SUBJECT CODE : 310254(A)

As per Revised Syllabus of

SAVITRIBAI PHULE PUNE UNIVERSITY

Choice Based Credit System (CBCS)

T.E. (Computer) Semester - VI (Elective - II)

INFORMATION SECURITY

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

Iresh A. Dhotre

M.E. (Information Technology)

Ex-Faculty, Sinhgad College of Engineering,

Pune.

Dr. Swati Nikam

Ph.D. (Computer Engineering)

M.E.(Computer Engineering), B.E.(Computer Engineering),

Associate Professor,

Dr. D. Y. Patil Institute of Technlogy, Pimpri,

Pune.

TECHNICAL PUBLICATIONS

SINCE 1993

An Up-Thrust for Knowledge

INFORMATION SECURITY

Subject Code : 310254(A)

T.E. (Computer Engineering) Semester - VI (Elective - II)

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
Email : sales@technicalpublications.org Website : www.technicalpublications.org

Printer :
Yogiraj Printers & Binders
Sr.No. 10/1A,
Ghule Industrial Estate, Nanded Village Road,
Tal. - Haveli, Dist. - Pune - 411041.

ISBN 978-93-5585-039-3

SPPU 19

PREFACE

The importance of **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 **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 the chapters in the 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 the subject.

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

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
V. S. Bagad
J. A. Dhotre
Dr. Swati Nikam

Dedicated to God.

SYLLABUS

Information Security - 310254(A)

Credit :	Examination Scheme :
03	Mid-Sem (TH) : 30 Marks End-Sem (TH) : 70 Marks

Unit I Introduction to Information Security

Foundations of Security, Computer Security Concepts, The OSI Security Architecture, Security attacks, Security services, Security mechanism, A Model for Network Security. **(Chapter - 1)**

Unit II Symmetric Key Cryptography

Classical Encryption Techniques : Stream Ciphers, Substitution Techniques : Caesar Cipher, Mono alphabetic Ciphers, Play fair Cipher, Hill Cipher, Poly alphabetic Ciphers, Transposition Techniques, Block Ciphers and Data Encryption standards, 3DES, Advanced Encryption standard. **(Chapter - 2)**

Unit III Asymmetric Key Cryptography

Number theory : Prime number, Fermat and Euler theorems, Testing for primality, Chinese reminder theorem, discrete logarithm, Public Key Cryptography and RSA, Key Management, Diffie-Hellman key exchange, El Gamal algorithm, Elliptic Curve Cryptography. **(Chapter - 3)**

Unit IV Data Integrity Algorithms And Web Security

Cryptographic Hash Functions : Applications of Cryptographic Hash Functions, Two Simple Hash Functions, Requirements and Security, Hash Functions Based on Cipher Block Chaining, Secure Hash Algorithm (SHA), SHA-3, MD4, MD5. **Message Authentication Codes :** Message Authentication Requirements, Message Authentication Functions, Requirements for Message Authentication Codes, Security of MACs. **Digital Signatures :** Digital Signatures, Schemes, Digital Signature standard, PKI X.509 Certificate.

Web Security issues, HTTPS, SSH, Email security : PGP, S/MIME, IP Security : IPSec. **(Chapter - 4)**

Unit V Network and System Security

The OSI Security architecture, Access Control, Flooding attacks, DOS, Distributed DOS attacks Intrusion detection, Host based and network based Honeypot, Firewall and Intrusion prevention system, Need of firewall, Firewall characteristics and access policy, Types of Firewall, DMZ networks, **Intrusion prevention system :** Host based, Network based, Hybrid.

Operating system Security, Application Security, Security maintenance, Multilevel Security, Multilevel Security for role based access control, Concepts of trusted system, Trusted computing. **(Chapter - 5)**

Unit VI Cyber Security and Tools

Introduction, Cybercrime and Information Security, Classification of Cybercrimes, The legal perspectives-Indian perspective, Global perspective, Categories of Cybercrime, Social Engineering, Cyber stalking, Proxy servers and Anonymizers, Phishing, Password Cracking, Key-loggers and Spywares, The Indian IT Act-Challenges, Amendments, Challenges to Indian Law and Cybercrime Scenario in India, Indian IT Act. **(Chapter - 6)**

Table of Contents

Unit I

Unit II

Unit III

Unit IV

Unit V

Unit VI

Notes

UNIT I

1 Introduction to Information Security

Syllabus

Foundations of Security, Computer Security Concepts, The OSI Security Architecture, Security attacks, Security services, Security mechanism, A Model for Network Security.

Contents

1.1 Foundations of Security

- Security means protecting assets, whether from attackers invading networks, natural disasters, vandalism, loss or misuse. Information security is defined as "protecting information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction,".
- Security is an area of increasing and grave concern to programmers. Security attacks abound and all too often the "way in" for the perpetrators is through a "hole" left by an unwary programmer. Therefore, software developers today need to worry about security as never before. They need clear guidance on safe coding practices.
- The dictionary defines security as "the quality or state of being free from danger" or "measures taken to guard against espionage or sabotage, crime, attack or escape."
- There are many different types of computer security threats and problems, but they can be classified into large classes as follows :
  1. **Physical security :** A personal computer can be stolen. A large computer center can be broken into and equipment taken. Fire, electrical surges and floods can damage computer hardware and network connections and cause loss of data.
  2. **Rogue software :** We have all heard of computer viruses. Small, sneaky programs that invade our computers and spread quickly and silently. Viruses are just one aspect of the general threat posed by rogue software.
  3. Most computers are connected to networks and most local networks are connected to the Internet. Thus, there is a large class of computer security threats that are related to networks and fall under the category of network security. This wide area of security includes threats such as port scanning, spoofing, password cracking, spyware and identity theft.

1.2 Computer Security Concepts

SPPU : Dec.-16,17, April-16, 17, May-18, 19, March-20

- The history of information security begins with computer security.
- Network security, to protect networking components, connections and contents.
- Information security to protect the confidentiality, integrity and availability of information assets, whether in storage, processing or transmission.
- Physical security consists of all mechanisms used to ensure that physical access to the computer systems and networks is restricted to only authorize users.
- 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.
- Security is required because the widespread use of data processing equipment, the security of information felt to be valuable to an organization was provided primarily by physical and administrative means.
- Network security measures are needed to protect data during their transmission.
- Following are the examples of security violations.
  1. User A transmits a sensitive information file to user B. The unauthorized user C is able to monitor the transmission and capture a copy of the file during its transmission.
  2. A message is sent from a customer to a stockbroker with instructions for various transactions. Subsequently, the investments lose value and the customer denies sending the message.
  3. While transmitting the message between two users, the unauthorised user intercepts the message, alters its contents to add or delete entries and then forwards the message to destination user.

1.2.1 Basic Terminologies in 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. Key : Some critical information used by the cipher, known only to the sender and receiver.

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

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

  h. Cryptanalysis : The study of principles and methods of transforming an unintelligible message back into an intelligible message *without* knowledge of

the key. Also called **code-breaking.** Cryptanalysis is to break an encryption. Cryptanalyst can do any or all of the three different things :

1. Attempt to break a single message.
2. Attempt to recognize patterns in encrypted messages, in order to be able to break subsequent ones by applying a strainghtforward decryption algorithm.
3. Attempt to find general weakness in an encryption algorithm, without necessarily having intercepted any messages.

i. Cryptology : Both cryptography and cryptanalysis.

j. Code : An algorithm for transforming an plaintext message into an unintelligible one using a code-book.

1.2.2 Categories

- Various categories of computer security are :
  1. Cryptography 2. Data security
  3. Computer security 4. Network security
- Cryptography is data encryption and decryption.
- Data security is ensuring safe data from modification and corruption.
- Computer security is formal description of security policies. It includes protection, preventation and detection of unauthorized use of computer.
- Network security is protection of data on the network during transmission or sharing.

1.2.3 Techniques

- Commonly used security techniques are as follows :
  1. Encryption : Used to protect information and data. It is cryptography techniques. Different types of encryption are used for providing security.
  2. Access control : Access to data or computer is controlled by using some mechanism. Access control is a security technique that regulates who or what can view or use resources in a computing environment. It is a fundamental concept in security that minimizes risk to the business or organization.
  3. Data backup : Data backup refers to saving additional copies of your data in separate physical or virtual locations from data files in storage. If you lose your data, recovery could be slow, costly or impossible. It is important that you secure, store and backup your data on a regular basis.

4. Firewall : Firewall is a network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules.
5. Antivirus software : Many antivirus software programs include real-time threat detection and protection to guard against potential vulnerabilities as they happen, as well as system scans that monitor device and system files looking for possible risks.
6. Intrusion detection systems : IDS can offer protection from external users and internal attackers. It also automatically monitors the Internet to search for any of the latest threats which could result in a future attack.
7. Series of confidence : It ensure that all software use has been authentic.

1.2.4 Elements of Information 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. 1.2.1 Relationship between Confidentiality Integrity and Availability.

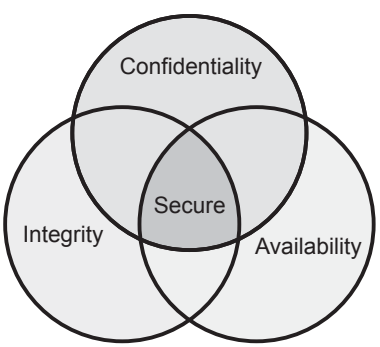


Fig. 1.2.1 Relationship between confidentiality integrity

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.

1.2.5 Threats and Vulnerability

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.

Vulnerability

- 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.
- The specificity of technical jargon reflects the way experts have identified clear distinctions between practical realities of their fields of expertise and can help clarify even for oneself how one should address the challenges that arise.
- Other examples of vulnerability include these :
  1. A weakness in a firewall that lets hackers get into a computer network.
  2. Unlocked doors at businesses.
  3. Lack of security cameras.

Review Questions

1. *List and explain categories of information security.* **SPPU : April-17, Marks 5**
2. *What are the categories of computer security.* **SPPU : Dec.-16, Marks 5**
3. *List and explain different security techniques.* **SPPU : April-16, Marks 4**
4. *What are various security technique used in cyber security.* **SPPU : Dec.-17, Marks 5**
5. *What are the elements of information security ? Explain in brief.* **SPPU : May-18, Marks 5**
6. *List and explain various elements of information security.* **SPPU : April-16, Marks 4, May-19, Marks 5**
7. *Define cryptography, encrytion, decryption, plain text, cipher text and cryptanalyst.* **SPPU : March-20, Marks 5**

1.3 The OSI Security Architecture

- The international telecommunication union telecommunication standardization sector recommendation X.800 security architecture for OSI. It is useful to managers as a way of organizing the task of providing security.
- To assess effectively the security needs of an organization and to evaluate and choose various security products and policies, we need some systematic way of defining the requirements for security and characterizing the approaches to satisfying those requirements. The OSI security architecture focuses on three essential parts : Security attacks, security mechanisms and security services.
- It focuses on security attacks, mechanisms and services. These can be defined below :
  1. **Security attack :** Any action that compromises the security of information owned by an organization.
  2. **Security mechanism :** A process that is designed to detect, prevent or recover from a security attack.
  3. **Security service :** A processing or communication service that enhances the security of the data processing systems and the information transfers of an organization.

1.3.1 Vulnerabilities in OSI Model

- How does the security framework work ? The security architecture is mapped to the customer's enterprise architecture using the Open Systems Interconnect (OSI) networking model. The security framework has security solutions for all the pieces of the enterprise infrastructure that supports the goals of the organization.

- The security framework operates and protects that infrastructure at each of the operational levels of the OSI model. As transactions take place from end-to-end of the enterprise architecture, these transactions utilize technologies that operates at all the levels of the OSI model as well. Since security extends into policies and procedures and supports business driven goals, the security framework has added two additional layers to the model, the financial and political layers. These layers began as a tongue-in-cheek joke at the National Security Agency in the mid-nineties.
- However, security of information systems really does have to match the budget and the business objectives of an organization and these layers have achieved legitimacy in their own right.

1. Physical Layer

- Layer one of the OSI model is the physical layer where the wire over which electronic impulses run to create the magic. At this layer, the security framework protects the cable plant, the wiring and telecommunications infrastructure.
- The physical layer is protected by redundant power and WAN connection. It also means protecting the physical hardware in network closets, server farms and systems in raised floor spaces. Protecting the physical layer entails locks, alarms on entrances, climate controls and access to data centers.

2. Data Link and Network Layers

- At the data link and network layers, the security framework protects systems with a number of technologies. VPNs protect information by encrypting it and sending it through encrypted tunnels through networks or the internet. Network intrusion detection systems or NIDS watch traffic flowing over the wires looking for bit stream patterns that could indicate attacks or malicious intent.
- Host intrusion detection systems monitor bit streams entering the host machines at the Network Interface Card (NIC) level, also looking for suspicious patterns. Virus scanning at this level looks for patterns that indicate malicious code that fits signatures for known viruses.

3. Network and Transport Layers

- At the network and transport layer, the security framework uses firewalls to do stateful inspection of packets entering and leaving the network. Routers, using Access Control Lists or ACLs filter IP packets, preventing traffic from going to systems that have no need for it.
- Utilizing IP address schemes, network engineers can plan and implement routing tables that protect networks with router ACLs, making firewall rules easier to write and deploy and thwarting attacks such as address spoofing. At the network

and transport layers, virus scanning software opens attachments in messaging packets such as e-mail, looking for embedded viruses or malicious code.

4. Session, Presentation and Application Layers

- At the session, presentation and application layers, the security framework uses a number of techniques and tools to secure systems. Some of these techniques are policies for system management such as hardening the operating systems, keeping patch levels and OS revisions up to date, running with only the services needed to support the business processes and turning off all other process, running processes with limited system privileges, etc.
- All of these management techniques contribute to security at the session, presentation and application layer and are the kind of system controls that automatically enforce security policies.

5. Presentation and Application Layers

- At the presentation and application layers, the security framework utilizes user account management to control access to the network, systems and applications. The security framework relies on system managers to control access to their machines, network administrators to manage user access to their networks and application managers such as Data Base Administrators (DBA) to control access to applications and data.
- At this level, the security framework includes virus scanning applications to scan hard drives and system memory for malicious code, updating scan engines and virus signatures. Host Intrusion Detection Systems (HIDS), active in the lower levels of the model, work at the presentation and application layer to watch for changes to critical system files and other system behaviour that might indicate an attacker trying to gain control of the system.
- The security framework can also control user access centrally using a Role/Rule-Based Access Control (RBAC) engine, that uses a directory such as LDAP or Active Directory that contains information about users and the systems and resources to which the users are authorized access. PKI and digital certificates can be used at this level to provide digital signatures, encryption and non-repudiation at the application level.

1.4 Security Attacks

SPPU : March-19, 20

- A security attack is an unauthorized attempt to steal, damage or expose data from an information system. There are two types of attacks that are related to security namely **passive and active attacks**.
- In an active attack, an attacker tries to modify the content of the messages. In a passive attack, an attacker observes the messages and copies them.

1.4.1 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. 1.4.1. 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.

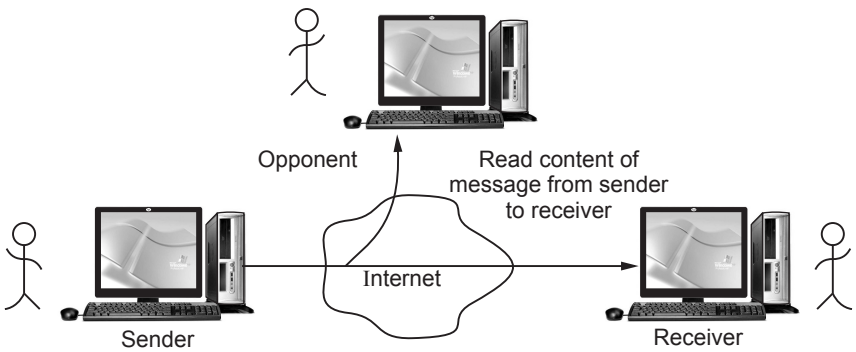


Fig. 1.4.1 Release of message contents

- **Traffic analysis :** Mask the contents of message so that opponents could not extract the information from the message. Encryption is used for masking Fig. 1.4.2 shows the traffic analysis.

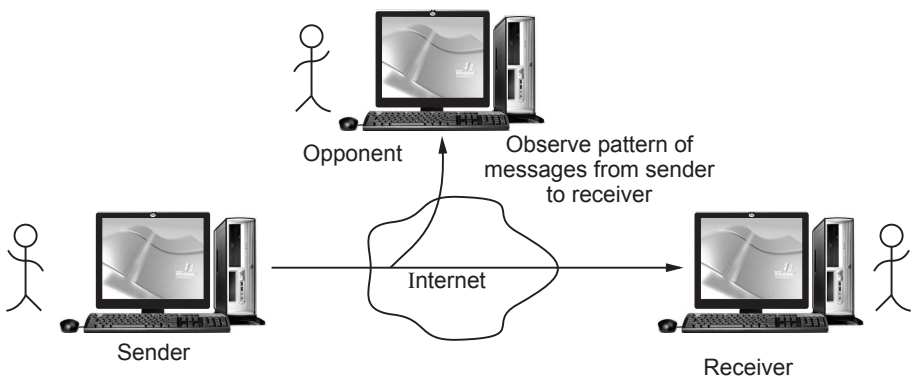


Fig. 1.4.2 Traffic analysis

- 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.

1.4.2 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. 1.4.3 shows masquerade.

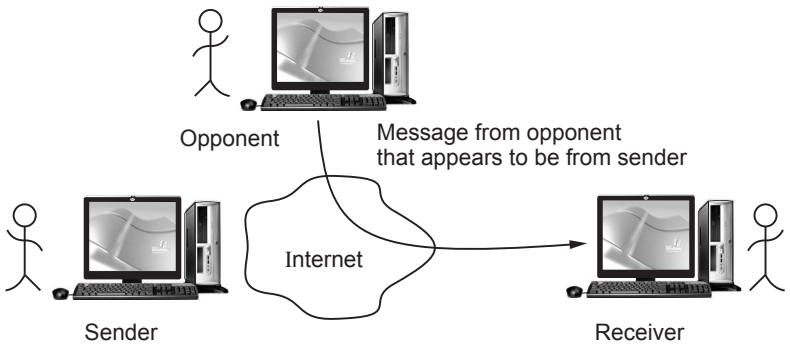


Fig. 1.4.3 Masquerade

- **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. 1.4.4 shows replay attack.

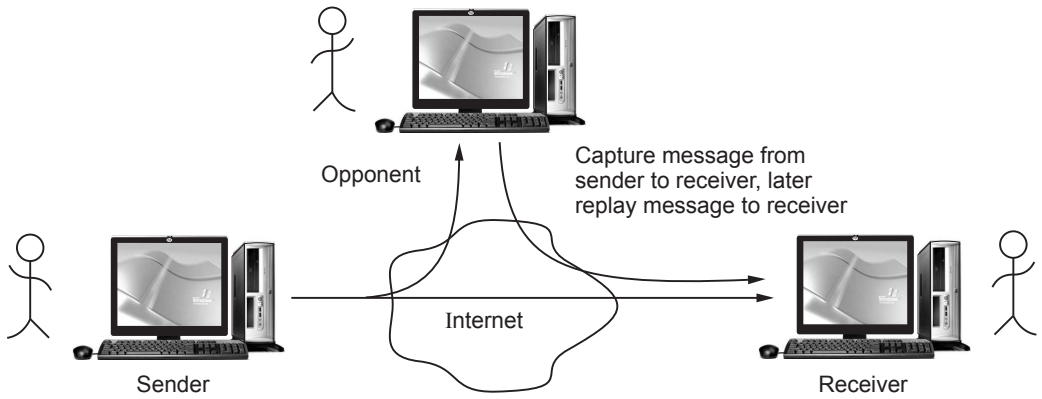


Fig. 1.4.4 Replay

3. Modification of message

- It involves some change to the original message. It produces an unauthorized effect. Fig. 1.4.5 shows the modification of message.

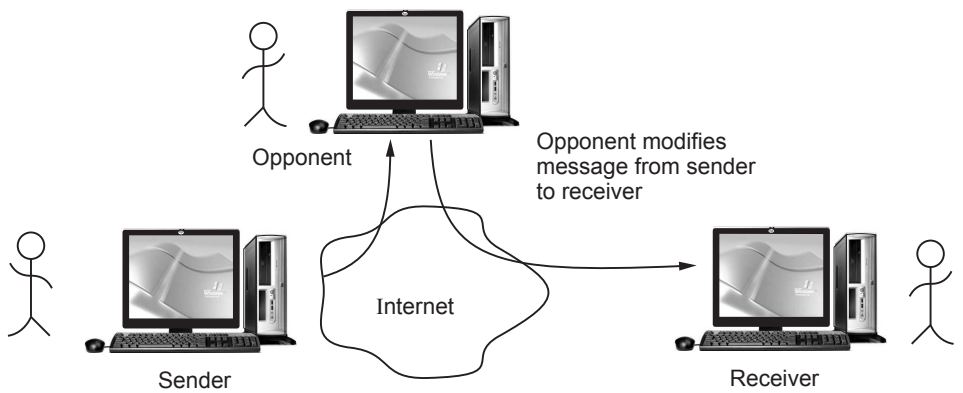


Fig. 1.4.5 Modification of message

- 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. 1.4.6 shows denial of service attack.

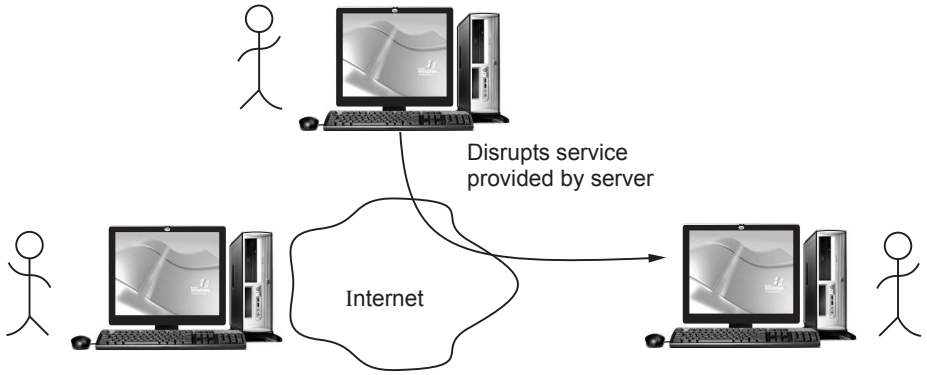


Fig. 1.4.6 Denial of service

- 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. 1.4.7 shows the 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.

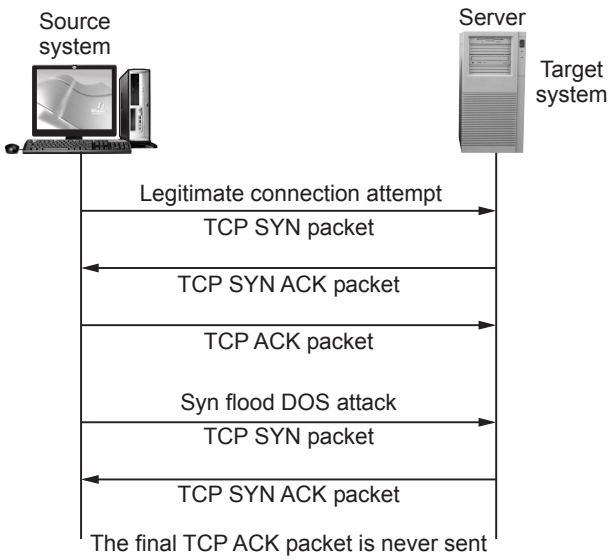


Fig. 1.4.7 SYN flood DOS attack

- 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.

1.4.3 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.

Review Questions

1. *How information security attacks are classified ? Give example for each.* **SPPU : March-19, Marks 5**
1. *Explain passive and active attacks with examples.* **SPPU : March-20, Marks 5**

1.5 Security Services

- X.800 defines a security service as a service provided by a protocol layer of communicating open systems, which ensures adequate security of the systems or of data transfers.
- X.800 divides security services into five different categories.
  1. Authentication 2. Access control 3. Data confidentiality
  4. Data integrity 5. Nonrepudiation

1. Authentication

- Authentication is the process of determining whether someone or something is, in fact, who or what it is declared to be. In public and private computer network, authentication is commonly done through the use of login passwords.

- Two specific authentication services are defined in X.800 :
  a. Peer entity authentication
  b. Data origin authentication
- **Peer entity authentication** used in association with a logical connection to provide confidence in the identity of the entities connected.
- Data origin outhentication enables the recepient to verify that the message have not been tempered in transit (data integrity) and they originally from expected sender (authenticity).
- **Data origin authentication** does not provide protection against the duplication or modification of data units. This type of service supports applications like electronic mail where there are no prior interactions between the communicating entities.

2. Access control

- It is the ability to limit and control the access to host systems and applications via communications links.
- This service controls who can have access to a resource.

3. Data confidentiality

- Confidentiality is the concealment of information or resources. It is the protection of transmitted data from passive attacks.
- Confidentiality is classified into
  1. **Connection confidentiality :** The protection of all user data on a connection.
  2. **Connectionless confidentiality :** The protection of all user data in a single data block.
  3. **Selective field confidentiality :** The confidentiality of selected fields within the user data on a connection or in a single data block.
  4. **Traffic flow confidentiality :** The protection of the information that might be derived from observation of traffic flows.

4. Data integrity

- Integrity can apply to a stream of messages a single message or selected fields within a message.
- Modification causes loss of message integrity.
- Data integrity can be classified as
  1. Connection integrity with recovery
  2. Connection integrity without recovery
  3. Selective field connection integrity

4. Connectionless integrity
5. Selective field connectionless integrity

- Connection integrity with recovery provides for the integrity of all user data on a connection and detects any modification, insertion, deletion or replay of any data within an entire data sequence with recovery attempted.
- Connection integrity without recovery provides only detection without recovery.
- Selective field connection integrity provides for the integrity of selected fields within the user data of a data block transferred over a connection.
- Connectionless integrity provides for the integrity of a single connectionless data block and may take the form of detection of data modification.

5. Nonrepudiation

- Nonrepudiation prevents either sender or receiver from denying a transmitted message.
- 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.

1.6 Security Mechanism

SPPU : April-16, March-19,20

- X.800 defined security mechanisms as follows
  1. **Specific security mechanisms :** May be incorporated into the appropriate protocol layer in order to provide some of the OSI security services.
     - **a. Encipherment :** The use of mathematical algorithms to transform data into a form that is not readily intelligible.
     - **b. Digital signature :** Data appended to or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source and integrity the data unit and protect against forgery.
     - **c. Access control :** A variety of mechanisms that enforce access rights to resources.
     - **d. Data integrity :** A variety of mechanisms used to ensure the integrity of a data unit or stream of data units.
     - **e. Authentication exchange :** A mechanism intended to ensure the identity of an entity by means of information exchange.
     - **f. Traffic padding :** The insertion of bits into gaps in a data stream to frustrate traffic analysis attempts.

g. **Notarization :** The use of a trusted third party to assure certain properties of a data exchange.

2. **Pervasive security mechanisms :** Mechanisms that are not specific to any particular OSI security service or protocol layer.

   a. **Trusted functionality :** That which is perceived to be correct with respect to some criteria.

   b. **Event detection :** Detection of security relevant events.

   c. **Security label :** The marking bound to resource that names or designates the security attributes of that resource.

   d. **Security recovery :** Deals with requests from mechanisms, such as event handling and management functions and takes recovery actions.

1.6.1 Security Policy

- Security policy is a definition of what it means to be secure for a system, organization or other entity.
- For an organization, it addresses the constraints on behavior of its members as well as constraints imposed on adversaries by mechanisms such as doors, locks, keys and walls.
- A security policy is a written document in an organization outlining how to protect the organization from threats, including computer security threats and how to handle situations when they do occur.
- A security policy must identify all of a company's assets as well as all the potential threats to those assets. Company employees need to be kept updated on the company's security policies. The policies themselves should be updated regularly as well.
- Access control : It is the ability to limit and control the access to host systems and applications via communications links. This service controls, who can have access to a resource.
- A security policy establishes what must be done to protect information stored on computers. A well written policy contains sufficient definition of "what" to do so that the "how" can be identified and measured or evaluated.
- Security to the information can be provided by using internal approach and external approach.
- Internal approach : Protect from internal attacks by using necessary measures.
- External approach : Protect from outside attacks.

- In general, a good security policy does the following :
  1. Communicates clear and concise information and is realistic;
  2. Includes defined scope and applicability;
  3. Consistent with higher-level policy and guidance;
  4. Open to change based on new risks and vulnerabilities;
  5. Identifies the areas of responsibility for users, administrators and management;
  6. Provides sufficient guidance for development of specific procedures;
  7. Balances protection with productivity;
  8. Identifies how incidents will be handled.

Review Questions

1. *What are the security approaches used to implement security policy ?* **SPPU : April-16, Marks 2**
2. *List the differences between security and privacy.* **SPPU : March-19, Marks 5**
3. *What are different security policies ? Explain.* **SPPU : March-19,20, Marks 5**

1.7 A Model for Network Security

SPPU : April-16, 17, May-16,17,18, March-19, Dec.-19

- A message is to be transferred from source to destination across some sort of internet. Both the sides must cooperate for the exchange of the data.
- A logical information channel is established by defining a route through the internet from source to destination.
- All the techniques for providing security have two components :
  1. A security related transformation on the information to be sent.
  2. Some secret information shared by the two principles, it is hoped, unknown to the opponent.
- Fig. 1.7.1 shows the network security model.
- A trusted third party is needed to achieve secure transmission.
- Basic tasks in designing a particular security service.
  1. Design an algorithm for performing the security related transformation.
  2. Generate the secret information to be used with the algorithm.
  3. Develop methods for the distribution and sharing of the secret information.

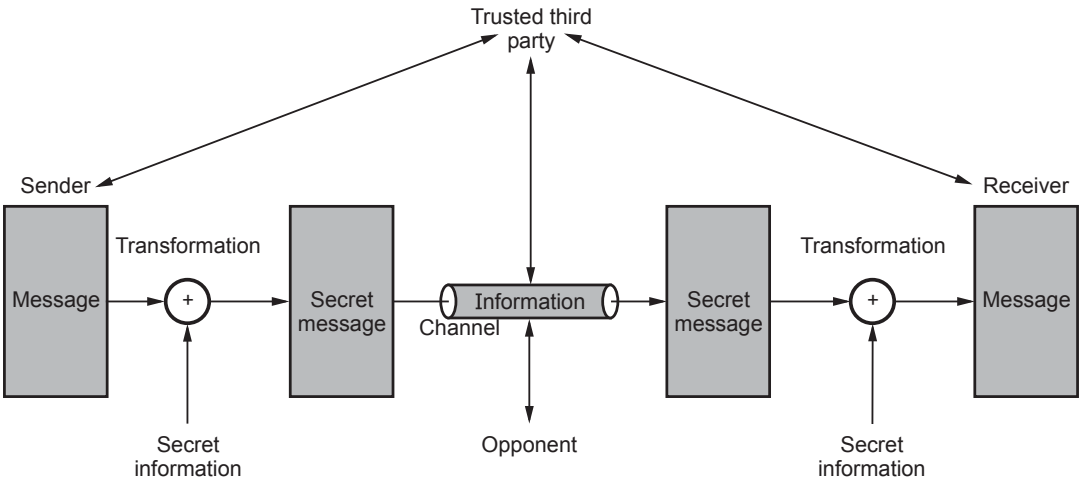


Fig. 1.7.1 Network security model

4. Specify a protocol to be used by the two principles that makes use of the security algorithm and the secret information to achieve a particular security service.

Review Questions

1. *Draw and explain operational model of network security.* **SPPU : April-16, Marks 4, May-17, Marks 5**
2. *Draw and explain operational model of security.* **SPPU : April-17, Marks 5**
3. *Explain the operational model of network security in detail.* **SPPU : May-16, Marks 5**
4. *Explain operational model of network security.* **SPPU : May-18, Marks 5**
5. *Explain operational security model for network security.* **SPPU : March-19, Marks 5**
6. *Explain operational model of security in detail.* **SPPU : Dec.-19, Marks 5**

1.8 Multiple Choice Questions

Q.1 The original message is called as _____.

a ciphertext b plaintext
c cryptography d encryption

Q.2 The process of converting plaintext to ciphertext is called as_____.

a encryption b decryption
c substitution d transposition

Q.3 Interception, interruption, _____and fabrication are the system security threats.

a traffic analysis
b masquerade
c replay
d modification

Q.4 Which of the following is NOT types of active attack ?

a Masquerade
b Replay
c Traffic analysis
d Modification of message

Q.5 _____ attacks are called as masquerade attacks.

a Interception
b Interruption
c Modification
d Fabrication

Q.6 _____ attacks are very difficult to detect because they do not involve any alternation of data.

a Active
b Passive
c Active and passive
d None of these

Q.7 The process of trying to break any cipher text message to obtain the original plain text message itself is called as _____.

a cryptanalyst
b cryptography
c cryptology
d cryptanalysis

Q.8 The process of converting the ciphertext into plaintext is called_____.

a encryption
b decryption
c substitution
d transposition

Q.9 Which one of the following is an active attack ?

a Masquerade
b Traffic analysis
c Eavesdropping
d Shoulder surfing

Q.10 Which of the following is passive attack ?

a Relay attack
b Masquerade
c Traffic analysis
d Denial of service

Q.11 _____ is the concealment of information or resources. It is the protection of transmitted data from passive attacks.

a Integrity
b Availability
c Authentication
d Confidentially

Q.12 Security _____ is a process that is designed to detect, prevent or recover from a security attack.

a policy
b services
c mechanism
d none

Answer Keys for Multiple Choice Questions :

Q.1	b	**Q.2**	a	**Q.3**	d
Q.4	c	**Q.5**	b	**Q.6**	b
Q.7	d	**Q.8**	b	**Q.9**	a
Q.10	c	**Q.11**	d	**Q.12**	c

❑❑❑

UNIT II

2 Symmetric Key Cryptography

Syllabus

Classical Encryption Techniques : Stream Ciphers, Substitution Techniques : Caesar Cipher, Mono alphabetic Ciphers, Play fair Cipher, Hill Cipher, Poly alphabetic Ciphers, Transposition Techniques, Block Ciphers and Data Encryption standards, 3DES, Advanced Encryption standard.

Contents

2.1 Introduction to Symmetric Key Cryptography

- A symmetric encryption model has five ingredients.
  1. Plaintext 2. Encryption algorithm 3. Secret key
  4. Ciphertext 5. Decryption algorithm
- Fig. 2.1.1 shows the conventional encryption model.

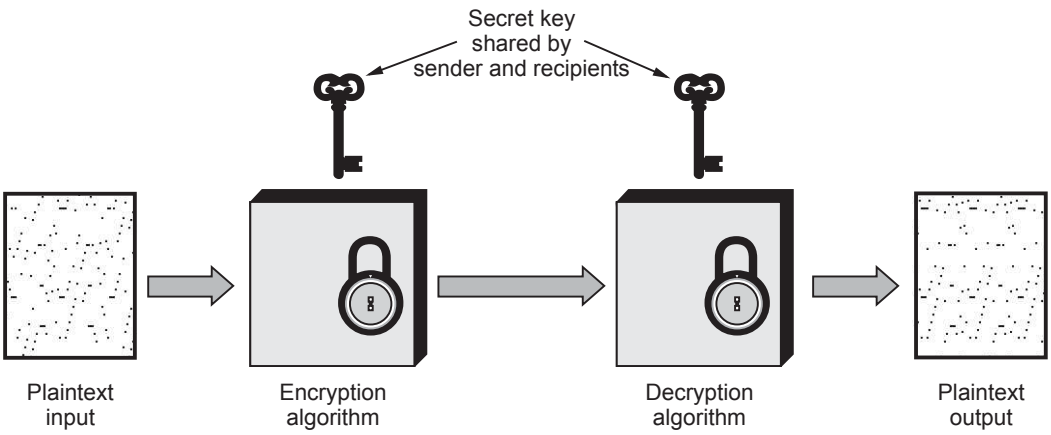


Fig. 2.1.1 Conventional encryption model

- **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 original intelligible message, referred to as plaintext is converted into random nonsense, referred to as ciphertext. The science and art of manipulating message to make them secure is called **cryptography.**
- An original message to be transformed is called the plaintext and the resulting message after the transformation is called the ciphertext.
- The process of converting the plaintext into ciphertext is called encryption. The reverse process is called decryption. The encryption process consists of an algorithm and a key. The key controls the algorithm.
- The objective is to design an encryption technique so that it would be very difficult or impossible for an unauthorized party to understand the contents of the ciphertext.

- A user can recover the original message only by decrypting the ciphertext using the secret key. Depending upon the secret key used, the algorithm will produce a different output. If the secret key changes, the output of the algorithm also changes.
- Fig. 2.1.2 shows model of conventional cryptosystem.

