internet Protocol (IPv4 and IPv6) by means of additional headers for secure communication across LAN, WAN and Internet.
- IPSec is a set of protocols and mechanism that provide confidentiality, authentication, message integrity and replay detection at IP layer. The device (firewall or gateway) on which the IPSec mechanism reside is called as **security gateway**.
- IPSec has two modes of operation.
  1. Transport mode
  2. Tunnel mode
- IPSec uses two protocols for message security.
  1. Authentication Header (AH) protocol.
  2. Encapsulating Security Payload (ESP) protocol.

5.2.1 Applications of IPSec

1. Secure connectivity over the Internet : AVirtual Private Network (VPN) can be established over the Internet. This reduces cost of private networks and network management overheads.

2. Secure remote access over the Internet : With IPSec, Secure access to a company network is possible.

3. Extranet and intranet connectivity : With IPSec, secure communication with other organizations, ensures authentication and confidentiality and provide a key exchange mechanism.

4. Enhanced electronic-commerce security : Use of IPSec enhances the security in electronic commerce applications.

5.2.2 IP Security Scenario

Fig. 5.2.1 shows an IP security scenario. (See Fig. 5.2.1 on next page)

- Many organizations have LAN at multiple places. The IPSec protocols are used which operates in networking devices e.g. router or firewall.
- The IPSec networking encrypt and compress the outgoing traffic while it decrypt and decompress all incoming traffic. These processes are transparent to workstations and servers on LAN.

5.2.3 Benefits of IPSec

1. IPSec provides strong security within and across the LANs.
2. IPSec in a firewall avoids bypass if all traffic from the outside must use IP.
3. No need to change software for implementing IPSec.
4. IPSec is below transport layer and hence is transparent to applications.

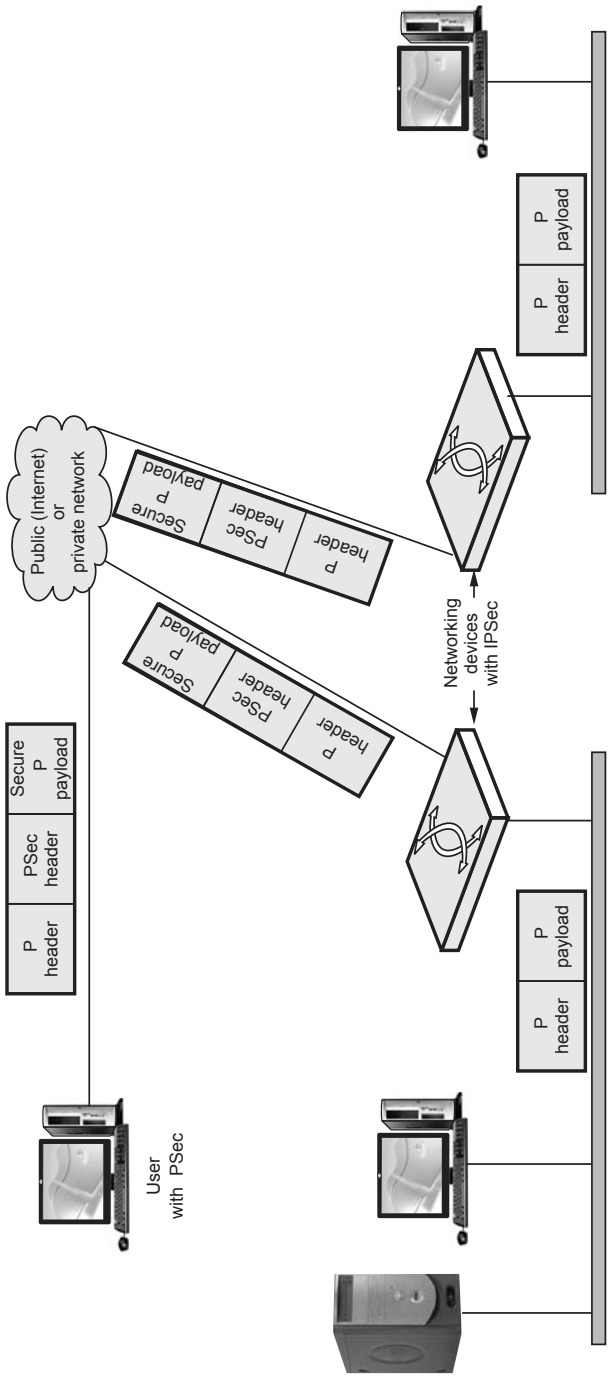


Fig. 5.2.1 IPSec scenario

5. IPSec is transparent to end users also.
6. If required IPSec can provide security to individual users.

Board Questions

1. *Describe IP security architecture.*
   MSBTE : Summer-16, Marks 4
2. *What is IP security ? Describe authentication header mode of IP security.*
   MSBTE : Winter-16, Marks 4
3. *Describe IPsec configuration.*
   MSBTE : Summer-17, Marks 4
4. *Explain IPSec security with help of diagram.*
   MSBTE : Winter-18, Marks 4

5.3 IP Secuirty Architecture

- IPSec mechanism uses Security Policy Database (SPD) which determines how a messages are to handle also the security services needed and path the packet should take.
- Various documents are used to define complex IPSec specification. The overall architecture of IPSec is constituted by three major components.
  1. IPSec documents
  2. IPSec services
  3. Security Associations (SA)

5.3.1 IPSec Documents

- IPSec specifications are described in various documents. Few important documents and specifications described are as under -

Sr. No.	Documents	Specifications
1.	RFC 2401	Overview of security architecture.
2.	RFC 2402	Packet authentication extension to IPv4 and IPv6.
3.	RFC 2406	Packet encryption extension to IPv4 and IPv6.
4.	RFC 2408	Key management capabilities

- All above specifications are essentially supported by IPv6 and are optional for IPv4. The security features are incorporated as extension header to the main IP header for both IPv4 and IPv6.
- The extension header for authentication is called as Authentication Header (AH) and the extension header for encryption is called as Encapsulating Security Payload (ESP) header.
- Besides RFC various other documents are published by Internet Engineering Task Force (IETF). These documents can be divided into seven groups.
- IPSec protocol consists of seven different groups of document as shown in Fig. 5.3.1.

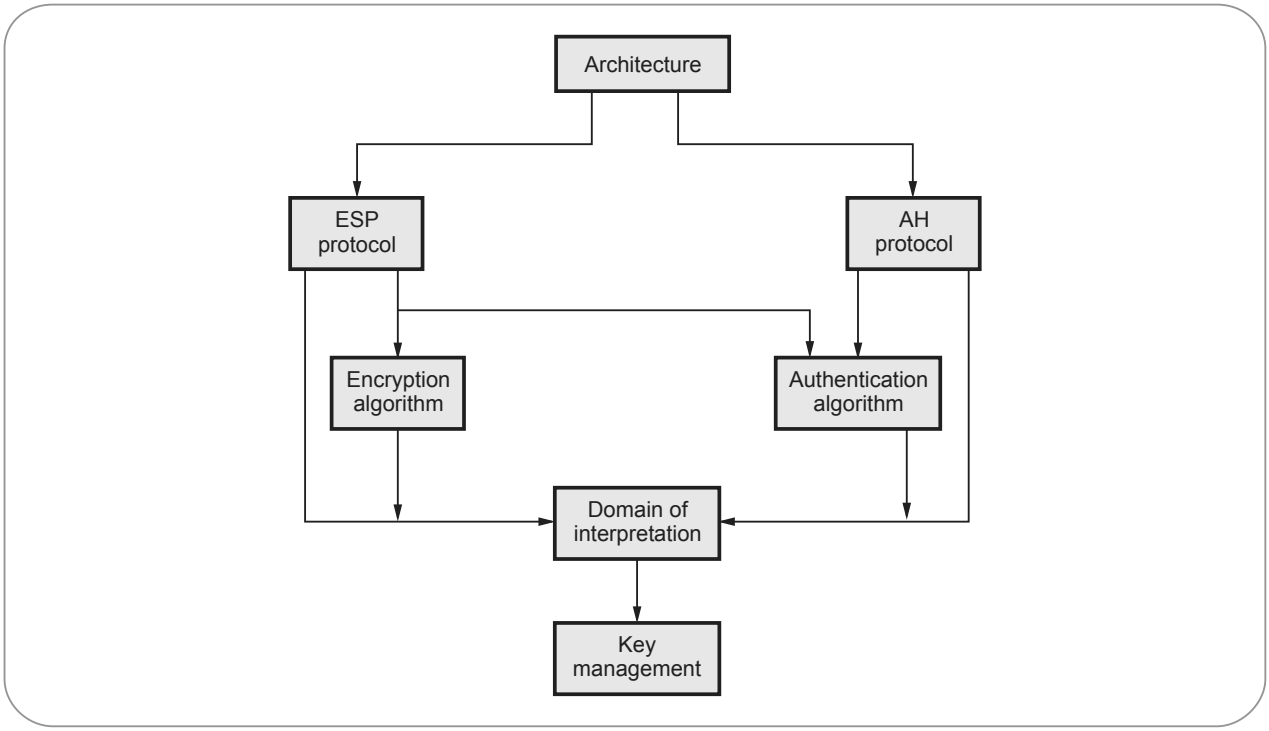


Fig. 5.3.1 IPSec document

1. **Architecture :** Covers security requirements, definitions, IPSec technology.
2. **Encapsulating Security Payload (ESP) :** Covers packet format, packet encryption authentication.
3. **Authentication Header (AH**) : Covers packet format, general issues.
4. **Authentication algorithm :** Encryption algorithms used for ESP.
5. **Key management :** Key management schemes.
6. **Domain of Interpretation (DoI) :** Values to relate documents with each other.

5.3.2 IPSec Services

- IPSec provides security services at IP layer by selecting required security protocols, algorithms and cryptographic keys as per the services requested.
- Two protocols performs the function of providing security. These are authentication header protocol and protocol for encapsulating security payload. The services provide by these protocols are -
  a. Access control
  b. Connectionless integrity
  c. Data origin authentication
  d. Rejection of replayed packets
  e. Confidentiality
  f. Limited traffic flow confidentiality

IPSec protocol suit

- IP packet consists of two parts; IP header and data. IPSec features are incorporated into an additional IP header called extension header. Different extension headers are used for different services.

- IPSec defines two protocols.
  1. AH 2. ESP
- The services provided by ESP protocol is possible with and without authentication option. Various services by AH and ESP protocols are summarized in Table 5.3.1.

Sr. No.	Service	AH protocol	ESP protocol	
			Encryption only	Encryption + Authentication
1.	Access control	Yes	Yes	–
2.	Connectionless integrity	Yes	–	Yes
3.	Data origin authentication	Yes	–	Yes
4.	Rejection of packets	Yes	Yes	Yes
5.	Confidentiality	Yes	Yes	Yes
6.	Limited traffic flow confidentiality	–	Yes	Yes

Table 5.3.1

5.3.3 Security Associations (SA)

- Security Association (SA) is the common between authentication and confidentiality mechanisms. An association is a one-way relationship between transmitter and receiver. For a two-way secure exchange two security associations are required.
- A security association is defined by parameters.
  1. Security Parameters Index (SPI)
  2. IP destination address
  3. Security protocol identifiers

1. **Security Parameters Index (SPI) :** SPI is a string of bit assigned to this SA and has local significance only. SPI is located in AH and ESP headers. SPI enables the receiving system under which the packet is to process.
2. **IP destination address :** It is the end point address of SA which can be end user system or a network system (firewall / router).
3. **Security protocol identifiers :** Security protocol identifier indicates whether the association is an AH or ESP security association.

5.3.4 SA Parameters

- A Security Association (SA) is normally defined by following parameters.

1. **Sequence number counter :** Sequence number counter is a 32-bit value that indicates the sequence number field in AH or ESP.
2. **Sequence counter overflow :** Sequence counter overflow is a flag used to indicate whether overflow of the sequence number counter should generate an auditable event and prevent further transmission of packets on SA.

3. Anti-replay window : Anti - replay window determines whether on inbound AH or ESP packet is a replay.

4. AH information : AH information includes authentication algorithm, keys, key life times and related parameters being used with AH.

5. ESP information : ESP information includes encryption and authentication algorithm, keys, initialization values required for ESP implementation.

6. IPSec protocol mode : IPSec protocol mode can be tunnel, transport or wildcard.

7. Path MTU : Path MTU means observed path maximum transmission unit which indicates maximum size of a packet that can be transmitted without fragmentation.

5.3.5 Transport Mode

- AH and ESP can support two modes of operation.
  1. Transport mode
  2. Tunnel mode
- Transport mode mainly provide protection for upper layer protocols. The protection extends to the payload of an IP packet. For example, TCP or UDP segment or ICMP packet.
- The transport mode is suitable for end-to-end communication between two workstations.
- In transport mode, ESP encrypts the IP payload excluding IP header. Authentication of IP payload is optional.
- AH authenticates the IP payload and specific portions of IP header.

5.3.6 Tunnel Mode

- Tunnel mode provides protection to entire IP packets. Security fields are added to IP packets and entire packet (AH or ESP packet + Security packet) is new IP packet with a new IP header.
- Entire new IP packet travels through a tunnel from one point to other over IP network. No router over the network are able to detect inner IP header. Since original packet is encapsulated by new larger packet having different source and destination address.
- Tunnel mode is preferred when one or both ends of an SA a security gateway such as a firewall or router that implements IPSec.
- In tunnel mode, number of hosts on network with firewalls may engage in secure transmission without IPSec. The unsecured packets generated are tunneled through external networks by tunnel mode SAs or IPSec in firewall or router.
- ESP encrypts and optionally authenticates the entire inner IP packet including IP header.
- AH authenticates the entire inner IP packet and selected portion of outer IP header.
- The tunnel mode and transport mode functionality is summarized in Table 5.3.2.

Protocol	Transport mode	Tunnel mode
AH	Authenticates IP paylaod and selected portion of IP header.	Authenticates entire IP packet and selected portion of outer IP header.
ESP	Encrypts IP payload and IPv6 extension headers.	Encrypts entire inner IP packet.
ESP with Authentication	Authenticates IP payload and not IP header. Encrypts IP payload and IPv6 header.	Authenticates inner IP packet. Encrypts entire inner IP packet.

Table 5.3.2

5.4 Authentication Header (AH)

- It provides support for data integrity and authentication of IP packets.
- Data integrity service insures that data inside IP packets is not altered during the transit.
- Authentication service enables and end user to authenticate the user at the other end and decides to accept or reject packets accordingly.
- Authentication also prevents the IP spoofing attack.
- AH is based on the MAC protocol, i.e. two communication parties must share a secret key.
- AH header format is shown in Fig. 5.4.1.
  1. **Next header** - This is 8-bits field and identifies the type of header that immediately follows the AH.

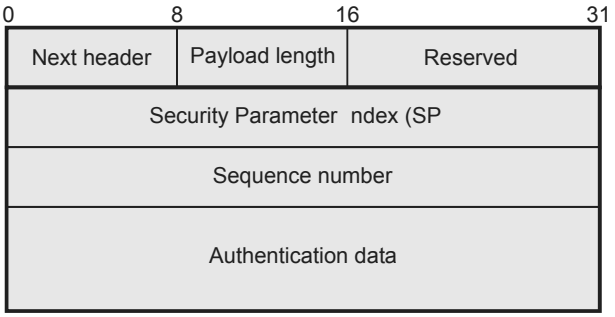


Fig. 5.4.1 IPSec authentication header format

2. **Payload length** - Contains the length of the AH in 32-bit words minus 2. Suppose that the length of the authentication data field is 96-bits (or three 32-bit words) with a three word fixed header, then we have a total of 6-words in the header. Therefore this field will contain a value of 4.
3. **Reserved** - Reserved for future use (16-bit).
4. **SPI** - Used in combination with the SA and DA as well as the IPSec protocol used (AH or ESP) to uniquely identify the security association for the traffic to which a datagram belongs.
5. **Sequence number** - To prevent replay attack.

Replay attack

1. Suppose user A wants to transfer some amount to user C's bank account.
2. Both user A and C have the accounts with bank B.
3. User A might send an electronic message to bank B requesting for the funds transfer.
4. User C could capture this message and send a second copy of the message to bank B.
5. Band B have no idea that this is an unauthorized message.
6. User C would get the benefit of the funds transfer twice.

Authentication data

Also called Integrity check value for the datagram. This value is the MAC used for authentication and integrity purposes.

5.4.1 AH Transport Mode

- The position of the AH is between the original IP header and original TCP header of the IP packet.
- Fig. 5.4.2 shows the AH in transport mode.

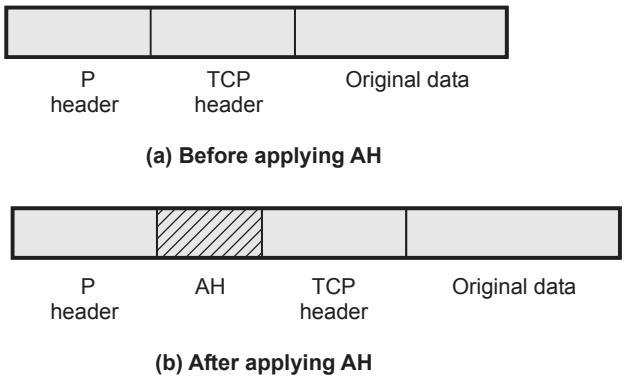


Fig. 5.4.2 Transport mode

5.4.2 AH Tunnel Mode

- The entire original IP packet is authenticated.
- AH is inserted between the original IP header and a new outer IP header.
- Fig. 5.4.3 shows AH tunnel mode.

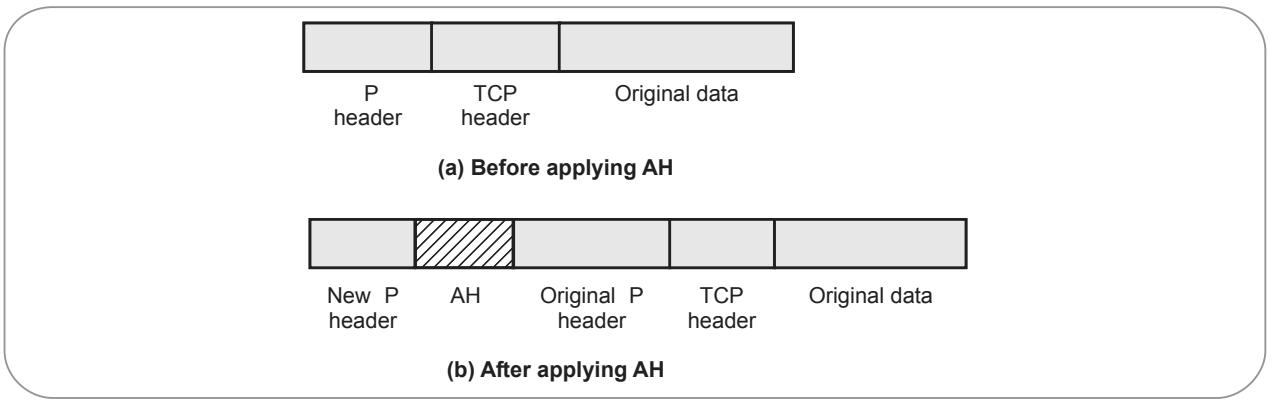


Fig. 5.4.3 Tunnel mode

5.5 Encapsulating Security Payload (ESP)

- Encapsulating Security Payload (ESP) provides confidentiality services and limited traffic flow confidentiality. An authentication service is optional feature.

5.5.1 ESP Format

- Fig. 5.5.1 shows IPSec ESP format.

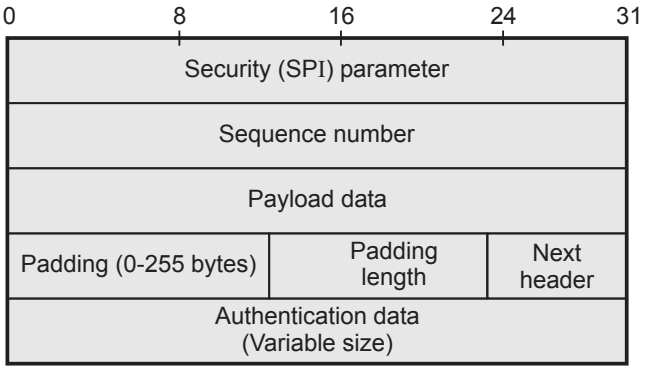


Fig. 5.5.1 ESP format

1. **SPI -** It is 32-bits field used in combination with the source and destination address. It identifies a security association.
2. **Sequence number -** This 32-bit field is used to prevent replay attacks.
3. **Payload data -** This is a transport level segment (transport mode) or IP packet (tunnel mode) that is protected by encryption.
4. **Padding -** It contains the padding bits.
5. **Padding length -** Indicates the number of pad bytes immediately preceding this field.
6. **Next header -** It identifies the type of encapsulated data in the payload.
7. **Authentication data -** It is variable length field contains the authentication data called as the integrity check value for the datagram.

5.5.2 Encryption and Authentication Algorithms

- The payload data, padding, pad length and next header fields are encrypted by ESP.
- Various algorithms used for encryption are -

  1. Three-key triple DES 2. RCS 3. IDEA
  4. Three-key triple IDEA 5. CAST 6. Blowfish

5.5.3 Padding

- Padding field is used for various purposes such as
  1. To expand the plain text if an encryption algorithm requires the plain text to be a multiple of number of bytes.
  2. To assure the alignment of cipher text to make it integer multiple of 32-bits.
  3. To provide partial traffic flow confidentiality by concealing the actual length of payload.

5.5.4 Comparison between AH and ESP

Sr. No.	AH	ESP
1.	Defined in RFC 2402	Defined in RFC 2406
2.	AH mandatory for IPv6 compliance.	Use of ESP with IPv6 is optional.
3.	Provides stronger authentication in transport mode.	Authentication provided is not as strong as AH.
4.	Requires less overhead since it only inserts a header into the IP packet.	Requires more overhead as it inserts a header and trailer.
5.	Provides connectionless integrity and data origin authentication for IPv4 and IPv6	Provides confidentiality, data origin authentication, connectionless integrity, an anti-reply service and limited traffic flow confidentiality.
6.	Protects as much of the IP header as possible as well as upper level protocol data.	It only protects those IP header fields that it encapsulates.
7.	It provides a packet authentication service.	It encrypts and /or authenticates data.

Board Question

1. *Give IP sec configuration. Describe AH and ESP modes of IPSEC.* **MSBTE : Summer-15, Marks 8**

5.6 Email Security

- Email security describes various techniques for keeping sensitive information in email communication and accounts secure against unauthorized access, loss, or compromise.

- Email remains a key productivity tool for today's organizations, as well as a successful attack vector for cyber criminals.

5.6.1 PGP

- PGP stands for Pretty Good Privacy. It was developed originally by Phil Zimmerman. However, in its incarnation as OpenPGP, it has now become an open standard. PGP is open-source. Although PGP can be used for protecting data in long-term storage, it is used primarily for email security.
- PGP is a complete e-mail security package that provides privacy, authentication, digital signatures, and compression all in an easy to use form.
- The complete package, including all the source code, is distributed free of charge via the Internet. Due to its quality, zero price, and easy availability on UNIX, Linux, Windows and Mac OS platforms, it is widely used today.
- PGP encrypts data by using a block cipher called IDEA, which uses 128-bit keys. IDEA is similar to DES and AES. Key management uses RSA and data integrity uses MDS.

Characteristics of PGP

1. PGP is available free world wide.
2. PGP can run on various platform windows, UNIX and machintosh.
3. The algorithms used are extremely secure.
4. World wide acceptability.
5. PGP is not developed and controlled by government or standard organization.
6. PGP is on an Internet Standards track.

- **PGP works as follows**
- Suppose user A wants to send a message (P) to user B in a secure way. Both the user have private and public RSA keys. Each user knows the other's user public key. User A uses PGP program for security purpose. At sender side i.e. at user A, PGP apply the hash function to the plain text message using MD5 and that message is encrypted. After encrypting again apply hash function using own private RSA key. Fig. 5.6.1 shows this process.
- When message is received by user B, he decrypts the hash with user A public key and verifies that the hash is correct. MD5 is the difficult to break. The encrypted hash and original message are concatenated into a single message P_1 and compressed using the ZIP program (P_1.Z).
- Using 128-bit IDEA message key (K_m), the ZIP program is encrypted with IDEA. Also K_m is encrypted with user B's public key (B_P). These two components are then concatenated and converted to base64.
- When this is received by user B, he reverses the base64 encoding and decrypts the IDEA key using his private RSA key. Using this key, user B decrypts the message to get P_1.Z. After decompressing P_1.Z, user B gets the plaintext message.
- For getting correct message, user B separates the plaintext from hash and decrypts the hash using user A public key. If the plaintext hash agrees with his own MD5 computation, user B knows that P is the correct message and that message came from user A.

Notation used in PGP

K_S = Session key used in conventional encryption scheme

PR_a = Private key of user A, used in public key encryption scheme

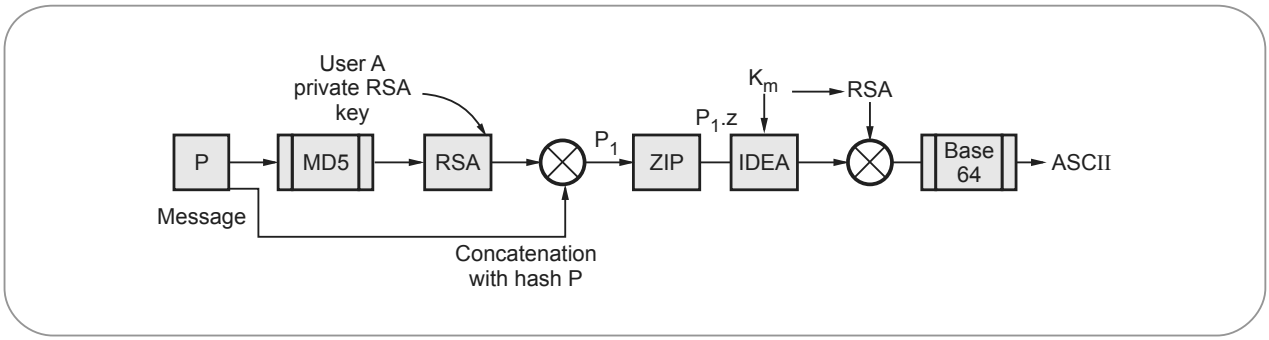


Fig. 5.6.1 PGP process

PU_a = Public key of user A, used in public key encryption scheme

EP = Pubilc key encryption

DP = Public key decryption

EC = Conventional encryption

DC = Conventional decryption

H = Hash function

|| = Concatenation

Z = Compression using ZIP algorithm

R64 = Conversion to radix 64 ASCII format

5.6.1.1 PGP Operation

- PGP operation involves five different services.
  1. Authentication
  2. Confidentiality
  3. Compression
  4. E-mail compatibility
  5. Segmentation.