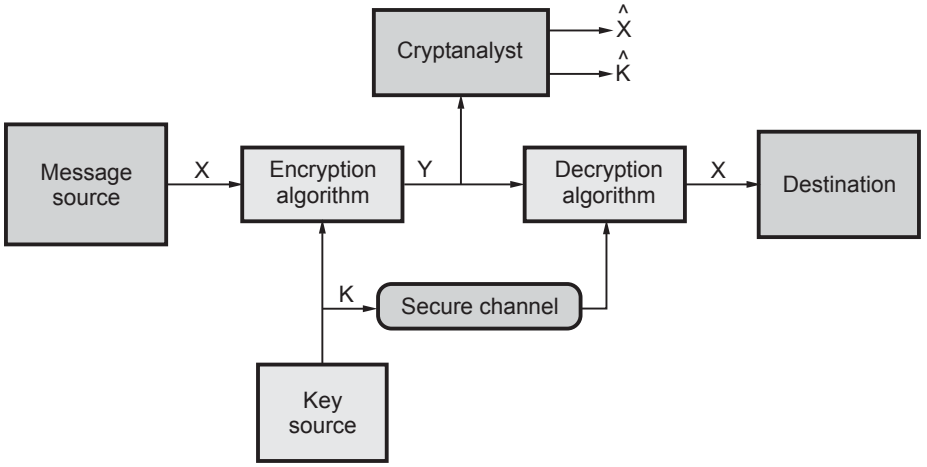


Fig. 2.1.2 Model of conventional cryptosystem

- The security of the conventional encryption depends on the several factors. The encryption algorithm must be powerful. Decryption message must be difficult. The algorithm depend on the secrecy of the key only. The algorithm is upon to all but only key is to keep secret. As shown in the diagram, the message source is the plaintext. i.e. X with the message X and encryption key K as input and ciphertext Y, we can write this as,

$$Y = E(K, X) \quad \ldots(2.1.1)$$

- Using equation (2.1.1) Y is to be produced by using encryption algorithm E as a function of the plaintext X. The intended receiver in possession of the key, is able to invert the transformation.

$$X = D(K, Y) \quad \ldots(2.1.2)$$

- An opponent, observing Y but not having access to K or X, must attempt to recover X and K or both X and K. It is assumed that the opponent does have knowledge of the encryption (E) and decryption (D) algorithms.

2.1.1 Advantages of Symmetric Key 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.

2.1.2 Disadvantages of Symmetric Key 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.

2.2 Cryptography

SPPU : Dec.-19, March-20

- Cryptography is the practice and study of techniques for secure communication in the presence of third parties.
- Cryptography is the science of writing in secret code and is an ancient art.
- Cryptography is not only protects data from theft or alteration, but can also be used for user authentication. There are, in general, three types of cryptographic schemes typically used to accomplish these goals : Secret key cryptography, public-key cryptography, and hash functions.

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 plaintext 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.

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 secrete 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.

The various type of cryptanalytic attacks based on the amount of information known to the cryptanalyst.

2.2.1 Linear Cryptanalysis

- Linear cryptanalysis tries to take advantage of high probability occurrences of linear expressions involving plaintext bits, "ciphertext" bits and subkey bits. It is a known plaintext attack.

- Performing linear cryptanalysis on a block cipher usually consists of three steps :
  1. Find linear approximations of the non-linear parts of the encryption algorithm (usually only the substitution boxes, known as S-boxes).
  2. Combine linear approximations of S-boxes with the rest of the (linear) operations done in the encryption algorithm, to obtain a linear approximation of the entire encryption algorithm. This linear approximation is a function which relates the plaintext bits, the ciphertext bits, and the bits of the private key.
  3. Use the linear approximation as a guide for which keys to try first. This leads to substantial computational savings over trying all possible values of the key. Multiple linear approximations may be used to further cut down the number of keys that need to be tried.

2.2.2 Differential Cryptanalysis

- Differential cryptanalysis is an approach to cryptanalysis whereby differences in inputs are mapped to differences in outputs and patterns in the mappings of plaintext edits to ciphertext variation are used to reverse engineer a key.
- Differential cryptanalysis aims to map bitwise differences in inputs to differences in the output in order to reverse engineer the action of the encryption algorithm. It is again aiming to approximate the encryption algorithm looking to find a maximum likelihood estimator of the true encryption action by altering plaintexts and analyzing the impact of changes to the plaintext to the resulting ciphertext. Differential cryptanalysis is therefore a chosen plaintext attack.
- The main difference from linear attack is that differential attack involves comparing the XOR of two inputs to the XOR of the corresponding output.
- Differential attack is a **chosen-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 ΔC's given ΔP may reveal information about the key.
- 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 !!!

2.2.3 Difference between Linear and Difference Cryptanalysis

Sr. No.	Linear cryptanalysis	Differential cryptanalysis
1.	Linear cryptanalysis focus on statistical analysis against one round of decrypted ciphertext	Differential analysis focuses on the statistical analysis of two inputs and two outputs of a cryptographic algorithm.
2.	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 choosing
3.	Linear cryptanalysis is a general form of cryptanalysis based on finding affine approximations to the action of a cipher	Differential cryptanalysis is a general form of cryptanalysis applicable primarily to block ciphers, but also to stream ciphers and cryptographic hash functions.
4.	linear cryptanalysis "only" requires known plaintext	Differential cryptanalysis requires chosen plaintext

Review Questions

1. *Describe linear and differential cryptanalysis with suitable example.*
   SPPU : Dec.-19, Marks 5
2. *What is cryptanalysis ? Explain various cryptanalysis technique.*
   SPPU : March-20, Marks 5

2.3 Stream Ciphers

- Stream cipher algorithms are designed to accept a crypto key and a stream of plaintext to produce a stream of ciphertext.
- Fig. 2.3.1 shows the stream cipher.

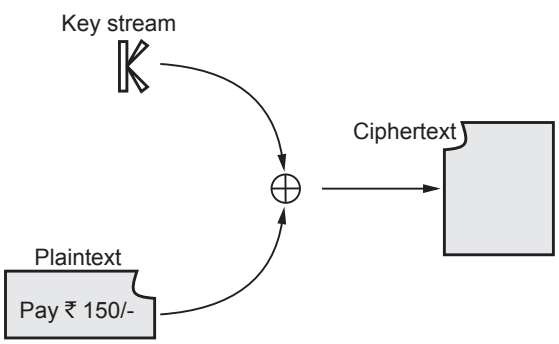


Fig. 2.3.1 Stream cipher

- Stream cipher is similar to a one time pad.
- A stream cipher encrypts smaller block of data, typically bits or bytes.
- A key stream generator outputs a stream of bits $K_1, K_2, K_3 \ldots\ldots K_i$.
- This key stream is XORed with a stream of plaintext bits $P_1, P_2, P_3 \ldots\ldots P_i$ to produce the stream of ciphertext bits.

  $$C_i = P_i \oplus K_i$$

- At the description end, the ciphertext bits are XORed with an identical key stream to recover the plaintext bits.

  $$P_i = C_i \oplus K_i$$

- The system security depends entirely on the insides of the keystream generator.

2.3.1 Advantages and Disadvantages of Stream Cipher

Advantages :

1. Speed of transformation
2. Low error propagation.

Disadvantages :

1. Low diffusion
2. Susceptibility to malicious insertation and modifications.

2.3.2 Comparison between Stream and Block Cipher

Sr. No.	Stream cipher	Block cipher
1.	Stream ciphers operate on smaller units of plaintext.	Block ciphers operate on larger block of data.
2.	Faster than block cipher.	Slower than stream cipher.
3.	Stream cipher processes the input element continuously producing output one element at a time.	Block cipher processes the input one block of element at a time, producing an output block for each input block.
4.	Requires less code.	Requires more code.
5.	Only one time of key use.	Reuse of key is possible.
6.	Ex. - One time pad	Ex. - DES
7.	Application - SSL (secure connections on the web.)	Application - Database, file encryption.
8.	Stream cipher is more suitable for hardware implementation.	Easier to implement in software.

2.4 Substitution Techniques

SPPU : April-16, May-16,17,18,19, Dec.-16,17,19, March-20

- 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.

2.4.1 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.

2.4.2 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.

2.4.3 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.

2.4.4 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.

$$C = KP \bmod 26$$

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

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

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

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

  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.

2.4.5 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. 2.4.1 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	I	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. 2.4.1

- **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.

2.4.6 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.

2.4.7 Feistel Cipher

- Fig. 2.4.2 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. 2.4.2 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

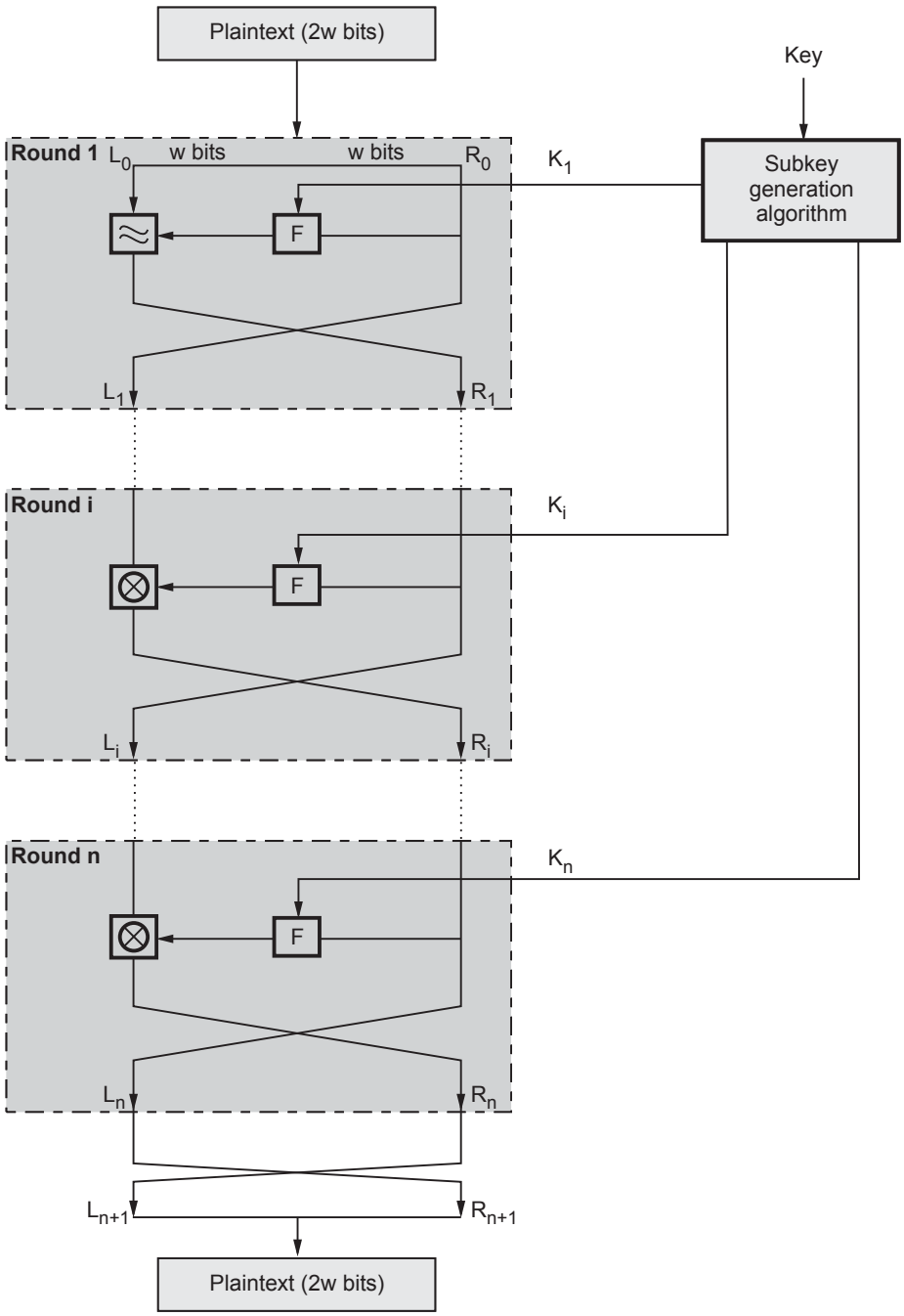


Fig. 2.4.2 Classical feistel network

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,

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

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

- 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.

2.4.8 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.

Example 2.4.1 *Encrypt the message "PAY" using Hill cipher with the following key matrix and show the decryption to get the original plain text.*

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

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

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

Example 2.4.2 *Use play fair cipher to encrypt the following message "This is a columnar transposition" use key - APPLE.* **SPPU : April-16, (In Sem), Marks 5**

Solution : Message = This is a columnar transposition

Key = APPLE
Encryption :

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

Message = Th is is ac ol um na rt ra ns po si ti on

Ciphertext = UG MQ MQ BH MB SO IE SU MT BK QM NQ KN

Example 2.4.3 *Using hill cipher encrypt plain text "COE" use key "ANOTHERBZ".*

SPPU : May-16, (End Sem), Marks 5

Solution : Plain text = COE

Key = ANOTHERBZ

For plaintext COE, here C = 2 O = 14 E = 4

Therefore $P = \begin{pmatrix} 2 \\ 14 \\ 4 \end{pmatrix}$

For key ANOTHERBZ the numbers are 0, 13, 14, 19, 6, 4, 17, 1, 25

The numbers in the matrix form :

$$K = \begin{pmatrix} 0 & 13 & 14 \\ 19 & 6 & 4 \\ 17 & 1 & 25 \end{pmatrix}$$

Ciphertext = (Key X Plaintext) Mod 26

Encryption is as follows :

$$C = \begin{pmatrix} 0 & 13 & 14 \\ 19 & 6 & 4 \\ 17 & 1 & 25 \end{pmatrix} \begin{pmatrix} 2 \\ 14 \\ 4 \end{pmatrix} \bmod 26$$

$$= \begin{pmatrix} 238 \\ 138 \\ 148 \end{pmatrix} \bmod 26 = \begin{pmatrix} 4 \\ 8 \\ 18 \end{pmatrix}$$

Ciphertext := 4 = E , 8 = I and 18 = S

Ciphertext = EIS

Example 2.4.4 *Use polyalphabetic ciphers to encrypt plain text "SHE IS VERY HAPPY AND BEAUTIFUL GIRL" use key 'ANOTHER'* **SPPU : Dec.-17, (End Sem), Marks 5**

Solution :

Keyword	anoth	erano	thera	nothe	ranot	heran
Plaintext	sheis	veryh	appya	ndbea	utifu	lgirl
Ciphertext	SUSBZ	ZVRLV	TWTPA	ARULE	LTVTN	SKZRY

Example 2.4.5 *Using hill cipher encrypt the message 'ESSENTIAL'. The key for encryption is 'ANOTHERBZ'.* **SPPU : May-19 (End Sem), Marks 5**

Ans. :

$$\text{Key matrix } K = \begin{bmatrix} 0 & 13 & 14 \\ 19 & 6 & 4 \\ 17 & 1 & 25 \end{bmatrix}$$

$$\text{Plaintext matrix } P = \begin{bmatrix} 4 & 4 & 8 \\ 18 & 13 & 0 \\ 18 & 19 & 11 \end{bmatrix}$$

Ciphertext matrix $C = K \times P \bmod 26$

$$C = \begin{bmatrix} 0 & 13 & 14 \\ 19 & 6 & 4 \\ 17 & 1 & 25 \end{bmatrix} \begin{bmatrix} 4 & 4 & 8 \\ 18 & 13 & 0 \\ 18 & 19 & 11 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 486 & 435 & 154 \\ 256 & 230 & 196 \\ 536 & 556 & 411 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 18 & 19 & 24 \\ 22 & 22 & 14 \\ 16 & 10 & 21 \end{bmatrix} \bmod 26$$

$$C = \begin{bmatrix} S & T & Y \\ W & W & D \\ Q & K & V \end{bmatrix} \bmod 26$$

Ciphertext = SWQTWKYDV

Review Questions

1. *Use play fair cipher to encrypt the following message "This is a columnar transposition" use key - APPLE.* **SPPU : April-16, March-19, Marks 5**
2. *Using hill cipher encrypt plain text "COE" use key "ANOTHERBZ".* **SPPU : May-16, Marks 5**
3. *Explain feistel cipher in detail.* **SPPU : Dec.-16, Marks 5**
4. *Using Playfair cipher encrypt message. " We live in a world full of beauty " use key " ANOTHER ".* **SPPU : May-17, Marks 5**
5. *Use poly alphabetic ciphers to encrypt plain text "SHE IS VERY HAPPY AND BEAUTIFUL GIRL" use key 'ANOTHER'.* **SPPU : Dec.-17, Marks 5**
6. *Explain the operation of polyalphabetic cipher.* **SPPU : May-18, Marks 5**
7. *Encrypt the plain text 'COE' using hill cipher, use keyword 'ANOTHERBZ'.* **SPPU : May-18, Marks 5**
8. *Explain Monoalphabetic and polyalphabetic ciphers with appropriate examples.* **SPPU : March-19, Marks 5**
9. *Using Hill Cipher encrypt the message 'ESSENTIAL'. The key for encryption is 'ANOTHERBZ.* **SPPU : May-19, Marks 5**
10. *Distinguish between Substitution and transposition ciphers.* **SPPU : Dec.-19, Marks 5**
11. *Use Playfail Cipher to encrypt the message "Weliveina world full of beauty". Use key 'ANOTHER'.* **SPPU : March-20, Marks 5**

2.5 Transposition Techniques

SPPU : May-16,19, Dec.-16,19, April-17

- 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.

2.5.1 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.

Example 2.5.1 *Use the transposition cipher to encrypt the plain text "WE ARE THE BEST" use the key "HEAVEN".* **SPPU : May-16, End Sem, Marks 3**

Solution :

Key	→	H	E	A	V	E	N
Key number	→	4	2	1	6	3	5
Plaintext	→	W	E	A	R	E	T
		H	E	B	E	S	T

Arrange the key number as per ascending order.

Key	→	A	E	E	H	N	V
Key number	→	1	2	3	4	5	6
Plaintext	→	A	E	E	W	T	R
		B	E	S	H	T	E

Ciphertext = ABEEESWHTTRE

Example 2.5.2 *Use transposition cipher to encrypt plain text 'I love my India' and use the key 'HEAVEN'. [Use single columnar transposition].*

SPPU : May-19 (End Sem), Marks 5

Solution :

KEY	→	H	E	A	V	E	N
Key number	→	4	2	1	6	3	5
Plaintext	→	I	L	O	V	E	M
		Y	I	N	D	I	A

Arrange the key number as per ascending order

KEY	→	A	E	E	H	N	V
Key number	→	1	2	3	4	5	6
Plaintext	→	O	L	E	I	M	V
		N	I	I	Y	A	D

Cithertext = ONLIEIIYMAVD

Review Questions

1. *What is transposition cipher ? Use transposition cipher to encrypt the plain text "WE ARE THE BEST" use key "HEAVEN".* **SPPU : May-16, Dec.-16, April-17, Marks 5**
2. *Use transposition cipher to encrypt plain text 'I Love my India' and use the key HEAVEN'. [Use single columnar transposition].* **SPPU : May-19, Marks 5**
3. *What is transposition cipher ? Use transposition cipher to encrypt the plain text "WE ARE THE BEST" use key "HEAVEN".* **SPPU : Dec.-19, Marks 5**

2.6 Block Ciphers

SPPU : April-17, May-19, Dec.-19

- A block cipher operates on blocks of data.
- Algorithm breaks the plaintext into blocks and operates on each block independently.
- A block cipher operates on blocks of data.
- Algorithm breaks the plaintext into blocks and operates on each block independently.
- Usually blocks are 8 or 16 bytes long.
- Security of block ciphers depends on the design of the encryption function.
- Software implementations of block ciphers run faster than software implementation of the stream ciphers.
- Errors in transmitting one block generally do not affect other blocks.
- Each block is enciphered independently, using the same key, identical plaintext blocks produce identical ciphertext blocks.
- Suppose that plaintext is 227 bytes long and the cipher you are using operates on 16-byte blocks.
- Algorithm grabs the first 16-bytes of data, encrypts them using the key table.
- Algorithm produces 16-bytes of ciphertext.
- After first block, algorithm takes next block.
- The key table does not change from block to block.

Plaintext = 227 bytes

Block size = 16 bytes = $\frac{227}{16}$

= 14 blocks plus 3 bytes

- Algorithm encrypts 14 blocks and 3 bytes remain.
- For encrypting last 3 bytes data padding is used.
- Extra bytes are added to make the last block size to 16 bytes.
- Whoever decrypts the ciphertext must be able to recognize the padding.
- One problem with block ciphers is that if the same block of plaintext appears in two places, it encrypts to the same ciphertext.
- To avoid having these kinds of copies in the ciphertext, feedback modes are used.
- Cipher block chaining does not require the extra information to occupy bit spaces, so every bit in the block is part of the message.

- Before a plaintext block is enciphered, that block is XOR'ed with preceding ciphertext block.
- In addition to the key, this technique requires an initialization vector to XOR the initial plaintext block.
- For decrypting the data, copy a block of ciphertext, decrypt it and XOR the result with the preceding block of ciphertext.
- Taking E_K to be the encipherment algorithm with key K and I to be the initialization vector, the cipher block chaining technique is

$$C_o = E_K(m_o \oplus I)$$

$$C_i = E_K(m_i \oplus C_{i-1}) \quad \text{for } i > 0$$

2.6.1 Advantages and Disadvantage of Block Cipher

Advantages :

1. High diffusion
2. Immunity to insertation of symbols.

Disadvantages :

1. Slowness of encryption
2. Error propagation.

Review Question

1. *What is block cipher ? Explain counter mode of block cipher.*

SPPU : April-17,May-19,Dec.-19, Marks 5

2.7 Block Cipher Modes of Operation

SPPU : April-16, May-17, March-19,20

Different types of cipher block modes are discussed here.

1. Electronic Code Book (ECB)

- A block of plaintext encrypts into a block of Ciphertext. Block size is 64-bits.
- Each block is encrypted independently.
- Plaintext patterns are not concealed since identical blocks of plaintext give identical blocks of ciphertext.
- It is not necessary to encrypt the file linearly.

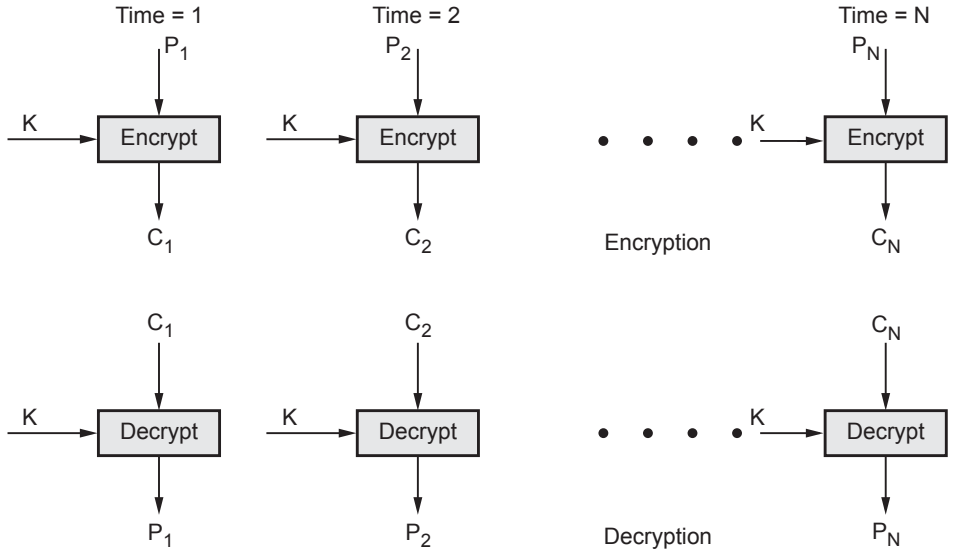


Fig. 2.7.1 ECB mode

- User can encrypt the 10 blocks in the middle first, then the blocks at the end, and finally the blocks in the beginning.
- Because of this, encrypted files are accessed randomly like a data base.
- It is very easy to parallelize the process.
- Pad the last block with some regular pattern i.e. zeros, ones to make it a complete block.
- End of file character is used to denote the final plaintext byte before padding.
- ECB method is ideal for a short amount of data, such as an encryption key.
- For lengthy messages, the ECB mode may not be secure.
- Used in secure transmission of single values i.e. an encryption key.
- ECB has security problems that limit its usability.
- Patterns in the plaintext can yield patterns in the ciphertext.
- It is also easy to modify a ciphertext message by adding, removing or switching encrypted blocks.
- Synchronization error is unrecoverable.

2. Cipher Block Chaining Mode (CBC)

- The plaintext is XORed with the previous ciphertext block before it is encrypted.
- The CBC mode is iterative mode.
- After a plaintext block is encrypted, the resulting ciphertext is also stored in a feedback register.

- Before the next plaintext block is encrypted, it is XORed with the feedback register to become the next input to the encrypting routine.
- The encryption of each block depends on all the previous blocks.
- A ciphertext block is decrypted normally and also saved in a feedback register.
- After the next block is decrypted, it is XORed with the results of the feedback register.
- Mathematically it is

$$C_i = E_k(P_i \oplus C_{i-1})$$

$$P_i = C_{i-1} \oplus D_k(C_i)$$

- It hides patterns in the plaintext.
- In order to guarantee that there is always some random looking ciphertext to apply to the actual plaintext, the process is started with a block of random bits called the Initialization Vector (IV).
- When used in networking messages, most CBC implementations add the IV to the beginning of the message in plaintext.
- A single bit error in a plaintext block will affect that ciphertext block and all subsequent ciphertext blocks.
- CBC mode is self recovering.

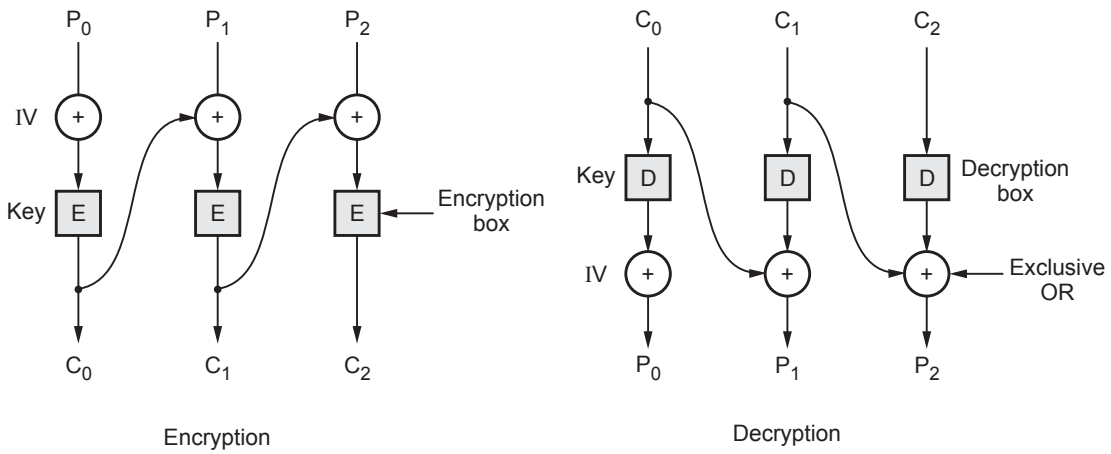


Fig. 2.7.2 CBC

- Two blocks are affected by an error, but the system recovers and continues to work correctly for all subsequent blocks. Synchronization error is unrecoverable.
- Encryption is not parallelizable.
- Decryption is parallelizable and has a random access property.

3. Cipher Feedback Mode (CFB)

- Data is encrypted in units that are smaller than a defined block size.
- It is possible to convert the DES into stream cipher using cipher feedback mode.
- Fig. 2.7.3 shows encryption and decryption process.

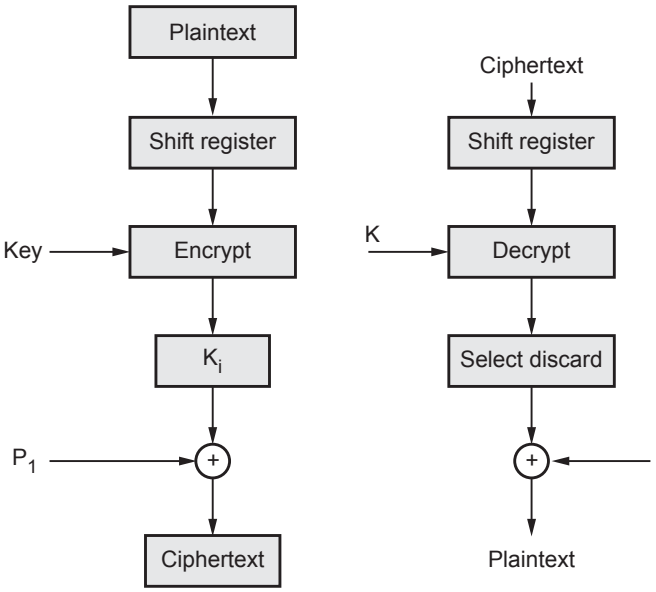


Fig. 2.7.3 CFB Modes

- More than one message can be encrypted with the same key, provided that a different initialization vector is used.
- CFB speed is the same as the block cipher.
- Encryption is not parallelizable, decryption is parallelizable and has a random access property.
- CFB is self recovering with respect to synchronization errors as well.

Advantages

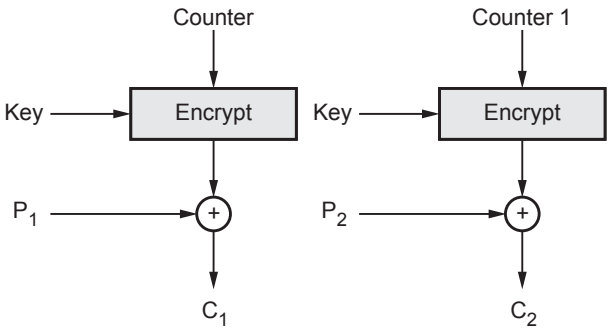
1. Simplicity
2. Need not be used on a byte boundary.
3. Input to the block cipher is randomized.
4. Ciphertext size is the same size as the plaintext size.

Disadvantages

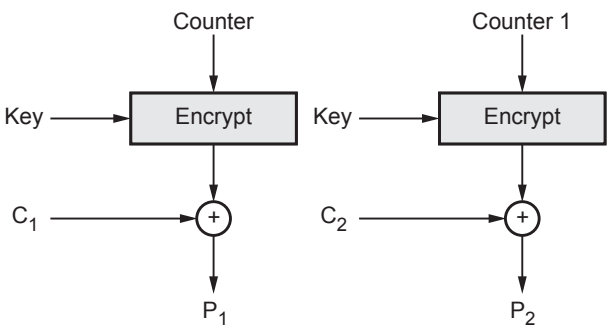
1. Encryption is not parallelizable.
2. Plaintext is somewhat difficult to manipulate.

4. Counter Mode

- Block ciphers in counter mode use sequence numbers as the input to the algorithm.
- More than one message can be encrypted with the same key, provided that a different initialise vector is used.
- Plaintext is very easy to manipulate, any change in ciphertext directly affects the plaintext.
- Synchronization error is unrecoverable.
- A ciphertext error affects only the corresponding bit of plaintext.
- **Encryption :** The counter is encrypted and then XORed with the plaintext block to produce the ciphertext block.
- Fig. 2.7.4 shows encryption and decryption.



(a) Encryption



(b) Decryption

Fig. 2.7.4 Counter mode

Advantages

1. Simple to implement.
2. It provides confidentiality.
3. Random access of block is possible.
4. Efficiency is same as block cipher.

Review Questions

1. *Explain the operation of Cipher Block Chaining (CBC) Mode.*	**SPPU : April-16, Marks 5**
2. *Explain Cipher Feedback Mode (CFB) block cipher.*	**SPPU : May-17, Marks 5**
3. *Explain following algorithm modes : i) ECB ii) OFB*	**SPPU : March-19, Marks 5**
4. *Write short note on electronic code book.*	**SPPU : March-20, Marks 5**

2.8 Simple DES

- 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 :**

$$P10(k_1 k_2 k_3 k_4 k_5 k_6 k_7 k_8 k_9 k_{10}) = k_3 k_5 k_2 k_7 k_4 k_{10} k_1 k_9 k_8 k_6$$

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 :

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

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. 2.8.1 shows one round of a Feistel system.

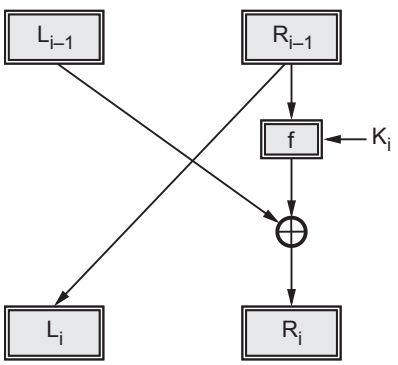


Fig. 2.8.1 One round of a Feistel system

- 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 $K_1, K_2 \ldots\ldots K_n$ and for decryption will be $K_n, \ldots K_{n-1} \ldots\ldots K_1$.
- **Function $f(R_{i-1}, K_i)$:** The function $f(R_{i-1}, K_i)$, depicted in the Fig. 2.8.2 below, is described in following steps.

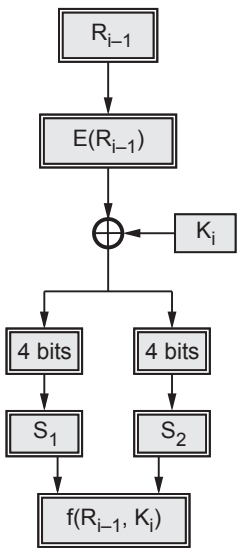


Fig. 2.8.2 The function f (R_{i-1}, k_i)

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.

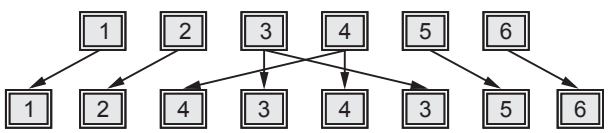


Fig. 2.8.3 The expansion function, $E(R_{i-1})$

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.

2.9 Data Encryption Standard

SPPU : April-16,17, May-16,17,18, Dec.-17, March-19,20

- 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. 2.9.1 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. 2.9.1 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.