1. Authentication

- Signatures are attached to the message or file are detached signatures are also supported and are stored and transmitted separately from the message it signs.
- The digital signature is generated by either
  i) SHA-1 and RSA
  ii) DSS/SHA-1
- Sender authentication consists of the sender attaching his/her digital signature to the email and the receiver verifying the signature using public-key cryptography. Here is an example of authentication operations carried out by the sender and the receiver :
  1. At the sender's end, the SHA-1 hash function is used to create a 160-bit message digest of the outgoing email message.
  2. The message digest is encrypted with RSA using the sender's private key and the result prepended to the message. The composite message is transmitted to the recipient.
  3. The receiver uses RSA with the sender's public key to decrypt the message digest.
  4. The receiver compares the locally computed message digest with the received message digest.
- The description was based on using a RSA/SHA based digital signature. PGP also support DSS/SHA based signature. DSS stands for Digital Signature Standard. PGP also supports datached signatures that can be sent separately to the receiver. Detached signatures are also useful when a document must be signed by multiple individuals.
- Fig. 5.6.2 shows an authentication only.

2. Confidentiality

- Confidentiality is provided by encrypting messages to be transmitted. The algorithms used for encrypties are CAST-128, IDEA, 3DES with multiple keys.
- Only a portion of plaintext is encrypted with each key and there is no relationship with keys. Hence, the public key algorithm is secure.
- This service can be used for encrypting disk files. As you'd expect, PGP uses symmetric-key encryption for confidentiality. The user has the choice of three different block-cipher algorithms for this purpose : CAST-128, IDEA, or 3DES, with CAST-128 being the default choice.

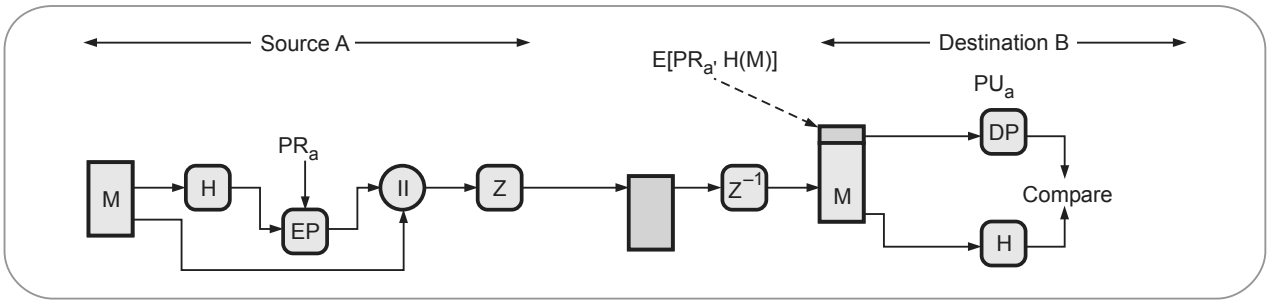


Fig. 5.6.2 Authentication

1. Sender generates message and random 128-bit number to be used as session key for this message only.
2. Message is encrypted, using CAST-128 / IDEA/3DES with session key.
3. Session key is encrypted using RSA with recipient's public key, then attached to message.
4. Receiver uses RSA with its private key to decrypt and recover session key.
5. Session key is used to decrypt message.

• Fig. 5.6.3 shows a confidentiality operation.

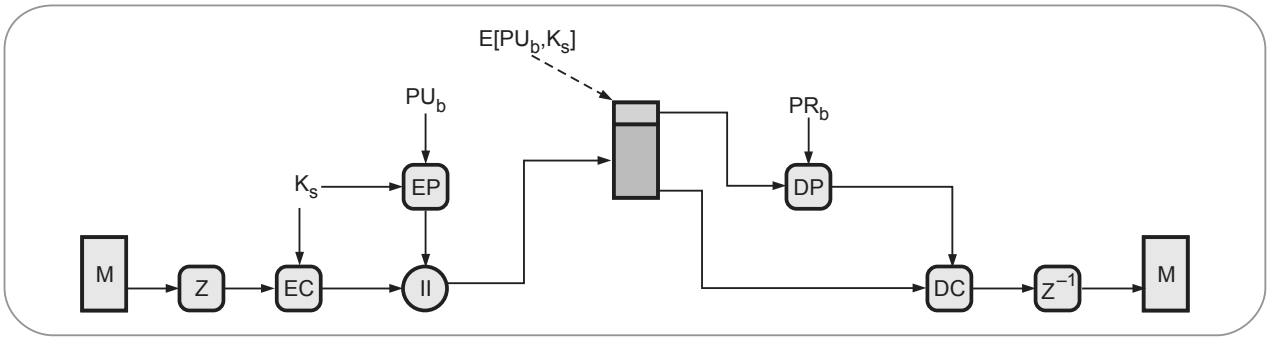


Fig. 5.6.3 Confidentiality

Confidentiality and Authentication

• May be both services used same message

a. Create signature for plain text and attach to message

b. Encrypt both message and signature using CAST - 128 or IDEA or TDEA

c. Attach RSA encrypted session key

• Fig. 5.6.4 shows confidentiality and authentication

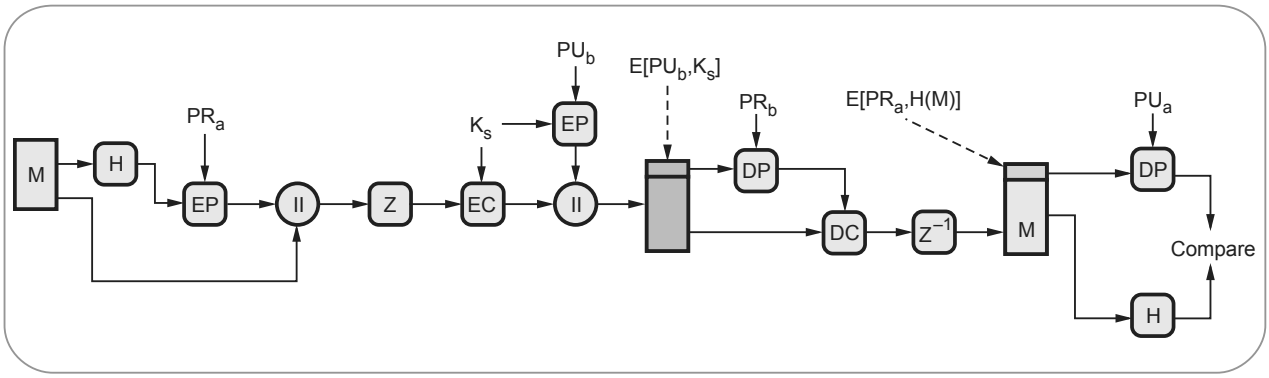


Fig. 5.6.4 Confidentiality and authentication

• When both services are used, the sender first signs the message with its own private key, then encrypts the message with a session key, and then encrypts the session key with the recipient's public key.

3. Compression

• Before encryption, the message alongwith signature is compressed. Compression of message saves space and ease of transmission. PGP makes use of a compression package called ZIP. Another algorithm lampd-ZIV LZ77 is also used in zip compression scheme.

- By Default PGP compresses the email message after applying the signature but before encryption. This is to allow for long-term storage of uncompressed messages along with their signatures. This also decouples the encryption algorithm from the message verification procedures.
- Compression is achieved with the ZIP algorithm.

4. E-mail compatibility

- PGP encrypts the block of transmitted message. Some system uses ASCII text, PGP converts it into raw 8-bit binary stream to a stream of printable ASCII characters. The scheme is called radix-64 conversion.
- After receiving, the incoming data is converted into binary by radix-64. Then the encrypted message is recovered by using session key and then decompressed.
- Since encryption, even when it is limited to the signature, results in arbitrary binary strings, and since many email systems only permit the use of ASCII characters, we have to be able to represent binary data with ASCII strings.
- PGP uses radix-64 encoding for this purpose.
- Radix-64 encoding, also known as Base-64 encoding has emerged as probably the most common way to transmit binary data over a network. It first segments the binary stream of bytes (the same thing as bytes) into 6-bit words.
- The 2^6 = 64 different possible 6-bit words are represented by printable characters as follows : The first 26 are mapped to the uppercase letters A through Z, the next 26 to the lowercase a through z, the next 10 to the digits 0 through 9, and the last two to the characters / and +. This causes each triple of adjoining bytes to be mapped into four ASCII characters.
- The Base-64 character set includes a 65^{th} character, '=', to indicate how many characters the binary string is short of being an exact multiple of 3 bytes. When the binary string is short one byte, that is indicated by terminating the Base-64 string with a single '='. And when it is short two bytes, the termination becomes '=='.

5. Segmentation and reassembly

- The length of E-mail is usually restricted to 50,000 octecks. Longer messages are broken-up into smaller segments and mailed separately.
- PGP provides subdivision of messages and reassembly at the receiving end.
- Fig. 5.6.5 shows transmission of PGP messages

Transmission of PGP message

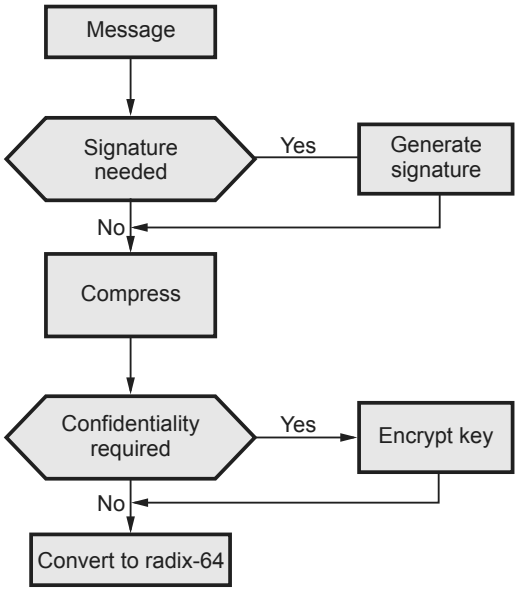


Fig. 5.6.5 Transmission of PGP message

Reception of PGP message

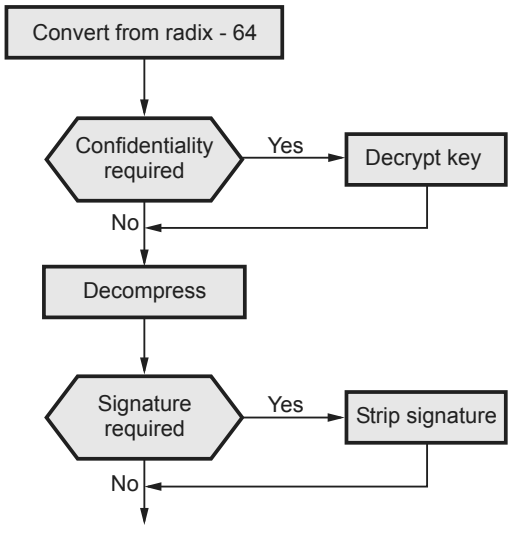


Fig. 5.6.6 Reception of PGP message

5.6.2 S/MIME

- S/MIME is a Secure / Multipurpose Internet Mail Extension. It is a security enthancement to the MIME Internet e-mail format standard.
- RFC 822 defines a format for text messages that are sent using electronic mail. The RFC 822 standard applies only to the contents.
- MIME is an extension to the RFC 822 framework that is intended to address some of the problems and limitations of the use of SMTP.
- **SMTP limitations**
  1. SMTP cannot transmit executable files or binary objects.
  2. SMTP cannot transmit text data that includes national language characters.
  3. SMTP servers may reject mail message over a certain size.
  4. SMTP gateways to X.400 electronic mail networks cannot handle nontextual data included in X.400 messages.
  5. SMTP gateways that translate between ASCII and the character code EBCDIC do not use a consistent set of mappings, resulting in translation problems.

5.6.2.1 Multipurpose Internet Mail Extensions

- MIME is a supplementary protocol that allows non-ASCII data to be sent through SMTP.
- MIME defined by IETF to allow transmission of non-ASCII data via e-mail.
- It allows arbitary data to be encoded in ASCII for normal transmission.
- All media types that are sent or received over the world wide web (www) are encoded using different MIME types.
- Messages sent using MIME encoding include information that describes the type of data and the encoding that was used.
- RFC822 specifies the exact format for mail header lines as well as their semantic interpretations.
- Fig. 5.6.7 shows the working of MIME.
- MIME define five headers.
  1. MIME - Version
  2. Content - Type
  3. Content - Transfer - Encoding
  4. Content - Id
  5. Content - Description

Mail Message Header

- From : iresh@e-mail.com
- To : rupali@sinhgad.edu
- MIME - Version : 1.0
- Content - Type : image/gif
- Content - Transfer - Encoding : base64

..... data for the image .....

....

....

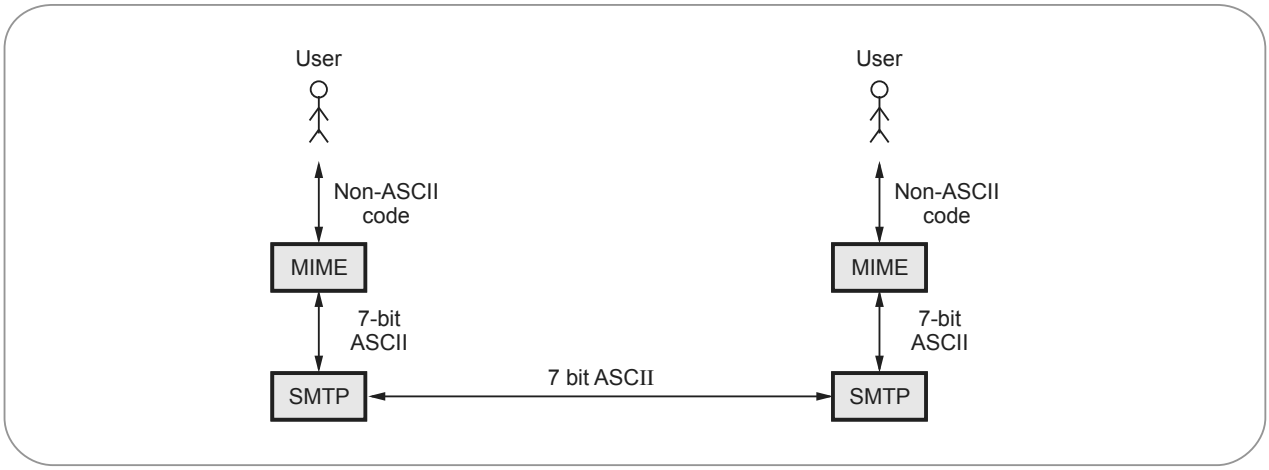


Fig. 5.6.7 MIME

MIME Types and Subtypes

- Each MIME content - type must contain two identifiers :
  - Content type
  - Content subtype
- There are seven standardized content-types that can appear in a MIME content - type declaration.

Type	Subtype	Description
Text	Plain	Unformatted text
Multipart	Mixed	Body contains ordered parts of different data types
	Parallel	Same as above, but no order
	Digest	Similar to mixed, but the default is message
	Alternative	Parts are different versions of the same message
Video	MPEG	Video is in MPEG format
Audio	Basic	Single channel encoding of voice at 8 kHz. (Sound file)
Image	JPEG	Image is in JPGE format
	GIF	Image is in GIF
Message	Partial and external body	An entire e-mail message or an external reference to a message
Application	Postscript	Adobe postscript
	Octet stream	General binary data

Content - Transfer Encoding

- This header defines the method to encode the messages into 0 and 1 for transport.

Content-Transfer-Encoding : < Type >

The five types of encoding is listed below.

Type	Description
7 bit	ASCII characters and short lines.
8 bit	Non-ASCII characters and short lines.
Binary	Non-ASCII characters with unlimited length lines.
Base 64	6 bit blocks of data are encoded into 8 bit ASCII characters.
Quoted printable	Non-ASCII characters are encoded as an equal sign followed by an ASCII code.

Mail Message Format

- SMTP requires all data to be 7-bit ASCII characters and all non-ASCII data must be encoded as ASCII strings.
- Additional lines in the message header declare MIME content type.

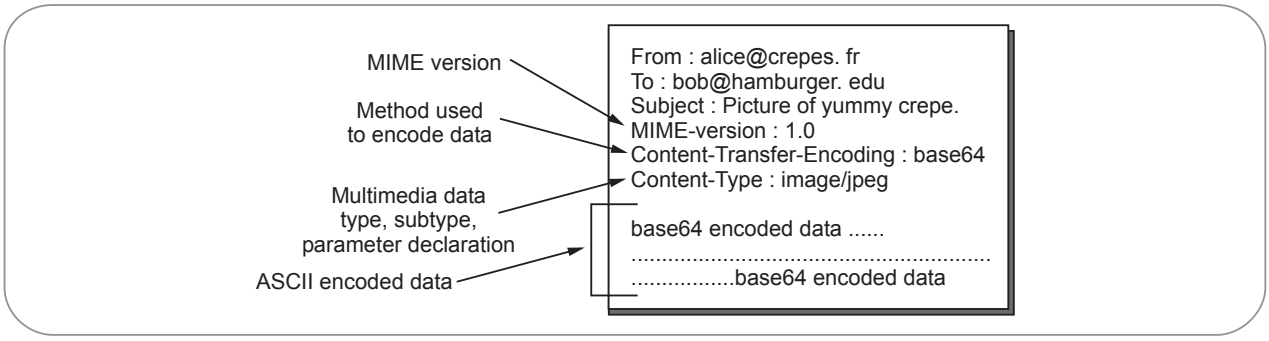


Fig. 5.6.8

5.6.2.2 Message Headers

- The message headers include the addresses of the receiver and the sender. Each header consists of the type of header, a colon, and the content of the header. Following is the sample of the complete header for a message.

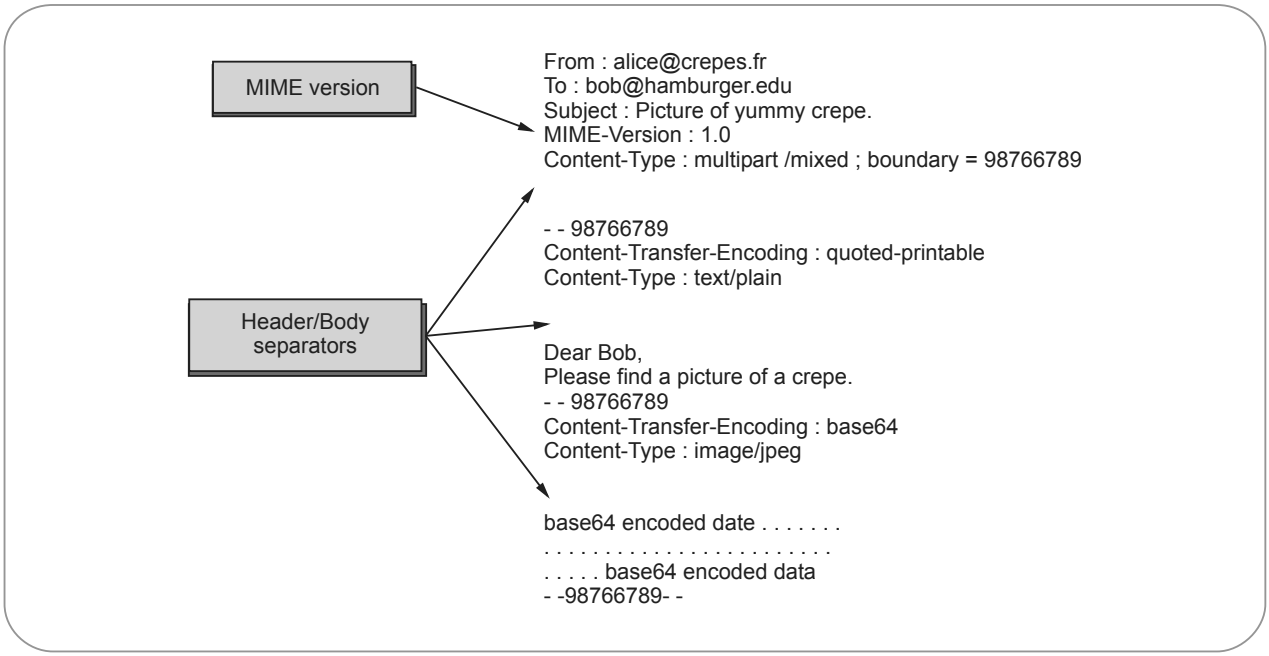


Fig. 5.6.9

Multipart Type

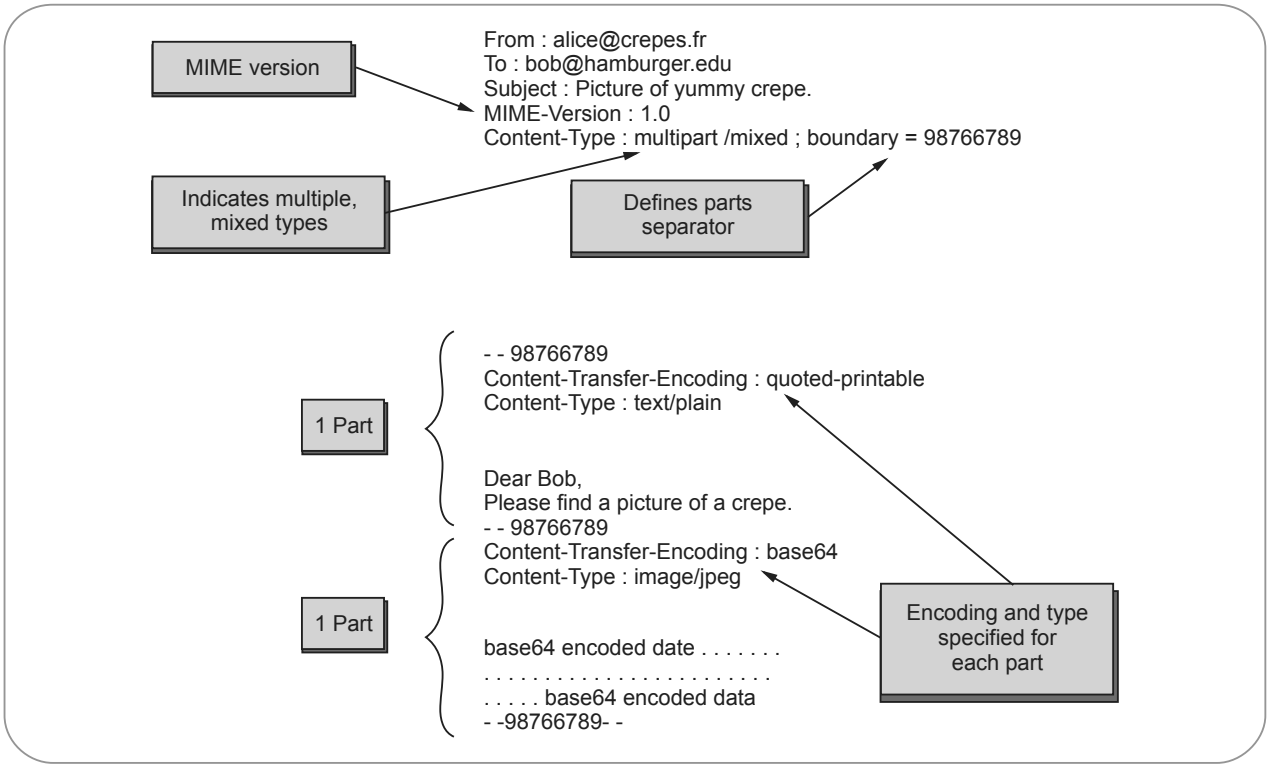


Fig. 5.6.10

5.6.2.3 S/MIME Functionality

- **Functions** are as follows
  1. Enveloped data
  2. Signed data
  3. Clear signed data
  4. Signed and enveloped data
- **Enveloped data** consists of encrypted content of any type and encrypted content encryption keys for one or more recipients.
- A **singed data** message can only be viewed by a recipient with S/MIME capability. Base64 encoding method is used for encoding content and signature.
- In **clear signed data**, a digital signature of the content is formed. Here only the digital signature is encoded using base64. Recipients without S/MIME capability can view the message content, although they cannot verity the signature.
- **Signed and enveloped data :** Signed only and encrypted only entities may be nested, so that encrypted data may be signed and signed data or clear signed data may be encrypted.

5.6.3 Privacy Enhanced Mail (PEM)

- Primary goal of PEM is to add security services for e-mail users in the internet community. Began in 1985 as an activity of the Privacy and Security Research Group (PSRG) and defined in RFCs 1421/1422/1423/1424.