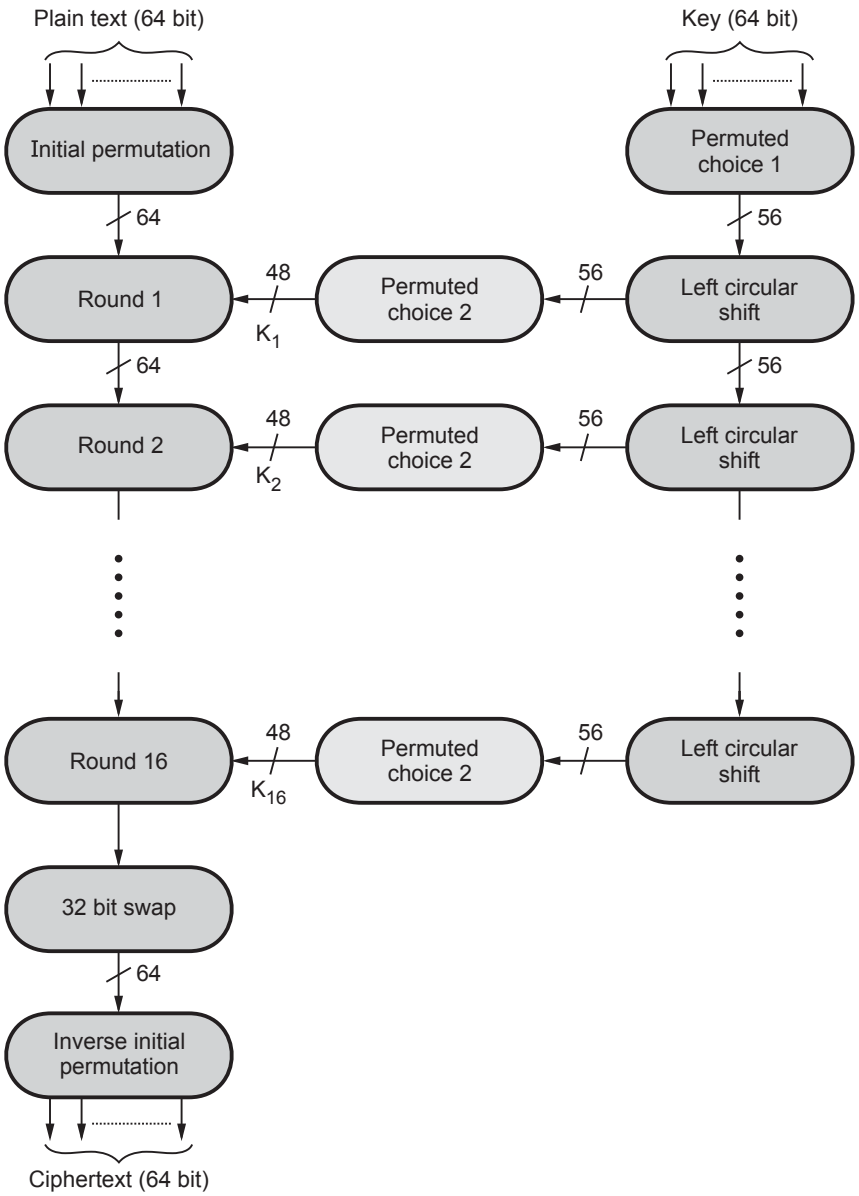


Fig. 2.9.1 DES encryption algorithm

- 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

2.9.1 Details of Single Round

- Fig. 2.9.2 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 :

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

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

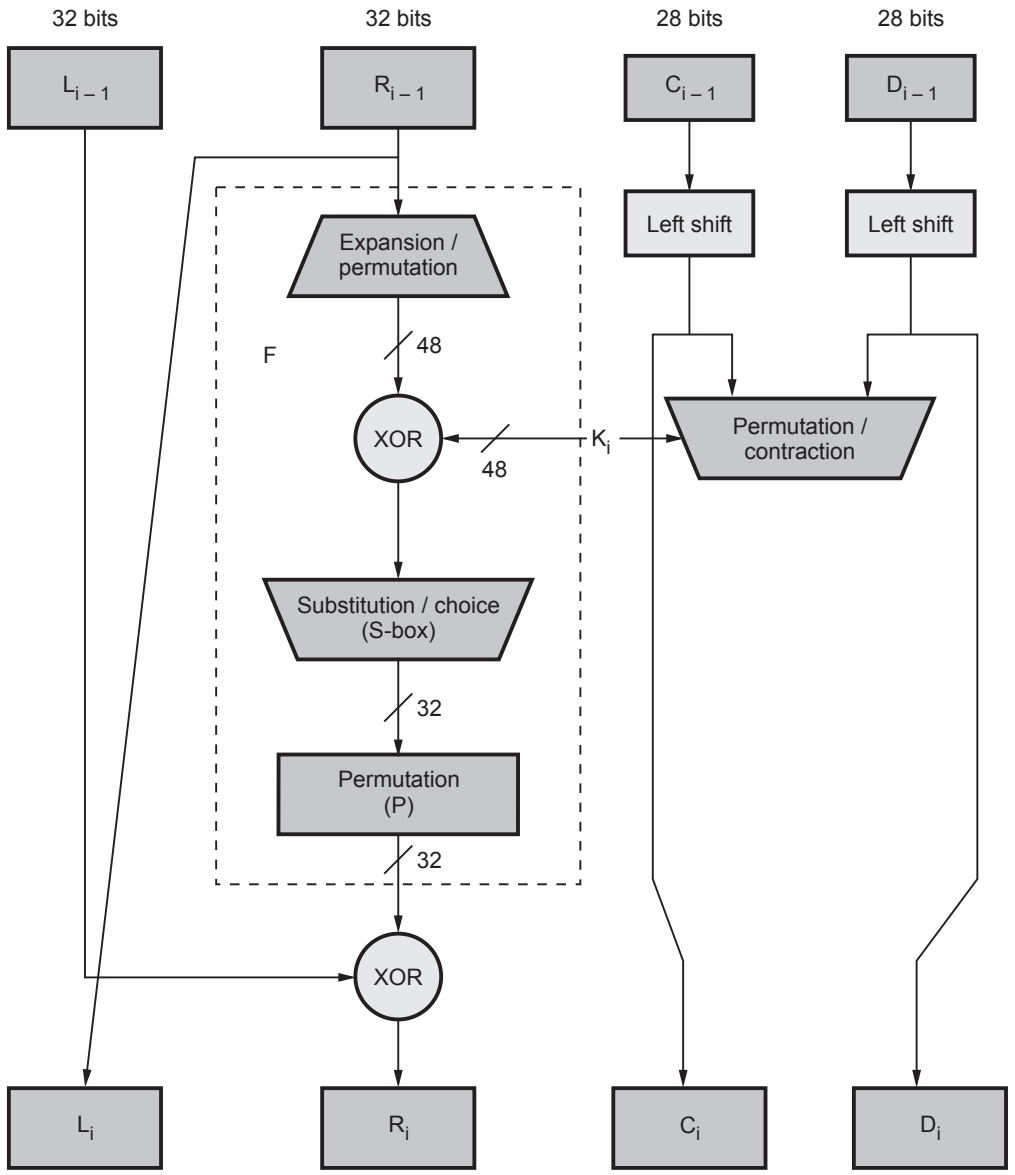


Fig. 2.9.2 Single round of DES algorithm

- 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. 2.9.3 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.

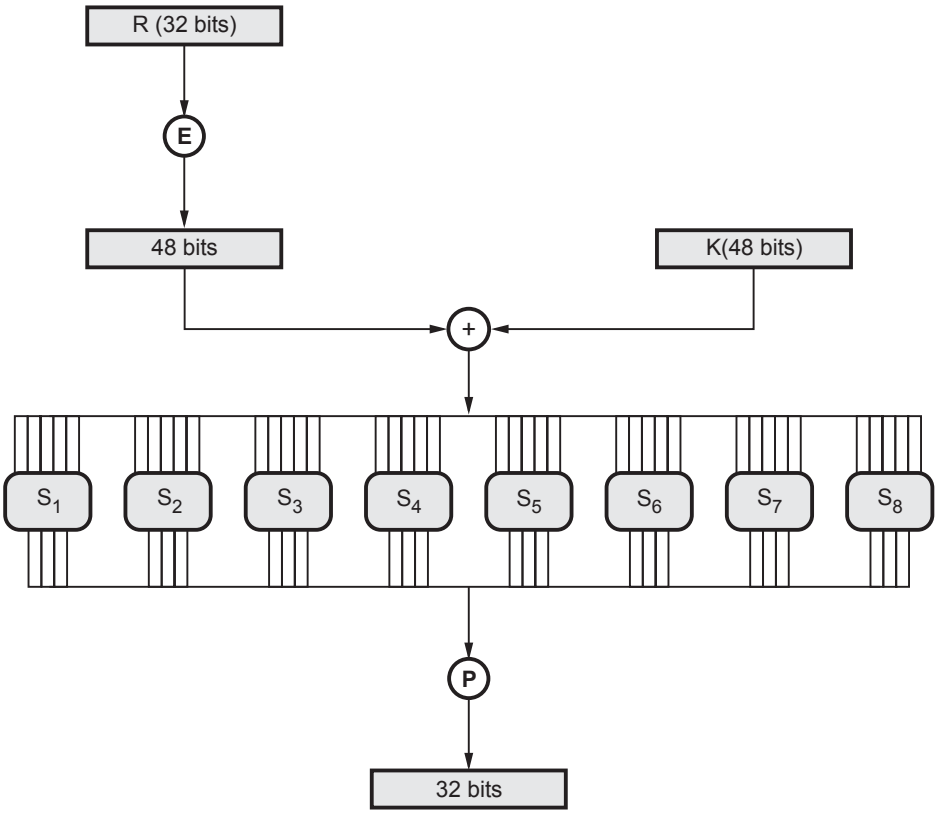


Fig. 2.9.3 S-boxes in the function (F)

- 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

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. 2.9.4 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.

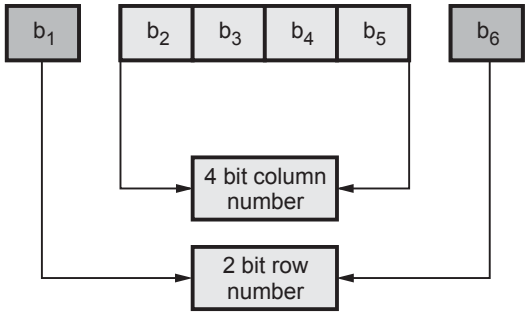


Fig. 2.9.4 Selecting entry in S-box

2.9.2 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 $F(R_{i-1}, K_i)$.

2.9.3 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.
- 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 :

$$\left.\begin{aligned} L' &= R \\ R' &= L\ (+)\ f(R, K) \end{aligned}\right\} \quad \ldots (2.9.1)$$

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 (2.9.1) 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,

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. 2.9.5

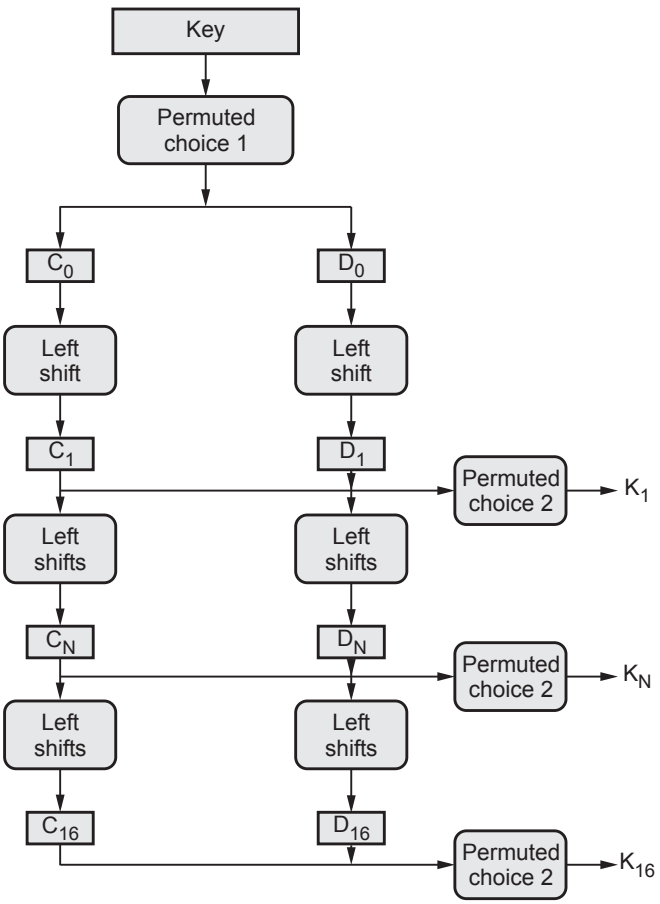


Fig. 2.9.5 Key generation techniques

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.

2.9.4 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.

2.9.5 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.

2.9.6 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.

2.9.7 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.

2.9.8 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.

2.9.9 Double DES

- Using two encryption stages and two keys.
  A) The plain text to ciphertext is as follows,

$$C = E_{K_2}(E_{K_1}(P)) \text{ where } k_1 \text{ and } k_2 \text{ are the key.}$$

  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. 2.9.6 shows the meet-in-the-middle attack for double DES.

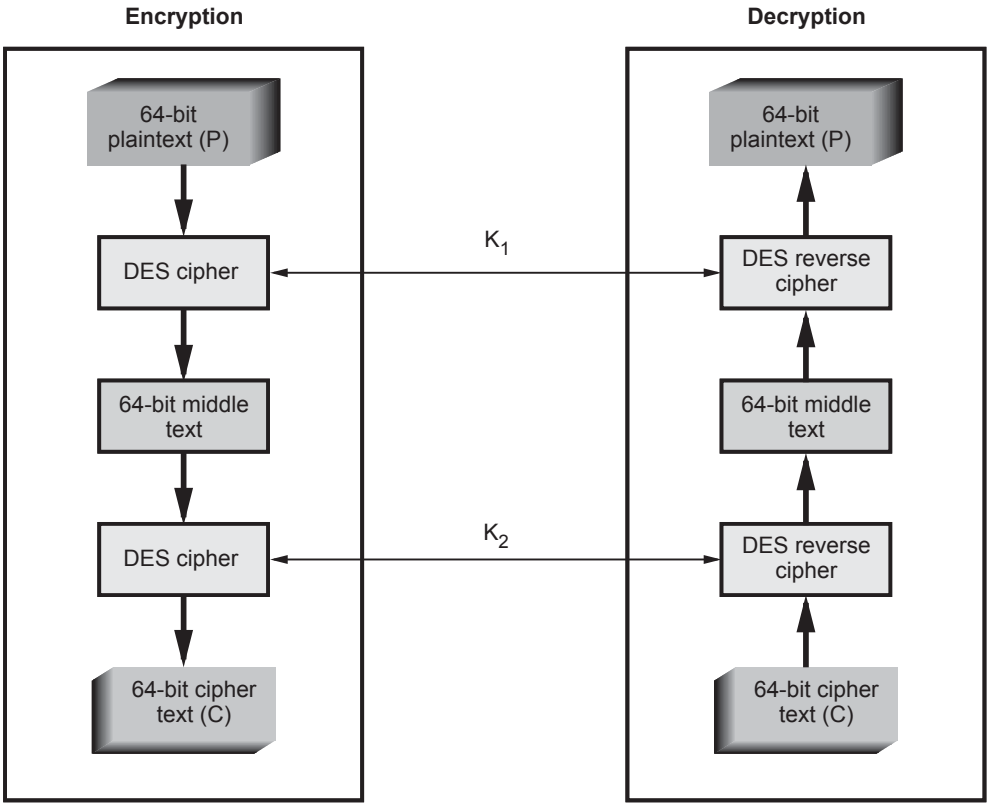


Fig. 2.9.6 Meet-in-the-middle attack for double DES

2.9.10 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. 2.9.7 shows the 3DES method with three key.

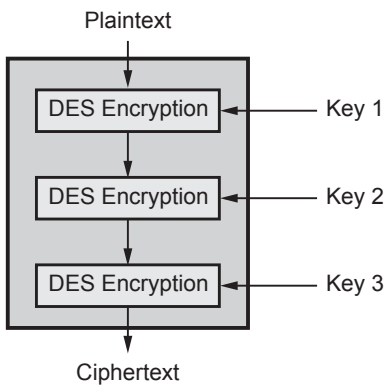


Fig. 2.9.7 3DES with three key method

- 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.
- 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.

Review Questions

1. *Explain the operation of DES algorithm in detail.* **SPPU : April-16, 17, Marks 5**
2. *Explain 3DES algorithm in detail.* **SPPU : May-16, Marks 5**
3. *What is weak key in DES algorithm ? Explain with example.* **SPPU : May-17, Marks 5**
4. *Explain operation of 3DES algorithm.* **SPPU : Dec.-17, Marks 5**
5. *Explain the operation of triple DES algorithm.* **SPPU : May-18, Marks 5**
6. *Explain the operation of DES algorithm in detail.* **SPPU : March-19, Marks 5**
7. *Explain DES algorithm with diagram.* **SPPU : March-20, Marks 5**

2.10 Confusion and Diffusion

Diffusion

- Diffusion is making output dependent on previous input (plain/cipher-text). Ideally, each output bit is influenced by every previous input bit.
- These are measures to thwart cryptanalysis based on statistical analysis. In diffusion, the statistical structure of the plaintext is dissipated into long range statistics of the cipher-text.
- This is achieved by having each plaintext letter affect the value of many cipher-text digits, which is equivalent to saying that each cipher-text digit is affected by many plaintext digits.
- The letter frequencies in the cipher-text will be more nearly equal than in the plaintext.

Confusion

- In Shannon's original definitions, confusion makes the relation between the key and the cipher-text as complex as possible. Confusion is making the output dependent on the key. Ideally, every key bit influences every output bit. Confusion tries to hide the connection between the cipher-text and the secret key.
- Confusion seeks to make the relationship between the statistics of the cipher-text and the value of the encryption key as complex as possible. This is achieved by the use of a complex substitution algorithm. These operations became the cornerstone of modern block cipher design.

2.10.1 Distinguish between Diffusion and Confusion

No.	Diffusion	Confusion
1.	Diffusion hides the relation between the ciphertext and the plaintext.	Confusion hides the relation between the ciphertext and key.
2.	If a single symbol in the plaintext is changed, several or all symbols in the ciphertext will also be changed.	If a single bit in the key is changed, most or all bits in the ciphertext will also be changed.
3.	In diffusion, the statistical structure of the plain text is dissipated into long-range statistics of the cipher text. This is achieved by permutation.	In confusion, the relationship between the statistics of the cipher text and the value of the encryption key is made complex. It is achieved by substitution.

2.11 Advanced Encryption Standard

SPPU : April-16, May-17, 19

- Advanced Encryption Standard (AES) is a symmetric key block cipher published by the NIST in December 2001.

2.11.1 Evaluation Criteria for AES

- NIST evaluation criteria for AES are
  1. Security
  2. Cost
  3. Algorithm and implementation characteristics.

1. Security

- This refers to the effort required to cryptanalyse an algorithm. Following parameters are also consider for evaluation.
  a. **Actual security** compared to other submitted algorithms.
  b. **Randomness :** The extent to which the algorithm output is indistinguishable from a random permutation on the input block.

c. **Soundness** of the mathematical basis for the algorithm's security.

d. Other security factors raised by the public during the evaluation process.

2. Cost

a. Licensing requirements : When the AES is issued, the algorithm specified in the AES shall be available on a worldwide, non-exclusive, royalty free basis.

b. Computational efficiency : The evaluation of computational efficiency will be applicable to both hardware and software implementations.

c. Memory requirements : The memory requirement for implementing the algorithm in hardware and software will be considered.

3. Algorithm and Implementation Characteristics

This category includes a variety of considerations, including flexibility, suitability for a variety of hardware and software implementations; and simplicity, which will make an analysis of security more straight forward.

The following criteria were used in the final evaluation :

1. **General security :** NIST relied on the public security analysis conducted by the cryptographic community.
2. **Software implementations :** It includes execution speed, performs across a variety of platforms and variation of speed with key size.
3. Restricted space environments.
4. Hardware implementations.
5. Attacks on implementations.
6. Encryption versus decryptions.
7. Key agility.
8. Other versatility and flexibility.
9. Potential for instruction level parallelism.

2.11.2 AES Cipher

- AES is a non-Feistel cipher that encrypts and decrypts a data block of 128-bits.
- The key size can be 128, 192 or 256-bits. It depends on number of rounds.
- The number of rounds : 10 rounds for 128-bits, 12 rounds for 192-bits and 14 rounds for 256-bits.

Characteristics

1. Resistance against all known attacks.
2. Speed and code compactness on a wide range of platforms.
3. Design simplicity.

- For 128-bits AES, each round contains four steps :
  i. Byte substitution ii. Row shift
  iii. Column mixing iv. Round key addition
- The input to the encryption and decryption algorithms is a single 128-bit block. The block is represented as a row of matrix of 16 bytes.
- Fig. 2.11.1 shows the overall structure of AES.

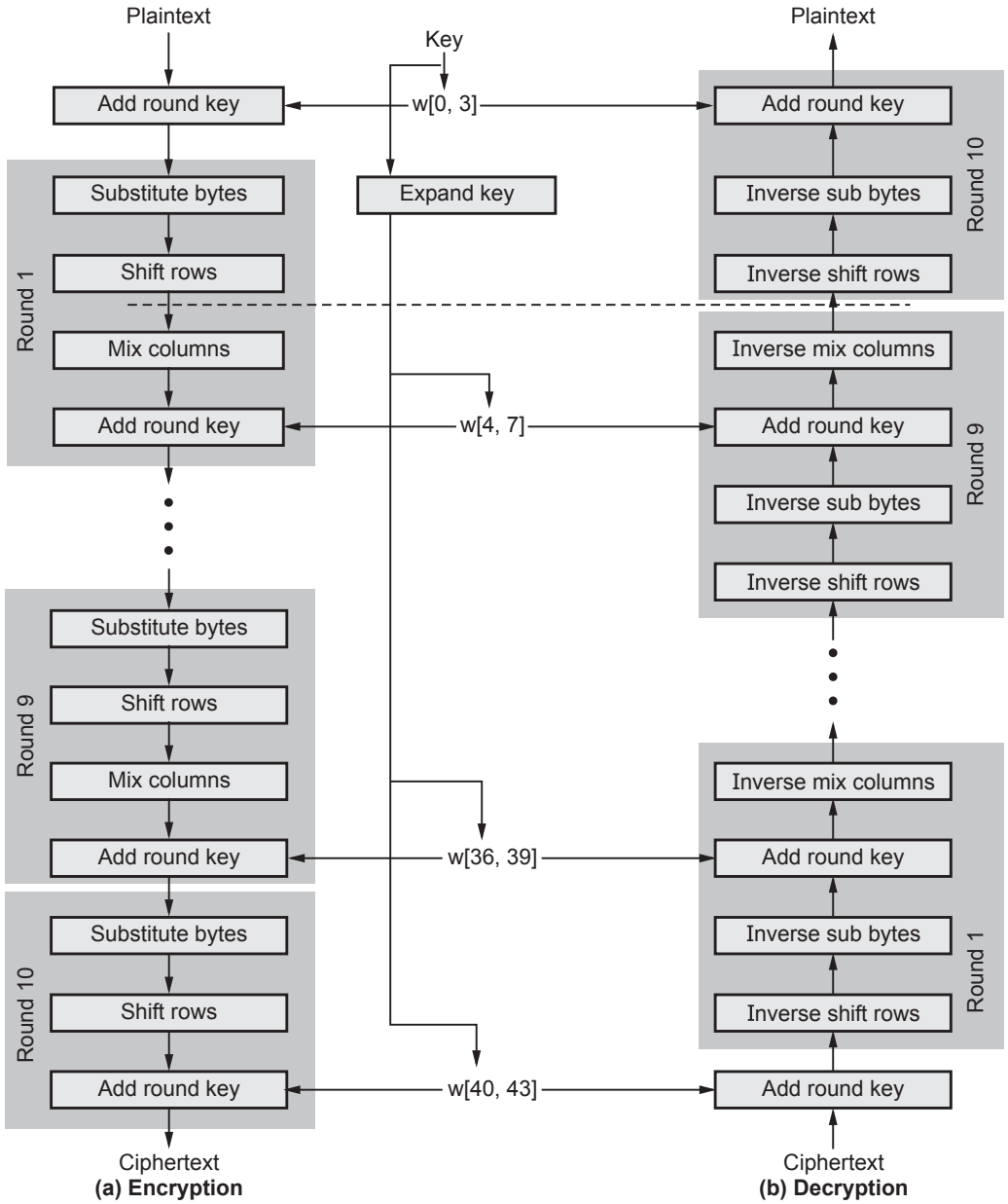


Fig. 2.11.1 AES encryption and decryption

- AES use several rounds in which each round is made of several stages. Data block is transformed from one stage to another.
- Data block is referred to as **state**. Block is copied into state array which is modified at each stage of encryption or decryption. After the final stage, state is copied to an output matrix.

Comments about the AES structure

1. AES structure is not a Feistel structure.
2. The key that is provided as input is expanded into an array of forty-four 32-bit words, w(i).
3. Four different stages are used, one of permutation and three of substitution.
4. For both encryption and decryption, the cipher begins with an AddRoundkey stage, followed by nine rounds that each includes all four stages, followed by a tenth round of three stages.
5. Only the AddRoundkey stage make use of the key.
6. The AddRoundkey stage is, in effect, a form of Vernam Cipher and by itself would not be formidable.
7. Each stage is easily reversible.
8. The decryption algorithm makes use of the expanded key in reverse order.
9. Once it is established that all four stages are reversible, it is easy to verify that decryption does recover the plaintext.
10. The final round of both encryption and decryption consists of only three stages.

2.11.3 Comparison between AES and DES

Sr. No.	Parameters	AES	DES
1	Block size	128-bits	64-bits
2	Key length	128, 192, 256-bits	56-bits (effective length)
3	Encryption primitives	Substitution, shift, bit mixing	Substitution, Permutation
4	Cryptographic primitives	Confusion, Diffusion	Confusion, Diffusion
5	Design rationale	Closed	Open

Review Questions

1. *Explain operation of AES algorithm and state its application.* **SPPU : April-16, Marks 5**
2. *Explain the operation in key expansion process in AES algorithm.* **SPPU : May-17, Marks 5**
3. *Explain working of AES in detail.* **SPPU : May-19, Marks 5**

2.12 Multiple Choice Questions

Q.1 A symmetric encryption model has _____ ingredients.

a four b three

c five d six

Q.2 The one time pad is susceptible to a _____.

a chosen plain text attack b known plain text attack

c known cipher text attack d none of these

Q.3 Secret key cryptography is also known as _____.

a symmetric key cryptography

b asymmetric key cryptography

c private key cryptography

d quantum cryptography

Q.4 In cryptography, what is cipher ?

a Encrypted message

b Decrypted message

c Algorithm for performing encryption and decryption

d Both (a) and (b)

Q.5 Which is the largest disadvantage of the symmetric encryption ?

a More complex and therefore more time-consuming calculations.

b Problem of the secure transmission of the secret key.

c Less secure encryption function.

d Isn't used any more.

Q.6 _____ DES was designed to increase the size of the DES key.

a Double b Triple

c Quadruple d None of the above

Q.7 ECB and CBC are _____ ciphers.

a block b stream

c field d product

Q.8 The AES key expansion algorithm takes as input a _____ key and produces a linear array of 156 bytes.

a 8-byte
b 12-byte
c 16-byte
d 24-byte

Q.9 Substitution box provides _____.

a confusion
b diffusion
c both confusion and diffusion
d none of these

Q.10 DES encrypts data in block size of _____ bits each.

a 32
b 56
c 64
d 128

Q.11 DES consists of _____ rounds to perform the substitution and transposition techniques.

a 16
b 18
c 21
d 25

Q.12 DES uses a key generator to generate sixteen _____ round keys.

a 32-bit
b 42-bit
c 48-bit
d 56-bit

Q.13 _____ is the first step in DES.

a Key transformation
b Expansion permutation
c S-box substitution
d P-box substitution

Q.14 DES has _____ weak keys.

a 2
b 4
c 6
d 8

Q.15 The input block length in AES is _____.

a 56 bits
b 64 bits
c 112 bits
d 128 bit

Q.16 Differential attack is a _____.

a chosen text

b chosen-plaintext attack

c cipher text only

d known plaintext

Q.17 DES encryption standard is a _____ cipher published by the NIST.

a asymmetric key block

b symmetric key stream

c asymmetric key stream

d symmetric key block

Answer Keys for Multiple Choice Questions :

Q.1	c	**Q.2**	d	**Q.3**	a	**Q.4**	c
Q.5	b	**Q.6**	b	**Q.7**	a	**Q.8**	c
Q.9	a	**Q.10**	c	**Q.11**	a	**Q.12**	c
Q.13	a	**Q.14**	c	**Q.15**	d	**Q.16**	b
Q.17	d						

❑❑❑

UNIT III

3 Asymmetric Key Cryptography

Syllabus

Number theory : *Prime number, Fermat and Euler theorems, Testing for primality, Chinese reminder theorem, discrete logarithm, Public Key Cryptography and RSA, Key Management, Diffie-Hellman key exchange, El Gamal algorithm, Elliptic Curve Cryptography*

Contents

3.1 Number Theory

- Number theory is the study of the integers.
- In modern cryptographic system, the messages are represented by numerical values prior to being encrypted and transmitted. The encryption processes are mathematical operations that turn the input numerical values into output numerical values.
- Mathematical tools are required for building, analyzing and attacking the cryptosystems.

3.1.1 Divisibility

Definition : *Given two integers 'a' and 'b', we say 'a' divides 'b' if there is an integer c such that b = ac. If a divides b, we write a|b.*

For example : 7/63 because $7 \times 9 = 63$

- A consequence of this definition is that every number divides zero. Since a.0 = 0 for every integer a. If a divides b, then b is a ***multiple*** of a. For example, 63 is a multiple of 7.
- The following statements about divisibility hold.
  1. If a | b, then a | bc for all c.
  2. If a | b and b | c, then a | c.
  3. If a | b and a | c, then a | sb + tc for all s and t.
  4. For all c ≠ 0, a | b if and only if ca | cb.

Example 3.1.1 *Which of the following is true ?*
1. 77 | 7 2. 7 | 77 3. 24 | 24 4. 0 | 24 5. 24 | 0

Solution :

1. 77 | 7 : False bigger number can't divide smaller positive number
2. 7 | 77 : True because $77 = 7 \cdot 11$
3. 24 | 24 : True because $24 = 24 \cdot 1$
4. 0 | 24 : False, only 0 is divisible by 0
5. 24 | 0 : True, 0 is divisible by every number $(0 = 24 \cdot 0)$

3.1.2 Prime Number

- A prime number is an integer that can only be divided without remainder by positive and negative values of itself and 1.
- Any integer a > 1 can be factored in a unique way as

$$a = p_1^{a1} p_2^{a2} p_3^{a3} \ldots\ldots p_t^{at}$$

Where $p_1 < p_2 < \ldots < p_t$ are prime numbers and where each a_i is a positive integer. This is known as the fundamental theorem of arithmetic.

- If p is the set of all prime numbers then any positive integer a can be written uniquely in the following form :

$$a = \prod_{PE^p} p^{a_p} \text{ where each } a_p \geq 0$$

3.1.2.1 Relatively Prime Numbers

- **Definition :** Two integers a and b are **relatively prime** if gcd (a, b) = 1.
- The integers a1, a2, ..., an are **pair-wise relatively prime** if gcd (ai, aj) = 1 whenever $1 \leq i < j \leq n$.
- **Example 1 :** Are 15, 17 and 27 pair-wise relatively prime ? *No, because gcd (15, 27) = 3.*
- **Example 2 :** Are 15, 17 and 28 pair-wise relatively prime ? *Yes, because gcd (15, 17) = 1, gcd (15, 28) = 1 and gcd (17, 28) = 1.*
- Number that is relatively prime to another number means that the GCD of the two numbers is 1. Therefore, it does not mean that either of the numbers has to be prime.
- The method for calculating the number of relatively prime numbers less than a given number involves prime factorization, which can be reviewed in positive integral divisors.
  1. Find the exponential prime factorization of the number.
  2. Taking each term separately, change the term to 2 numbers :
     a. Subtract 1 from the base for the first number.
     b. Subtract 1 from the exponent and evaluate the expression for the second number.
  3. Multiply all the numbers together found in step 2.

Example : How many numbers less than 20 are relatively prime to 20 ?

- The prime factorization of 20 is : $2^2 \times 5^1$
- Taking 2^2 first, we get : $2-1=1$ and $2^2-1=2$
- Taking 5^1 we get : $5-1=4$ and $5^1-1=1$
- Multiplying all of them together we get : (1) (2) (4) (1) or 8.
- The answer is 8. The numbers which are relatively prime are 1, 3, 7, 9, 11, 13, 17 and 19. So indeed there are 8.

Example 3.1.2 *Is 97 a prime ?*

Solution : The floor of $\sqrt{97}$ = 9. The primes less than 9 are 2, 3, 5, and 7. We need to see if 97 is divisible by any of these numbers. It is not, so 97 is a prime.

3.1.3 Greatest Common Divisor

- Definition. A positive integer d is called the greatest common divisor of the nonzero integers a and b if
  i) d is a divisor of both a and b, and
  ii) Any divisor of both a and b is also a divisor of d.
- We will use the notation gcd(a, b), or simply (a, b), for the greatest common divisor of a and b.
- Greatest Common Divisor gcd(a,b) is the largest number that divides both a and b.
- If a and b share no common factors, they are called relatively prime.

Example 3.1.3 *Find gcd (1403, 1081).*

Solution : 1403 = 1081.1 + 322

1081 = 322.3 + 115

322 = 115.2 + 92

115 = 92.1 + 23

92 = 23.4 + 0

The last nonzero remainder is 23, so gcd(1403, 1081) = 23.

Example 3.1.4 *Find gcd (120 , 70).*

Solution : 120 = 70 +50

70 = 50 +20

50 = $20 \times 2 + 10$

20 = $10 \times 2 + 0$

Therefore gcd (120,70) = 10.

- It is always possible to write gcd(a, b) as a linear combinations of a and b. That is, there exist integers x and y such that gcd(a, b) = ax+by (x or y may be negative).
- In fact, though we have not proved it, gcd(a, b) is the smallest positive linear combination of a and b. Once we use the Euclidean algorithm to find gcd(a, b) we can then retrace our steps to write gcd(a, b) in the form ax+by.

3.2 Fermat and Euler Theorems

Prime Number

- A prime number is divisible only by 1 and itself.
  For example : {2, 3, 5, 7, 11, 13, 17, …}
- 1 could also be considered prime, but it's not very useful.
- To factor a number n is to write it as a product of other numbers.
- For example $n = a * b * c$ Or, 100 = 5 * 5 * 2 * 2
- Prime factorization of a number n is writing it as a product of prime numbers.
  i.e. 143 = 11 * 13

Relatively prime numbers

- Two numbers are relatively prime if they have no common divisors other than 1. For example 10 and 21 are relatively prime, in respect to each other, as 10 has factors of 1, 2, 5, 10 and 21 has factors of 1, 3, 7, 21.
- The Greatest Common Divisor (GCD) of two relatively prime numbers can be determined by comparing their prime factorizations and selecting the least powers.
- For example : $125 = 5^3$ and $200 = 2^3 * 5^2$
  $GCD(125, 200) = 2^0 * 5^2 = 25$
- If the two numbers are relatively prime the GCD will be 1.
- Consider the following :
  10 = (1, 2, 5, 10) and 21 = (1, 3, 7, 21) then GCD (10, 21) = 1
- It then follows, that a prime number is also relatively prime to any other number other than itself and 1.

Fermat's Little Theorem

- If p is prime and a is an integer not divisible by p, then . . .
  $a^{p-1} \equiv 1 \pmod{p}$.
- And for every integer a :
  $a^p \equiv a \pmod{p}$.
- This theorem is useful in public key (RSA).

3.2.1 Fermat's and Euler's Theorems

Fermat's theorem

If p is prime and a is a positive integer not divisible by p, then $a^{p-1} \equiv 1 \bmod(p)$.

Proof : Consider the set of positive integers less than p : {1, 2, … p – 1} and multiply each element by a, modulo p, to get the set X = {a mod p, 2a mod p, …… (p – 1) a

mod p}. None of the elements of X is equal to zero because p does not divide a. Further more no two of the integers in X are equal.

Euler's theorem

Euler's theorem states that for every a and n that are relatively prime :

$$a^{\phi(n)} \equiv 1 \pmod{n} \quad \ldots (3.2.1)$$

Proof : Equation (3.2.1) is true if n is prime because in that case $\phi(n) = (n - 1)$ and Fermat's theorem holds. It also holds for any integer n. Recall that $\phi(n)$ is the number of positive integers less than n that are relatively prime to n. Consider the set of such integers, labelled as follows :

$$R = \{x_1, x_2, x_{\phi(n)}\}$$

That is, each element x_1 of R is a unique positive integer less than n with

gcd $(x_i, n) = 1$. Now multiply each element by a, modulation n :

$$S = \{(ax_1 \bmod n), (ax_2 \bmod n) \ldots\ldots (ax_{\phi(n)} \bmod n)\}$$

The set S is a permutation of R.

Therefore,

$$\prod_{i=1}^{\phi(n)} (ax_i \bmod n) = \prod_{i=1}^{\phi(n)} x_i$$

$$\prod_{i=1}^{\phi(n)} ax_i \equiv \prod_{i=1}^{\phi(n)} x_i \pmod{n}$$

$$a^{\phi(n)} \times \left[\prod_{i=1}^{\phi(n)} x_i\right] \equiv \prod_{i=1}^{\phi(n)} x_i \pmod{n}$$

$$a^{\phi(n)+1} \equiv a \pmod{n}$$

Example 3.2.1 *Explain Fermat's little theorem and solve the following using the same : i) 15^{18} mod 17 ii) 5^{27} mod 13*

Solution : Fermat's little theorem

1. If p is prime and a is an integer not divisible by p, then . . .

$$a^{p-1} \equiv 1 \pmod{p}.$$

2. And for every integer a :

$$a^{p-1} \equiv 1 \pmod{p}.$$

3. This theorem is useful in public key (RSA).

Fermat's theorem

If p is prime and a is a positive integer not divisible by p, $a^{p-1} \equiv 1\ a^{p-1} \bmod(p)$.

Proof : Consider the set of positive integers less than p : {1, 2, … p – 1} and multiply each element by a, modulo p, to get the set X = {a mod p, 2a mod p, …… (p – 1) a mod p}. None of the elements of X is equal to zero because p does not divide a. Further more no two of the integers in X are equal.

i) $15^{18} \bmod 17$

$$= [(15 \bmod 17) \times (15^{17} \bmod 17)] \bmod 17$$

$$= [(-2 \bmod 17) \times (-2 \bmod 17)] \bmod 17$$

$$= 4 \bmod 17$$

ii) $527 \bmod 13$

$$= [(5^{14} \bmod 13) \times (5^{13} \bmod 13)] \bmod 13$$

$$= [(12 \bmod 13) \times (5 \bmod 13)] \bmod 13$$

$$= 8 \bmod 13$$

3.3 Testing for Primality

Two properties of prime numbers

1. If p is prime and a is a positive integer less than p, then $a^2 \bmod p = 1$ if an only if either a mod p = 1 or mod p = – 1 and p = p – 1. By the rules of modular arithmetic (a mod p) (a mod p) = a^2 mod p.
   Thus if either a mod p = 1 or a mod p = –1 then a^2 mod p = 1. Conversely, if a^2 mod p = 1, then $(a \bmod p)^2 = 1$ which is true only for a mod p = 1 or a mod p = –1.
2. Let p be a prime number greater than 2. We can then write $p - 1 = 2^k q$, with k > 0, q odd. Let a be any integer in the range 1 < a < p – 1. Then one of the following conditions is true.
   a) a^q is congruent to 1 modulo p. That is $a^q \bmod p = 1$ or equivalently $a^q \equiv 1 \pmod{p}$.
   b) One of the numbers $a^q, a^{2q}, a^{4q}, \ldots\ldots a^{2^{K-1}q}$ is congruent to – 1 modulo p. That is, there is some number j in the range $(1 \le j \le K)$ such that $a^{2^{j-1}q} \bmod p = -1 \bmod p = p - 1$ or equivalently, $a^{2^{j-1}q} = -1 \pmod{p}$.