- It consists of extensions to existing message processing software plus a key management infrastructure.
- Developed by IETF, to add encryption, source authentication and integrity protection to e-mail. Allows both public and secret long-term keys and message key is always symmetric. It also specifies a detailed certification hierarchy.
- Uses symmetric cryptoraphy to provide (optional) encryption of messages.
- The use of X.509 certificates is the base for public key management in PEM.
- This certification hierarchy supports universal authentication of PEM users.
- PEM can be used in a wider range of messaging environments. PEM represents a major effort to provide security for an application that touches a vast number of users within the Internet and beyond.
- PEM was designed to have backward compatibility with existing mail system.
- PEM depends on a successful establishment of the certification hierarchy that underlies asymmetric key management.
- **Problem :** PEM does not support security services to multimedia files (MIME)

PEM Security Services

1. Integrity, which ensures a message recipient that the message has not been modified en route.
2. Authenticity, which ensures a message recipient that a message was sent by the indicated originator.
3. Non-repudiation, which allows a message to be forwarded to a third party, who can verify the identity of the originator.
4. Confidentiality (optional), which ensures a message originator that the message text will be disclosed only to the desingated recipients.

PEM Message Processing

Step 1 :

- Uses the canonicalization specified by SMTP to ensure a uniform presentation syntax among a heterogeneous collection of computer systems.
- The shortcoming is that it restricts the input to 7-bit ASCII.
- The reason is that the Internet e-mail imposes the same restrictions.

Step 2 :

- A MIC is calculated over the canonicalized message to permit uniform verification in the heterogeneous environments.
- The cannonical (padded as required) message text is then (optionally) encrypted using a per-message symmetric key.
- The encryption action is performed only if the message is of type ENCRYPTED.

Step 3 :

- Renders an ENCRYPTED or MIC-ONLY message into a printable form suitable for transmission via SMTP.
- This encoding step transforms the (optionally encrypted) message text into a restricted 6-bit alphabet.
- A MIC-CLEAR messages are not subject to any portion of the third processing step.

PEM Message Types

- ENCRYPTED is a signed, encrypted and encoded (in step 3) message.
- MIC-ONLY is a signed, but not encrypted, encoded message.
- MIC-ONLY is a signed, but not encrypted, and message that is not encoded.
- Specially so it can be sent to a mixed set of recipients, some of whom use PEM and some do not.

PEM Message Delivery Processing (1)

- Recipient receives a PEM message.
- Scans the PEM header for the version and the type (ENCRYPTED, MIC-ONLY, MIC-CLEAR).

- If ENCRYPTED or MIC-ONLY then decode the 6-bit encoding back to ciphertext or canonical plaintext form.
- If ENCRYPTED then decrypt the symmetric message key using the private component of his public key pair and decrypt the message using the symmetric message key.
- Validate the public key of the sender by validating a chain of certificates.
- Validate the digital signature using the public component of the public key of the sender.
- The canonical form is translated into the local representation and presented to the recipient.

5.6.4 SMTP

- Simple mail transfer protocol is a popular network services in Email communication.
- Simple mail transfer protocol is system for sending messages to other computer users based on email.
- Simple mail transfer protocol is request response based activity.
- Simple mail transfer protocol also provides email exchange process.
- Simple mail transfer protocol attempts to provide reliable service but not guarantees to sure recovery from failure.

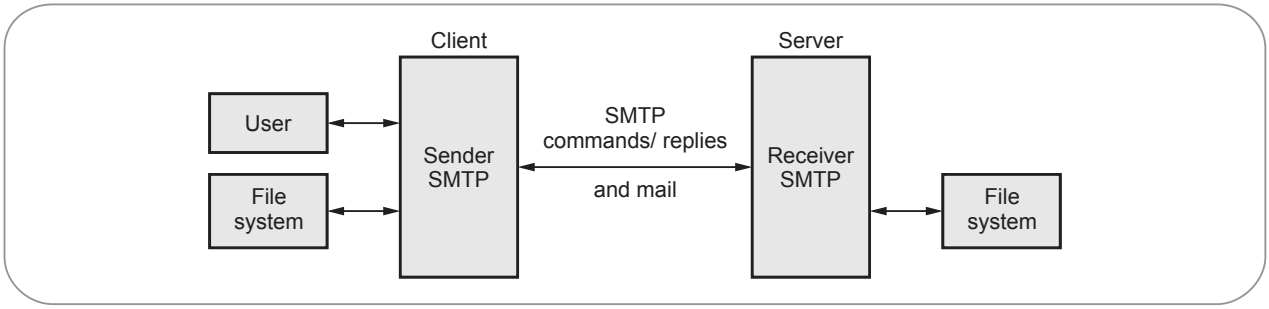


Fig. 5.6.11

Board Questions

1. *Describe PGP with reference to email security.* **MSBTE : Summer-15, Marks 4**
2. *Explain working of PGP email security.* **MSBTE : Winter-15, Marks 4**
3. *What is PGP ? How PGP is used for eamail security ?* **MSBTE : Summer-16, Marks 8**
4. *Explain e-mail security techniques (protocols).* **MSBTE : Winter-16, 17, Marks 4**
5. *Describe PGP with suitable diagram.* **MSBTE : Summer-17, Marks 4**
6. *Describe the working of PEM e-mail security and PGP with reference to e-mail security.* **MSBTE : Summer-18, Marks 8**
7. *What is PGP ? How PGP is used for email security ?* **MSBTE : Winter-18, Marks 4**
8. *Explain working principle of PGP.* **MSBTE : Summer-19, Marks 4**

5.7 Public Key Infrastructure (PKI)

- Management and handling of the pieces of secret information is generally referred to as **key management.**
- Activities of key management includes selection, exchange, storage, certification, revocation, changing, expiration and transmission of the key.

- Key management is the set of processes and mechanisms which support key establishment and maintenance of ongoing keying relationship between parties, including replacing older key with new keys.
- Two major issues in key management are :
  1. Key life time 2. Key exposure

Key life time - limit of use which can be measured as a duration of time.

Issue related to key :

1. Users must be able to obtain securely a key pair suited to their efficiency and security needs.
2. Keys need to be valid only until a specified expiration date.
3. The expiration date must be chosen properly and publicized securely.
4. User must be able to store their private keys securely.
5. Certificates must be unforgettable, obtainable in a secure manner.

1. Public Key Infrastructure

- Public Key Infrastructure (PKI) is a well-known technology that can be used to establish identities, encrypt information and digitally sign documents.
- PKI identifies and manages relationships of parties in an electronic exchange, serving a wide array of security needs including access control, confidentiality, integrity, authentication and non-repudiation.
- PKI also uses unique Digital Certificates (DC) to secure eCommerce, email, data exchange and Virtual Private Networks (VPN) and intranets and is also used to verify the identity and privileges of each user.
- The Certificate Authority (CA) provides a full life-cycle management of public keys and certificates, including issuance, authentication, storage, retrieval, backup, recovery, updating and revocation to the PKI.
- All users of PKI must have a registered identity, which is stored in a digital certificate issued by a CA.
- Remote users and sites using public private keys and public key certificates can authenticate each other with a high degree of confidence.
- Authentication is dependent on three conditions :
  1. It must be established that each party have a private key that has not been stolen or copied from the owner.
  2. The certificate must be issued to the owner in accord with the stated policy of the certificate issuer.
  3. The policies of the certificate issuer must be satisfactory to the parties so as to verify identity.

5.7.1 Benefits of PKI

1. **Confidential communication :** Only intended recipients can read files.
2. **Data integrity :** Guarantees files are unaltered during transmission.
3. **Authentication :** Ensures that parties involved are who they claim to be.
4. **Non-repudiation :** Prevents individuals from denying.

5.7.2 Limitation of PKI

The problems encountered deploying a PKI can be categorized as follows :

1. Public key infrastructure is new
2. Lack of standards
3. Shortage of trained personnel
4. Public key infrastructure is mostly about policies.

5.7.3 Certificate and Certificate Authority

- **Certificates** are digital documents that are used for secure authentication of communicating parties.
- A certificate binds identity information about an entity to the entity's public key for a certain validity period.
- A certificate is digitally signed by a Trusted Third Party (TTP) who has verified that the key pair actually belongs to the entity.
- Certificates can be thought of as analogous to passports that guarantee the identity of their bearers.

- **Authorities :** The trusted party who issues certificates to the identified end entities is called a **Certification Authority (CA).**
- Certification authorities can be thought of as being analogous to governments issuing passports for their citizens.
- A certification authority can be managed by an external certification service provider or the CA can belong to the same organization as the end entities.
- CAs can also issue certificates to other (sub) CAs. This leads to a tree-like **certification hierarchy.**
- The highest trusted CA in the tree is called a root CA.
- In large organizations, it may be appropriate to delegate the responsibility for issuing certificates to several different certificate authorities.
- For example, the number of certificates required may be too large for a single CA to maintain; different organizational units may have different policy requirements; or it may be important for a CA to be physically located in the same geographic area as the people to whom it is issuing certificates.
- The X.509 standard includes a model for setting up a hierarchy of the certification authority.
- Fig. 5.7.1 shows the hierarchy of certificate authorities.

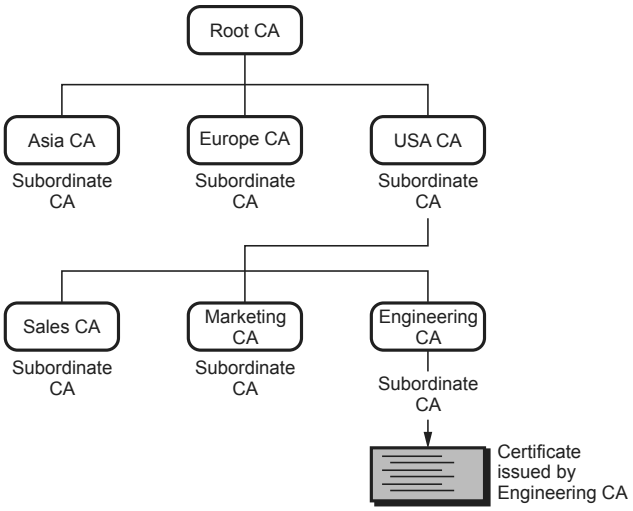


Fig. 5.7.1 Hierarchy of CA

- In the Fig. 5.7.1, the root CA is at the top of the hierarchy. The root CA's certificate is a self-signed certificate : That is, the certificate is digitally signed by the same entity.
- The CAs, that are directly subordinate to the root CA, have CA certificates signed by the root CA. CAs under the subordinate CAs in the hierarchy have their CA certificates signed by the higher-level subordinate CAs.
- Organizations have a great deal of flexibility in terms of the way they set up their CA hierarchies.
- **Certificate chains :** Certificate chain is series of certificates issued by successive CAs.
- In some cases, a CA can delegate the actual identification of end entities as well as some other administrative tasks to a separate entity, the **Registration Authority (RA).**

5.7.4 Verifying Certificates

- When authentication is required, the entity presents a signatures it has generated from authentication data using its private key, and a certificate corresponding to that key.
- The receiving entity can verify the signature with the public key of the sender contained in the certificate.
- Next the receiving entity must verify the certificate itself by checking the validity time of the certificate and the signature of the CA in the certificate.
- If the CA is a sub CA, the receiving entity must also verify the signatures of all higher-level CAs up to the root CA.
- The list of certificates needed for verification is called a **certification path.**
- If all signatures are valid and the receiving entity trusts the root CA, the first entity will be authenticated successfully.
- If a private key of an end entity is compromised or the right to authenticate with a certificate is lost before its natural expiration date, the CA must revoke the certificate and inform all PKI users about this.
- The CA will periodically publish a **Certificate Revocation List (CRL)**.
- The CRL is a list identifying the revoked certificates and it is signed by the CA.
- The end entities should check the latest CRL whenever they are verifying a validity of a certificate.

5.7.5 Key Length and Encryption Strength

- The strength of encryption depends on both the cipher used and the length of the key.
- Encryption strength is often described in terms of the size of the keys used to perform the encryption : In general, longer keys provide stronger encryption.
- Key length is measured in bits. For example, 128-bit keys for use with the RC4 symmetric-key cipher supported by SSL provide significantly better cryptographic protection than 40-bit keys for use with the same cipher.
- Roughly speaking, 128-bit RC4 encryption is 3×10^{26} times stronger than 40-bit RC4 encryption.
- Different ciphers may require different key lengths to achieve the same level of encryption strength.
- The RSA cipher used for public-key encryption, for example, can use only a subset of all possible values for a key of a given length, due to the nature of the mathematical problem on which it is based.
- Other ciphers, such as those used for symmetric key encryption, can use all possible values for a key of a given length, rather than a subset of those values.
- Thus a 128-bit key for use with a symmetric key encryption cipher would provide stronger encryption than a 128-bit key for use with the RSA public-key encryption cipher.

5.8 X.509 Certificate

- X.509 is part of X.500 recommendations for directory service i.e. set of servers which maintains a database of information about users and other attributes.
- X.509 defines authentication services e.g. certificate structure and authentication protocols. Also X.509 also defines alternative authentication protocols base on use of public-key certificates. The X.509 certificate format is emplied in S/MIME, IP security, SET and SSL/TLS.
- X.509 standard uses RSA algorithm and hash function for digital signature. Fig. 5.8.1 shows generation of public key certificate.

5.8.1 X.509 Format of Certificate

- The current version of the standard is version 3, called as X.509V3. The general format of digital certificate X.509V3 is shown in Fig. 5.8.2.

1	Version
2	Certificate Serial Number
3	Signature Algorithm Identifier
4	Issuer Name
5	Period of Validity
6	Subject Name
7	Subject's Public Key Info.
8	Issuer Unique Identifier
9	Subject Unique Identifier
10	Extensions
11	Signature

Fig. 5.8.2 X.509 Digital certificate format version 3

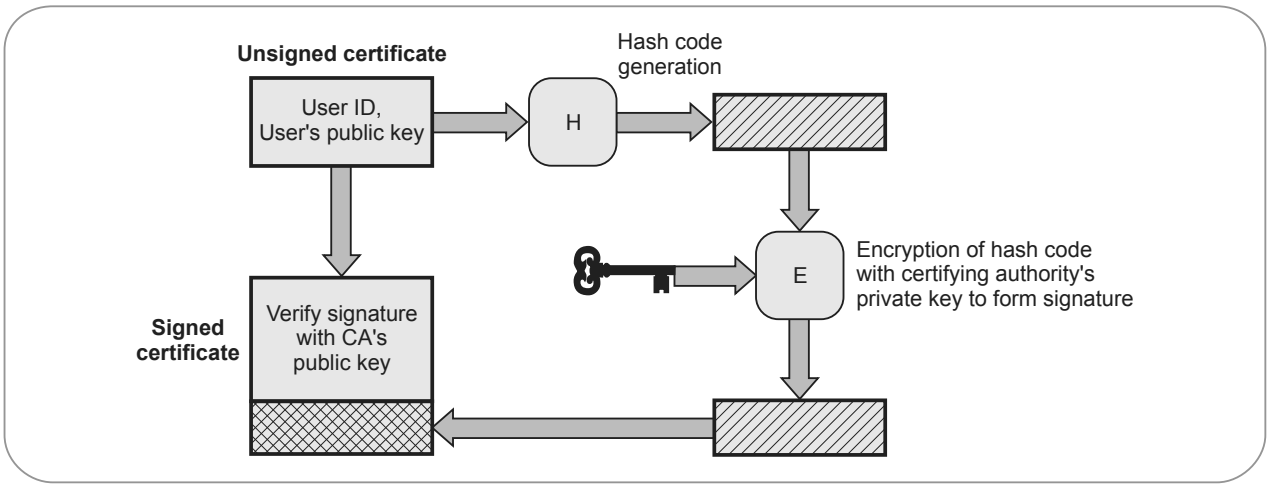


Fig. 5.8.1 Public key certificate

1. **Version** : Identifies successive versions of certificate format the default is version.
2. **Certificate Serial Number** : It contains an unique integer number, which is generated by Certification Authority (CA).
3. **Signature Algorithm Identifier** : Identifies the algorithm used by the CA to sign the certificate.
4. **Issuer Name** : Identifies the distinguished name of the CA that created and signed this certificate.
5. **Period of Validity** : Consists of two date-time values (not before and not after) within which the certificate is valid.
6. **Subject Name** : It specifies the name of the user to whom this certificate is issued.
7. **Subject's Public Key Information** : It contains public key of the subject and algorithms related to that key.
8. **Issuer Unique Identifier** : It is an optional field which helps to identify a CA uniquely if two or more CAs have used the same Issuer Name.
9. **Subject Unique Identifier** : It is an optional field which helps to identify a subject uniquely if two or more subjects have used the same Subject Name.
10. **Extensions** : One or more fields used in version 3. These extensions convey additional information about the subject and issuer keys.
11. **Signature :** It contains hash code of the fields, encrypted with the CA's private key. It includes the signature algorithm identifier.

Standard notations for defining a certificate

$$CA\langle\langle A\rangle\rangle = CA\{V, SN, AI, CA, T_A A, A_P\}$$

where,

CA<<A>> indicates the certificate of user A issued by certification authority CA.

CA{V..... A_P} indicates signing of V.....A_P by CA.

5.9 Cyber Crime

- Cybercriminals may use computer technology to access personal information, business trade secrets, or use the Internet for exploitive or malicious purposes.
- Criminals can also use computers for communication and document or data storage. Criminals who perform these illegal activities are often referred to as hackers.
- Cybercrime may also be referred to as computer crime. A **cybercriminal** is an individual who commits cybercrimes, where he/she makes use of the computer either as a tool or as a target or as both.
- The Department of Justice categorizes computer crime in three ways:
  1. The computer as a target : Attacking of other computers. For example, spreading viruses in the computer.
  2. The computer is used like a weapon : Using a computer to commit "traditional crime" that like in the physical world. For example, it is like fraud or illegal gambling.
  3. The computer as an accessory : Using a computer as a "fancy filing cabinet" to store illegal or stolen information.
- Cybercrime requires no physical contact with victims. They can be located anywhere in the world. This both reduces the chances of being caught and makes it very difficult for law enforcement to fingerprint a cybercriminal.
- It also greatly increases the potential number of victims of an attack and the return on investment.

Reasons for success of cyber criminals

- Today's cyber security paradigm is a reactive cycle : when a threat is exposed, it is analyzed and a counter-solution is designed with response times varying from weeks to years.
- The trouble is that attackers can easily reuse pieces of previous malware, modify them, and create a brand new threat, bypassing the newly updated security measures.
- Attackers can simply copy pieces of code from previous malware, such as exploits, decryptors or modules (keyloggers, backdoors etc.), and incorporate them into the new malware they are developing.

- Alternatively, attackers can imitate the operational methods performed by other malware, needed for the success of the operation.
- Cybercriminals often work in organized groups. They are as follows :
  1. **Programmers :** Write code or programs used by cybercriminal organization
  2. **Distributors :** Distribute and sell stolen data and goods from associated cybercriminals
  3. **IT experts :** Maintain a cybercriminal organization's IT infrastructure, such as servers, encryption technologies and databases
  4. **Hackers :** Exploit systems, applications and network vulnerabilities
  5. **Fraudsters :** Create and deploy schemes like spam and phishing
  6. **System hosts and providers :** Host sites and servers that possess illegal contents
  7. **Cashiers :** Provide account names to cybercriminals and control drop accounts
- There are many reasons why cyber-criminals are doing cyber-crime. Some of the reasons are given below :
  1. Difficulty in personal identification
  2. For the sake of recognition.
  3. For earning quick money.
  4. Low marginal cost of online activity due to global reach.
  5. Start as hobby and then any reason.
  6. Catching by law and enforcement agency is less effective and more expensive.
  7. New opportunity to do legal acts using technical architecture.
  8. Official investigation and criminal prosecution is rare.

5.9.1 Types of Cyber Crimes

- There are many types of cyber crimes and the most common ones are explained below :

1. **Hacking :** This is a type of crime wherein a person's computer is broken into so that his personal or sensitive information can be accessed.
2. **Theft :** This crime occurs when a person violates copyrights and downloads music, movies, games and software.
3. **Cyberstalking :** This is a kind of online harassment wherein the victim is subjected to a barrage of online messages and emails.
4. **Identity Theft :** This has become a major problem with people using the Internet for cash transactions and banking services. In this cyber crime, a criminal accesses data about a person's bank account, credit cards, debit card and other sensitive information to siphon money or to buy things online in the victim's name.
5. **Malicious Software :** These are Internet-based software or programs that are used to disrupt a network. The software is used to gain access to a system to steal sensitive information or data or causing damage to software present in the system.
6. **Child soliciting and Abuse :** This is also a type of cyber crime wherein criminals solicit minors via chat rooms for the purpose of child pornography.

Example of Cyber Crime :

a. Online banking fraud
b. Fake antivirus
c. `Stranded traveler' scams
d. `Fake escrow' scams
e. Advanced fee fraud
f. Infringing pharmaceuticals
g. Copyright-infringing software
h. Copyright-infringing music and video
i. Online payment card fraud
j. In-person payment card fraud
k. Industrial cyber-espionage and extortion
l. Welfare fraud

- The trafficking, distribution, posting, and dissemination of obscene material including pornography, indecent exposure, and child pornography, constitutes one of the most important Cybercrimes known today.

- Stealing the significant information, data, account number, credit card number transmit the data from one place to another. Hacking and cracking are amongst the gravest Cybercrimes known till date.

5.9.2 Software Piracy

- Software piracy is the illegal copying, distribution, or use of software.
- Most retail programs are licensed for use at just one computer site or for use by only one user at any time. By buying the software, you become a licensed user rather than an owner
- Software piracy is such a profitable "business" that it has caught the attention of organized crime groups in a number of countries.
- Software piracy causes significant lost revenue for publishers, which in turn results in higher prices for the consumer.
- Software piracy applies mainly to full-function commercial software. The time-limited or function-restricted versions of commercial software called shareware are less likely to be pirated since they are freely available.
- Similarly, freeware, a type of software that is copyrighted but freely distributed at no charge.

Types of software piracy include :

1. **Soft-lifting :** Borrowing and installing a copy of a software application from a colleague.
2. **Client-server overuse :** Installing more copies of the software than you have licenses for.
3. **Hard-disk loading :** Installing and selling unauthorized copies of software on refurbished or new computers.
4. **Counterfeiting :** Duplicating and selling copyrighted programs.
5. **Online piracy :** Typically involves downloading illegal software from peer-to-peer network, Internet auction or blog. (In the past, the only place to download software was from a bulletin board system and these were limited to local areas because of long distance charges while online.)

5.9.3 Cybercrime Investigation Process

- Cybercrime investigation is done to determine the nature of crime and collect evidence e.g. hardware, software related with the crime.
- This is used to stop a crime in progress, report crime which was done in the past.
- Relevant IT training is necessary for Cybercrime investigation.
- First step of investigation team is to secure computers, networks & components that are connected with crime.
- Investigators may clone the system to explore it. They can take a detailed audit of a computer.
- **Interviews :** Investigators arrange interviews with victims, witness.
- **Surveillance :** Investigators checks the digital activities, monitors all elements of suspect.
- **Forensics :** Mining a computer for all related information to detect potential evidence.
- **Undercover :** Steps to uncover to trap criminals using fake online identities.
- Obtain a search warrant and seize the victims equipment
- Identify the victim's configuration.
- Acquire the evidence carefully.

Board Questions

1. *Explain cyber crime.* **MSBTE : Winter-15, Marks 4**
2. *Define cyber crime. List different types of cyber crimes.* **MSBTE : Summer-16, Marks 4**
3. *Describe pornography and software piracy related to Cyber crime.* **MSBTE : Winter-16, Marks 4**
4. *Describe the process of cyber crime investigation.* **MSBTE : Summer-17, Marks 4**
5. *What is pornography ?* **MSBTE : Summer-17, Marks 4**
6. *What is software piracy ?* **MSBTE : Winter-17, Marks 4**
7. *Explain Cyber crime.* **MSBTE : Winter-17, Marks 4**
8. *What is software piracy ?* **MSBTE : Winter-17, Marks 4**
9. *What is cyber crime ? Describe hacking and cracking related to cybercrime.* **MSBTE : Winter-18, Marks 4**

5.10 Cyber Laws

- The IT Act covers cyber laws and crimes, which are subject to the Indian Penal Code. Such cyber crimes include :
  - Crimes related to technical aspects, such as unauthorized access and hacking, trojan attack, virus and worm attack, email related attacks (email spoofing and email spamming, email bombing) and Denial Of Service attacks (DOS). DOS include :
  1. Consumption of limited or non-renewable resources like NW bandwidth and RAM, alteration or destruction of configuration information, destruction or alteration of network components, and pornography.
  2. Forgery
  3. IPR violations, which include software piracy, copyright infringement, trademark violations, etc. This also includes cyber terrorism, Banking and credit card related crimes, e-Commerce and investment frauds, sale of illegal articles, defamation.
  4. Cyber stacking, identity theft, data diddling, theft of internet hours.
  5. Breach of privacy and confidentiality.

5.10.1 Advantages of Cyber Law

- The IT Act 2000 attempts to change outdated laws and provides ways to deal with cyber crimes. Such laws are required so that people can perform purchase transactions over the Net through credit cards without fear of misuse. The Act offers the much-needed legal framework so that information is not denied legal effect, validity or enforceability, solely on the ground that it is in the form of electronic records.
- In view of the growth in transactions and communications carried out through electronic records, the Act seeks to empower government departments to accept filing, creating and retention of official documents in the digital format. The Act has also proposed a legal framework for the authentication and origin of electronic records / communications through digital signature.
  - From the perspective of e-commerce in India, the IT Act 2000 and its provisions contain many positive aspects. Firstly, the implications of these provisions for the e-businesses would be that email would now be a valid and legal form of communication in our country that can be duly produced and approved in a court of law.
  - Companies shall now be able to carry out electronic commerce using the legal infrastructure provided by the Act.
  - Digital signatures have been given legal validity and sanction in the Act.
  - The Act throws open the doors for the entry of corporate companies in the business of being Certifying Authorities for issuing Digital Signatures Certificates.
  - The Act now allows Government to issue notification on the web thus heralding e-governance.
  - The Act enables the companies to file any form, application or any other document with any office, authority, body or agency owned or controlled by the appropriate Government in electronic form by means of such electronic form as may be prescribed by the appropriate Government.
  - The IT Act also addresses the important issues of security, which are so critical to the success of electronic transactions. The Act has given a legal definition to the concept of secure digital signatures that would be required to have been passed through a system of a security procedure, as stipulated by the Government at a later date.
  - Under the IT Act, 2000, it shall now be possible for corporates to have a statutory remedy in case if anyone breaks into their computer systems or network and causes damages or copies data. The remedy provided by the Act is in the form of monetary damages, not exceeding ₹ 1 crore.