3.4 Chinese Reminder Theorem

- Find a number x such that have remainders of 1 when divided by 3, 2 when divided by 5 and 3 when divided by 7. i.e.
  1. $x = 1 \bmod 3$
  2. $x = 2 \bmod 5$
  3. $x = 3 \bmod 7$
- Integers can be represented by their residues modulo a set of pair-wise relatively prime moduli. For example : In Z_{10}, integer 8 can be represented by the residues of the 2 relatively prime factors of 10 (2 and 5) as a tuple (0, 3).
- Let $M = m_1 \times m_2 \times m_3 \times ... \times m_k$, where m_i's are pairwise relatively prime, i.e. $\gcd(m_i, m_j) = 1, 1 \leq i \neq j \leq k$.
- Assertion.
  1. $A \leftrightarrow (a_1, a_2, ... a_k)$, where $A \in Z_m$, $a_i \in Z_{mi}$ and $a_i = A \bmod m_i$ for $1 \leq i \leq k$.
  a) One to one correspondance (bijection) between Z_M and the cartesian product $Z_{m1} \times Z_{m2} \times ... \times Z_{mk}$.
  b) For every integer A such that $0 \leq A < M$, there is a unique k-tuple $(a_1, a_2, ... a_k)$ with $0 \leq a_i < m_i$.
  c) For every such k-tuple $(a_1, a_2, ... a_k)$, there is a unque A in Z_M.
  d) Transformation from A to $(a_1, a_2, ... a_k)$ is unique
  e) Computing A from $(a_1, a_2, ... a_k)$ is done as follows :
     1. Let $M_i = M/m_i$ for $1 \leq i \leq k$; i.e. $M_i = m_1 \times m_2 \times ... \times m_{i-1} \times .. \times m_k$
     2. Note that $M_i \equiv 0 \pmod{m_j}$ for all $j \neq i$
     3. Let $c_i = M_i \times (M_i^{-1} \bmod m_i)$ for $1 \leq i \leq k$
     4. Then $A \equiv (a_1c_1 + a_2c_2 + ... + a_kc_k) \bmod M$
     5. $\leftarrow a_i = A \bmod m_i$, since $c_j \equiv M_j \equiv 0 \pmod{m_i}$ if $j \neq i$ and $c_i \equiv 1 \pmod{m_i}$
- Operations performed on the elements of Z_M can be equivalently performed on the corresponding k-tuples by performing the operation independently in each co-ordinate position.
  Example : $A \leftrightarrow (a_1, a_2, ... a_k)$, $B \leftrightarrow (b_1, b_2, ... b_k)$

$$(A + B) \bmod M \leftrightarrow ((a_1 + b_1) \bmod m_1, ... (a_k + b_k) \bmod m_k)$$

$$(A - B) \bmod M \leftrightarrow ((a_1 - b_1) \bmod m_1, ... (a_k - b_k) \bmod m_k)$$

$$(A \times B) \bmod M \leftrightarrow ((a_1 \times b_1) \bmod m_1, ... (a_k \times b_k) \bmod m_k)$$

- CRT provides a way to manipulate (potentially large) numbers mod M in terms of tuple of smaller numbers.

Chinese remainder theorem :

Suppose gcd (m, n) = 1. given a and b, there exists exactly one solution x (mod mn) to the simultaneous congruence under certain conditions.

$$x \equiv a \pmod{m}, \quad x \equiv b \pmod{n}.$$

Proof :

- There exist integers s, t such that ms + nt = 1. Then ms ≡ 1 (mod n) and nt ≡ 1 (mod m). Let x = bms + ant. Then x ≡ ant ≡ a (mod m) and x ≡ bms ≡ b (mod n), as desired.
- Suppose x_1 is another solution. Then $x \equiv x_1 \pmod{m}$ and $x \equiv x_1 \pmod{n}$, so $x\text{-}x_1$ is a multiple of both m and n.

Lemma :

Let m, n be integers with gcd (m, n) = 1. If an integer c is a multiple of both m and n, then c is a multiple of mn.

Proof :

Let c = mk = nl. Write ms + nt = 1 with integers s, t. Multiply by c to obtain
c = cms + cnt = mnls + mnkt = mn (ls + kt).

- To finish the proof of the theorem, let $c = x - x_1$ in the lemma to find that $x - x_1$ is a multiple of mn. Therefore, $x \equiv x_1 \pmod{mn}$. This means that any two solutions x to the system of congruences are congruent mod mn, as claimed.

Example 3.4.1 *Solve x ≡ 3 (mod 7), x ≡ 5 (mod 15).*

Solution : x ≡ 80 (mod 105) (**Note :** 105 = 7·15). Since 80 ≡ 3 (mod 7) and 80 ≡ 5 (mod 15), 80 is a solution. The theorem guarantees that such a solution exists, and says that it is uniquely determined mod the product mn, which is 105 in the present example.

How to solve :

- One way, which works with small numbers m and n, is to list the numbers congruent to b (mod n) until you find one that is congruent to a (mod m).
- For example, the numbers congruent to 5 (mod 15) are
  5, 20, 35, 50, 65, 80, 95, ...

  Mod 7, there are 5, 6, 0, 1, 2, 3, 4, ... since we want 3 (mod 7), we choose 80.
- For slightly larger numbers m and n, making a list would be inefficient. However, a similar idea works. The numbers congruent to b (mod n) are of the form b + nk with k an integer, so we need to solve b + nk ≡ a (mod m). This is the same as
  $$nk \equiv a - b \pmod{m}.$$
- Since gcd (m, n) = 1 by assumption, there is a multiplicative inverse i for n (mod m). Multiplication by 1 gives,

$$k \equiv (a - b)\, i \pmod{m}.$$

Substituting back into $x = b + nk$, then reducing mod mn, gives the answer.

Example 3.4.2 *Solve $x \equiv 7 \pmod{12345}$, $x \equiv 3 \pmod{11111}$.*

Solution : First, we know from our calculations in section that the inverse of 11111 (mod 12345) is i = 2471.

Therefore $k \equiv 2471\ (7 - 3) \equiv 9884 \pmod{12345}$. This yields $x = 3 + 11111 \equiv 9884 \equiv 109821127 \pmod{(11111.12345)}$.

Example 3.4.3 *In a chinese remainder theorem, let $n = 210$ and let $n_1 = 5$, $n_2 = 6$, $n_3 = 7$. Compute f^{-1} (3, 5, 2), i.e. given $x_1 = 3$, $x_2 = 5$, $x_3 = 3$, compute x.*

Solution :

$$N_1 = n_2 \times n_3 = 42$$

$$N_2 = n_1 \times n_3 = 35$$

$$N_3 = n_1 \times n_2 = 30$$

$$v_1 \equiv (N_1)^{-1} \equiv 42^{-1} \equiv 2^{-1} \equiv 3 \pmod{5}$$

$$v_2 \equiv (N_2)^{-1} \equiv 35^{-1} \equiv 5^{-1} \equiv 5 \pmod{6}$$

$$v_3 \equiv (N_3)^{-1} \equiv 30^{-1} \equiv 2^{-1} \equiv 4 \pmod{7}$$

$$x \equiv a_1 v_1 N_1 + a_2 v_2 N_2 + a_{133} N_3$$

$$\equiv 126 + 875 + 360$$

$$\equiv 1361$$

$$x \equiv 101 \pmod{210}$$

Example 3.4.4 *State chinese remainder theorem and find X for the given set of congruent equations using CRT.*

X = 2 (mod 3)

X = 3 (mod 5)

X = 2 (mod 7).

Solution : The Chinese Remainder Theorem (CRT) tells us that since 3, 5 and 7 are co-prime in pairs then there is a unique solution modulo $3 \times 5 \times 7 = 105$.

$n_1 = 3, \quad n_2 = 5, \quad n_3 = 7$

$N = n_1 \times n_2 \times n_3 = 3 \times 5 \times 7 = 105.$

$c_1 = 2, \quad c_2 = 3, \quad c_3 = 2$

Now $N_1 = N/n_1 = 105/3$

$$N_1 = 35 \quad \text{and} \quad \text{so } d_1 = 35^{-1} \pmod 3 = 2,$$

$$N_2 = N/n_2 = 105/5 = 21 \text{ and so } d_2 = 21^{-1} \pmod 5 = 1, \text{ and}$$

$$N_3 = N/n_3 = 105/7 = 15 \text{ and so } d_3 = 15^{-1} \pmod 7 = 1.$$

Hence
$$x = (2 \times 35 \times 2) + (3 \times 21 \times 1) + (2 \times 15 \times 1)$$
$$= 233$$
$$\equiv 233 \pmod{105} = 23$$

The solution is x = 23. You can check that by noting that the relations

$$23 = 7 \times 3 + 2 \equiv 2 \pmod 3$$

$$23 = 4 \times 5 + 3 \equiv 3 \pmod 5$$

$$23 = 3 \times 7 + 2 \equiv 2 \pmod 7$$

are all satisfied for this value of x.

3.5 Euclid's Algorithm

- The Euclidean algorithm is an algorithm for finding the greatest common divisor of two positive integers.
- The greatest common divisor of two integers is defined as : An integer c is called the gcd(a, b) (read as the greatest common divisor of integers a and b) if the following 2 conditions hold :
  1) $c \mid a \cup c \mid b$
  2) For any common divisor d of a and b, $d \mid c$.
- Rule 2 ensures that the divisor c is the greatest of all the common divisors of a and b.
- One way we could find the gcd of two integers is by trial and error. Another way is that we could prime factorize each integer and from the prime factorization, see which factors are common between the two integers. However, both of these become very time consuming as soon as the integers are relatively large.
- However, Euclid devised a fairly simple and efficient algorithm to determine the gcd of two integers. The algorithm basically makes use of the division algorithm repeatedly.
- Let's say you are trying to find the gcd(a, b), where a and b are integers with $a^3 b > 0$.

- Euclid's algorithm says to write out the following :

$$a = q_1 b + r_1, \quad \text{where } 0 < r < b$$
$$b = q_2 r_1 + r_2, \quad \text{where } 0 < r_2 < r_1$$
$$r_1 = q_3 r_2 + r_3, \quad \text{where } 0 < r_3 < r_2$$
$$\vdots$$
$$r_i = q_{i+2} r_{i+1} + r_{i+2}, \quad \text{where } 0 < r_{i+2} < r_{i+1}$$
$$\vdots$$
$$r_{k-1} = q_{k+1} r_k$$

- Euclid's algorithm says that the gcd(a, b) = $\mathbf{r_k}$
- Consider computing gcd(125, 87)

$$125 = 1 * 87 + 38$$
$$87 = 2 * 38 + 11$$
$$38 = 3 * 11 + 5$$
$$11 = 2 * 5 + 1$$
$$5 = 5 * 1$$

Thus, we find gcd(125, 87) = 1

Example 3.5.1 *Find gcd (125, 20)*

Solution : $125 = 6 * 20 + 5$

$20 = 4 * 5,$

Thus, the gcd(125, 20) = 5

3.5.1 Extended Euclidean Algorithm

- One of the consequences of the Euclidean algorithm is as follows :
  Given integers a and b, there is always an integral solution to the equation ax + by = gcd(a,b).
- Furthermore, the Extended Euclidean Algorithm can be used to find values of x and y to satisfy the equation above. The algorithm will look similar to the proof in some manner.
- Consider writing down the steps of Euclid's algorithm :

$$a = q_1 b + r_1, \quad \text{where } 0 < r < b$$
$$b = q_2 r_1 + r_2, \quad \text{where } 0 < r_2 < r_1$$
$$r_1 = q_3 r_2 + r_3, \quad \text{where } 0 < r_3 < r_2$$
$$\vdots$$

.

$$r_i = q_{i+2} r_{i+1} + r_{i+2}, \quad \text{where } 0 < r_{i+2} < r_{i+1}$$

.

$$r_{k-2} = q_k r_{k-1} + r_k, \quad \text{where } 0 < r_k < r_{k-1}$$

$$r_{k-1} = q_{k+1} r_k$$

- Consider solving the second to last equation for r_k. You get

$$r_k = r_{k-2} - q_k r_{k-1}, \text{ or}$$

$$\gcd(a, b) = r_{k-2} - q_k r_{k-1}$$

Now, solve the previous equation for r_{k-1} :

$$r_{k-1} = r_{k-3} - q_{k-1} r_{k-2},$$

and substitute this value into the previous derived equation :

$$\gcd(a, b) = r_{k-2} - q_k (r_{k-3} - q_{k-1} r_{k-2})$$

$$\gcd(a, b) = (1 + q_k q_{k-1}) r_{k-2} - q_k r_{k-3}$$

- Now we have expressed gcd(a, b) as a linear combination of r_{k-2} and r_{k-3}. Next we can substitute for of r_{k-2} in terms of r_{k-3} and r_{k-4}, so that the gcd(a, b) can be expressed as the linear combination of r_{k-3} and r_{k-4}. Eventually, by continuing this process, gcd(a, b) will be expressed as a linear combination of a and b as desired.
- Find integers x and y such that : 135x +50y = 5.
- Use Euclid's algorithm to compute gcd(135, 50) :

$$135 = 2 * 50 + 35$$

$$50 = 1 * 35 + 15$$

$$35 = 2 * 15 + 5$$

$$15 = 3 * 5$$

- Now, let's use the Extended Euclidean algorithm to solve the problem :
  5 = 35 – 2 * 15, from the second to last equation 35 = 2 * 15 + 5.
- But, we have that
  15 = 50 – 35, from the third to last equation 50 = 1 * 35 + 5.
- Now, substitute this value into the previously derived equation :

$$5 = 35 - 2 * (50 - 35)$$

$$5 = 3 * 35 - 2 * 50$$

- Now, finally use the first equation to determine an expression for 35 as a linear combination of 135 and 50 :

$$35 = 135 - 2 * 50.$$

- Plug this into our last equation :

$$5 = 3 *(135 - 2 * 50) - 2 * 50$$

$$5 = 3 * 135 - 8 * 50$$

So, a set of solutions to the equation is x = 3, y = –8.

Example 3.5.2 *Using Euclidean algorithm calculate gcd (16, 20) and gcd (50, 60).*

Solution : gcd (16, 20)

Step 1 : $a_1 = 20, \quad b_1 = 16$ **Step 2 :** $a_2 = 16 \quad b_2 = 4$

$20 = 16 \times 1 + 4$ $16 = 4 \times 4 + 0$

Here $r_2 = 0$ and so the last non-zero reminder is $r_2 = 4$.

Thus gcd (16, 20) = 4

gcd (50, 60)

$$a_1 = 60, \quad b_1 = 50$$

$$a_1 = b_1 q_1 + r_1 = 50 \times 1 + 10$$

$$a_2 = 50, \quad b_2 = 10 = b_2 q_2 + r_2 = 10 \times 5 + 0$$

Here $r_2 = 0$ and so the last non-zero remainder is $r_2 = 10$. Thus gcd (50, 60) = 10

Example 3.5.3 *Using Euclidean algorithm calculate GCD (48, 30) and GCD (105, 80).*

Solution : Using Euclidean algorithm calculate GCD :

GCD(48, 30)

$$48 = 1 \times 30 + 18 \text{ gcd}(30, 18)$$

$$30 = 1 \times 18 + 12 \text{ gcd } (18, 12)$$

$$18 = 1 \times 12 + 6 \text{ gcd}(12, 6)$$

$$12 = 2 \times 6 + 0 \text{ gcd}(6, 0)$$

Therefore, GCD(48, 30) = 6

GCD(105, 80)

$$105 = 1 \quad 80 + 25 \text{ gcd}(80, 25)$$

$$80 = 3 \quad 25 + 5 \text{ gcd } (25, 5)$$

$$25 = 5 \quad 5 + 0 \text{ gcd}(5, 0)$$

Therefore, GCD(105, 80) = 5

3.6 Discrete Logarithm

- Discrete logarithms are fundamental to a number of public key algorithms, including Diffie-Hellman key exchange and the DSA.

The powers of an integer, modulo n

- Every a and n that are relatively prime :

$$a^{\phi(n)} \equiv 1 \pmod{n} \quad \text{... (3.6.1)}$$

where $\phi(n)$ Euler's quotient function, is the number of positive integers less than 'n' and relatively prime to 'n'.

- For more general expression :

$$a^{m} \equiv 1 \pmod{n} \quad \text{... (3.6.2)}$$

If a and n are relatively prime, then there is at least one integer m that satisfies equation (3.6.2), namely $m = \phi(n)$.

- Consider the powers of 7, modulo 19 :

$$7^1 = 7 \bmod (19)$$

$$7^2 = 49 = 2 \times 19 + 11 \equiv 11 \pmod{19}$$

$$7^3 = 343 = 18 \times 19 + 1 \equiv 1 \pmod{19}$$

$$7^4 = 2401 = 126 \times 19 + 7 \equiv 7 \pmod{19}$$

$$7^5 = 16807 = 884 \times 19 + 11 \equiv 11 \pmod{19}$$

- The sequence is periodic and the length of the period is the smallest positive exponent 'm' such that $7^m \equiv 1 \pmod{19}$.
- The **logarithm** of a number is defined to be the power to which some positive base must be raised in order to equal the number. For base x and for a value y :

$$y = x^{\log_x(y)}$$

- The properties of logarithms include the following :

a. $\log_x(1) = 0$

b. $\log_x(x) = 1$

c. $\log_x(yz) = \log_x(y) + \log_x(z)$ ... (3.6.3)

d. $\log_x(y^r) = r \times \log_x(y)$ ... (3.6.4)

- The power of 'a' (primitive root) from 1 through (p – 1) produce each integer from 1 through (p – 1) exactly once.
- We also know that any integer 'b' satisfies

$$b \equiv r \pmod{p} \quad \text{for some r, where } 0 \le r \le (p-1)$$

by the definition of moduler arithmetic.

- It follow that for any integer 'b' and a primitive root 'a' of prime number 'p', we can find a unique exponent 'i' such that

$$b \equiv a^i \pmod{p} \qquad \text{where } 0 \le i \le (p-1)$$

This exponent is referred to as the **discrete logarithm** of the number 'b' for the base a (mod p). We denote this value as $d\log_{a,p}(b)$.

$d\log_{a,p}(1) = 0$, because $a^0 \bmod p = 1 \bmod p = 1$

$d\log_{a,p}(a) = 1$, because $a^1 \bmod p = a$

3.6.1 Computing Discrete Logarithm

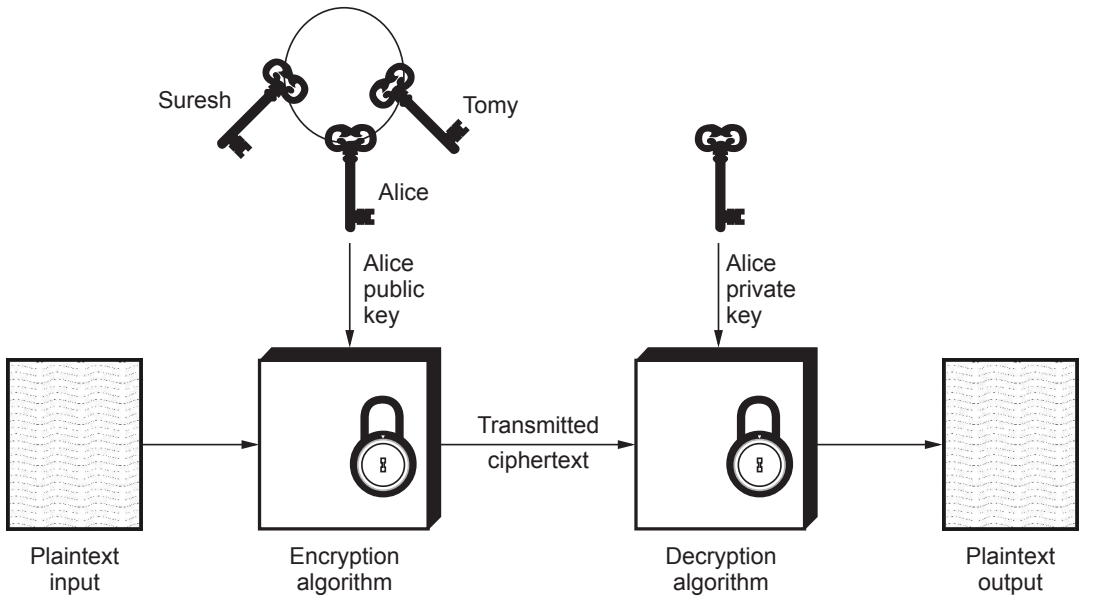
- We want to find a unique integer x such that $\alpha^x = \beta \pmod{n}$.
- We can find x by solving : $x = \log_\alpha \beta \pmod{n}$.
- Logarithms in real numbers are easy to calculate, partially because the log function is continuous and monotonically increasing.
- Discrete logarithms do not have either of these properties. For example, in a (mod 5) system, the powers of 2 are 1, 2, 4, 3.
- This wraparound makes the discrete log function significantly harder to compute than the ordinary log function.
- **Multiplicative group :** A set of congruence classes that is relatively prime to the modulus. We used the group Z_p, where the modulus is a prime number and the group is cyclic (the values repeat).
- **Order of a group :** The number of elements in a group, which can be found using Euler's totient function.
  1. For Z_p, this is $p - 1$.
  2. For Z_p^k, it is $(p-1)\,p^{k-1}$
- **Generators and primitive elements :** An element that produces the other elements of the group when raised to various powers, primitive elements are also generators.
- **Problem :** We have a multiplicative group (G, *), α is a generator of G having order n and β is an element generated by α. Remember, we want to find a unique integer x such that $\alpha^x = \beta \pmod{n}$, by solving $x = \log_\alpha \beta \pmod{n}$.
- Computing $\alpha^x = \beta$ for a given x is simple and efficient using the square and multiply algorithm for exponentiation.

- Computing $a = \log_{\alpha} \beta$ is difficult and can consume a large amount of time and memory for large values, such as those used in cryptography.
- This property makes discrete logs ideal for cryptographic applications because one function is easy, but the inverse function is difficult.
- There is a class of public-key cryptosystems that use the discrete logarithm problem for key generation and encryption/decryption.

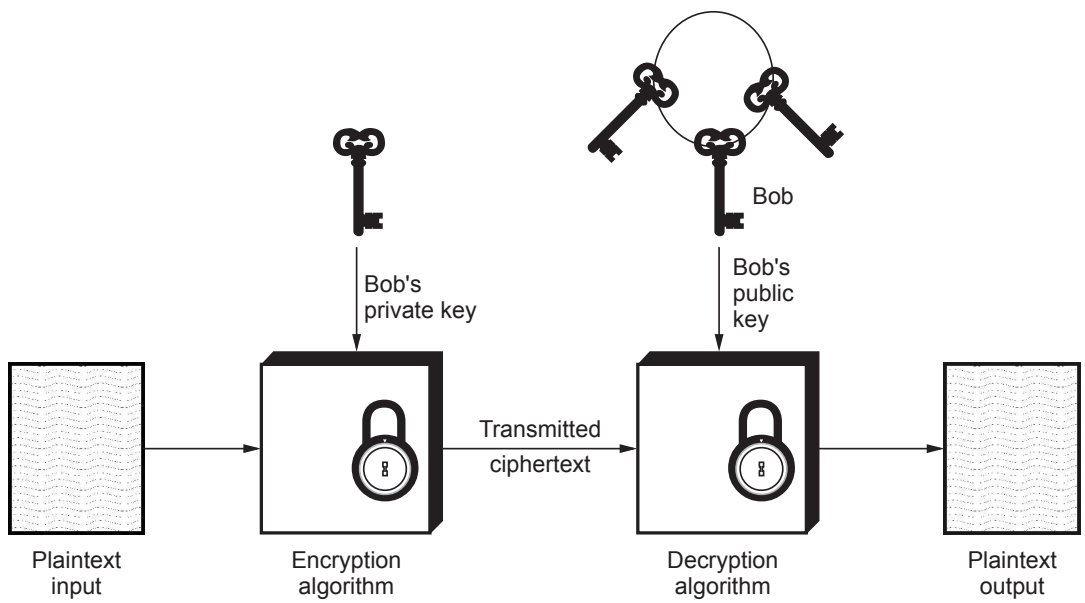
3.7 Public Key Cryptography

SPPU : May-16, 18, April-17

- 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. 3.7.1 shows public key cryptography. (See Fig. 3.7.1 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.
  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.



(a) Encryption



(b) Authentication

Fig. 3.7.1 Public key cryptography

- 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. 3.7.2 shows the process of public key algorithm.

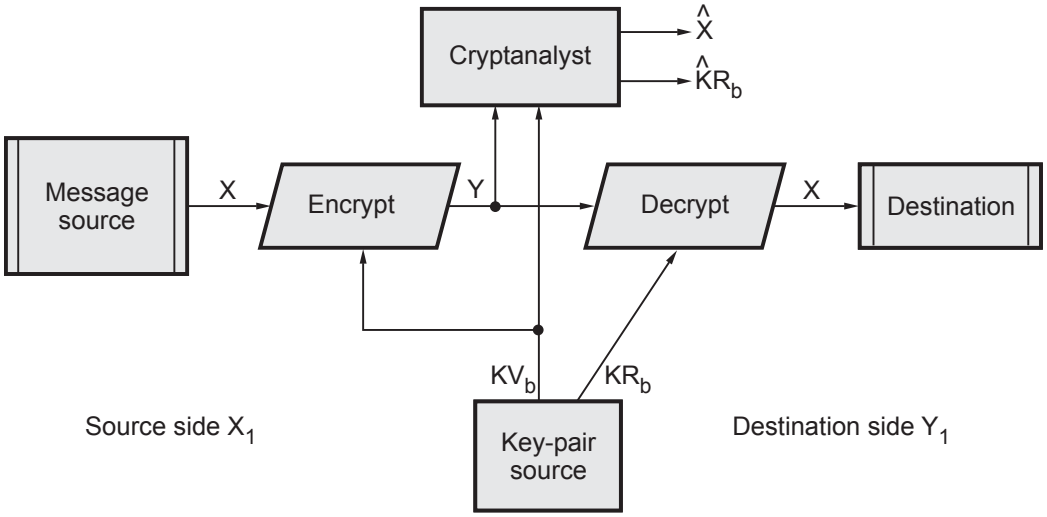


Fig. 3.7.2 Public key cryptosystem secrecy

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

3.7.1 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.

3.7.2 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.

Example 3.7.1 *Perform encryption and decryption using RSA algorithm for p = 17, q = 11, e = 7 and M = 2.*

Solution : P = 17 q = 31 and e = 7

$$n = p \times q = 17 \times 31 = 527$$

$$\phi(n) = (p - 1)(q - 1)$$

$$= (17 - 1)(31 - 1) = 480$$

$$d = (1 + k\,\phi(n)) / e = (1 + 480k) / 7$$

$$= -959 / 7 = -137 \quad \text{(for } k = -2\text{)}$$

$$d = -137 \pmod{480} = 343$$

$$\text{Encryption (C)} = M^e \pmod{n} = 2^7 \pmod{527} = 128$$

$$\text{Decryption M} = C^d \pmod{n} = 128^{343} \pmod{527} = 2$$

Review Questions

1. *Explain various public key distribution approaches.* **SPPU : May-16, Marks 5**
2. *What are different approaches of public key distribution ? Explain any one.* **SPPU : April-17, Marks 5**
3. *Compare between symmetric key encryption and asymmetric key encryption.* **SPPU : May-18, Marks 5**

3.8 RSA SPPU : Aug.-15, Dec.-15, 17, Oct.-16, April-16, 17, 19, May-17, 18, March-20

- RSA is a block cipher in which the plaintext and ciphertext are integers between 0 and n – 1 for some n.
- A typical size for n is 1024 bits.
- The RSA algorithm developed in 1977 by Rivest, Shamir, Adleman (RSA) at MIT. RSA algorithm is public key encryption type algorithm. In this algorithm, one user uses a public key and other user uses a secret (private key) key.
- In the RSA algorithm each station independently and randomly chooses two large primes p and q number, and multiplies them to produce $n = pq$ which is the modulus used in the arithmetic calculations of the algorithm.
- The details of the RSA algorithm are described as follows :
- **Key generation :**
  1) Pick two large prime numbers p and q, $p \neq q$;
  2) Calculate $n = p \times q$;
  3) Calculate $\phi(n) = (p - 1)(q - 1)$;
  4) Pick e, so that $\gcd(e, \phi(n)) = 1$, $1 < e < \phi(n)$;
  5) Calculate d, so that $d \cdot e \bmod \phi(n) = 1$, i.e. d is the multiplicative inverse of e in mod $\phi(n)$;
  6) Get public key as $K_U = \{e, n\}$;
  7) Get private key as $K_R = \{d, n\}$.
- **Encryption :**

For plaintext block $P < n$, its ciphertext $C = P^e \bmod n$.

- **Decryption :**

For ciphertext block C, its plaintext is $P = C^d \bmod n$.

Why RSA works :

- As we have seen from the RSA design, RSA algorithm uses modular exponentiation operation. For $n = p \cdot q$, e which is relatively prime to $\phi(n)$, has exponential inverse in mod n.
- Its exponential inverse d can be calculated as the multiplicative inverse of e in mod $\phi(n)$. The reason is illustrated as follows :
  Based on Euler's theorem, for y which satisfies $y \bmod \phi(n) = 1$, the following equation holds :

$$x^y \bmod n = x \bmod n$$

AS $d \cdot e \bmod \phi(n) = 1$, we have that $p^{ed} \equiv P \bmod n$. So the correctness of RSA cryptosystem is shown as follows :

- **Encryption :** $C = P^e \bmod n$;
- **Decryption :** $P = C^d \bmod n = (P^e)^d \bmod n = P^{ed} \bmod n = P \bmod n = P$.

Why RSA is secure :

- The premise behind RSA's security is the assumption that factoring a big number (n into p and q) is hard. And thus it is difficult to determine $\phi(n)$. Without the knowledge of $\phi(n)$, it would be hard to derive d based on the knowledge of e.

Advantages

1. RSA can be used both for encryption as well as for digital signatures.
2. Trapdoor in RSA is in knowing value of n but not knowing the primes that are factors of n.

Disadvantages

1. If any one of p, q, m, d is known, then the other values can be calculated. So secrecy is important.
2. To protect the encryption, the minimum number of bits in n should be 2048.

3.8.1 Attacks on RSA

Attacks on RSA algorithm are as follows :

1. **Brute force :** This involves trying all possible private keys.
2. **Mathematical attacks :** This involves the factoring the product of two primes.
3. **Timing attacks :** These depends on the running time of the description algorithm.
4. **Chosen ciphertext attacks :** This type of attack exploits properties of the RSA algorithm.

3.8.1.1 Computing $\phi(n)$

- Computing $\phi(n)$ is no easier that factoring n. For, if n and $\phi(n)$ are known, and n is the product of two primes p, q, then n can be easily factored, by solving the two equations.

$$n = pq \quad \text{... (3.8.1)}$$

$$\phi(n) = (p - 1)(q - 1) \quad \text{... (3.8.2)}$$

for the two unknowns p and q.

- If we substitute $q = n/p$ into the equation (3.8.2), we obtain a quadratic equation in the unknown value p :

$$p^2 - (n - \phi(n) + 1)\, p + n = 0 \quad \text{... (3.8.3)}$$

- The two roots of equation (3.8.3) will be p and q, the factors of n. If a cryptanalyst can learn the value of $\phi(n)$, then he can factor 'n' and break the system.

3.8.1.2 Timing Attacks

- Kocher described a new attack on RSA in 1995.
- If the attacker Eve knows Alice's hardware in sufficient detail and is able to measure the decryption times for several known cipher-texts, she can deduce the decryption key (d) quickly. This attack can also be applied against the RSA signature scheme.
- In 2003, Boneh and Brumley demonstrated a more practical attack capable of recovering RSA factorizations over a network connection. This attack takes advantage of information leaked by the chinese remainder theorem optimization used by many RSA implementations.
- One way to thwart these attacks is to ensure that the decryption operation takes a constant amount of time for every cipher-text. However, this approach can significantly reduce performance.
- There is simple counter-measures against timing attacks :
  1. **Constant exponentiation time :** Ensure that all exponentiations take the same time, but this will degrade performance.
  2. **Random delay :** Better performance could be achieved by adding a random delay to the exponentiation algorithm to confuse the timing attack.
  3. **Blinding :** Multiply the cipher-text by a random number before performing exponentiation. This process prevents the attacker from knowing what cipher-text bits are being processed inside the computer and therefore prevents the bit-by-bit analysis essential to the timing attack. RSA data security reports a 2 % to 10 % performance penalty for blinding.

3.8.1.3 Mathematical Attacks

- We can identify three approaches to attacking RSA mathematically :
  1. Factor n into two prime factors, this enables calculation of **$\phi(n) = (p - 1)(q - 1)$, which in turn, enables determination of $d = e^{-1} \bmod \phi(n)$.**
  2. Determine $\phi(n)$ directly, without first determining p and q.
  3. Determine d directly, without first determining $\phi(n)$.
- Most discussions of cryptanalysis of RSA have focused on the task of factoring n into its two prime numbers. Determining $\phi(n)$ given n is equivalent to factoring n.

- With presently known algorithms, determining d given e and n appears to at least as time consuming as the factoring problem.

3.8.1.4 Adaptive Chosen Cipher-text Attacks

- In 1998, Daniel Bleichenbacher described the first practical adaptive chosen cipher-text attack, against RSA-encrypted messages using the PKCS#1 v1 padding scheme.
- Due to flaws with the PKCS#1 scheme, Bleichenbacher was able to mount a practical attack against RSA implementations of the secure socket layer protocol and to recover session keys.
- As a result of this work, cryptographers now recommend the use of provably secure padding schemes such as optimal asymmetric encryption padding and RSA laboratories has released new versions of PKCS#1 that are not vulnerable to these attacks.

Example 3.8.1 *For the given values p = 19, q = 23 and e = 3 find n, $\phi(n)$ and d using RSA algorithm.*

Solution :

$$n = p * q$$

$$n = 19 \times 23$$

$$\mathbf{n = 437}$$

$$\phi(n) = (p - 1) * (q - 1)$$

$$\phi(n) = 18 \times 22$$

$$\phi(n) = \mathbf{396}$$

$$e.d. = 1 \bmod \phi(n)$$

$$3d = 1 \bmod 396$$

$$d = \frac{1}{3}$$

Example 3.8.2 *Using the RSA algorithm, encrypt the following :*

i) p = 3, q = 11, e = 7, M = 12

ii) p = 7, q = 11, e = 17, M = 25

iii) Find the corresponding ds for i) and ii) and decrypt the ciphertext.

Solution : i)

$$n = p * q$$

$$n = 3 * 11 = 33$$

$$\phi(n) = (p - 1)\,(q - 1)$$

$$\phi(n) = 2 * 10 = 20$$

$$e \cdot d = 1 \bmod \phi(n)$$

$$7 \cdot d = 1 \bmod 20$$

$$d = 3$$

$$\text{Ciphertext (C)} = M^e \bmod n$$

$$= 12^7 \bmod 33$$

$$C = 12$$

ii)

$$n = p * q = 7 * 11 = 77$$

$$\phi(n) = (p - 1) * (q - 1) = 6 \times 10 = 60$$

$$e \cdot d = 1 \bmod \phi(n) \Rightarrow 17\ d = 1 \bmod 77$$

$$d = 3$$

$$\text{Ciphertext (C)} = M^e \bmod n$$

$$= 25^{17} \bmod 77 \Rightarrow 77 \Rightarrow c = 9$$

$$C = 12$$

iii) Decryption :

$$M = c^d \bmod n$$

In case (i) $M = 12^3 \bmod 33 = 12$

In case (ii) $M = 9^{57} \bmod 77 = 25$

Example 3.8.3 *In RSA system the public key of a given user is e = 7 and n = 187*

i) What is the private key of this user ?

ii) If the intercepted ciphertext is c = 11 and sent to a user whose public key is e = 7 and n = 187. What is the plaintext ?

iii) What are the possible approaches to defeating the RSA algorithm ?

Solution : i) $n = p * q$

$$n = 11 \times 17 \Rightarrow 187$$

$$\phi(n) = (p - 1)\ (q - 1)$$

$$= (17 - 1)\ (11 - 1) = 16 \times 10 = 160$$

$$e \cdot d = 1 \bmod \phi(n)$$

$$7\ d = 1 \bmod 160$$

$$7 \times 23 = 1 \bmod 160$$

Public key PU

$(e, n) = 7, 187$

Private key PR

$(d, n) = 23, 187$

ii) $c = 11, \quad e = 7, \quad n = 187$

Plaintext $p = c^d \bmod n$

$= 11^{23} \bmod 187$

$= 79720245 \bmod 187$

$\therefore$ Plaintext $= 88$

Example 3.8.4 *Explain about the RSA algorithm with example as : p = 11, q = 5, e = 3 and PT = 9.*

Solution : $p = 11, \quad q = 5$

$$n = p * q = 11 \times 5 = 55$$

$$\phi(n) = (p-1) * (q-1) = 10 * 4$$

$$= 40$$

$$e = 3 \text{ and } m = 9$$

$$\gcd(\phi(n), (e) = \gcd(40, 3) = 1$$

$$d \equiv e^{-1} (\bmod \phi(n))$$

$$d \times e^{-1} (\bmod \phi(n)) = 1$$

$$3d \bmod 40 = 1$$

$$d = 27$$

public key $pu = \{e, n\} = \{3, 55\}$

private key $pr = \{d, n\} = \{27, 55\}$

Encryption : $C = M^e \bmod n$

$= 9^3 \bmod 55 = 14$

decryption : $M = c^d \bmod n$

$M = 14^{27} \bmod 55 = 9$

Example 3.8.5 *Perform encryption and decryption using RSA algorithm. p = 7, q = 11, e = 17 and M = 8.* **SPPU : Oct.-16, Marks 6**

Solution : RSA algorithm :

$$N = p \times q$$
$$= 7 \times 11$$
$$= 77$$

$$\text{Calculate } \phi(n) = (p - 1)(q - 1)$$
$$= (7 - 1)(11 - 1)$$
$$= 6 \times 10$$
$$= 60$$

So, $e = 17$

Determine d such that

$$ed = 1 \bmod \phi(n)$$
$$17d = 1 \bmod 60$$

According to GCD :

$$60 = 17 * 3 + 9$$
$$17 = 9 * 1 + 8$$
$$9 = 8 * 1 + 1$$
$$8 = 1 * 8 + 0$$

Therefore, we have :

$$1 = 9 - 8 = 9 - (17 - 9)$$
$$= 9 - (17 - (60 - 17 * 3))$$
$$= 60 - 17 * 3 - (17 - 60 + 17 * 3)$$
$$= 60 - 17 * 3 + 60 - 17 * 4$$
$$= 60 * 2 - 17 * 7$$

Hence, we get,

$$d = e^{-1} \bmod f(n)$$
$$= e^{-1} \bmod 60$$
$$= -7 \bmod 60$$
$$= (53 - 60) \bmod 60$$
$$= 53$$

So, the public key is {17, 77} and the private key is {53, 77}

Encryption :

$$\text{Ciphertext (C)} = M^e \bmod N$$

$$= (8)^{17} \bmod 77$$

$$C = 57$$

Example 3.8.6 *In a public key cryptosystem using RSA, given N = 187 and the encryption key (E) as 17, find out the corresponding private key (D).*

SPPU : Dec.-15 (End Sem), Marks 6

Solution :

$$N = 187$$

$$N = p \times q = 17 \times 11$$

$$N = 187$$

So $p = 17, \quad q = 11$

$$\phi(n) = (p - 1) \times (q - 1)$$

$$= (17 - 1) \times (11 - 1) = 160$$

$$ED = 1 \bmod \phi(n)$$

$$17\ d = 1 \bmod 160$$

$$d = 113$$

Example 3.8.7 *Let the given data be - Prime numbers p = 11, q = 19 and the plain text to be sent is 4. Assume public key e as 23. Using RSA algorithm determine the cipher text for the given plain text. Also perform the reverse process of finding the plain text. Also perform the reverse process of finding the plain text from the cipher text.*

SPPU : Aug.-15 (In Sem), Marks 6

Solution : Given p = 11, q = 19, plain text (m) = 40,

Public key e = 23

$$n = p \times q = 11 \times 19 = 209$$

$$\phi(n) = (p - 1) \times (q - 1)$$

$$= (11 - 1) \times (19 - 1) = 180$$

Encryption :

$$C = M^e \pmod n = (40)^{23} \bmod 180$$

$$C = 160$$

Example 3.8.8 *For the given parameters 'P' = 3 and 'Q' = 19 find the value of 'e' and 'd' using RSA algorithm and encrypt message 'M' = 6.* **SPPU : April-16, (In Sem.), Marks 5**

Solution : P = 3 Q = 19

$$N = PQ = 3 \times 19$$

$$N = 57$$

$$\text{Calculate } \phi(n) = (P - 1)(Q - 1) = (3 - 1)(19 - 1)$$

$$= 36$$

Public key 'e' is calculated by using Euclid algorithm. Using 36, GCD is calculated and 5 and 7 gives GCD = 1

So you can select e = 5 or 7. Here we selected e = 7

So public key (7, 57)

Private key generation (d) :

$$\text{Determine d such that } ed = 1 \bmod \phi(n)$$

$$7d = 1 \pmod{36}$$

$$7 \times 31 = 1 \pmod{36}$$

So d = 31

Encryption of message :

$$\text{Ciphertext (C)} = M^e \bmod n = 6^7 \bmod 57$$

$$C = 9$$

Example 3.8.9 *Use RSA algorithm to encrypt the plaintext " 3 " use following parameters p = 11, q = 3, e = 13.* **SPPU : May-17, (End Sem), March-20, Marks 5**

Solution : p = 11, q = 3, e = 13

Plaintext = 3

$$N = p \times q = 11 \times 3 = 33$$

$$\phi(n) = (p-1)(q-1) = (11-1)(3-1) = 20$$

$$e = 13 ;$$

Determine d such that

$$ed = 1 \bmod \phi(n)$$

$$13\,d = 1 \bmod 20$$

$$13 \times 17 = 1 \bmod 20$$

$$221 = 1 \bmod 20$$

So $d = 17$

Ciphertext $(C) = M^e \bmod (n)$

$$C = 3^{13} \bmod 33$$

$$C = 27$$

Example 3.8.10 *Given two prime numbers P = 17 and Q = 29 find out N, E and D in an RSA encryption process.* **SPPU : April-19, (In Sem), Marks 5**

Solution : Given data : P = 17, Q = 27

$$N = P \times Q = 17 \times 27 = 459$$

$$(N) = (P-1)\times(Q-1) = (17-1)\times(27-1) = 416$$

The number e is allowed to be any number, which has no factors in common with this new number 416

We can break 416 into a bunch of prime numbers multiplied together :
$416 = 2\times2\times2\times2\times2\times13$

So there are lots of possibilities. Let's suppose chooses e = 5.

$$e\times d = 1 \bmod ((N))$$

$$5\times d = 1 \bmod (416)$$

$$d = 83$$

Review Questions

1. *For the given parameters 'P' = 3 and 'Q' = 19 find the value of 'e' and 'd' using RSA algorithm and encrypt message 'M' = 6.* **SPPU : April-16, Marks 5**
2. *What is public key cryptography ? Explain RSA algorithm used for public key cryptography.* **SPPU : April-17, Marks 5**
3. *Use RSA algorithm to encrypt the plaintext " 3 " use following parameters p = 11, q = 3, e = 13.* **SPPU : May-17, March-20, Marks 5**
4. *Explain RSA algorithm with suitable example.* **SPPU : Dec.-17, Marks 5**
5. *Explain operation of RSA public key encryption algorithm.* **SPPU : May-18, Marks 5**

3.9 Key Distribution

SPPU : April-16

- The purpose of public key cryptography is
  1. The distribution of public keys.
  2. The use of public key encryption to distribute secret keys.

3.9.1 Distribution of Public Keys

- Different methods have been proposed for the distribution of public keys. These are
  1. Public announcement.
  2. Publicly available directory.
  3. Public key authority.
  4. Public key certificates.

1. Public announcement

- In public key algorithm, any participant can **send** his or her public key to any other participant or **broadcast** the key to the community at large.
- Fig. 3.9.1 shows the public key distribution.

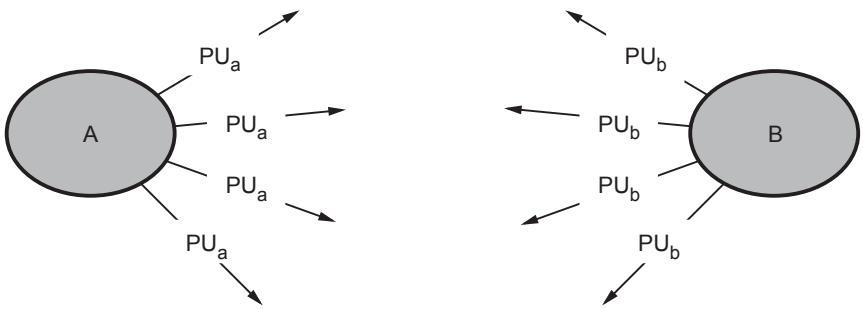


Fig. 3.9.1 Public key distribution

- Because of the growing popularity of PGP, which makes use of RSA, many PGP users have adopted the practice of appending their public key to messages that they send to public forums, such as USENET newgroups and Internet mailing lists.
- The disadvantage is that, anyone can forge such a public announcement. That is, some user could pretend to be user A and send a public key to another participant or broadcast such a public key.

2. Public available directory

- Greater degree of security can be achieved by maintaining a publicly available dynamic directory of public keys. Maintenance and distribution of the public

directory would have to be the responsibility of some trusted entity or organization.

- Fig. 3.9.2 shows public key publication.

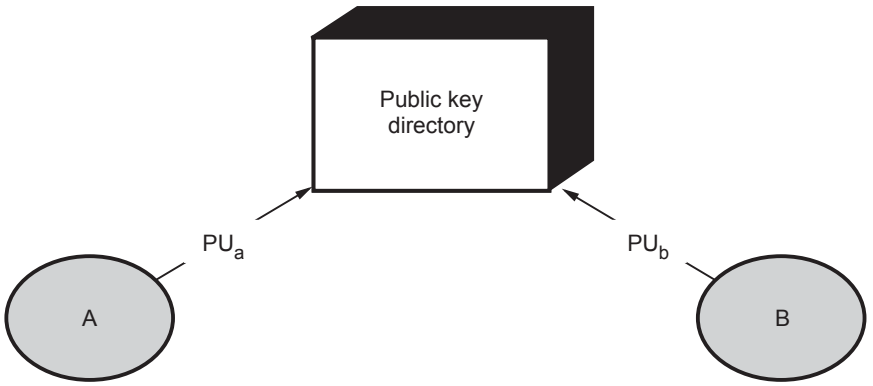


Fig. 3.9.2 Public key publication

- Such a scheme would include the following elements :
  1. The authority maintains a directory with a {name, public key} entry for each participant.
  2. Each participant registers a public key with the directory authority. Registration would have to be in person or by some form of secure authenticated communication.
  3. A participant may replace the existing key with a new one at any time.
  4. Participants could also access the directory electronically.

3. Public key authority

- Fig. 3.9.3 shows public key distribution scenario. (See Fig. 3.9.3 on next page)
- Following steps occur in public key distribution.
  1. A sends a timestamped message to the public key authority containing a request for the current public key of B.
  2. The authority responds with a message that is encrypted using the authority's private key, PR_{auth}. The message also contains B's public key (PU_b), original request and timestamp.
  3. A stores B's public key and also uses it to encrypt a message to B containing an identifier of A (ID_A) and a nonce (N_1) which is used to identify this transaction uniquely.
  4. B retrieves A's public key from the authority in the same manner as A retrieved B's public key.

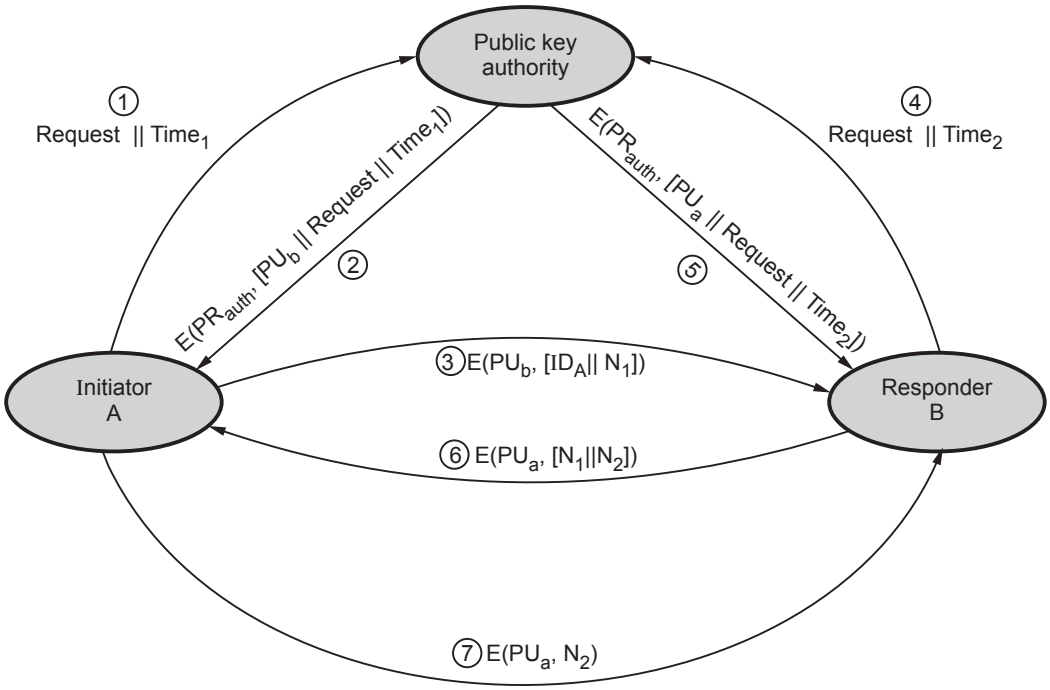


Fig. 3.9.3 Public key distribution scenario

5. Public keys have been securely delivered to A and B and they may begin their protected exchange.
6. B sends a message to A encrypted with PU_a and containing A's nonce (N_1) as well as a new nonce generated by B(N_2).
7. A returns N_2, encrypted using B's public key, to assure B that its correspondent is A.

Drawback

Public key authority could be somewhat of a bottleneck in the system. The directory of name and public keys maintained by the authority is vulnerable to tampering.

4. Public key certificates

- Certificates can be used by participants to exchange keys without contacting a public key authority. Certificate consists of a public key plus an identifier of the key owner, with the whole block signed by a trusted third party.
- The third party is a certificate authority, such as government agency or a financial institution, that is trusted by the user community.
- A user can present his or her public key to the authority in a secure manner, and obtain a certificate. The user can then publish the certificate.

- Requirements on this scheme :
  1. Any participant can read a certificate to determine the name and public key of the certificate's owner.
  2. Any participant can verify that the certificate originated from the certificate authority and is not counterfeit.
  3. Only the certificate authority can create and update certificates.
  4. Any participant can verify the currency of the certificate.
- A certificate scheme is illustrated in Fig. 3.9.4. Each participant applies to the certificate authority, supplying a public key and requesting a certificate.

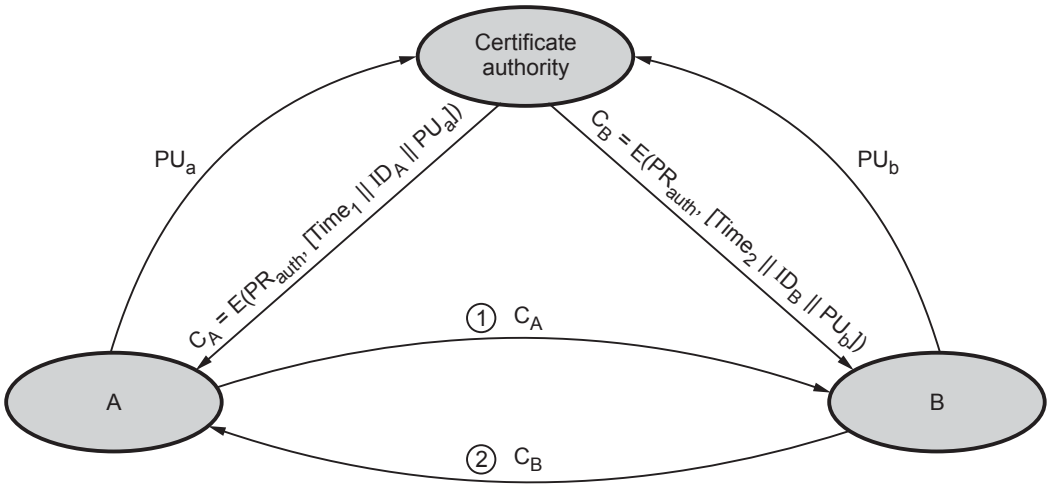


Fig. 3.9.4 Exchange of public key certificates

- For participant A, the authority provides a certificate of the form

$$C_A = E(PR_{auth}, [T \,||\, ID_A \,||\, PU_a])$$

where PR_{auth} is the private key used by the authority and T is a timestamp.

3.9.2 Distribution of Secret Keys using Public Key Cryptography

- Public key encryption provides for the distribution of secret key to be used for conventional encryption.

Simple secret key distribution

If user A wishes to communicate with user B, the following procedure is employed :

1. User A generates a public/private key pair $\{PU_a, PR_a\}$ and transmits a message to user B consisting of PU_a and an identifier of A, ID_A.
2. User B generates a secret key (K_s) and transmits it to user A, encrypted with A's public key.

3. User A computes $D(PR_a, E(PU_a, K_s))$ to recover the secret key. Because only A can decrypt the message, only user A and user B know the identity of K_s.
4. User A discards PU_a and PR_a and user B discards PU_a.
5. Fig. 3.9.5 shows use of public key encryption.

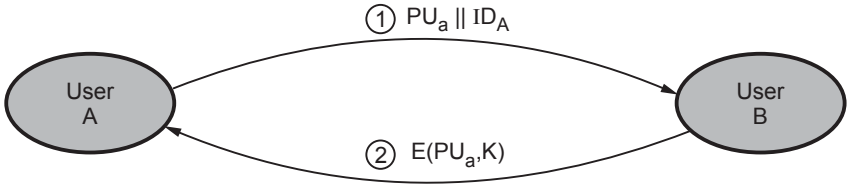


Fig. 3.9.5 Use of public key encryption

- User A and B can now securely communicate using conventional encryption and the session key K_s. At the completion of the exchange, both user A and B discard K_s.
- The protocol discussed above is insecure against an adversary who can intercept messages and then either relay the intercepted message or substitute another message. Such an attack is known as a **man in middle attack.**

Secret key distribution with confidentiality and authentication

- Fig. 3.9.6 shows the public key distribution of secret keys.

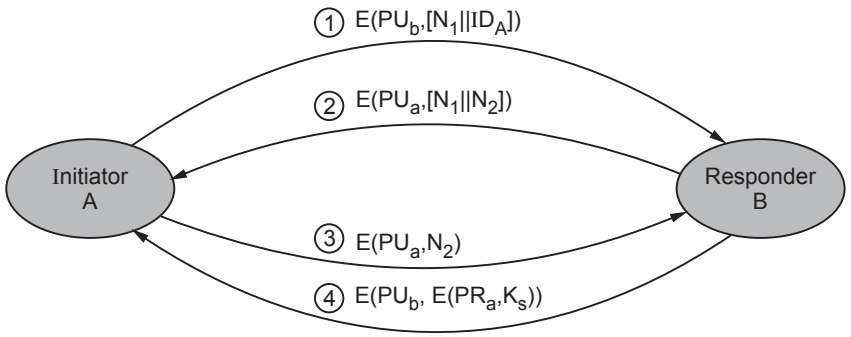


Fig. 3.9.6 Public key distribution of secret keys

- It provides protection against both passive and active attacks.
  1. A uses B's public key to encrypt a message to B containing an identifier of A (ID_A) and a nonce (N_1), which is used to identify this transaction uniquely.
  2. B sends a message to A encrypted with PU_a and containing A's nonce (N_1) as well as a new nonce generated by B(N_2).
  3. A returns N_2, encrypted using B's public key, to assure B that its correspondent is A.
  4. A selects a secret key K_s and sends $M = E(PU_b, E(PR_a, K_s))$ to B.
  5. B computes $D(PU_a, D(PR_b, M))$ to recover the secret key.

3.9.3 Key Distribution and Certification

- 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.

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.

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.

2. Certificate

- **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. 3.9.7 shows the hierarchy of certificate authorities.

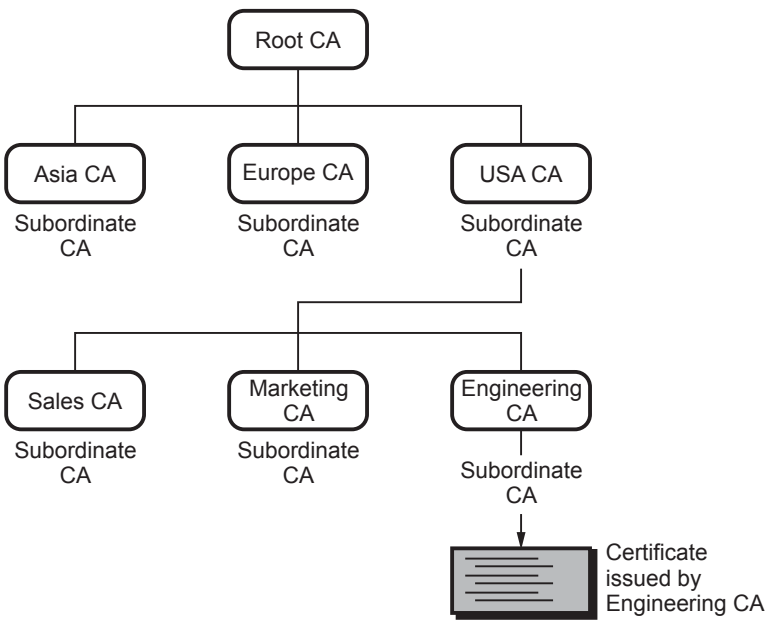


Fig. 3.9.7 Hierarchy of CA

- In the Fig. 3.9.7, 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).**

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.

3. 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.

3.9.4 Key Distribution

- For symmetric encryption to work, the two parties to an exchange must share the same key, and that key must be protected from access by others. **Key distribution** refers to the means of delivering a key to two parties who wish to exchange data, without allowing others to see the key.
- For two parties A and B, key distribution can be achieved in a number of ways, as follows.
  1. User A can select a key and physically deliver it to user B.
  2. A third party can select the key and physically deliver it to user A and user B.
  3. If user A and user B have previously and recently used a key, one party can transmit the new key to the other, encrypted using the old key.
  4. If user A and user B each has an encrypted connection to a third party C, C can deliver a key on the encrypted links to user A and user B.
- For manual delivery of key, **options 1 and 2** are used. These options are suitable for **link encryption.**
- Option 3 is suitable for link encryption or end-to-end encryption.
- For end-to-end encryption, some variation on option 4 has been widely adopted.
- The use of a key distribution center is based on the use of a hierarchy of keys. Minimum two levels of keys are used. Fig. 3.9.8 shows the use of a key hierarchy.
- Communication between end systems is encrypted using a temporary key, often referred to as a **session key**. The **session key** is used for the duration of a logical connection, such as a frame relay connection, or transport connection and then discarded.

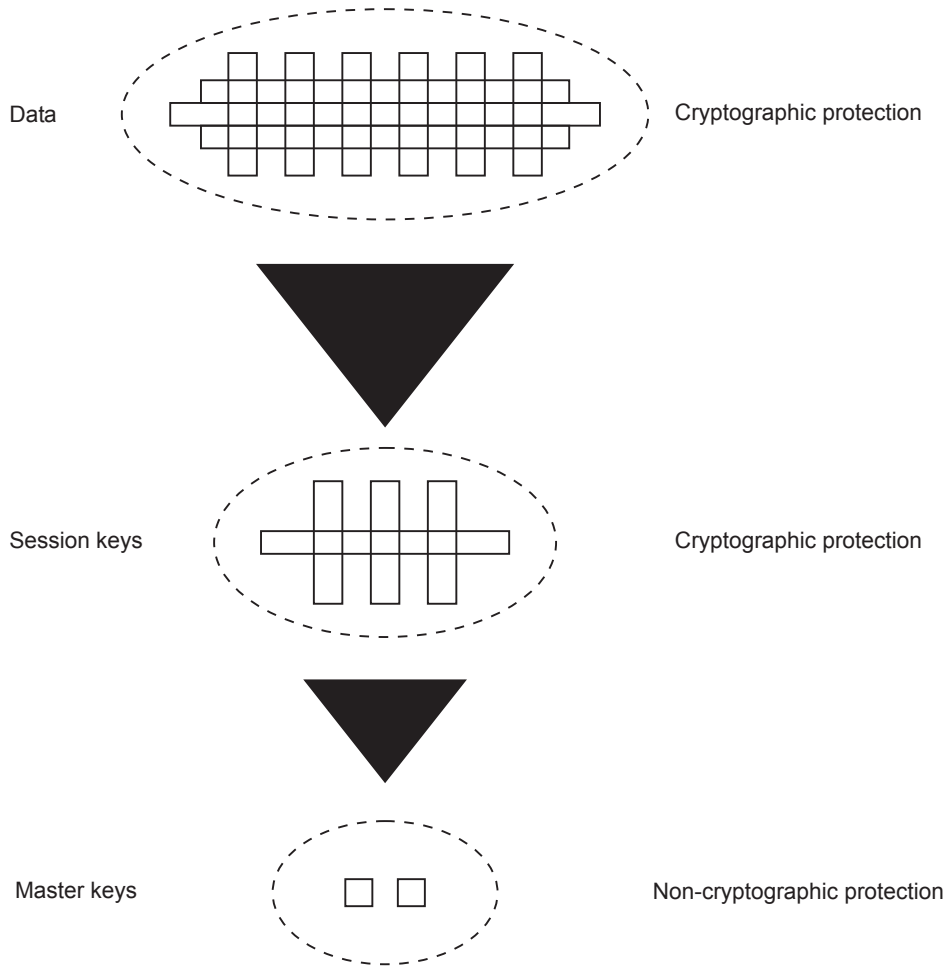


Fig. 3.9.8 Use of a key hierarchy

- Session keys are transmitted in encrypted form, using a **master key** that is shared by the key distribution center and an end system or user. For each end user, there is a unique master key that it shares with the key distribution center.

A key distribution scenario

- User A wishes to establish a logical connection with user B and requires a one time session key to protect the data transmitted over the connection. User A has a master key (K_a), known only to itself and the KDC. User B shares the master key K_b with the KDC. The following steps occur :
  1. A issues a request to the KDC for a session key to protect a logical connection to B. The message includes the identity of A and B and a unique identifier (N_1) for this transaction.
  2. KDC responds with a message encrypted using K_a.

3. A stores the session key for use in the upcoming session and forward to B the information that originated at the KDC for B :
4. User B sends a nonce N_2 to A.

- Fig. 3.9.9 shows the key distribution scenario.

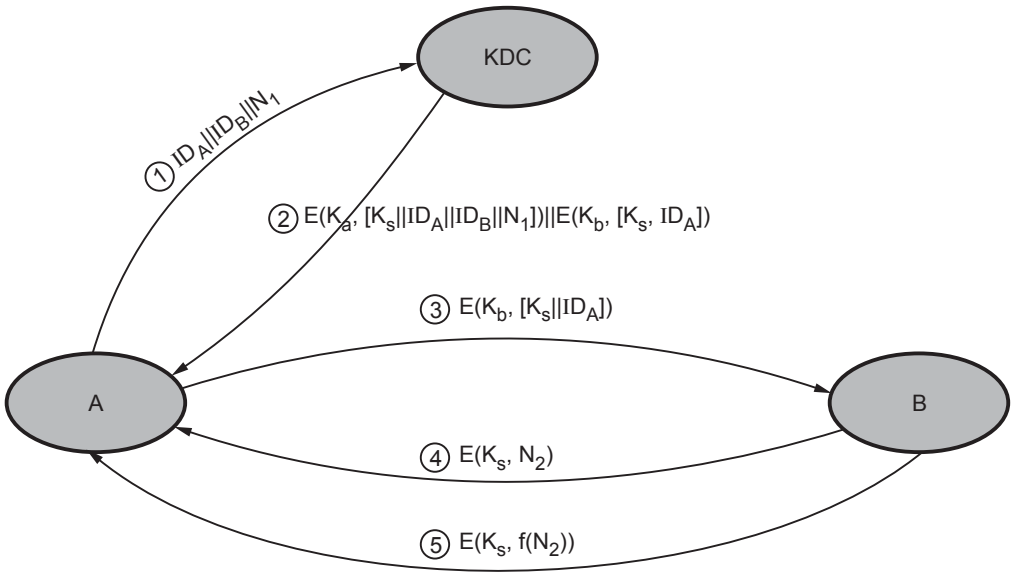


Fig. 3.9.9 Key distribution scenario

- Steps 1, 2 are used for key distribution and steps 3, 4, 5 for authentication.

Session key lifetime

1. **For connection-oriented protocol**
   - Use the same session key for the length of time that the connection is open. Use new session key for each new session.
   - For long lifetime, change the session key periodically.
2. **For connectionless protocol**
   - The most secure approach is to use a new session key for each exchange. For connectionless protocol, such as a transaction-oriented protocol, there is no explicit connection initiation or termination.

Transparent key control scheme

- Fig. 3.9.10 shows automatic key distribution for connection - oriented protocol.
- Assume that communication make use of a connection-oriented end-to-end protocol, such as TCP.

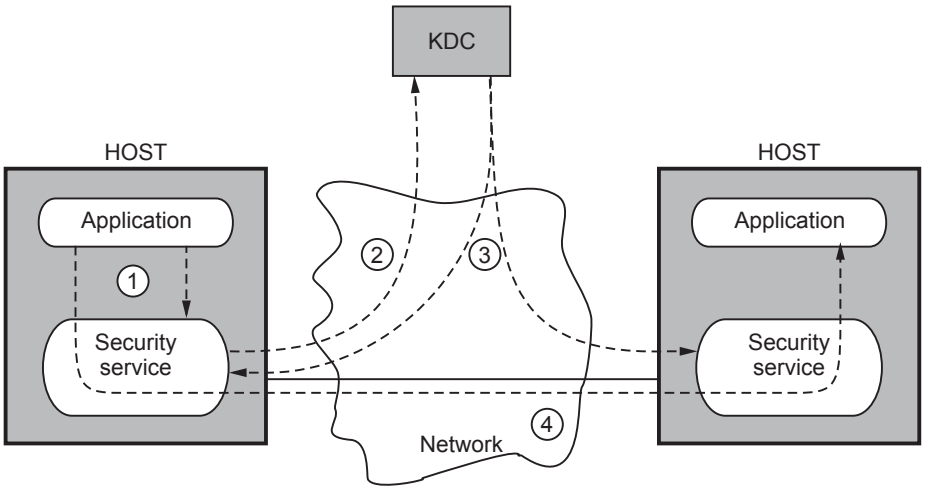


Fig. 3.9.10 Automatic key distribution for connection-oriented protocol

- Following steps occurs :
  1. Host sends packet requesting connection.
  2. Session Security Module (SSM) saves that packet and applies to the KDC for permission to establish the connection.
  3. KDC distributes session key to both hosts.
  4. The requesting SSM can now release the connection request packet, and a connection is set up between the two end systems.

Decentralized key control

- Decentralized approach requires that each end system be able to communicate in a secure manner with all potential parter end systems for purposes of session key distribution.

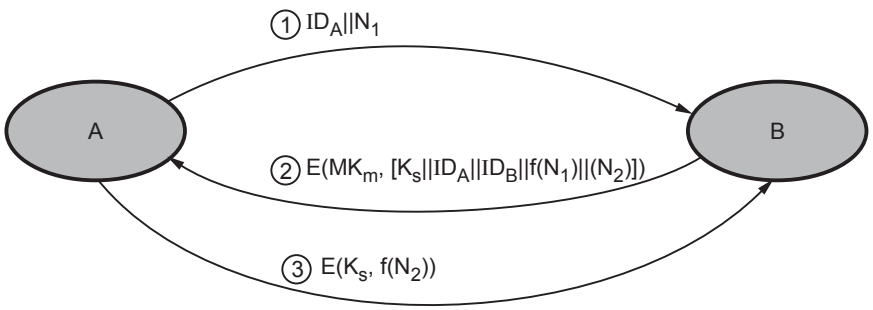


Fig. 3.9.11 Decentralized key distribution

- A session key may be established with the following sequence of steps.
  1. A issues a request to B for a session key and includes a none, N_1.
  2. B responds with a message that is encryped using the shared master key.
  3. Using the new session key, A returns f (N_2) to B.

Review Question

1. *What are the methods used in key distribution in public key cryptography.*

SPPU : April-16, Marks 5

3.10 Diffie-Hellman Key Exchange

SPPU : May-07, April-16, 19

- The Diffie-Hellman key agreement protocol was developed by Diffie and Hellman in 1976. This protocol allows two users to exchange a secret key over an insecure medium without any prior secrets.
- The protocol has two system parameters p and g. They are both public and may be used by all the users in a system.
- Parameter p is a prime number and parameter g is an integer less than p, with the following property :
  1. For every number n between 1 and p – 1 inclusive.
  2. There is a power k of g such that $n = g^k \bmod p$.
- The protocol depends on the discrete logarithm problem for its security. It assumes that it is computationally infeasible to calculate the shared secret key, $k = g^{ab} \bmod p$ given the two public values $g^a \bmod p$ and $g^b \bmod p$ when the prime p is sufficiently large.
- The Diffie-Hellman key exchange is vulnerable to a man-in-the-middle attack. This vulnerability is present because Diffie-Hellman key exchange does not authenticate the participants. Possible solutions include the use of digital signatures and other protocol variants.
- Suppose Alice and Bob want to agree on a shared secret key using the Diffie-Hellman key agreement protocol. They proceed as follows :
  1. First, Alice generates a random private value a and Bob generates a random private value b.
  2. Both a and b are drawn from the set of integers. They derive their public values using parameters p and g and their private values.
  3. Alice's public value is $g^a \bmod p$ and Bob's public value is $g^b \bmod p$.
  4. They then exchange their public values.

5. Finally, Alice computes $g^{ab} = (g^b)^a \mod p$.
6. Bob computes $g^{ba} = (g^a)^b \mod p$.
7. Since $g^{ab} = g^{ba} = k$, Alice and Bob now have a shared secret key k.

Algorithm :

- Select two numbers (1) prime number q (2) α an integer that is a primitive root of q.
- Suppose the users A and B wish to exchange a key.
  1. User A select a random integer $X_A < q$ and computes $Y_A = \alpha^{X_A} \mod q$.
  2. User B selects a random integer $X_B < q$ and compute $Y_B = \alpha^{X_B} \mod q$.
  3. Both side keeps the X value private and makes the Y value available publicly to the other side.
  4. User A computes the key as $K = (Y_B)^{X_B} \mod q$.
  5. User B computes the key as $K = (Y_A)^{X_B} \mod q$.
- Both side gets same results :

$$K = (Y_B)^{X_A} \mod q$$

$$= (\alpha^{X_B} \mod q)^{X_A} \mod q$$

$$= (\alpha^{X_B})^{X_A} \mod q = \alpha^{X_B X_A} \mod q$$

$$= (\alpha^{X_A} \mod q)^{X_B} \mod q$$

$$= (Y_A)^{X_B} \mod q$$

Example

- Key exchange is based on the use of the prime number and a primitive root of prime number.
- Prime number $q = 353$
  Primitive root $\alpha = 3$
- A and B select secret keys.
  $X_A = 97$ $X_B = 233$
- Calculates the public keys

$$A \text{ computes } Y_A = \alpha^{X_A} \mod q$$

$$= (3)^{97} \mod 353$$

$$= (1.9080 \times 10^{97}) \mod 353 = 40$$

B computes $Y_B = \alpha^{X_B} \bmod q$

$= (3)^{233} \bmod 353$

$= (1.4765 \times 10^{111}) \bmod 353 = 248$

- After they exchange public keys, each can compute the common *secret key*.

A computes $K = (Y_B)^{X_A} \bmod q = (248)^{97} \bmod 353$

$= (1.8273 \times 10^{232}) \bmod 353 = 160$

B computes $K = (Y_A)^{X_B} \bmod q = (40)^{233} \bmod 353$

$= (1.9053 \times 10^{373}) \bmod 353 = 160$

Example 3.10.1 *User A and B use the Diffie-Hellman key exchange technique with a common prime q = 71 and a primitive root α = 7.*

a) If user A has private key $X_A = 5$, what is A's public key Y_A ?

b) If user B has private key $X_B = 12$, what is B's public key Y_B ?

c) What is the shared secret key ?