5.11 Compliance Standards

- The International Organization for Standardization (ISO), established in 1947, is anon-governmental international body that collaborates with the International Electro technical Commission (IEC) and the International Telecommunication Union

(ITU) on Information and Communications Technology (ICT) standards.

- The following are commonly referenced ISO security standards :
  1. ISO / IEC 27002 : 2005 (Code of Practice for Information Security Management)
  2. ISO / IEC 27001 : 2005 (Information Security Management System - Requirements)
  3. ISO / IEC 15408 (Evaluation Criteria for IT Security)
  4. ISO / IEC 13335 (IT Security Management)

5.11.1 Information Security Management

5.11.1.1 Introduction

- As a model for information security, ISO 27001 is a generic standard designed for all sizes and types of organizations including governmental, non-governmental, and non-profit organizations. It requires the managing body of an organization to plan, implement, maintain and improve ISMS.
- The ISMS model ensures the selection of adequate security controls based on organizational objectives to protect all information assets, including both wire-line and wireless assets.
- ISO 27001 was published and came into effect on October 15, 2005.
- ISO 27001 covers all types of organizations. This international standard specifies the requirements for establishing; implementing, operating, monitoring, reviewing, maintaining and improving documented ISMS within the context of the organization's overall business risks. It specifies requirements for the implementation of security controls customized to the needs of individual organizations or parts thereof.
- The ISMS is designed to ensure the selection of adequate and proportionate security controls that protect information assets and give confidence to interested parties.
- ISO 27001 is not a mandatory law; it is more of a collection of "best practices" and "industry practice proven knowledge" related to ISMS. ISO 27001 is the formal standard against which organizations may seek independent certification of their ISMS. ISO 27001 is a "top down" information management approach.

History

- When British companies analyzed risks related to exchanging information and data with their customers and partners, they discovered that a lot of fraud and security breaches occurred due to the lack of control and auditing. This allowed for many security holes to go unnoticed until a fraud happened.
- Based on initiatives of British companies at the end the last century, the United Kingdom Government's Department of Trade and Industry (DTI) wrote the BS 7799 norm which was then published by the British Standards Institute (BSI) in 1995. The BS 7799 norm deals with the security of information systems.
- As time went by, it appeared that the BS 7799 and later the revised BS 7799-2 did not address everything that was needed, and so ISO 27001 was introduced in the year 2005. ISO 27001 is the successor to the previous BS 7799. ISO 27001 takes information security to the next level because in addition to approaches for securing information systems, ISO 27001 also addresses IT/IS auditing, management, and processes for continuous improvements.

5.11.2 Purpose of ISO 27001

- Every business is having its own management information system which generates required information report of business deals, project progress status and employee information.
- Any interruption in the quality, quantity, relevance and distribution of your information systems can put your business at risk from attack due to information is exposed to a growing number and a wider variety of threats and vulnerabilities.
- Significant incidents involving hacking, altering and misuse of information, online fraud thus losses continue to make the headlines and cause concerns for customers and consumers in general.
- Thus the critical business information must be actively managed to protect confidentiality, maintain integrity and ensure availability of those information assets to employee, clients, consumers, shareholders, authorities and society at large.

- A certified information security management system demonstrates commitment to the protection of information and provides confidence that assets are suitably protected, whether held on paper, electronically, or as employee knowledge.
- Implementation of information security management systems as per ISO 27001 gives a systematic approach to minimizing the risk of unauthorized access or loss of information and ensuring the effective deployment of protective measures for securing the same.
- It provides a framework for organizations to manage their compliance with legal and other requirements, and improve performance in managing information securely.

5.11.2.1 Clause

- ISO 27001 is divided into eleven complementary sections or clauses. It is also significant that each of the eleven sections / clauses is equally important as components of good security management. The eleven steps to good security management are :

Clause no.	Clause name	Remarks
1.	Security policy	Security policy, a top-level statement endorsed by the senior management team on which all security processes and procedures are subsequently based.
2.	Organization of information security	Organization of information security, a published security organization that shows clearly who is responsible for security and who is authorized to deal with security issues.
3.	Asset management	Asset management, a good understanding of what is important to the organization and where good security is important.
4.	Human resources security	Human resources security, careful recruiting and management of personnel employed in key positions.
5.	Physical and environmental security	Physical and environmental security, ensuring that the physical security precautions match the need expressed in the corporate policy.
6.	Communications and operations management	Communications and operations management, the provision of adequate tools and services to ensure that corporate information in these systems is properly monitored, managed and protected.
7.	Access control	Access control, close monitoring and control over who is authorized to read and to amend the organization's information especially within the information processing systems.
8.	Information systems acquisition, development and maintenance	Information systems acquisition, development and maintenance, the need to ensure that future development continues to meet and exceed the strength of protection in previous generations of production services.
9.	Information security incident management	Information security incident management is the process for managing any incident that may affect the well being of the organization.
10.	Business continuity management	Business continuity management is the ability to minimize the impact of major disasters on the business processes and requires comprehensive backup strategies to ensure that no corporate data is lost.
11.	Compliance	Compliance, the need to ensure that once good controls are put in place that they continue to work and to deliver the required level of protection to the organization's assets as well as meeting the legal and regulatory requirements for managing information.

Benefit of ISO 27001 at various level :

a. At the organizational level : Commitment

b. At the legal level : Compliance

c. At the operating level : Risk management

d. At the commercial level : Credibility and confidence

e. At the financial level : Reduced costs

f. At the human level : Improved employee awareness

- Fig. 5.11.1 shows the ISO PDCA model used to implement the ISMS; the PDCA model is sometimes referred to as an ISMS cycle. Use this model to develop, maintain, and continually improve the ISMS. The objective of implementing ISMS is to have an overall management system built in consideration of business risk to implement, operate, monitor, maintain, and improve information security.

5.11.3 PDCA Cycle

- The PDCA model is an internationally accepted model and followed by most well known standards and management systems. The PDCA model is also called the Deming Cycle after the founder Dr. W. Edwards Deming
- The standard introduces a cyclic model known as the "Plan-Do-Check-Act" (PDCA) model that aims to establish, implement, monitor and improve the effectiveness of an organization's ISMS.
- The PDCA cycle has these four phases :

  a) "Plan" phase : Establishing the ISMS

  b) "Do" phase : Implementing and operating the ISMS

  c) "Check" phase : Monitoring and reviewing the ISMS

  d) "Act" phase : Maintaining and improving the ISMS
- Fig. 5.11.1 shows the PDCA model for ISMS processes.

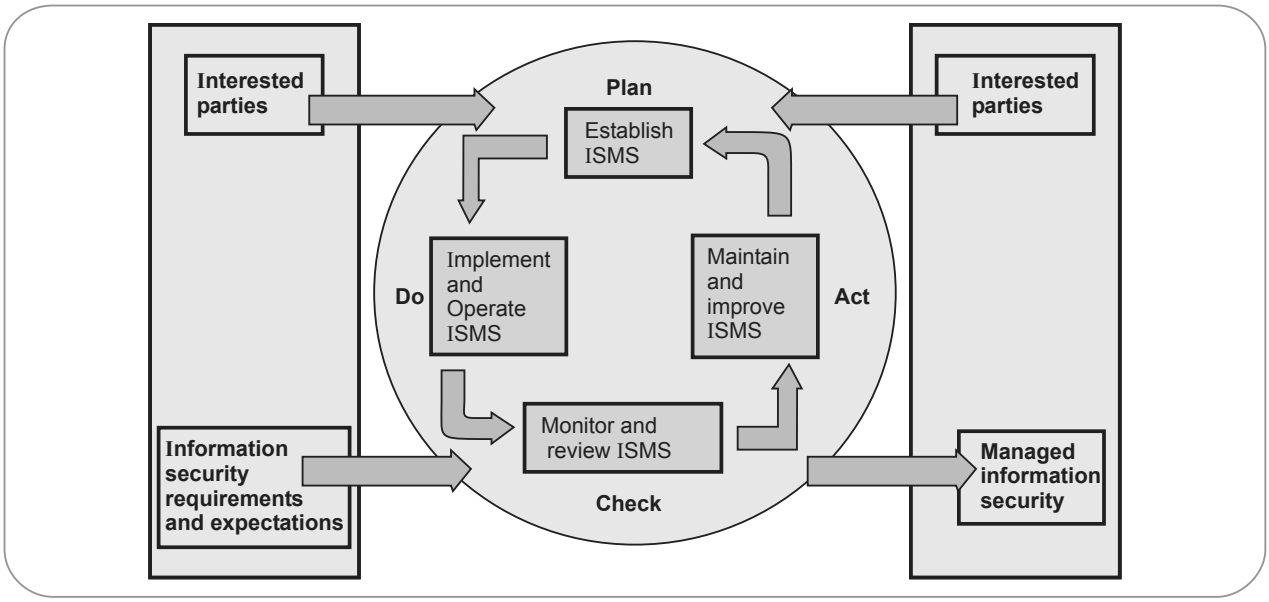


Fig. 5.11.1 PDCA model for ISMS process

No.	Phases	Operations
1.	**Plan**	Establish ISMS policy, objectives, processes and procedures relevant to managing risk and improving information security to deliver result in accordance with organizations overall policies and objective.
2.	**Do**	Implement and operate the ISMS policy, controls, processes and procedures.
3.	**Check**	Assess and where applicable, measure process performance against ISMS policy, objective and practical experience and report the result to management for review.
4.	**Act**	Take corrective and preventative actions, based on the results of the internal ISMS audit and management review or other relevant information to achieve continual improvement of the ISMS.

- There are well defined guidelines for each phase i.e. PLAN, DO, CHECK and ACT. This means that when you implement ISO 27001 you will be following a P-D-C-A approach. Let us look at the specific steps to be executed in each of the four phases.

PLAN phase

- In the PLAN phase, you will focus on establishing the ISMS. This consists of :
  1. Defining the scope of the ISMS.
  2. Defining the ISMS policy.
  3. Defining the risk assessment approach of the organization.
  4. Identifying the risks.
  5. Analyzing risk treatment options.
  6. Selecting control objectives and controls for treatment of risks.
  7. Obtaining management approval and authorization for risk treatment and residual risks.
  8. Preparing "Statement of Applicability".

DO phase

- In the DO phase, we will focus on implementing and operating the ISMS. This consists of,
  1. Defining and implementing a risk treatment plan.
  2. Selecting appropriate controls.
  3. Defining how to measure the effectiveness of the controls.
  4. Implementing training and awareness programs.
  5. Managing the operation of the ISMS.
  6. Managing the resources for operating the ISMS.
  7. Implementing security incident detection and response procedures.

CHECK phase

- CHECK phase consists of,
  1. Executing monitoring and reviewing procedures.
  2. Measuring the effectiveness of controls.
  3. Reviewing risk assessments and reviewing residual risks.
  4. Conducting internal ISMS audits.
  5. Undertaking management review of the ISMS.
  6. Updating security plans based on review and findings.
  7. Recording actions and events that may have an impact on the performance of the ISMS.

ACT phase

- ACT phase, which focuses on maintaining and improving the ISMS. The steps in this phase are :
  1. Implement the identified improvements in the ISMS.
  2. Taking appropriate corrective and preventive actions.
  3. Communicate the actions and improvements to all relevant parties.
  4. Ensure that the improvements achieve their intended objectives.

5.11.4 Certification

- Certification is achieved through a process of external audit. A number of bodies are approved for ISO 27001 audit work. As with any external certification, regular surveillance and re-certification audits are required to maintain the certification.
- An ISMS may be certified compliant with ISO/IEC 27001 by a number of accredited registrars worldwide. Certification against any of the recognized national variants of ISO/IEC 27001 by an

accredited certification body is functionally equivalent to certification against ISO/IEC 27001 itself.

- In some countries, the bodies that verify conformity of management systems to specified standards are called "certification bodies", in others they are commonly referred to as "registration bodies", "assessment and registration bodies", "certification/ registration bodies", and sometimes "registrars".
- The ISO/IEC 27001 certification, like other ISO management system certifications, usually involves a three-stage audit process :

1. **Stage 1 :** It is a preliminary, informal review of the ISMS, for example checking the existence and completeness of key documentation such as the organization's information security policy, Statement of Applicability (SoA) and Risk Treatment Plan (RTP). This stage serves to familiarize the auditors with the organization and vice versa.
2. **Stage 2 :** Stage 2 is a more detailed and formal compliance audit, independently testing the ISMS against the requirements specified in ISO/IEC 27001. The auditors will seek evidence to confirm that the management system has been properly designed and implemented, and is in fact in operation, for example by confirming that a security committee or similar management body meets regularly to oversee the ISMS. Certification audits are usually conducted by ISO/IEC 27001 lead auditors.
3. **Stage 3 :** Stage 3 involves follow-up reviews or audits to confirm that the organization remains in compliance with the standard. Certification requires periodic maintenance.