Solution :

a) A's public key Y_A

$Y_A = \alpha^{X_A} \bmod q = (7)^5 \bmod 71$

$= 16807 \bmod 71 = 51$

b) B's public key Y_B

$Y_B = \alpha^{X_B} \bmod q = (7)^{12} \bmod 71$

$= 13841287201 \bmod 71 = 4$

c) Shared secret key

i) At user A $K = (Y_B)^{X_A} \bmod q$

$= (4)^5 \bmod 71 = 1024 \bmod 71$

$K = 30$

The man in middle attack can work against the Diffie-Hellman key exchange algorithm, causing it to fail.

Advantages

1. Any user can choose a random x and publish g^x in a public database such as a phone book.
2. Phone book must be maintained by a TTP.
3. Other users can look up the database and get the public key for the individual and use it to encrypt the message.
4. Ideal for use with emails.

Disadvantages

1. Does not protect against man-in-the-middle attacks.
2. Even can intercept all traffic between Alice and Bob and generate separate keys for communication with them.
3. If Allice sends an encrypted message for Bob with his public key, Eve simply forwards it.
4. For large prime p, (p – 1) is an even number and so Z_p^* will have an subgroup of order 2.

Example 3.10.2 *If generator g = 2 and n or P = 11, using Diffie-Hellman algorithm solve the following :*

i) Show that 2 is a primitive root of 11.

ii) If A has a public key '9' what is A's private key ?

iii) If B has a public key '3' what is B's private key ?

iv) Calculate the shared secret key.

Solution : i)

$2^1 \bmod 11 = 2$

$2^2 \bmod 11 = 4$

$2^3 \bmod 11 = 8$

$2^4 \bmod 11 = 5$

$2^5 \bmod 11 = 10$

$2^6 \bmod 11 = 9$

$2^7 \bmod 11 = 7$

$2^8 \bmod 11 = 3$

$2^9 \bmod 11 = 6$

Using 2 as integer, we get all the integer values between 1 to 11. So 2 is a primitive root of 11.

ii) Public key = 9

$2^6 \bmod 11 = 9$

$X_A = 6$

iii) $Y_B = (11)^6 \bmod 9$

$Y_B = 1$

iv) Shared secret key :

$K = (Y_B)^{XA} \bmod q$

$K = 3^6 \bmod 11$

$K = 3$

Example 3.10.3 *Consider a Diffie-Hellman scheme with a common prime q = 11 and a primitive root α = 2.*

i) If user A has the public key Y_A = 9; what is A's private key X_A ?

ii) If user A has a public key Y_A = 3 ; what is the shared secret key X_A ?

SPPU : May-07, Marks 8

Solution : i) q = 11, α = 2, Y_A = 9, X_A = ?

$2 \bmod 11 = 2$

$2^2 \bmod 11 = 4$

$2^3 \bmod 11 = 8$

$2^4 \bmod 11 = 5$

$2^5 \bmod 11 = 10$

$2^6 \bmod 11 = 9$

$2^7 \bmod 11 = 7$

$2^8 \bmod 11 = 3$

Since $2^e \bmod 11$ for $0 < i < 11$ contains all numbers from 1 to 11 – 1, the size of this set is equal to ϕ (q), the order of q.

From the above values $2^6 \bmod 11 = 9$ therefore $X_A = 6$

ii) From the above values

$\alpha^{X_A} \bmod 11 = Y_A$

$$2^{X_A} \bmod 11 = 3$$

$$2^{X_8} \bmod 11 = 3$$

$$\therefore \quad X_A = 8$$

Example 3.10.4 *Find the key exchanged between Alok and Bobby considering following data.*
i) n = 11 ii) g = 5 iii) X = 2, Y = 3
Find value of A, B and secret key K. **SPPU : April-19 (In sem), Marks 5**

Solution :

$$A = g^x \bmod n = 5^2 \bmod 11$$

$$A = 3$$

$$B = g^y \bmod n = 5^3 \bmod 11$$

$$B = 4$$

$$\text{Secret key } K_1 = B^x \bmod n = 4^2 \bmod 11$$

$$K_1 = 5$$

$$\text{Secret key } K_2 = A^y \bmod n = 3^3 \bmod 11$$

$$K_2 = 5$$

Review Question

1. *Explain "Diffie-Hellman" key exchange algorithm with suitable example.*
SPPU : April-16, Marks 5

3.11 El Gamal Algorithm

SPPU : May-18

- The ElGamal algorithm provides an alternative to the RSA for public key encryption.
  1. Security of the RSA depends on the difficult of factoring large integers.
  2. Security of the ElGamal algorithm depends on the difficulty of computing discrete logs in a large prime modulus.
- ElGamal has the disadvantage that the ciphertext is twice as long as the plaintext.
- It has the advantages the same plaintext gives a different ciphertext each time it is encrypted.
- Like RSA, the ElGamal system is a public key algorithm so it has one set of key numbers that are published and another secret number that is used for deciphering.

1. The keys are generated by selecting a large prime number p. It is recommended that p – 1 be divisible by another large prime.
2. Compute a generator number g and select a random integer "a" less than p – 1.
3. With these numbers compute $b = g^a \pmod p$.
4. The public key consists of the three number (p, g, b) and the secret key is the number a.
5. To find "a" given the public key, an attacker must be able to solve the discrete logarithm problem.

Encryption :

- If Bob wants to send a message to Alice he begins by looking up her public key (p, g, b) and representing the message as an integer m in the range 0 to p – 1.
- He then selects a random key, k that is less than p – 1.
- Using these numbers, Bob computes two numbers :

$$c_1 = g^k \quad \text{and} \quad c_2 = mb^k$$

- He sends (c_1, c_2) to Alice.

Decryption :

- When Alice receives the cipher-text, she will recover the plaintext using her secret key, "a" to compute :

$$m = c_2 c_1^{-a} \bmod p$$

- This works because :

$$c_2 c_1^{-a} = mb^k (g^k)^{-a} \; mb^k \; (g^a)^k \; (g^k)^{-a}$$

$$= mg^{ak} \; g^{-ak} = m \pmod p$$

- Bob should choose a different random integer k for each message he sends to Alice. If M is a longer message, so it is divided into blocks, he should choose a different k for each block.
- Say he encrypts two messagers (or blocks) M_1 and M_2, using the same k, producing cipher-texts.
- Eve intercepts both cipher-text messages and discovers one plaintext message M_1, she can compute the other plaintext message M_2.

Example : Alice selected her initial prime number p = 11, found the primitive element g = 7 and selected her random secret key a = 2, then her public key is :

$$b = 7^2 \bmod 11 = 5$$

- She would publish her public key : (11, 7, 5)
- Bob wants to send the letter "a" to Alice.
  1. He first breaks it up into a set of numbers where each number is less than 11 (the value of p).
  2. Since the ASCII representation of "a" is 01100001, he might break it up into four messages (01 10 00 01) or in decimal (1, 2, 0, 1).
  3. Next, he would select a random number k = 3 and then compute and send to Alice :

m	c_1	c_2
1	$7^3 \bmod 11 = 2$	$1 \times 5^3 \bmod 11 = 4$
2	$7^3 \bmod 11 = 2$	$2 \times 5^3 \bmod 11 = 8$
0	$7^3 \bmod 11 = 2$	$0 \times 5^3 \bmod 11 = 0$
1	$7^3 \bmod 11 = 2$	$1 \times 5^3 \bmod 11 = 4$

- The cipher-text is ((2, 4), (2, 8), (2, 0), (2, 4)).

Deciphering a Message

- When Alice receives this message from Bob, she uses her secrete key a = 2 as follows :

  (2, 4) : m = 4(2) – 2 = 4(4) – 1 = 12 mod 11 = 1 (4 and 3 are inverse mod 11)

  (2, 8) : m = 8(2) – 2 = 8(4) – 1 = 24 mod 11 = 2

  (2, 0) : m = 0(2) – 2 = 0(4) – 1 = 0 mod 11 = 0

  (2, 4) : m = 1

  Alice reassembles the message into the letter "a".

Review Question

1. *Explain digital signature algorithm.* **SPPU : May-18, Marks 5**

3.12 Elliptic Curve Cryptography

SPPU : May-19, Dec.-16,19, March-20

- An elliptic curve is a set of points on the cooridnate plane satisfying an equation of the form $y^2 + axy + by = x^3 + cx^2 + dx + e$. In order to use elliptic curves for say, Diffie-Hellman, there needs to be some mathematical operation on two points in the set that will always produce a point also in the set.
- ECC can be done with at least two types of arithmetic, each of which gives different definitions of multiplication. The two types of arithmetic are

1. Zp arithmetic
2. GF (2^n) arithmetic, which can be done with shifts and ⊕ s.

- To form a cryptographic system using elliptic curves, we need to find a hard problem corresponding to factoring the product of two primes or taking the discrete logarithm.
- Consider the equation Q = KP where Q, P∈ E_P(a, b) and K < P. It is relatively easy to calculate Q given K and P, but it is relatively hard to determine K given Q and P. This is called the **discrete logarithm problem for elliptic curves.**

Example 3.12.1 *Consider the group $E_{23}(9, 17)$. This is the group defined by the equation $y^2 \bmod 23 = (x^3 + 9x + 17) \bmod 23$. What is the discrete logarithm K of Q = (4, 5) to the base P = (16, 5) ?*

Solution : The brute-force method is to compute multiples of P until Q is found.

Thus,

P = (16, 5)
2P = (20, 20)
3P = (14, 14)
4P = (19, 20)
5P = (13, 10)
6P = (7, 3)
7P = (8, 7)
8P = (12, 17)
9P = (4, 5)

Because 9P = (4, 5) = Q, the discrete logarithm Q = (4, 5) to the base P = (16, 5) is K = 9.

Analog of Diffie-Hellman key exchange

A key exchange between users A and B can be accomplished as follows

1. A selects an integer n_A less than n. This is A's private key. A then generates a public key,
   $P_A = n_A \times G$; the public key is a point in E_q (a, b).
2. B similarly selects a private key n_B and computes a public key P_B.
3. A generates the secret key $K = n_A \times P_B$.
   B generates the secret key $K = n_B \times P_A$.

The two calculations in step 3 produce the same result because

$$n_A \times P_B = n_A \times (n_B \times G)$$
$$= n_B \times (n_A \times G)$$
$$= n_B \times P_A$$

Elliptic curve encryption and decryption

- For an encryption/decryption, system requires a point G and an elliptic group $E_q(a, b)$ as parameters. Each user A selects a private key n_A and generates a public key $P_A = n_A \times G$.
- To encrypt and send message P_m to user B, A chooses a random positive integer K and produces the ciphertext C_m consisting of the pair of points

$$C_m = \{KG, P_m + KP_B\}$$

- To decrypt the ciphertext, B multiplies the first point in the pair by B's secret key and subtracts the result from the second point

$$= P_m + KP_B - n_B(KG)$$
$$= P_m + K(n_B\ G) - n_B(KG)$$
$$= P_m$$

Review Question

1. *Discuss elliptic curve cryptography in detail.*

SPPU : Dec.-16, May-19, Dec.-19 (End Sem), March-20, Marks 5

3.13 Multiple Choice Questions

Q.1 RSA _____ be used for digital signature.

a must no b cannot
c can d should not

Q.2 Man in the middle attack can endanger the security of Diffie Hellman method if two parties are not _____.

a joined b authenticated
c submitted d shared

Q.3 In the RSA algorithm, we select 2 random large values 'p' and 'q'. Which of the following is the property of 'p' and 'q' ?

a p and q should be divisible by Φ (n)
b p and q should be co-prime
c p and q should be prime
d p/q should give no remainder

Q.4 In RSA, Φ (n) = _____ in terms of p and q.

a (p)/(q)
b (p)(q)
c (p – 1)(q – 1)
d (p+1)(q+1)

Q.5 For p = 11 and q = 19 and choose e = 17. Apply RSA algorithm where message = 5 and find the cipher text.

a C = 80
b C = 92
c C = 56
d C = 23

Q.6 RSA stands for _____

a Rivest Shamir and Adleman
b Rock Shane and Amozen
c Rivest Shane and Amozen
d Rock Shamir and Adleman

Q.7 The _____ method provides a one-time session key for two parties.

a AES
b RSA
c Diffie-Hellman
d DES

Q.8 AES has _____ different configurations.

a two
b three
c four
d five

Q.9 In an asymmetric-key cipher, the sender uses the _____ key.

a private
b public
c either (a) or (b)
d neither (a) nor (b)

Q.10 The AES key expansion algorithm takes as input a _____ key and produces a linear array of 156 bytes.

a 8-byte
b 12-byte
c 16-byte
d 24-byte

Q.11 In public key cryptosystems, the private key is kept by _____.

a sender

b receiver

c sender and receiver

d all the connected devices to the network

Q.12 User A, if wanting to send an authenticated message to user B, it would encrypt the message with A's _____ private key.

a public key

b private key

c both key

d third party key

Q.13 In RAS algorithm, the public key pair is _____.

a [d, n]

b [p, q]

c [e, n]

d [p, n]

Q.14 In RAS algorithm, the private key pair is _____.

a [d, n]

b [p, q]

c [e, n]

d [p, n]

Answer Keys for Multiple Choice Questions :

Q.1	c	**Q.2**	b	**Q.3**	c
Q.4	c	**Q.5**	a	**Q.6**	a
Q.7	c	**Q.8**	b	**Q.9**	b
Q.10	c	**Q.11**	b	**Q.12**	b
Q.13	c	**Q.14**	a		

❑❑❑

UNIT IV

4 Data Integrity Algorithms and Web Security

Syllabus

Cryptographic Hash Functions : *Applications of Cryptographic Hash Functions, Two Simple Hash Functions, Requirements and Security, Hash Functions Based on Cipher Block Chaining, Secure Hash Algorithm (SHA), SHA-3, MD4, MD5.* ***Message Authentication Codes :*** *Message Authentication Requirements, Message Authentication Functions, Requirements for Message Authentication Codes, Security of MACs.* ***Digital Signatures :*** *Digital Signatures, Schemes, Digital Signature standard, PKI X.509 Certificate.*
Web Security issues, HTTPS, SSH, Email security : PGP, S/MIME, IP Security : IPSec

Contents

4.1 Cryptographic Hash Functions

- Encryption is a two-way function. Hashing is a one-way function in the sense that once encrypted, a hash value cannot be decrypted.
- A hash function is used to map the data of arbitrary size to generate an output of a fixed size, usually called the Hash Digest. However, if this hash function satisfies some well-established standards of security, integrity, and other conventions of similar scope, it can be called a Cryptographic Hash Function
- **Definition :** A hash function is a computationally efficient function mapping binary strings of arbitrary length to binary strings of some fixed length, called hash-values.
- The data to be encoded is often called the "message", and the hash value is sometimes called the message digest or simply digest.
- The most common cryptographic uses of hash functions are with digital signatures and for data integrity.
- When hash functions are used to detect whether the message input has been altered, they are called Modification Detection Codes (MDC).
- There is another category of hash functions that involve a secret key and provide data origin authentication, as well as data integrity; these are called Message Authentication Codes (MACs).

One-way hash function

- A one-way hash function, also known as a message digest, fingerprint or compression function, is a mathematical function which takes a variable-length input string and converts it into a fixed-length binary sequence.
- Furthermore, a one-way hash function is designed in such a way that it is hard to reverse the process, that is, to find a string that hashes to a given value (hence the name one-way.)
- A good hash function also makes it hard to find two strings that would produce the same hash value. All modern hash algorithms produce hash values of 128 bits and higher.
- Even a slight change in an input string should cause the hash value to change drastically. Even if 1 bit is flipped in the input string, at least half of the bits in the hash value will flip as a result. This is called an **avalanche effect.**
- A common way for one-way hash functions to deal with the variable length input problem is called a **compression function.** Compression functions work by viewing the data being hashed as a sequence of n fixed-length blocks.

- To compute the hash value of a given block, the algorithm needs two things : **the data in the block and an input seed.**
- The input seed is set to some constant value, c, and the algorithm computes the hash value h_1 of the first block. Next, the hash value of the first block, h_1 is used as the seed for the second block.
- The function proceeds to compute the hash value of the second block based on the data in the second block and the hash value of the first block, h_1. So, the hash value for block n is related to the data in block n and the hash value h_{n-1} (for n>1). The hash value of the entire input stream is the hash value of the last block.

Hash function

- A hash value h is generated by a function H of the form.

$$h = H(M)$$

where M = variable - length message

H(M) = fixed - length hash value.

4.1.1 Requirement and Security

- The purpose of a hash function is to produce a fingerprint of a file, message or other block of data.

Properties :

1. H can be applied to a block of data of any size.
2. H produces a fixed length output.
3. H(x) is relatively easy to compute for any given x, making both hardware and software implementations practical.
4. For any given value h, it is computationally infeasible to find x such that H(x) = h. This is called **one-way property.**
5. For any given block x, it is computationally infeasible to find $y \neq x$ such that H(y) = H(x). This is called as **weak collision resistance.**
6. It is computationally infeasible to find any pair (x, y) such that H(x) = H(y). This is called as **strong collision resistance.**

4.1.2 Applications of Cryptographic Hash Functions

- A typical use of a cryptographic hash would be as follows :
  1. Alice poses a tough math problem to Bob, and claims she has solved it. Bob would like to try it himself, but would yet like to be sure that Alice is not

bluffing. Therefore, Alice writes down her solution, appends a random nonce, computes its hash and tells Bob the hash value. This way, when Bob comes up with the solution himself a few days later, Alice can prove that she had the solution earlier by revealing the nonce to Bob.

2. Second application of secure hashes is verification of message integrity. Determining whether any changes have been made to a message, for example, can be accomplished by comparing message digests calculated before, and after, transmission. A message digest can also serve as a means of reliably identifying a file; several source code management systems, including Git, Mercurial and Monotone, use the sha1sum of various types of content (file content, directory trees, ancestry information, etc) to uniquely identify them.
3. A related application is password verification. Passwords are usually not stored in clear text, for obvious reasons, but instead in digest form. To authenticate a user, the password presented by the user is hashed and compared with the stored hash. This is sometimes referred to as one-way encryption.
4. Hash functions can also be used in the generation of pseudorandom bits. Hashes are used to identify files on peer-to-peer file sharing networks. For example, in an ed2k link, an MD4-variant hash is combined with the file size, providing sufficient information for locating file sources, downloading the file and verifying its contents. Magnet links are another example. Such file hashes are often the top hash of a hash list or a hash tree which allows for additional benefits.

4.1.3 Two Simple Hash Functions

- All hash functions operate using the following general principles.
  a) The input (message, file, etc.) is viewed as a sequence of n -bit blocks.
  b) The input is processed one block at a time in an iterative fashion to produce an n-bit hash function.
- One of the simplest hash functions is the bit-by-bit exclusive-OR (XOR) of every block. This can be expressed as :

$$C_i = b_{i1} \oplus b_{i2} \oplus \ldots \oplus b_{im}$$

Where

C_i = i^{th} bit of the hash code, $1 \leq i \leq n$

m = number of n-bit blocks in the input

b_{ij} = i^{th} bit in j^{th} block

$\oplus$ = XOR operation

- A simple way to improve matters is to perform a one bit circular shift or rotation, on the hash value after each block is processed.

The procedure is as follows

1. Initially set the n-bit hash value to zero.
2. Process each successive n-bit block of data as follows.

a. Rotate the current hash value to the left by one bit.

b. XOR the block into the hash value.

4.1.4 Birthday Attack

- A birthday attack refers to a class of brute-force attacks.
- The attack is named after the statistical property of birthday duplication - you only need 23 people to have a larger than 50 % chance that they are born on the same day of the year.
- This is due to the fact that each time you adding one person to the set of people you are looking for duplicates in, you are looking for duplicates against all the people already in the set, not just one of them.
- The same technique can be used to look for conflicts in one-way functions. Instead of taking one output of the one-way function, you create or acquire a set of values (let us call this a) that have a some property and then create another set of other values that have different properties (let us call this b) and try to find any value that is in both a and b. This is a much smaller problem that finding a value that match a particular value in a.
- The properties in a and b might for instance be
  1. a contains secure hashes of an innocent message and b contains one of a less innocent message, so the attacker can substitute the messages at a later date.
  2. a is the password hashes of a system the attacker wants to get an account on, and b is a set of password hashes that the attacker knows the passwords for.
  3. a is the set of public keys from a Discrete Logarithms based cryptosystem where g and p are static, while b is the set of g^e mod p functions that the attacker knows e for.
- Birthday attacks are often used to find collisions of hash functions. To avoid this attack, the output length of the hash function used for a signature scheme can be chosen large enough so that the birthday attack becomes computationally infeasible.
- Resistance against this attack is why the Unix password hashes use a salt.

4.2 Hash Functions Based on Cipher Block Chaining

- Hash functions based on using a cipher block chaining technique, but without using the secret key. Divide a message M into fixed-size blocks $M_1, M_2, \ldots, M_N$.
- Use a symmetric encryption system DES to compute the hash code G as
  H_o = initial value

  $H_i = E(M_i, H_{i-1})$

  $G = H_N$
- Similar to the CBC technique, no secret key. this scheme is subject to the birthday attack.
- Two major categories of hash functions are : **dedicated hash functions and block** cipher-based hash functions.
- Block cipher is a popular encryption-decryption primitive. To encrypt, the block cipher accepts a key K and a plaintext block x as input and produces a cipher text block c = E(K, x), also written as $c = E_K(x)$.
- Given a message M consisting of a sequence of 64-bit blocks $P_1; P_2; :::; P_N$, define the hash code h = H(M) as the block-by-block XOR of all blocks and append the hash code as the final block :

  $$h = P_{N+1} = P_1 \oplus P_2 \oplus \ldots \oplus P_N$$
- Encrypt the entire message plus the hash code using CBC mode to produce the encrypted message $C_1; C_2; :::; C_{N+1}$. There are several ways the ciphertext can be manipulated in such a way that it is not detectable by the hash code.
- By the definition of CBC :

CBC : $C_j = E(K, [C_{j-1} \oplus P_j])$

So we have;

$$P_1 = IV \oplus D(K, C_1)$$

$$P_i = C_{i-1} \oplus D(K, C_i)$$

$$P_{N+1} = C_N \oplus D(K, C_{N+1})$$

- But, P_{N+1} has the hash code.

$$P_{N+1} = P_1 \oplus P_2 \oplus \ldots \oplus P_N$$

$$= [IV \oplus D(K, C_1)] \oplus [C_1 \oplus D(K, C_2)] \cdot \oplus \ldots \oplus [Y_{C+1} \oplus D(K, C_N)]$$

- Because the terms in the preceding equation can be XOR'ed in any order, it follows that the hash code would not change if the ciphertext blocks were permuted.

4.3 Secure Hash Algorithm (SHA)

- The Secure Hash Algorithm (SHA) was developed by National Institute of Standards and Technology (NIST). It is based on the MD4 algorithm. Based on different digest lengths, SHA includes algorithms such as SHA-1, SHA-256, SHA-384, and SHA-512.
- Unlike encryption, given a variable length meassge **x**, a secure hash algorithm computes a function **h(x)** which has a fixed and often smaller number of bits. When a message of any length is less than 2^{64} bits is input, the SHA-1 produces a 160-bit output called message digest.
- SHA-1 called secure bacause it is computationally infeasible to find a message which corresponds to a given message digest, or to find two different messages which produce the same message digest.
- There are a number of attacks on SHA-1, all relating to what is known as collision resistance. For examples, if you are using SHA-1 for the storage of passwards, there are no passoword recovery attacks as at December 2011 that make use of the collision attacks on SHA-1.
- The most commonly used hash function from the SHA family is SHA-1. It is used in many applications and protocols that require secure and authenticated communications. SHA-1 is used in SSL/TLS, PGP, SSH, S/MIME, and IPSec.

Features of SHA-1 :

1. The SHA-1 is used to compute a message digest for a message or data file that is provided as input.
2. The message or data file should be considered to be a bit string.
3. The length of the message is the number of bits in the message (the empty message has length 0).
4. If the number of bits in a message is a multiple of 8, for compactness we can represent the message in hex.
5. The purpose of message padding is to make the total length of a padded message a multiple of 512.
6. The SHA-1 sequentially processes blocks of 512 bits when computing the message digest.
7. The 64-bit integer is 1, the length of the original message.
8. The padded message is then processed by the SHA-1 as n 512-bit block.

- SHA-1 was cracked in the year 2005 by two different research groups. In one of these two demonstrations, Xiaoyun Wang, Yigun Lisa Yin, and Hongbo Yu demonstrated that it was possible to come up with a collosion for SHA-1 within a

space of size only 2^{69}, which was far fewer that the security level of 2^{80} that is associated with this hash function.

- New hash function SHA-512 is introduced to overcome problem of SHA-1.

4.3.1 Secure Hash Algorithm (SHA-512)

- The Secure Hash Algorithm (SHA) was developed by the National Institute of Standards and Technology (NIST). SHA-1 produces a hash value of 160 bits.
- In 2002, NIST produced a revised version of the standard, FIPS 180-2, that defined three new version of SHA, with hash value lengths of 256,384 and 512 bits, known as SHA-256, SHA-384 and SHA-512.
- Comparison of SHA parameters

Sr. No.	Parameters	SHA-1	SHA-256	SHA-384	SHA-512
1.	Message digest size	160	256	384	512
2.	Message size	$< 2^{64}$	$< 2^{64}$	$< 2^{128}$	$< 2^{128}$
3.	Block size	512	512	1024	1024
4.	Word size	32	32	64	64
5.	Number of steps	80	64	80	80
6.	Security	80	128	192	256

- For both SHA-1 and SHA-256, one begins by converting the message to a unique representation of the message that is a multiple of 512 bits in length, without loss of information about its exact original length in bits, as follows : Append a 1 to the message.
- Then add as many zeroes as necessary to reach the target length, which is the next possible length that is 64-bits less than a whole multiple of 512 bits. Finally, as a 64-bit binary number, append the original length of the message in bits.

Description of SHA-1

- Expand each block of 512, when it is time to use it, into a source of 80 32-bit subkeys as follows : The first 16 subkeys are the block itself. All remaining subkeys are generated as follows : Subkey N is the exclusive OR of subkeys N-3, N-8, N-14 and N-16, subjected to a circular left shift of one place. Starting from the 160-bit block value (in hexadecimal).
  67452301 EFCDAB89 98BADCFE 10325476 C3D2E1F0

  As input for the processing of the *first* 512-bit block of the modified message, for each message block, do the following

- Encipher the starting value using the 80 sub keys for the current message block. Add each of the 32-bit pieces of the cipher text result to the starting value, modulo 2^32, of course and use that result as the starting value for handling the next message block.
- The starting value created at the end of handling the last block is the hash value, which is 160 bits long.

The SHA "block cipher" component

- The main calculation in SHA enciphers a 160-bit block using 80 32-bit subkeys in 80 rounds. This calculation is somewhat similar to a series of Feistel rounds, except that instead of dividing the block into two halves, it is divided into five pieces.
- An F-function is calculated from four of the five pieces, although it is really the XOR of a function of three of the pieces and a circular left shift of a fourth, and XORed with one piece, which is also modified by being XORed with the current round's subkey and a constant.
- The same constant is used over each group of 20 rounds. One of the other blocks is also altered by undergoing a circular left shift, and then the (160-bit) blocks are rotated.
- The F-function, as well as the constant, is changed every 20 rounds. Calling the five pieces of the 160-bit block being "encrypted" a, b, c, d and e, the rounds of the SHA "block cipher" component proceed as follows
- Change a by adding the current constant to it. The constants are, in hexadecimal
  - For rounds 1 to 20 : 5A827999
  - For rounds 21 to 40 : 6ED9EBA1
  - For rounds 41 to 60 : 8F1BBCDC
  - For rounds 61 to 80 : CA62C1D6
- Change a by adding the appropriate subkey for this round to it.
- Change a by adding e, circular left-shifted 5 places to it.
- Change a by adding the main f-function of b, c and d to it, calculated as follows :
  - For rounds 1 to 20, it is (b AND c) OR (NOT b) AND (d).
  - For rounds 21 to 40, it is b XOR c XOR d.
  - For rounds 41 to 60, it is (b AND c) OR (b AND d) OR (c AND d).
  - For rounds 61 to 80, it is again b XOR c XOR d.
- Change d by giving it a circular *right* shift of 2 positions (or, for consistency, a circular left shift of 30 places.)

- Then swap pieces, by moving each piece to the next earlier one, except that the old a value is moved to e.
- There are various types in SHA such as SHA-256, SHA-384, and SHA-512.

SHA-512 logic

- Fig. 4.3.1 shows message digest generation using SHA-512.

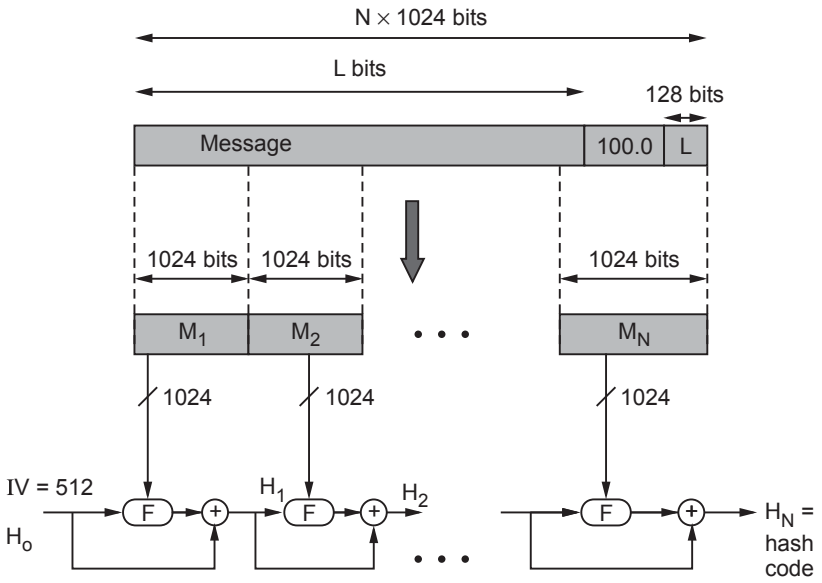


Fig. 4.3.1 Message digest using SHA-512

- The algorithm takes as input a message with a maximum length of less than 2^{128} bits and produces as output a 512-bit message digets. The input is processed in 1024-bit blocks.

Steps

1. **Append padding bits :** The message is padded so that its length is congruent to 896 modulo 1024. Padding consists of a single 1-bit followed by the necessary number of 0-bits.
2. **Append length :** A block of 128 bits is appended to the message. This block is treated as an unsigned 128-bit integer that contains the length of the original message (before the padding).
3. **Initialize has buffer :** A 512-bit buffer is used to hold intermediate and final results of the hash function. The buffer can be represented as eight 64-bit registers (a, b, c, d, e, f, g, h). These registers are initialised to the following 64-bit integers (hexadecimal values)

Sr. No.	Register	Values
1.	a	6A09E667F3BCC908
2.	b	BB67AE8584CAA73B
3.	c	3C6EF372FE94F82B
4.	d	A54FF53A5F1D36F1
5.	e	S10E527FADE682D1
6.	f	9B05688C2B3E6C1E
7.	g	1F83D9ABFB41BD6B
8.	h	5BE0CDI9137E2179

4. **Process message in 1024-bit blocks :** It consist of 80 rounds. Each round takes as input the 512-bit buffer value abcdefgh and updates the contents of the buffer. Each round t makes use of a 64-bit value W_t. The output of the last round is added to the input to the first round (H_{i-1}) to produce H_i.

- Fig. 4.3.2 shows the processing of a single 1024-bit block.
(See Fig. 4.3.2 on next page)

5. **Output :** The output from the N^{th} stage is the 512-bit message digest.

- The behaviour of SHA-512 is as-follows

$$H_0 = IV$$

$$H_i = SUM_{64}(H_{i-1}, abcdefghj)$$

$$MD = H_N$$

where IV = Initial value of the abcdefgh buffer.

$abcdefgh_i$ = The output of the last round of processing of the i^{th} message block.

N = The number of blocks in the message.

SUM_{64} = Addition modulo 2^{64} performed separately on each word of the pair of inputs.

MD = Final message digest value

SHA-512 round function

Each round is defined by the following set of equations.

$$T_1 = h + ch(e, f, g) + \left(\sum_1^{512} e\right) + W_t + K_t$$

$$T_2 = \left(\sum_0^{512} a\right) + Maj(a, b, c)$$

$$a = T_1 + T_2$$

$$b = a$$

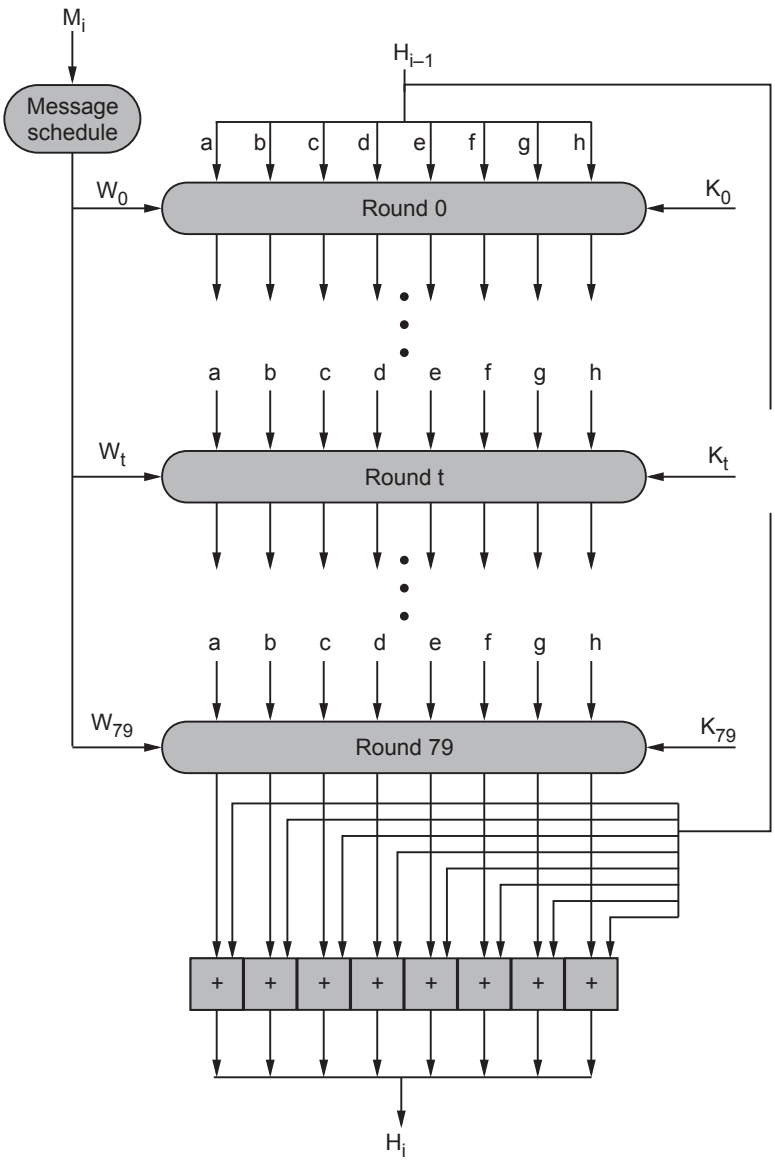


Fig. 4.3.2 SHA-512 processing of a single 1024-bit block

$c = b$

$d = c$

$e = d + T_1$

$f = e$

$g = f$

$h = g$

Fig. 4.3.3 shows single round operation.

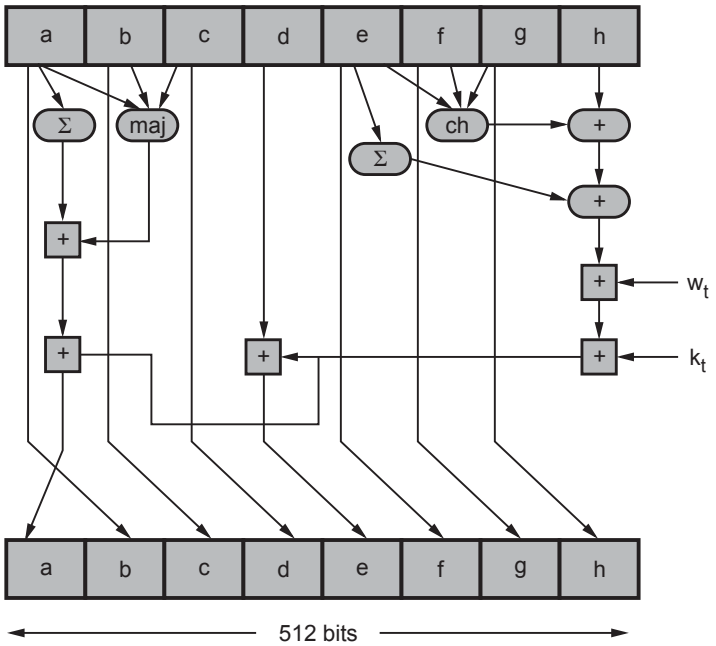


Fig. 4.3.3 Single round operation

Example 4.3.1 *Compare the performance of RIPEMD - 160 algorithm and SHA - 1 algorithm.*

Solution : RIPEMD-160 verses SHA-1 :

- brute force attack harder (160 like SHA-1 vs 128 bits for MD5)
- not vulnerable to known attacks, like SHA-1 though stronger
- RIPEMD-160 is slower than SHA-1
- RIPEMD-160 is more secure than SHA-1
- all designed as simple and compact
- SHA-1 optimised for big endian CPU's vs RIPEMD-160 optimised for little endian CPU's

4.3.2 SHA-3

- The SHA-3 family consists of six hash functions with digests (hash values) that are 128, 224, 256, 384 or 512 bits. SHA-3 also called Keccak, is a unidirectional function for generating digital prints of the selected length (the standard accepts 224, 256, 384 or 512 bits) from input data of any size.
- Fig. 4.3.4 shows SHA-3 Secure Hash Crypto Engine.