- If certification is a goal, analyze the specifications in ISO 27001 Sections 4 to 8, as these clauses are mandatory for certification. Sections 4 to 8 in the ISO 27001 standards are mandatory reading, as they describe how the organization should implement and construct its ISMS. In these sections, there are general requirements for the ISMS, including how to establish, manage, monitor, and maintain the ISMS.

Certification process for ISO 27001

- Certification India appoints a competent and suitable auditor or team of auditors to audit the organization against the standard and scope requested by the clients.
- Client has to file an application seeking standard for which to be certified. Gap analysis may be performed first to check readiness for the auditee organization which help organization to improve upon.
- Routine surveillance audits are carried out to evaluate continual improvement in the validity period. A re-certification audit is performed after every three years to maintain continuity of certification.

5.11.5 Benefits of ISO 27001

- Certifying your ISMS against ISO/IEC 27001 can bring the following benefits to your organization :
  a. Systematic identification of information security risks and its mitigation to reduce risk.
  b. Availability of internal controls and meets corporate governance and business continuity requirements in case of man made and natural disasters.
  c. Better protection of confidential data and reduced risks from hackers' attacks.
  d. Independently demonstration to compliance with legal and contractual requirements.
  e. Faster and easier recovery from the attacks and improved ability to survive disasters.
  f. Give proof to your customers and purchasers of the high level of security management.
  g. Staff members are well-informed and information security costs of your organization are managed.
  h. Internationally recognized and applicable to all sectors, giving you access to new markets across the world.
  i. Due to dependability of information and information systems, confidentiality, integrity and availability of information is essential to maintain competitive edge, cash-flow, profitability and commercial image.

j. Provide assurance to stakeholders such as shareholders, clients, consumers and suppliers.

k. Provide and enhanced customer confidence and satisfaction, which in turn can lead to increased business opportunities.

5.12 ISO 27001

- ISO/IEC 20000-1:2011 is a service management system (SMS) standard. It specifies requirements for the service provider to plan, establish, implement, operate, monitor, review, maintain and improve an SMS. The requirements include the design, transition, delivery and improvement of services to fulfil agreed service requirements.

ISO/IEC 20000-1:2011 can be used by :

- An organization seeking services from service providers and requiring assurance that their service requirements will be fulfilled;
- An organization that requires a consistent approach by all its service providers, including those in a supply chain;
- A service provider that intends to demonstrate its capability for the design, transition, delivery and improvement of services that fulfil service requirements;
- A service provider to monitor, measure and review its service management processes and services;
- A service provider to improve the design, transition, delivery and improvement of services through the effective implementation and operation of the SMS;
- An assessor or auditor as the criteria for a conformity assessment of a service provider's SMS to the requirements in ISO/IEC 20000-1:2011.

5.13 BS 25999

- BS 25999-2 was a British standard issued in 2007, and quickly became the main standard for business continuity management - it was superseded by ISO 22301 in 2012.
- Just like ISO 27001, ISO 9001, ISO 14001 and other standards that define management systems, BS 25999-2 also defines a business continuity management system which contains the same four management phases: planning, implementing, reviewing and monitoring, and finally, improving.
- The point of these four phases is that the system is continually updated and improved in order to be usable when a disaster occurs.
- The following are some of the key procedures and documents required by BS 25999-2:

1. Scope of the BCMS - Precise identification of that part of the organization to which business continuity management is applied.
2. BCM policy - Defining objectives, responsibilities, etc.
3. Human resources management.
4. Business impact analysis and risk assessment.
5. Defining business continuity strategy.
6. Business continuity plans.
7. Maintenance of plans and systems; improvement.

5.14 ITIL

- The ITIL (Information Technology Infrastructure Library) is a framework designed to standardize the selection, planning, delivery and maintenance of IT services within a business.
- The ITIL (Information Technology Infrastructure Library) has become the most effective standard in IT Service Management.
- ITIL helps organizations across industries offer their services in a quality-driven and cost-effective way.
- The framework was developed in the 1980s and the most recent update, ITIL 4 was published in February 2019.
- The goal is to improve efficiency and achieve predictable service delivery. The ITIL framework enables IT administrators to be a business service partner, rather than just back-end support.
- ITIL guidelines and best practices align IT department actions and expenses to business needs and change them as the business grows or shifts direction.

5.15 COBIT Framework

- COBIT is an IT management framework developed by the ISACA to help businesses develop, organize and implement strategies around information management and governance.
- First released in 1996, COBIT (Control Objectives for Information and Related Technologies) was initially designed as a set of IT control objectives to help the financial audit community better navigate the growth of IT environments.
- In 1998, the ISACA released version 2, which expanded the framework to apply outside the auditing community.
- Later, in the 2000s, the ISACA developed version 3, which brought in the IT management and information governance techniques found in the framework today.
- COBIT 4 was released in 2005, followed by COBIT 4.1 in 2007. These updates included more information regarding governance surrounding information and communication technology.
- In 2012, COBIT 5 was released and in 2013, the ISACA released an add-on to COBIT 5, which included more information for businesses regarding risk management and information governance.
- The ISACA announced an updated version of COBIT in 2018, ditching the version number and naming it COBIT 2019. This updated version of COBIT is designed to constantly evolve with "more frequent and fluid updates," according to the ISACA.
- COBIT 2019 was introduced to build governance strategies that are more flexible, collaborative and address new and changing technology.

❑❑❑

Notes

SOLVED SAMPLE TEST PAPER - I

Network and Information Security

T.Y. Diploma (Sem - VI) Elective - II

Computer Engg. Program Group (CO/CM/IF/CW)

Time : 1 Hour] **[Total Marks : 20**

Instructions :

1) All questions are compulsory.

2) Illustrate your answers with neat sketches whenever necessary.

3) Figures to the right indicate full marks.

4) Assume suitable data, if necessary.

5) Preferably write the answers in sequential order.

Q.1 Attempt any FOUR. **[8]**

a) *Compare passive attack and active attack.* **(Refer section 1.5.3)**

b) *What is information ?* **(Refer section 1.7)**

c) *Define entity authentication.* **(Refer section 2.1)**

d) *What is cryptology ?* **(Refer section 3.1)**

e) *List the advantages of hill cipher.* **(Refer section 3.2.4)**

f) *Define trojan horse.* **(Refer section 1.4.4)**

Q.2 Attempt any THREE. **[12]**

a) *Explain advantages and disadvantages of symmetric cryptography.* **(Refer sections 3.5.1 and 3.5.2)**

b) *Describe the process of biometric authentication with neat labelled diagram.* **(Refer section 2.3)**

c) *What is risk ? How it can be analyzed ?.* **(Refer section 1.3)**

d) *Describe the application patch and hotfix.* **(Refer section 1.6)**

e) *What is denial of service attack ? Explain in details.* **(Refer section 1.5.1)**

f) *Describe digital signature mechanism with neat diagram.* **(Refer section 3.10)**

❑❑❑

SOLVED SAMPLE TEST PAPER - II

Network and Information Security

T.Y. Diploma (Sem - VI) Elective - II

Computer Engg. Program Group (CO/CM/IF/CW)

Time : 1 Hour] **[Total Marks : 20**

Instructions :

1) All questions are compulsory.

2) Illustrate your answers with neat sketches whenever necessary.

3) Figures to the right indicate full marks.

4) Assume suitable data, if necessary.

5) Preferably write the answers in sequential order.

Q.1 Attempt any FOUR. **[8]**

a) *State functions and need of firewall.* **(Refer section 4.1.1)**

b) *What is DMZ ?* **(Refer section 4.2.1)**

c) *Describe term IDS.* **(Refer section 4.3.1)**

d) *Wht is kerberos ?* **(Refer section 5.1.1)**

e) *Explain SMTP.* **(Refer section 5.6.4)**

f) *What is cyber crime ?* **(Refer section 5.9)**

Q.2 Attempt any THREE. **[12]**

a) *Explain characteristics, working, design principles and limitations of firewall.* **(Refer section 4.1)**

b) *Describe DMZ with suitable example.* **(Refer section 4.2)**

c) *Describe Host based IDS with its advantages and disadvantages.* **(Refer section 4.3.3)**

d) *Explain the kerberos with help of suitable diagram.* **(Refer section 5.1)**

e) *Explain IPSec security with help of diagram.* **(Refer section 5.2)**

f) *Give IP sec configuration. Describe AH and ESP modes of IPSEC.* **(Refer section 5.4)**

❑❑❑

SOLVED SAMPLE QUESTION PAPER

Network and Information Security

T.Y. Diploma (Sem - VI) Elective - II

Computer Engg. Program Group (CO/CM/IF/CW)

Time : 3 Hours] **[Total Marks : 70**

Instructions :

1) All questions are compulsory.

2) Answr each next main Question on a new page.

3) Illustrate your answers with neat sketches whenever necessary.

4) Assume suitable data, if necessary.

5) Use of Non-programmable Electronic Pocket Calculate is permissible.

6) Mobile Phone, Pager and any other Electronic Communication devices are not permissible in Examination Hall.

7) Preferably write the answers in sequential order.

Q.1 Attempt any Five of the following **[10]**

a) *Define virus. List the phases of virus.* **(Refer section 1.4.1)**

b) *Define dumpster diving.* **(Refer section 2.2.3)**

c) *What is black and grey hat hackers ?* **(Refer section 1.5.10)**

d) *What is substitution cipher ?* **(Refer section 3.2)**

e) *State limitations of firewall.* **(Refer section 4.1.4)**

f) *Compare packet filter and proxies.* **(Refer section 4.1.3.4)**

g) *Compare AH and ESP.* **(Refer section 5.5.4)**

Q.2 Attempt any THREE of the following **[12]**

a) *What is CIA of security ? Descirbe in brief.* **(Refer section 1.1.2)**

b) *Describe the process of biometric authentication with neat labelled diagram.* **(Refer section 2.3)**

c) *With the help of neat diagram describe host based intrusion detection system.* **(Refer section 4.3.3)**

d) *Describe the application patch and hotfix.* **(Refer section 1.6)**

Q.3 Attempt any THREE of the following **[12]**

a) *Convert plan text to cipher text using Rail Fence Technique "COMPUTER SECURITY"* **(Refer example 3.3.5)**

b) *What is sniffing ? How to protect from sniffers ?.***(Refer section 1.5.8)**

c) *With neat sketch explain the working of network Based IDS.* **(Refer section 4.3.4)**

d) *Compare symmetric and asymmetric key cryptography.***(Refer section 3.9.2)**

Q.4 Attempt any THREE of the following **[12]**

a) *What is Kerberos ? Explain with diagram different servers involved in Kerberos.* **(Refer section 5.1.2)**

b) *Explain IPsec services.* **(Refer section 5.3.2)**

c) *Explain AH. Also explain modes of AH.* **(Refer section 5.4)**

d) *What is DES ? Explain DES encryption process.* **(Refer section 3.7)**

Q.5 Attempt any TWO of the following **[12]**

a) *Describe in brief : Piggybacking* **(Refer section 2.2.1)**

b) *What is One-Time Pad (OTP) security mechanism ?* **(Refer section 3.2.6)**

c) *Describe in brief : passive attack.* **(Refer section 1.5.2)**

Q.6 Attempt any TWO of the following **[12]**

a) *What is meant by access control ? Describe :*
i) DAC ii) MAC iii) RBAC. **(Refer section 2.4)**

b) *Explain Email security.* **(Refer section 5.6)**

c) *What is software piracy ?* **(Refer section 5.9.2)**

❑❑❑

T. Y. DIPLOMA SEM VI COMPUTER ENGINEERING PROGRAM GROUP . . .

1) Management *(V. S. Bagad)*
2) Programming with Python *(A. A. Puntambekar, Yogesh Patil)*
3) Mobile Application Development *(Vrushali Sonar, Narendra Joshi, Aniruddha D. Talole)*
4) Emerging Trends in Computer & Information Technology *(I. A. Dhotre)*
5) Web Based Application Development with PHP *(A. A. Puntambekar)*
6) Network & Information Security *(V. S. Bagad, I. A. Dhotre, M. S. Kalbande)*

For Orders

PUNE REGION CONTACT
Devendra : 9763209871

KOLHAPUR REGION CONTACT
Prashant : 9890674151
: 9665608108

NAGPUR REGION CONTACT
Shrikant : 8793079357

NASHIK REGION CONTACT
Shashikant : 8888861609

ONLINE SELLER
Scan this QR Code & visit us at
www.technicalpublications.org

Email : sales@technicalpublications.org

ISBN 978-93-89750-06-5

Published by :

TECHNICAL PUBLICATIONS®
SINCE 1993
An Up-Thrust for Knowledge

Find us
Website : www.technicalpublications.org
https://www.facebook.com/technicalpublications

Amit Residency, Office No.1, 412, Shaniwar Peth, Pune - 411030, M.S. INDIA.
Ph.: +91-020-24495496/97, Telefax : +91-020-24495497
Email : sales@technicalpublications.org Website : www.technicalpublications.org