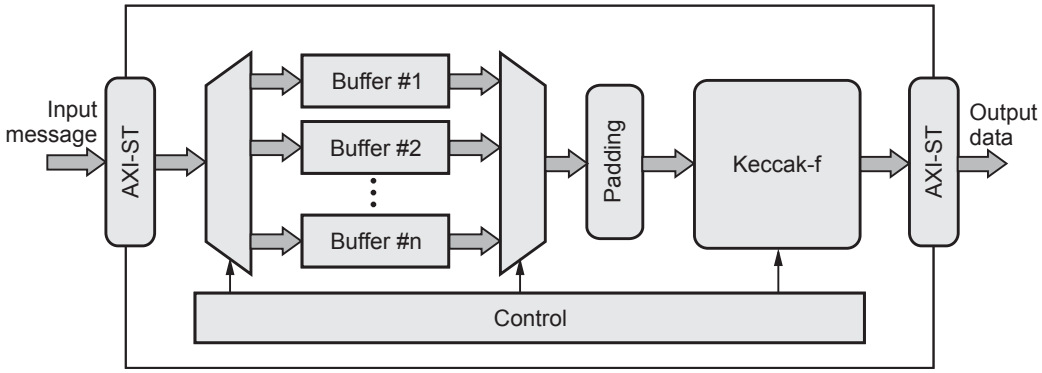


Fig. 4.3.4 SHA-3 Secure hash crypto engine

- The function Keccak-f is at the heart of the hash algorithm and is used in both phases of the sponge construction. Keccak-f is also referred to as Keccak- f permutation.
- The SHA-3 is a high-throughput, area-efficient hardware implementation of the SHA-3 cryptographic hashing functions. The core implements all the fixed-length and extendable hashing functions provisioned by standards.
- The hashing function is synthesis-time configurable; a version supporting run-time hashing function selection can be made available upon request.
- The number of SHA-3 permutation rounds per clock cycle is configurable at synthesis time, allowing users to trade throughput for silicon resources. Under its minimum configuration of one permutation per cycle, the core processes 24 to 56 bits per cycle depending on the hashing function. This throughput can scale by a factor of 2x, 3x, or 4x by implementing 2, 3, or 4 permutations per cycle respectively, enabling throughputs in excess of 100 Gbps in modern ASIC technologies.
- The core is designed for ease of use and integration and adheres to industry best-standards coding and verification practices. It requires no assistance from a host processor and uses standard AMBA® AXI4-Stream interfaces for input and output data.
- Technology mapping, timing closure and scan insertion are trouble-free, as the core contains no multi-cycle or false paths and uses only rising-edge-triggered D-type flip-flops, no tri-states and a single-clock/reset domain. Its reliability and low risk have been proven through rigorous verification and FPGA validation.

4.4 Message Digest

SPPU : April-16, 17, March-19, 20

- A message-digest algorithm is also called **a hash function** or a cryptographic hash function.
- It accepts a message as input and generates a fixed-length output, which is generally less than the length of the input message. The output is called a **hash value**, a fingerprint or a message digest.
- Message Digest 5 (MD5) processes the input text in 512-bit blocks. These blocks are further divided into 16 32-bit sub blocks.
- MD5 is a 128-bit hash.
- The MD5 algorithm is intended for digital signature applications, where a large file must be "compressed" in a secure manner before being encrypted with a private key under a public-key cryptosystem such as RSA.

4.4.1 MD5 Description

- Suppose if we have b-bit message as input, and that we wish to find its message digest. Here b is an arbitrary non-negative integer; b may be zero, it need not be a multiple of eight, and it may be arbitrarily large. The bits of the message written down as follows :

  m_0 m_1 ... m_{b-1}
- The following five steps are performed to compute the message digest of the message.

Step 1 : Append padding bits

- The message is "padded" so that its length is congruent to 448, modulo 512. Padding is always performed, even if the length of the message is already congruent to 448, modulo 512.
- Padding is performed as follows : a single "1" bit is appended to the message, and then "0" bits are appended so that the length in bits of the padded message becomes congruent to 448, modulo 512. In all, at least one bit and at most 512 bits are appended.

Step 2 : Append length

- A 64-bit representation of b is appended to the result of the previous step. In the unlikely event that b is greater than 2^{64}, and then only the low-order 64 bits of b are used.
- At this point the resulting message (after padding with bits and with b) has a length that is an exact multiple of 512 bits. Equivalently, this message has a length that is an exact multiple of 16 (32-bit) words.

- Let M[0 ... N-1] denote the words of the resulting message, where N is a multiple of 16.

Step 3 : Initialize MD buffer

- A four-word buffer (A, B, C, and D) is used to compute the message digest. Here each of A, B, C, D is a 32-bit register. These registers are initialized to the following values in hexadecimal :

  Word A : 01 23 45 67

  Word B : 89 ab cd ef

  Word C : fe dc ba 98

  Word D : 76 54 32 10

Step 4 : Process message in 16-word blocks

- We first define four auxiliary functions that each take as input three 32-bit words and produce as output one 32-bit word.

  F(X,Y,Z) = XY v not(X) Z

  G(X,Y,Z) = XZ v Y not(Z)

  H(X,Y,Z) = X xor Y xor Z

  I(X,Y,Z) = Y xor (X v not(Z))

- In each bit position F acts as a conditional: if X then Y else Z. The function F could have been defined using + instead of v since XY and not(X)Z will never have 1's in the same bit position.
- It is interesting to note that if the bits of X, Y, and Z are independent and unbiased, the each bit of
  F(X, Y, Z) will be independent and unbiased.
- The functions G, H, and I are similar to the function F, in that they act in "bitwise parallel" to produce their output from the bits of X, Y, and Z, in such a manner that if the corresponding bits of X, Y, and Z are independent and unbiased, then each bit of G(X,Y,Z), H(X,Y,Z), and I(X,Y,Z) will be independent and unbiased.
- This step uses a 64-element table T[1 ... 64] constructed from the sine function. Let T[i] denote the i-th element of the table, which is equal to the integer part of 4294967296 times abs(sin(i)), where i is in radians.

Step 5 : Output

- The message digest produced as output is A, B, C, and D. That is, we begin with the low-order byte of A, and end with the high-order byte of D.

4.4.2 Differences between MD4 and MD5

The following are the differences between MD4 and MD5 :

1. A fourth round has been added.
2. Each step now has a unique additive constant.
3. The function g in round 2 was changed from (XY v XZ v YZ) to (XZ v Y not(Z)) to make g less symmetric.
4. Each step now adds in the result of the previous step. This promotes a faster "avalanche effect".
5. The order in which input words are accessed in rounds 2 and 3 is changed, to make these patterns less like each other.
6. The shift amounts in each round have been approximately optimized, to yield a faster "avalanche effect." The shifts in different rounds are distinct.

4.4.3 Comparison between MD5 and SHA

Sr. No.	MD5	SHA
1.	MD length is 128-bits	Length is 160-bits
2.	Speed is faster than SHA	Slower than MD5
3.	Number of iteration is 64	Number of iteration is 80
4.	Buffer space is 128-bits	Buffer space is 160-bits
5.	MD5 is vulnerable to cryptanalytic attacks	SHA-1 appears not to be vulnerable to cryptanalytic attack
6.	MD5 uses a little endian scheme	SHA-1 uses a big endian scheme
7.	Simple to implement and do not need any large programs or complex table	Simple to implement and do not need any large programs or complex table.
8.	No limit on maximum message size.	Maximum message size is $2^{64} - 1$ bits.

Review Questions

1. *Explain operation of MD5 message digest algorithm.* **SPPU : April-16, Marks 5**
2. *What is message digest ? Compare MD5 with SHA - 1.* **SPPU : April-17, Marks 5**
3. *Explain in details the need and implementation of one way hash function (MD5).* **SPPU : March-19, Marks 5**
4. *Explain operation of MDS message digest algorithm.* **SPPU : March-20, Marks 5**

4.5 Message Authentication Codes

- Message authentication is a mechanism or service used to verify the integrity of a message. Message integrity guarantees that the message has not been changed. Message authentication guarantees that the sender of the message is authentic.
- A MAC algorithm, sometimes called a keyed hash function accepts as input a secret key and an arbitrary-length message to be authenticated and outputs a MAC. The MAC value protects both a message's data integrity as well as its authenticity, by allowing verifiers to detect any changes to the message content.
- Message Authentication Codes (MAC) also knows as a cryptographic check. The MAC is generated by a function C.

$$MAC = C(K, M)$$

where M = Variable length message

K = Secret key shared only by sender and receiver

$C(K, M)$ = Fixed length authenticator

- Security of the MAC generally depends on the bit length of the key. Weakness of the algorithm is the brute force attack.
- For a ciphertext - only attack, the opponent, given ciphertext C, would perform $P_i = D(K_i, C)$ for all possible key values K_i until a P_i was produced that matched the form of acceptable plaintext.
- MAC ensures that the message is coming from the correct sender, has not been changed, and that the data transferred over a network or stored in or outside a system is legitimate and does not contain harmful code. MACs can be stored on a hardware security module, a device used to manage sensitive digital keys.

Properties of message authentication codes :

1. Cryptographic checksum : A MAC generates a cryptographically secure authentication tag for a given message.
2. Symmetric : MACs are based on secret symmetric keys. The signing and verifying parties must share a secret key.
3. Arbitrary message size : MACs accept messages of arbitrary length.
4. Fixed output length : MACs generate fixed-size authentication tags.
5. Message integrity : MACs provide message integrity : Any manipulations of a message during transit will be detected by the receiver.
6. Message authentication : The receiving party is assured of the origin of the message.

7. No non-repudiation : Since MACs are based on symmetric principles, they do not provide non-repudiation.

- MACs provide two security services, message integrity and message authentication, using symmetric ciphers. MACs are widely used in protocols. Both of these services are also provided by digital signatures, but MACs are much faster.
- MACs do not provide non-repudiation.
- In practice, MACs are either based on block ciphers or on hash functions.
- HMAC is a popular MAC used in many practical protocols such as Transport Layer Security (TLS) indicated by a small lock in the browser.

4.5.1 Message Authentication Requirements

1. **Disclosure :** Release of message contents to any person or process not possessing the appropriate cryptographic key.
2. **Traffic analysis :** Discovery of the pattern of traffic between parties.
3. **Masquerade :** Insertion of messages into the network from a fraudulent source.
4. **Content modification :** Changes to the contents of a message, including insertion, deletion, transposition and modification.
5. **Sequence modification :** Any modification to a sequence of messages between parties, including insertion, deletion and reordering.
6. **Timing modification :** Delay or replay of messages.
7. **Source repudiation :** Denial of transmission of message by source.
8. **Destination repudiation :** Denial of receipt of message by destination.

- A digital signature is an authentication technique that also includes measures to counter repudiation by the source.

4.5.2 Application of MAC

- Following are the situations in which MAC used.
  1. Application in which the same message is broadcast to a number of destinations.
  2. Authentication of a computer program in plaintext is an attractive service.
  3. Another scenario is an exchange in which one side has a heavy load and cannot afford the time to decrypt all incoming messages.

4.5.3 MAC based on DES

- The data authentication algorithm based on DES, has been one of the most widely used MAC for a number of years. The algorithm can be defined as using the cipher block chaining mode of operation of DES with an initialization vector of zero.
- Fig. 4.5.1 shows the data authentication algorithm.

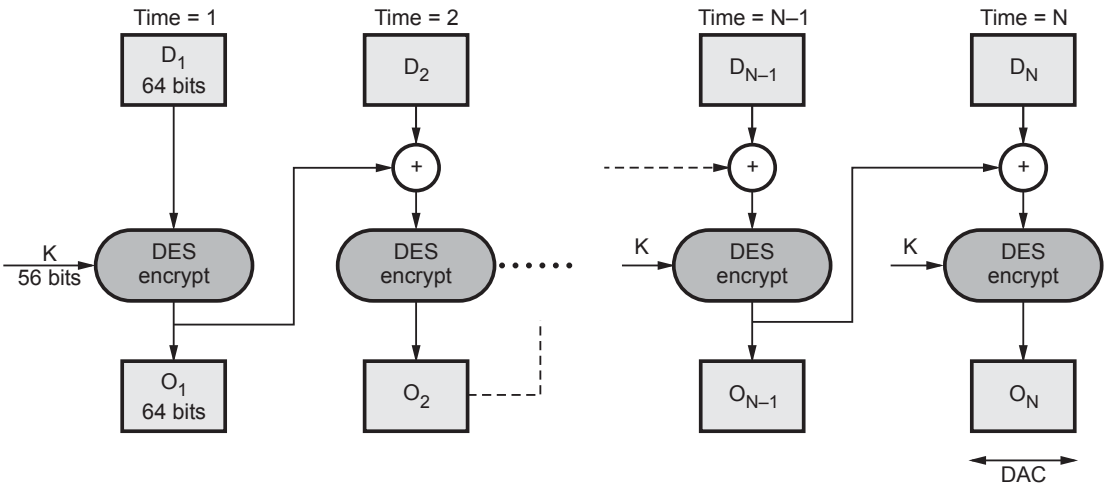


Fig. 4.5.1 Data authentication algorithm

- The algorithm can be defined as using the cipher block chaining mode of operation of DES. The data to be authenticated are grouped into contiguous 64-bit blocks : $D_1, D_2, D_3, \ldots, D_N$.
- Using the DES encryption algorithm (E) and a secret key (K), a Data Authentication Code (DAC) is calculated as follows

$$O_1 = E(K, D_1)$$

$$O_2 = E(K, [D_2 \oplus O_1])$$

$$O_3 = E(K, [D_3 \oplus O_2])$$

$$\vdots$$

$$\vdots$$

$$O_N = E(K, [D_N \oplus O_{N-1}])$$

- The DAC consists of either the entire block O_N or the leftmost M bits of the block, with $16 \leq M \leq 64$.

4.6 Digital Signatures

SPPU : May-18, Dec.-19

- 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

4.6.1 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.

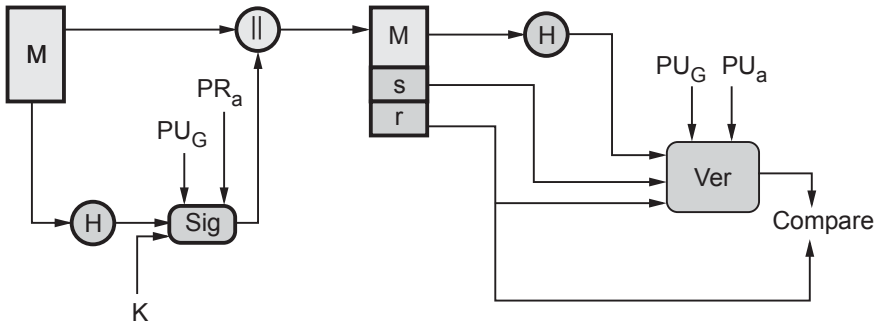


Fig. 4.6.1 DSS approach

- 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.

4.6.2 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.
- **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.

4.6.3 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. 4.6.1 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. 4.6.2 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.

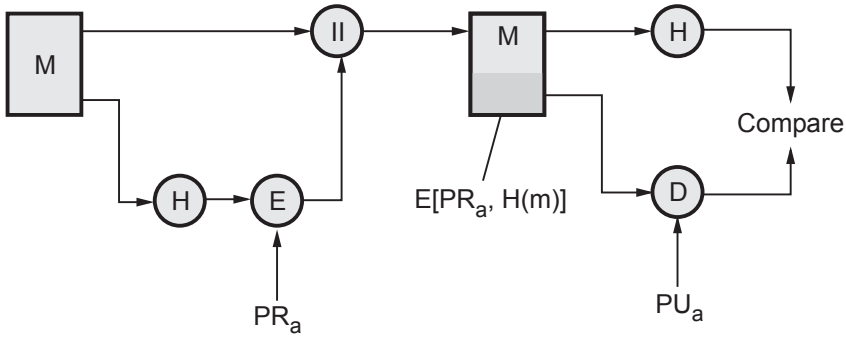


Fig. 4.6.2 RSA approach

4.6.4 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).
- 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. 4.6.3 shows the functions of signing and verifying.

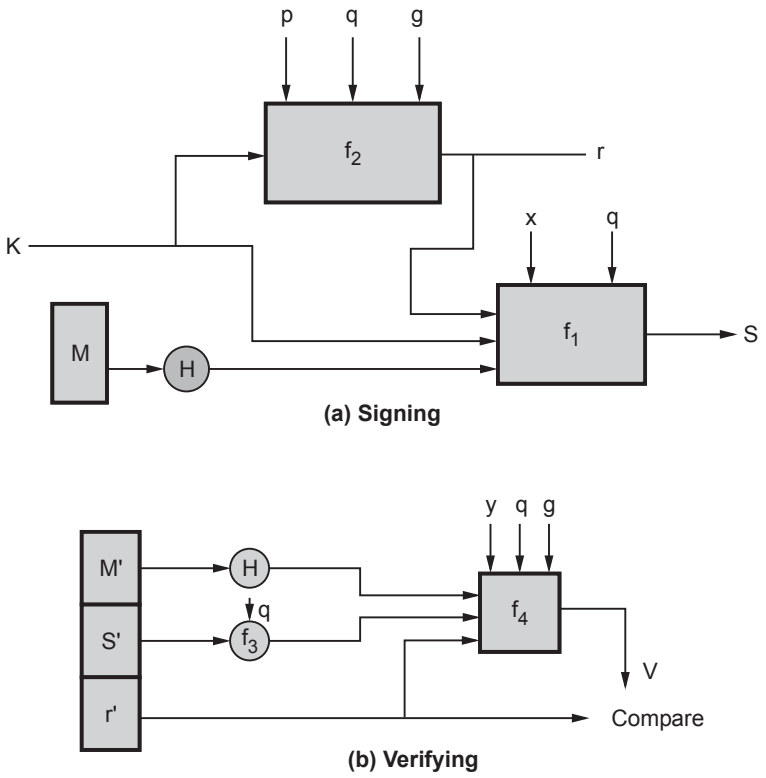


Fig. 4.6.3 Signing and verifying

Review Questions

1. *Explain digital signature algorithm.* **SPPU : May-18, Marks 5**
2. *Explain digital signature standard.* **SPPU : Dec.-19, Marks 5**

4.7 PKI

- 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.

Key Management :

- 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 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.

4.7.1 Benefits and Limitation of PKI

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.

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.

4.7.2 Certificate

- 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. 4.7.1 shows the hierarchy of certificate authorities.

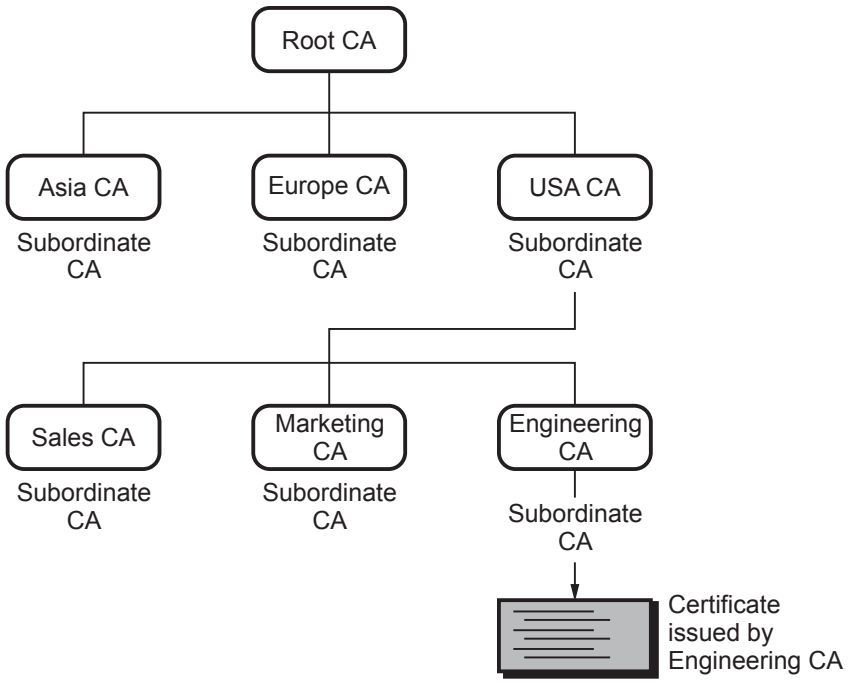


Fig. 4.7.1 Hierarchy of CA

- The root CA's certificate is a self-signed certificate : that is, the certificate is digitally signed by the same entity -- the root CA. 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).

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.

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. 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.

4.8 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. 4.8.1 shows generation of public key certificate.

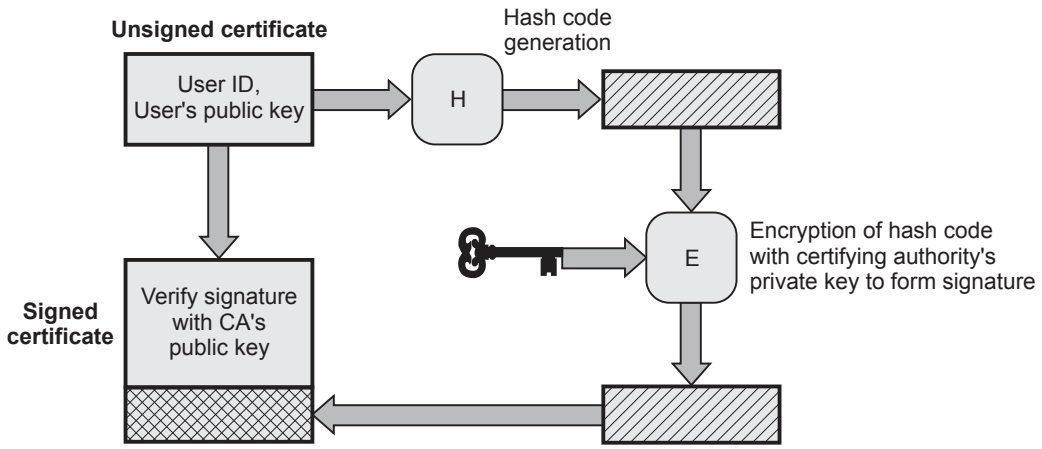


Fig. 4.8.1 Public key certificate

4.8.1 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. 4.8.2.

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. 4.8.2 X.509 Digital certificate format version 3

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,

$CA\langle\langle A\rangle\rangle$ indicates the certificate of user A issued by certification authority CA.

$CA\{V \ldots\ldots\ldots A_P\}$ indicates signing of $V \ldots\ldots A_P$ by CA.

4.8.2 Obtaining User's Certificate

- The characteristics of user certificate are -
  1. Any user who can access public key of CA can verify user public key.
  2. Only certification Authority (CA) can modify the certificate.
- All user certificates are placed in a directory for access of other users. The public key provided by CA is absolutely secure (w.r.t. integrity and authenticity).
- If user A has obtained a certificate from CA X_1 and user B has obtained a certificate from CA X_2. If A don't know the public key of X_2, then B's certificate

(issued by X_2) is useless to A. The user A can read B's certificate but A can not verify the signature. This problem can be resolved by securely exchanging the public keys by two CAs.

4.8.3 Revocation of Certificates

- The certificate should be revoked before expiry because of following reasons :
  1. User's private key is compromised.
  2. User is not certified by CA.
  3. CA's certificate is compromised.
- Each CA has a list of all revoked but not expired certificates. The Certificate Revocation List (CRL) is posted in directory signed by issuer and includes issuer's name, date of creation, date of next CRL. Fig. 4.8.3 Certificate revocation list. Each certificate has unique serial number of identify the certificate.

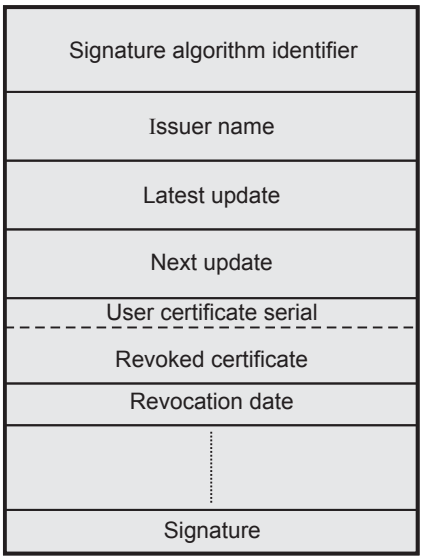


Fig. 4.8.3 Certificate revocation list

4.8.4 Authentication Procedures

- X.509 supports three types of authenticating using public key signatures. The types of authentication are
  1. One-way authentication
  2. Two-way authentication
  3. Three-way authentication

1. One-way authentication

- It involves single transfer of information from one user to other as shown in Fig. 4.8.4.

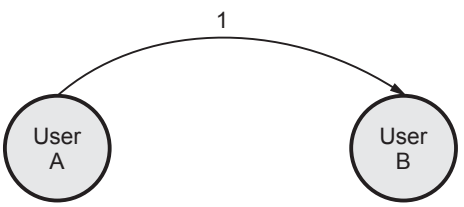


Fig. 4.8.4 One way authentication

2. Two-way authentication

- Two-way authentication allows both parties to communicate and verify the identity of the user.

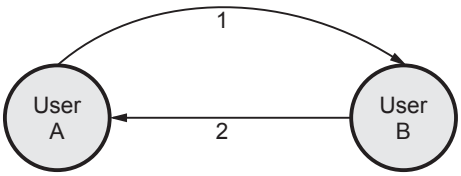


Fig. 4.8.5 Two-way authentication

3. Three-way authentication

- Three-way authentication is used where synchronized clockes are not available Fig. 4.8.6 shows three-way authentication.

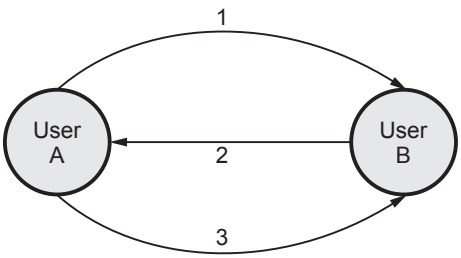


Fig. 4.8.6 Three-way authentication

4.8.5 Digital Certificate

- A data structure that securely binds an individual or entity to a public key used in cryptographic operations such as digital signatures or asymmetric encryption.
- To obtain digital certificate an organization must apply to a certification authority which is responsible for validating and ensuring the authenticity of requesting organization. The certificate will identify the name of the organization, a serial number, the validity date and the organization's public key where encryption to / from that organization is required.
- In addition, the digital certificate will also contain the digital signature of the certification authority to allow any recipient to confirm the authenticity of the digital certificate.
- A digital certificate is an ID that is carried with a file. To validate a signature, a certifying authority validates information about the software developers and then issues them digital certificates. The digital certificate contains information about the person to whom the certificate was issued, as well as information about the certifying authority that issued it. When a digital certificate is used to sign programs, ActiveX controls, and documents, this ID is stored with the signed item

in a secure and verifiable form so that it can be displayed to a user to establish a trust relationship.

- A digital certificate allows unique identification of an entity; it is essentially an electronic ID card, issued by a trusted third party. Digital certificates form part of the ISO authentication framework, also known as the X.509 protocol. This framework provides for authentication across networks.
- A digital certificate serves two purposes: it establishes the owner's identity, and it makes the owner's public key available. A digital certificate is issued by a Certification Authority (CA). It is issued for only a limited time, and when its expiry date has passed, it must be replaced.
- A digital certificate consists of :
  1. The public key of the person being certified
  2. The name and address of the person being certified, also known as the Distinguished Name (DN)
  3. The digital signature of the CA
  4. The issue date
  5. The expiry date
- The Distinguished Name is the name and address of a person or organization. You enter your Distinguished Name as part of requesting a certificate. The digitally-signed certificate includes not only your own Distinguished Name, but the Distinguished Name of the CA, which allows verification of the CA.
- To communicate securely, the receiver in a transmission must trust the CA that issued the certificate that the sender is using. This means that when a sender signs a message, the receiver must have the corresponding CA's signer certificate and public key designated as a trusted root key. For example, your web browser has a default list of signer certificates for trusted CAs. If you want to trust certificates from another CA, you must receive a certificate from that CA and designate it as a trusted root key.
- If you send your digital certificate containing your public key to someone else, what keeps that person from misusing your digital certificate and posing as you ? The answer is : your private key.
- A digital certificate alone is not proof of anyone's identity. The digital certificate allows verification only of the owner's identity, by providing the public key needed to check the owner's digital signature. Therefore, the digital certificate owner must protect the private key that belongs with the public key in the digital certificate. If the private key were stolen, anyone could pose as the legitimate owner of the digital certificate.

4.9 Web Security Issues

- The Web is very visible. The WWW is widely used by businesses, government agencies, and many individuals. But the Internet and the Web are extremely vulnerable to compromises of various sorts, with a range of threats.
- Complex software hides many security flaws. Web servers are easy to configure and manage. Users are not aware of the risks.
- These can be described as passive attacks including eavesdropping on network traffic between browser and server and gaining access to information on a Web site that is supposed to be restricted.
- Active attacks including impersonating another user, altering messages in transit between client and server, and altering information on a Web site. The Web needs added security mechanisms to address these threats.

Web Traffic Security Approaches

- Various approaches are used for providing security to the Web. One of the examples is IP security.
- Following table shows the comparison of threats on the web.

Parameters	Threats	Consequences	Countermeasures
Integrity	1. Modification of user data 2. Trojan horse browser 3. Modification of memory 4. Modification of message traffic in transit	1. Loss of information 2. Compromise of machine 3. Vulnerability to all other threats	Cryptographic checksums
Confidentiality	1. Eavesdropping on the Net 2. Theft of information from server 3. Theft of data from client 4. Information about network configuration 5. Information about which client talks to server	1. Loss of information 2. Loss of privacy	Encryption, Web proxies

Denial of Service	1. Killing of user threads 2. Flooding machine with bogus requests 3. Filling up disk or memory 4. Isolating machine by DNS attacks	1. Disruptive 2. Annoying 3. Prevent user from getting work done	Difficult to prevent
Authentication	1. Impersonation of legitimate users 2. Data forgery	1. Misrepresentation of user 2. Belief that false information is valid	Cryptographic techniques

- Fig 4.9.1 shows the relative location of security facilities in the TCP/IP protocol stack.

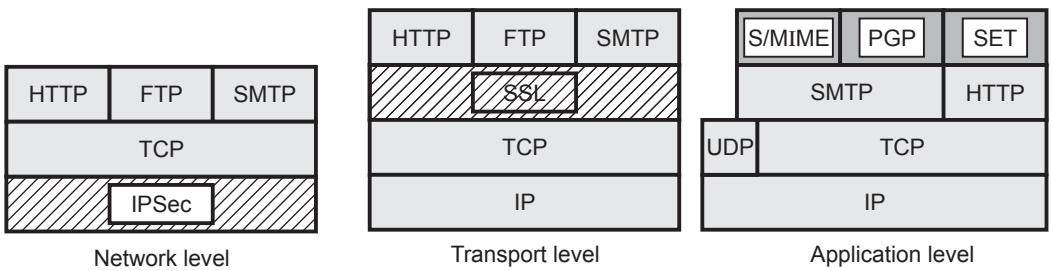


Fig. 4.9.1 Relative locations of security facilities in TCP/IP

4.9.1 Transport Layer Security (TLS)

- Transport Layer Security (TLS) is a feature of mail servers designed to secure the transmission of electronic mail from one server to another using encryption technology. TLS can reduce the risk of eavesdropping tampering and message forgery mail communications.
- TLS is a security protocol from the Internet Engineering Task Force (IETF) that is based on the Secure Sockets Layer (SSL) 3.0 protocol developed by Netscape.
- TLS was designed to provide security at the transport layer. TLS is a non-proprietary version of SSL. For transactions on Internet, a browser needs :
  1. Make sure that server belongs to the actual vendor.
  2. Contents of message are not modified during transition.
  3. Make sure that the imposter does not interpret sensitive information such as credit card number.
- Fig. 4.9.2 shows the position of TLS in the protocol.

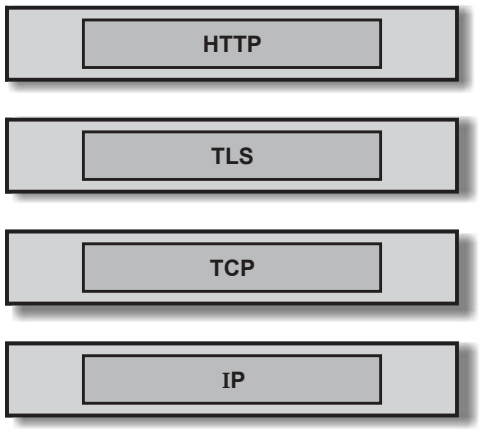


Fig. 4.9.2 TLS

- TLS has two protocols : Handshake and data exchange protocol
  1. **Handshake :** Responsible for negotiating security, authenticating the server to the browser and (optionally) defining other communication parameters. The TLS handshake protocol allows authentication between the server and client and the negotiation of an encryption algorithm and cryptographic keys before the application protocol transmits or receives any data.
  2. **Data exchange (record) protocol :** Data exchange (record) protocol uses the secret key to encrypt the data for secrecy and to encrypt the message digest for integrity. The TLS record protocol is designed to protect confidentiality by using symmetric data encryption.

Handshake protocol

- Fig. 4.9.3 shows the TLS handshake protocol.
  1. Browser sends a hello message that includes TLS version and some preferences.
  2. Server sends a certificate message that includes the public key of the server. The public key is certified by some certification authority, which means that the public key is encrypted by a CA private key.

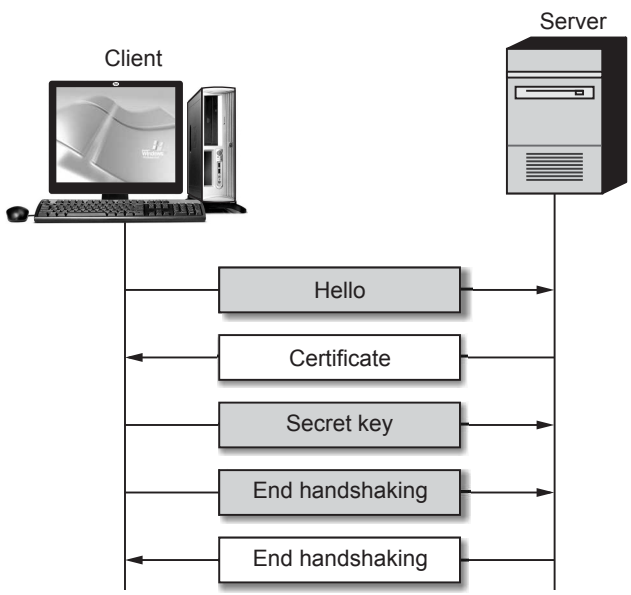


Fig. 4.9.3 TLS handshake protocol

Browser has a list of CAs and their public keys. It uses the corresponding key to decrypt the certification and finds the server public key. This also authenticates the server because the public key is certified by the CA.

3. Browser sends a secret key, encrypts it with the server public key and sends it to the server.
4. Browser sends a message, encrypted by the secret key to inform the server that handshaking is terminating from the browser key.
5. Server decrypts the secret key using it private key and decrypts the message using the secret key. It then sends a message, encrypted by the secret key, to inform the browser that handshaking is terminating from the server side.

4.9.2 Comparison between IPsec and TLS

Sr. No.	IPSec	TLS
1.	Type of security is device to device.	Type of security is application to application.
2.	It provides network segment protection.	It does not provides network segment protection.
3.	Application modification is required.	Application modification is not required.
4.	Traffic protected with data authentication and encryption is for all protocol.	Traffic protected with data authentication and encryption is only for TCP protocol.
5.	It controlled by using IPSec policy.	It controlled by using TLS policy.
6.	Scope of protection is for single connection for all traffic protocol.	Scope of protection is for single connection for TLS session.

4.10 HTTPS

- HTTPS (Hypertext Transfer Protocol Secure) is a secure version of the HTTP protocol that uses the SSL/TLS protocol for encryption and authentication. HTTPS uses port 443 by default. HTTPS is HTTP with encryption.
- The HTTPS protocol makes it possible for website users to transmit sensitive data such as credit card numbers, banking information and login credentials securely over the internet.
- **HTTP Problems :**
  1. HTTP Basic authentication is vulnerable to passive eavesdropping. Moreover, it provides no mechanism for explicit session expiration (i.e. logout).
  2. HTTP Digest authentication cannot guarantee sufficient support on all client platforms.
  3. Both mechanisms do not provide session tracking, but only authentication

- When properly configured, an HTTPS connection guarantees three things :
  1) Confidentiality : The visitor's connection is encrypted, obscuring URLs, cookies, and other sensitive metadata.
  2) Authenticity : The visitor is talking to the "real" website and not to an impersonator or through a person-in-the-middle.
  3) Integrity : The data sent between the visitor and the website has not been tampered with or modified.
- Secure HTTP indicates to user that page contents were not viewed or modified by a network attacker. Each S-HTTP file is either encrypted, contains a digital certificate, or both. For a given document, S-HTTP is an alternative to another well-known security protocol, Secure Sockets Layer (SSL).
- A major difference is that S-HTTP allows the client to send a certificate to authenticate the user whereas, using SSL, only the server can be authenticated.
- HTTPS is more likely to be used in situations where the server represents a bank and requires authentication from the user that is more secure than a user-id and password.
- Fig. 4.10.1 shows secure HTTP transactions.

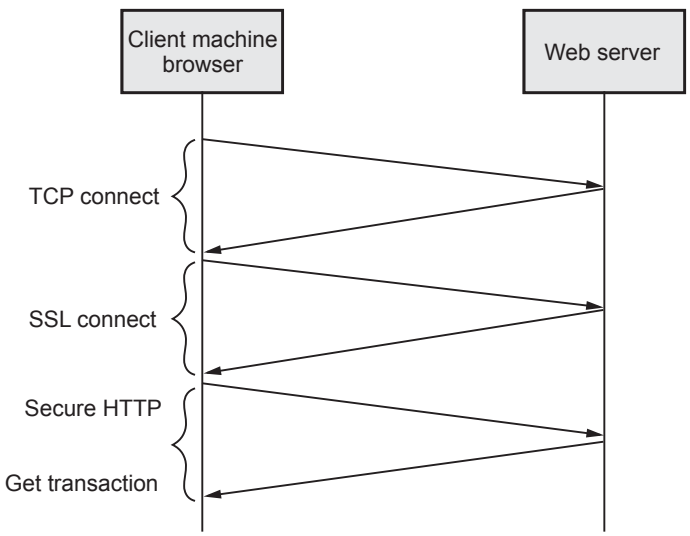


Fig. 4.10.1 HTTPS transaction

- In HTTPS, how does TLS/SSL encrypt HTTP requests and responses ?
- TLS uses a technology called public key encryption : there are two keys, a public key and a private key, and the public key is shared with client devices via the server's SSL certificate.

- When a client opens a connection with a server, the two devices use the public and private key to agree on new keys, called session keys, to encrypt further communications between them.
- All HTTP requests and responses are then encrypted with these session keys, so that anyone who intercepts communications can only see a random string of characters, not the plaintext.
- When a client makes a request over HTTPS, it first tries to locate a certificate on the server. If the cert is found, it attempts to verify it against its known list of Certificate Authorities (CA). If it is not one of the listed CAs, it might show a dialog to the user warning about the website's certificate. Once the certificate is verified, the SSL handshake is complete and secure transmission is in effect.
- Benefits of a HTTPS certificate are :
  1. Customer information like credit card numbers, bank account numbers is encrypted and cannot be intercepted
  2. Visitors can verify
  3. Customers are more likely to trust and complete purchases from sites that use HTTPS
- HTTPS does not use any a particular key certification scheme. It includes support for RSA, in-band, out-of-band and Kerberos key exchange. Like SSL, client public keys are not required.

4.11 SSH

- SSH stands for Secure Shell or Secure Socket Shell. It is a cryptographic network protocol that allows two computers to communicate and share the data over an insecure network such as the internet.
- Reasons to use SSH :
  1) Designed to be a secure replacement for rsh, rlogin, rcp, rdist, and telnet.
  2) Strong authentication. Closes several security holes (e.g., IP, routing, and DNS spoofing).
  3) Improved privacy. All communications are automatically and transparently encrypted.
  4) Arbitrary TCP/IP ports can be redirected through the encrypted channel in both directions
  5) The software can be installed and used even without root privileges.
  6) Optional compression of all data with gzip, which may result in significant speedups on slow connections.

- Features of SSH :
  1. Privacy : via strong end-to-end encryption- DES, IDEA, Blowfish
  2. Integrity : via 32 bit Cyclic Redundancy Check (CRC-32)
  3. Authentication : server via server's host key, client usually via password or public key
  4. Authorization : controlled at a server wide level or per account basis
  5. Forwarding : encapsulating another TCP based service such as Telnet within an SSH session
- Components of Secure Shell :
- SSHD Server : A program that allows incoming SSH connections to a machine, handling authentication, authorization.
- Clients : A program that connects to SSH servers and makes requests for service
- Session : An ongoing connection between a client and a server. It begins after the client successfully authenticates to a server and ends when the connection terminates.
- When SSHD is started, it starts listening on port22 for a socket. When a socket get connected the secure shell daemon spawns a child process. Which in turn generates an host key.
- After key is generated the secure shell daemon is ready for the local client to connect to another secure shell daemon or waits for a connection from remote host.
- Fig. 4.11.1 shows SSH protocol stack. SSH is organized as three protocols that typically run on top of TCP.

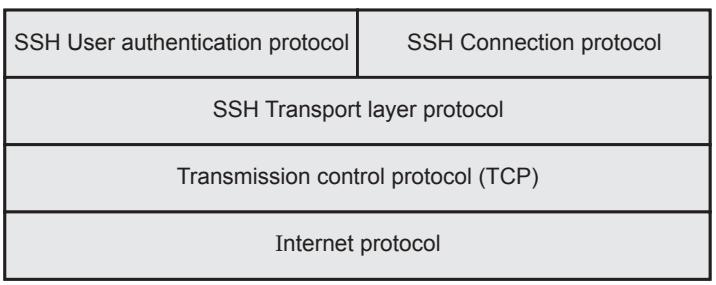


Fig. 4.11.1 SSH protocol stack

Functions of SSH protocol stack :

- Transport Layer Protocol provides server authentication, data confidentially and data integrity with forward secrecy. The transport layer may optionally provide compression.
- User authentication protocol : Authenticates the user to the server.

- Connection protocol : Multiplexes multiple logical communications channels over a single, underlying SSH connection.

SSH transport layer protocol :

- Server authentication is based on the server's public/private key pair.
  1. Host keys : One host may have many or many hosts could share one
  2. Client must have the server's public key in advance.
- Two alternative trust models defined in RFC4251.
  1. The client has a local DB associates each host name with public key.
  2. The host name to key association is certified by CA. The client only knows CA's public key and can verify all host keys certified by CA.
- SSH protocol is built into Unix and Linux servers to enable secure connections between systems. The connection is established by an SSH client that intends to connect to an SSH server.
- Fig. 4.11.2 shows working of SSH.

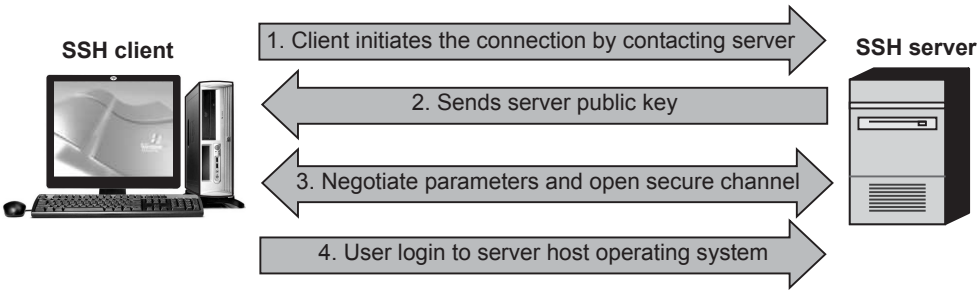


Fig. 4.11.2 Working of SSH

- The SSH client initiates the connection setup process and uses public key cryptography to verify the identity of the SSH server. After the setup phase, the SSH protocol uses strong symmetric encryption and hashing algorithms to ensure the privacy and integrity of the data that is exchanged between the client and server.
- SSH is a cryptographic protocol that creates a tunnel between two remote computers. Once the tunnel is established, the remote system shell is visible and shell commands can be securely transmitted across the connection.

Authentication :

- Server then decrypts the encrypted session key it received.
- Server sends a confirmation encrypted with this session key.
- Client receives confirmation, confirms server authentication.
- Client Authentication usually either by Password Authentication or Public key Authentication.

- Server confirms client authorization.
- Generates a 256 bit random challenge, encrypts it with clients public key and sends to client.
- Client decrypts challenge, generates a hash value with a session identifier (commonly generated random string at beginning of session) and sends to server.
- Server generates hash, if both match, session is authenticated.
- Fig. 4.11.3 shows binary packet protocol.

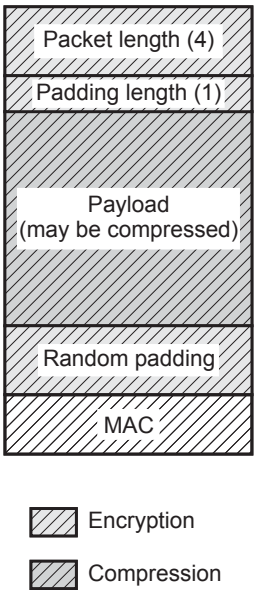


Fig. 4.11.3 Binary packet protocol

1. Packet length : Length of the packet not including the MAC and the packet length field.
2. Padding length : length of padding.
3. Payload : It is useful contents and might be compressed. Maximum payload size is 32768.
4. Random padding : It is 4-255 bytes. The total length of packet not including the MAC must be multiple of max(8, cipher block size) even if a stream cipher is used.
5. MAC : It is computed over the clear packet and an implicit sequence number.

Reasons to use SSH :

1. Designed to be a secure replacement for rsh, rlogin, rcp, rdist and telnet.

2. Strong authentication. Closes several security holes (e.g., IP, routing and DNS spoofing).
3. Improved primary. All communications are automatically and transparently encrypted.
4. Arbitrary TCP/IP ports can be redirected through the encrypted channel in both directions.
5. The software can be installed and used (with restricted functionality) even without root privileges.
6. Optional compression of all data with gzip (including forwarded X11 and TCP/IP port data), which may result in significant speedups on slow connections.

4.12 Email Security

SPPU : May-19, Dec.-19

- IP corresponds to the network layer in the OSI reference model and provides a connectionless best effort delivery service to the transport layer. An Internet Protocol (IP) address has a fixed length of 32 bits.
- IPv4 addresses are unique. Two devices on the internet can never have the same address at the same time.
- The address structure was originally defined to have a two level hierarchy : Network ID and host ID.
- The network ID identifies the network the host is connected to. The host ID identifies the network connection to the host rather than the actual host.
- IP addresses are usually written in dotted decimal notation so that they can be communicated conveniently by people.
- The IP address structure is divided into five address classes : Class A, Class B, Class C, Class D and Class E, identified by the most significant bits of the addresses.

4.12.1 IPv4 Header Format

- Packets in the IPv4 layer are called datagrams. A datagram is a variable length packet consisting of two parts : Header and data.
- Fig. 4.12.1 shows IPv4 header format
  1. **VER** is the field that contains the IP protocol version. The current version is 4.5 is an experimental version. 6 is the version for IPv6.
  2. **HLEN** is the length of the IP header in multiples of 32 bits without the data field.The minimum value for a correct header is 5 (i.e. 20 bytes), the maximum value is 15 (i.e., 60 bytes).

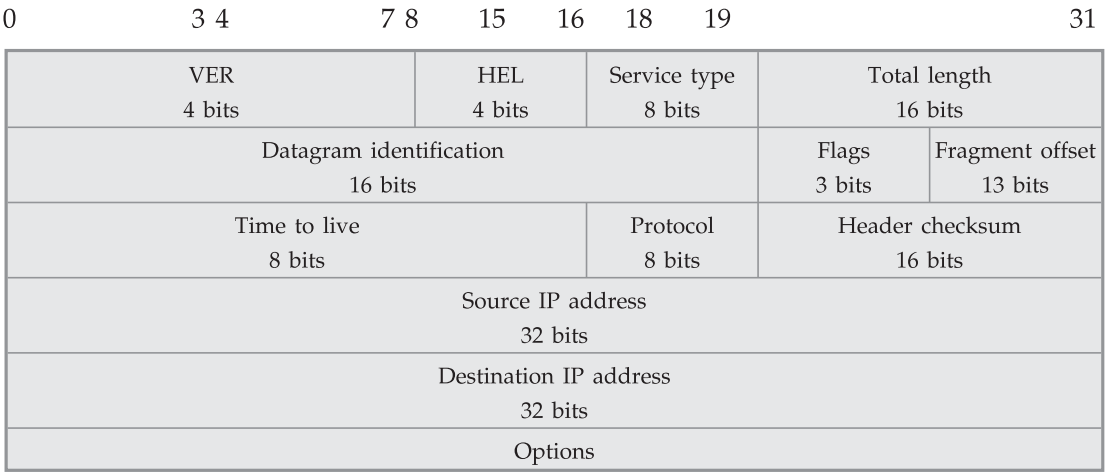


Fig. 4.12.1 IPv4 header format

3. **Service type :** The service type is an indication of the quality of service requested for this IP datagram. It contains the following information.

Precedence	Types of service	R

Precedence specifies the nature / priority :

000	Routine
001	Priority
010	Immediate
011	Flash
100	Flash override
101	Critical
110	Internetwork control
111	Internetwork control

TOS specifies the type of service value :

TOS bits	Description
1000	Minimize delay
0100	Maximum throughout
0010	Maximize reliability
0001	Minimize monetary cose
0000	Normal service

The last bit is reserved for future use.

4. **Total length** specifies the total length of the datagram, header and data, in octets.
5. **Identification** is a unique number assigned by the sender used with fragmentation.
6. **Flags** contain control flags :
   a. The first bit is reserved and must be zero;
   b. The 2nd bit is DF (Do not Fragment), 0 means allow fragmentation;
   c. The third is MF (More Fragments), 0 means that this is the last fragment.
7. **Fragment offset** is used to reassemble the full datagram. The value in this field contains the number of 64-bit segments (header bytes are not counted) contained in earlier fragments. If this is the first (or only) fragment, this field contains a value of zero.
8. **TTL** (Time To Live) specifies the time (in seconds) the datagram is allowed to travel. In practice, this is used as a hop counter to detect routing loops.
9. **Protocol number** indicates the higher level protocol to which IP should deliver the data in this datagram. E.g., ICMP = 1; TCP = 6; UDP = 17.
10. **Header checksum** is a checksum for the information contained in the header. If the header checksum does not match the contents, the datagram is discarded.
11. **Source/Destination IP addresses** are the 32-bit source/destination IP addresses.
12. **IP options** is a variable-length field (there may be zero or more options) used for control or debugging and measurement. For instance :
    a. The **loose source routing** option provide a means for the source of an IP datagram to supply explicit routing information;
    b. The **timestamp** option tell the routers along the route to put timestamps in the option data.
13. **Padding** is used to ensure that the IP header ends on a 32 bit boundary. The padding is zero.

Review Questions

1. *Compare PGP, MIME and S/MIME.*	**SPPU : May-19, Marks 6**
2. *What is backdoors and key escrow in PGP ?*	**SPPU : Dec.-19, Marks 9**

4.13 IP Security

SPPU : May-19, Dec.-19

- 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.

4.13.1 IP Security 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)

4.13.2 IPSec Document

- 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.

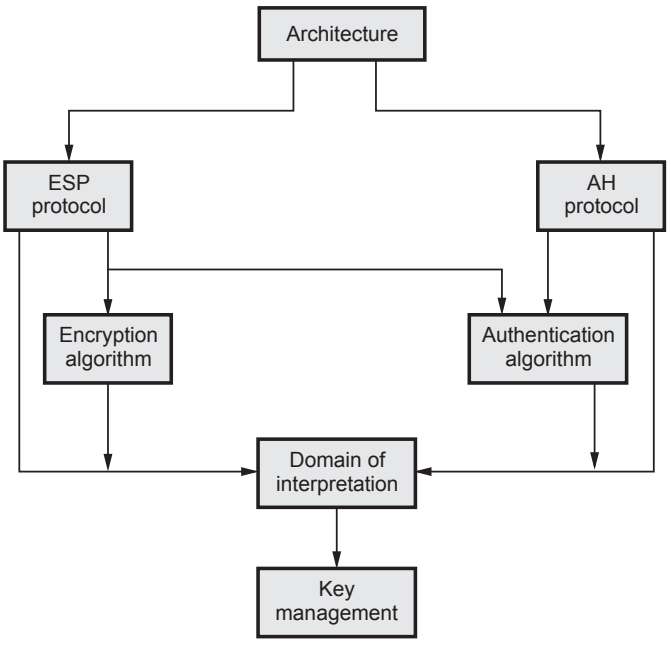


Fig. 4.13.1 IPSec document

- IPSec protocol consists of seven different groups of document as shown in Fig. 4.13.1.

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.

4.13.3 IPSec Services

- IPSec provides security serives 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 4.13.1.

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 4.13.1

4.13.4 Security Association

- 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.

4.13.5 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.

4.13.6 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.

4.13.7 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 4.13.2.

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 4.13.2

4.13.8 Application 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.

4.13.9 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.
5. IPSec is transparent to end users also.
6. If required IPSec can provide security to individual users.

Review Questions

1. *Discuss the working of IPSec. What are the benefits of IPSec.*
   SPPU : May-19, Marks 6
2. *Describe IPsec protocol with its components and security services.*
   SPPU : Dec.-19, Marks 8
3. *Describe briefly how IPsec works and enlist its applications. Distinguish between tunnel and transport mode of IPsec.*
   SPPU : Dec.-19, Marks 8

4.14 Authentication Header

- 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. 4.14.1.

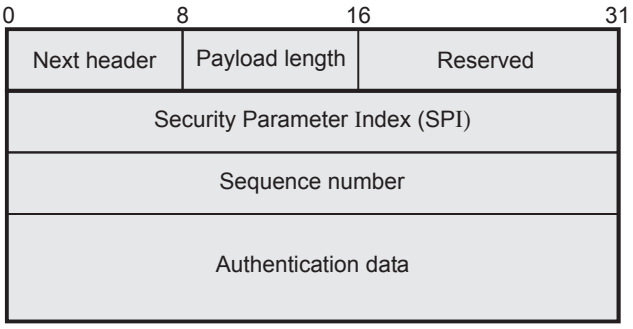


Fig. 4.14.1 IPSec authentication header format

1. **Next header** - This is 8-bits field and identifies the type of header that immediately follows the AH.
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.

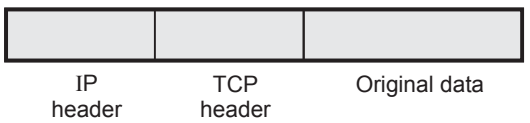
6. User C would get the benefit of the funds transfer twice.

Authentication data

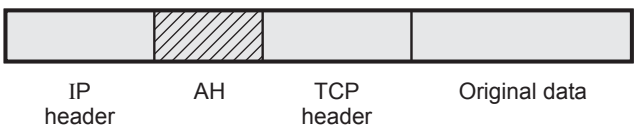
Also called Integrity check value for the datagram. This value is the MAC used for authentication and integrity purposes.

4.14.1 AH Transport Mode

- The position of the AH is between the original IP header and original TCP header of the IP packet.
- Fig. 4.14.2 shows the AH in transport mode.



(a) Before applying AH

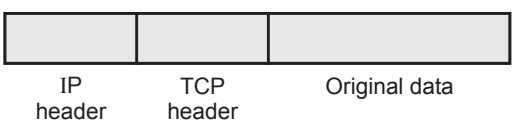


(b) After applying AH

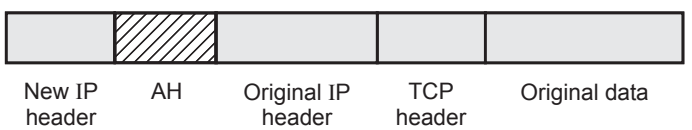
Fig. 4.14.2 Transport mode

4.14.2 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. 4.14.3 shows AH tunnel mode.



(a) Before applying AH



(b) After applying AH

Fig. 4.14.3 Tunnel mode

4.15 ESP

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

4.15.1 ESP Format

- Fig. 4.15.1 shows IPSec ESP format.

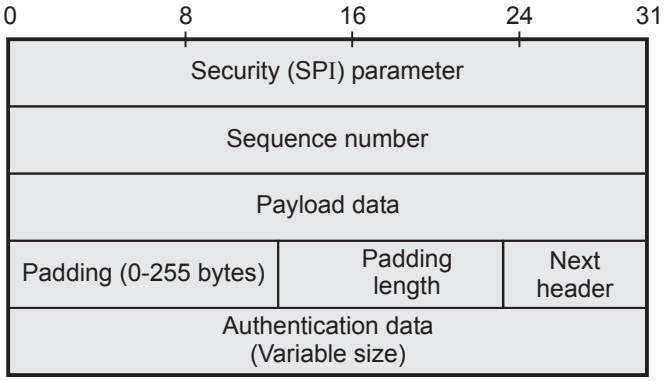


Fig. 4.15.1 ESP format

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.

4.15.2 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

4.15.3 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.

4.15.4 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.

4.16 Multiple Choice Questions

Q.1 PGP encrypts data by using a block cipher called _____ .

a international data encryption algorithm

b private data encryption algorithm

c internet data encryption algorithm

d none of the mentioned

Q.2 PGP is used in _____.

a browser security
b email security
c FTP security
d none of the above

Q.3 _____ is responsible for transferring the message from the MHS to the MS.

a Mail Delivery Agent
b Message transfer agent
c User agent
d All of these

Q.4 PGP _____ the message after applying the signature but before encryption.

a decompress
b compresses
c compress and decompress
d encryption

Q.5 The cryptography algorithms used in S/MIME are _____.

a IDEA
b RC4
c RSA, DES-3
d RC5.

Q.6 HTTS uses port number _____.

a 25
b 80
c 443
d 1024

Q.7 SSH stand for _____.

a Secure Socket Shell
b Secure Socket Layer
c Secure Session Handshake
d Secure Shell

Q.8 SSH connection protocol runs on the top of SSH _____.

a internet protocol
b transport layer protocol
c application layer protocol
d none of these

Q.9 The user initiates an SSH connection. SSH attempts to connect to port _____ on the remote host.

a 22
b 25
c 80
d 110

Q.10 Which of the following three users authentication method supported by SSH ?

a Private key, password, hostbased
b Public key, login, password

c Public key, password, hostbased

d Private key, password, serverbased

Q.11 An authentication technique which makes use of a secret key to generate a small fixed-size block of data, known as a _____.

a hash function

b message authentication code

c MD5

d none of these

Q.12 MAC provides _____.

a message confidentiality

b non-repudiation

c message authentication and integrity

d all of these

Q.13 A(n) _____ can be used to preserve the integrity of a document or a message.

a message digest

b message summary

c message confidentiality

d none of the above

Q.14 MD5 is a _____ bit hash.

a 64

b 128

c 256

d All of these

Q.15 MD5 processes the input text in _____ bit bloks.

a 128

b 256

c 512

d 1024

Q.16 Number of iteration is MD5 is _____.

a 16

b 24

c 32

d 64

Q.17 When an entire message is encrypted for _____ , using either sym-metric or asymmetric encryption, the security of the scheme generally depends on the bit length of the key.

a integrity

b non-repudiation

c availability

d confidentiality

Q.18 Source repudiation means _____.

a denial of receipt of message by destination

b denial of transmission of message by destination

c denial of transmission of message by source

d denial of receipt of message by source

Q.19 Destination repudiation means _____.

a denial of receipt of message by destination

b denial of transmission of message by destination

c denial of transmission of message by source

d denial of receipt of message by source

Q.20 A digital signature is an _____ mechanism that enables the creator of a message to attach a code that acts as a signature.

a authorization

b authentication

c both authorization and authentication

d none of these

Q.21 Digital signature standard cannot be used for _____.

a encryption

b decryption

c authorization

d all of them

Q.22 _____ helps in ensuring non-fradulent transactions on the web.

a Certificate authority

b Digital authority

c Dual authority

d Digital signature

Q.23 Digital signature envelope is decrypted by using _____.

a merchant private key

b payment public key

c merchant's public key

d payment's private key

Q.24 The recipient verifies the sender's identity using the sender's _____ .

a private key

b public key

c both key

d none of these

Q.25 For a digital signature, there is a _____ relationship between a signature and a message.

a one to many

b many to one

c many to many

d one to one

Answer Keys for Multiple Choice Questions :

Q.1	a	**Q.2**	b	**Q.3**	a
Q.4	b	**Q.5**	c	**Q.6**	c
Q.7	d	**Q.8**	b	**Q.9**	a
Q.10	c	**Q.11**	b	**Q.12**	c
Q.13	a	**Q.14**	b	**Q.15**	c
Q.16	d	**Q.17**	d	**Q.18**	c
Q.19	a	**Q.20**	b	**Q.21**	a
Q.22	a	**Q.23**	d	**Q.24**	b
Q.25	d				

❑❑❑

UNIT V

5 Network and System Security

Syllabus

The OSI Security architecture, Access Control, Flooding attacks, DOS, Distributed DOS attacks, Intrusion detection, Host based and network-based Honeypot, Firewall and Intrusion prevention system, Need of firewall, Firewall characteristics and access policy, Types of Firewall, DMZ networks, ***Intrusion prevention system :*** *Host based, Network based, Hybrid. Operating system Security, Application Security, Security maintenance, Multilevel Security, Multilevel Security for role-based access control, Concepts of trusted system, Trusted computing.*

Contents

5.1 Access Control

SPPU : Dec.-16, May-19

- 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 includes :
  1. Authentication of users
  2. Authorization of their privileges
  3. Auditing to monitor and record user actions
- Three types of access controls system are :
  1. Discretionary access control
  2. Mandatory access control
  3. Role-based access control

5.1.1 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 (DAC) is also called as an Identity-Based Access Control (IBAC).
- A Discretionary Access Control (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).

5.1.1.1 Drawbacks of DAC

- DAC system has two significant drawbacks :

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.

5.1.2 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.

5.1.2.1 Elements of MAC

- MAC has two key elements :

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.

5.1.2.2 MAC Implementations

- 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 (actually this uses a mix of MAC and DAC).

5.1.3 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.
  - Roles and their functions are often specified in the written documents of the organization.
  - 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.

5.1.3.1 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 (usually the developer defines the access given to each role, and the operational admin puts users into roles).
3. DAC definitions are typically attached to the data/resource, whereas RBAC is usually defined in two places : in code/configuration/metadata (the roles access), and on the user object (or table - the roles each user has).
4. DAC is administered "on the resource" (i.e. you administer each resource individually), whereas RBAC roles are centrally administered (who is associated with which roles).
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.

5.1.4 Access Control Matrix

- A password scheme used to allow access to a user's computer account may be viewed as the simplest instance of an access control matrix : each resource has a list of identities associated with it (e.g. a computer account which authorized entities may access), and successful corroboration of an identity allows access to the authorized resources as listed for that entity.
- The simplest framework for describing a protection system is the access control matrix model.
- Two fundamental concepts in field authorization are :
  1. Access Control Lists (ACLs)
  2. Capabilities (C-lists)

5.1.4.1 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.

- The VPN secure connection can be easily cracked by Ophcrack.
- Session keys and encryption are poorly implemented and vulnerable to attacks.
- The control channel is open to snooping and denial of service.

Counter measures

- Discontinue IKE aggressive mode use, use token based authentication scheme.

5. VoIP hacking

- VoIP on an IP network rely on multiple protocols, one for signaling and one for transport of encoded voice traffic.
- Two most common protocols are H.323 and SIP.

Most common VoIP attacks

1. Denial of service.
2. Spoofing the CLID (caller ID).
3. Injecting data into established call.
4. Attacking through services linked to VoIP, such as -
   - Advanced voice mail
   - Instant messaging
   - Calender services
   - User management
5. Accessing repository of recorded calls.

Counter measures

- Network segment between voice and data LANs.
- Authentication and encryption for all SIP communication.
- Replay IDS/IPS.

Review Question

1. *What is access control security services ?* **SPPU : Dec.-16, May-19, Marks 5**

5.2 Flooding Attacks

SPPU : May-16,17,18,19, Dec.-16, 17, 19

- Flooding attacks are classified based on network protocol used.
  1. ICMP flooding
  2. UDP flooding
  3. TCP SYN flooding

- Flood attacks are also known as Denial of Service (DoS) attacks. In a flood attack, attackers send a very high volume of traffic to a system so that it cannot examine and allow permitted network traffic. For example, an ICMP flood attack occurs when a system receives too many ICMP ping commands and must use all its resources to send reply commands.
- To prevent flood attacks, in the default packet handling page, you can specify thresholds for the allowed number of packets per second for different types of traffic. When the number of packets received on an interface exceeds the specified threshold, the device starts to drop traffic of that type on the interface.
- Understanding SYN flood attacks : Fig. 5.2.1 shows the SYN flood DOS attack.

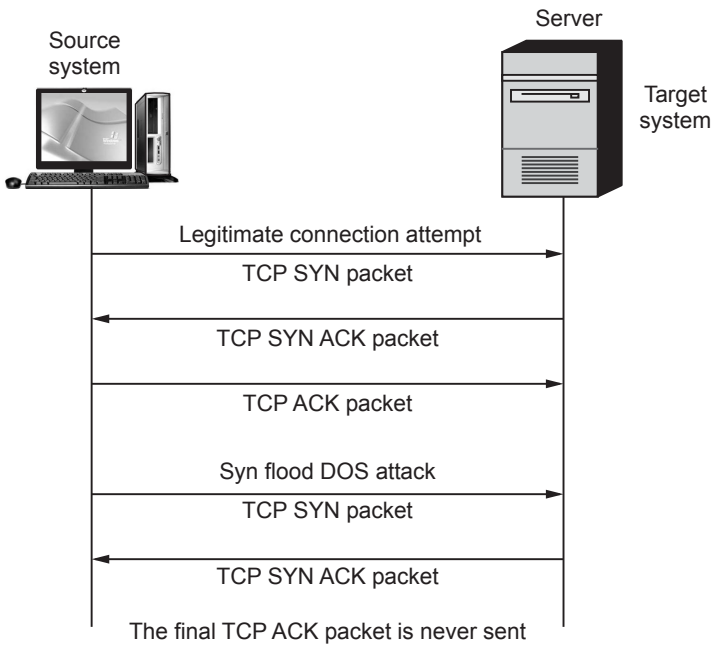


Fig. 5.2.1 SYN flood DOS attack

- 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.
- By flooding a host with incomplete TCP connections, the attacker eventually fills the memory buffer of the victim. Once this buffer is full, the host can no longer process new TCP connection requests. The flood might even damage the victim's operating system. Either way, the attack disables the victim and its normal operations

5.2.1 Distributed DOS Attacks

- A Distributed Denial of Service (DDoS) attack is an attempt to make an online service unavailable by overwhelming it with traffic from multiple sources. The target can be a server, website or other network resource. The flood of incoming messages, connection requests or malformed packets to the target system forces it to slow down or even crash and shut down, thereby denying service to legitimate users or systems.
- DDoS attacks can be classified into one of the following categories :
  1. Resource exhaustion (Bandwidth, CPU, Memory.)
  2. Vulnerability attacks
  3. Protocol attacks
- Targeted Web site is flooded with a vast number of meaningless messages sent by computers whose innocent users know nothing about the attack. The attack keeps legitimate users from using the site, causing inconvenience to users and monetary losses to the site's owners. Such an attack is referred to as Distributed Denial of Service (DDoS).
- A simple example of an internal resource attack is the SYN flood attack. Fig. 5.2.2 shows distributed SYN flood attack.

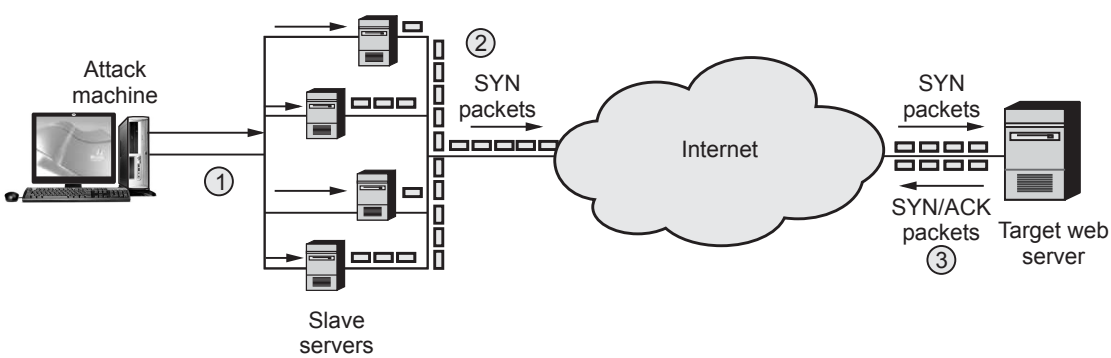


Fig. 5.2.2 Distributed SYN flood attack

1. The attacker takes control of multiple hosts over the Internet, instructing them to contact the target Web server.
2. The slave hosts begin sending TCP/IP SYN (synchronize/initialization) packets, with erroneous return IP address information, to the target.
3. Each SYN packet is a request to open a TCP connection. For each such packet, the Web server responds with a SYN/ACK (synchronize/acknowledge) packet, trying to establish a TCP connection with a TCP entity at a spurious IP address. The Web server maintains a data structure for each SYN request waiting for a response back and becomes bogged down as more traffic floods in. The result is that legitimate connections are denied while the victim machine is waiting to complete bogus "half-open" connections.

5.3 Intrusion Detection

- ***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.

5.3.1 Prevention

- **Intrusion prevention** is the process of performing intrusion detection and then stopping the detected incidents.
- **An Intrusion Prevention System (IPS)** is a network security/threat prevention technology that examines network traffic flows to detect and prevent vulnerability exploits.
- The main function of an IPS is to identify suspicious activity, and then log information, attempt to block the activity, and then finally to report it.
- Vulnerability exploits usually come in the form of malicious inputs to a target application or service that attackers use to interrupt and gain control of an application or machine.

- Following a successful exploit, the attacker can disable the target application (resulting in a denial-of-service state), or can potentially access to all the rights and permissions available to the compromised application.

5.3.2 Detection

- 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 behaviour.
- 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.
- IDS performs three tasks :
  a) An IDS monitors events of interests.
  b) An IDS generates significant data to systems administrators for analysis.
  c) An IDS creates alert for events when occurred.

5.3.3 Function and Strength of IDS

Intrusion detection systems perform the following functions well :

1. Monitoring and analysis of system events and user behaviors.
2. Testing the security states of system configurations.
3. Base lining the security state of a system, then tracking any changes to that baseline.
4. Recognizing patterns of system events that correspond to known attacks.
5. Recognizing patterns of activity that statistically vary from normal activity.
6. Managing operating system audit and logging mechanisms and the data they generate.
7. Alerting appropriate staff by appropriate means when attacks are detected.
8. Measuring enforcement of security policies encoded in the analysis engine.
9. Providing default information security policies.
10. Allowing non-security experts to perform important security monitoring function.

5.3.4 Types of IDS

5.3.4.1 Anomaly Detection

- An anomaly based intrusion detection system is a system for detecting computer intrusions and misuse by monitoring system activity and classifying it as either normal or anomalous.
- It examines ongoing traffic, activity, transactions, and behaviour in order to identify intrusions by detecting anomalies.
- For instance, anomaly-based IDS will detect that an IP packet is malformed. It does not detect that it is malformed in a specific way, but indicates that it is anomalous.
- The classification is based on heuristics or rules, rather than patterns or signatures, and will detect any type of misuse that falls out of normal system operation.
- Anomaly detectors construct profiles representing normal behavior of users, hosts, or network connections. These profiles are constructed from historical data collected over a period of normal operation.
- The detectors then collect event data and use a variety of measures to determine when monitored activity deviates from the norm.
- Another method is to define what normal usage of the system comprises using a strict mathematical model, and flag any deviation from this as an attack. This is known as strict anomaly detection.
- The measures and techniques used in anomaly detection include : Threshold detection, statistical measures, and rule-based measures.

Advantages of anomaly detection

1. IDSs based on anomaly detection detect unusual behavior and thus have the ability to detect symptoms of attacks without specific knowledge of details.
2. Anomaly detectors can produce information that can in turn be used to define signatures for misuse detectors.

Disadvantages of anomaly detection

1. Anomaly detection approaches usually produce a large number of false alarms due to the unpredictable behaviors of users and networks.
2. Anomaly detection approaches often require extensive "training sets" of system event records in order to characterize normal behavior patterns.

5.3.4.2 Signature-based Detection

- A signature based IDS will monitor packets on the network and compare them against a database of signatures or attributes from known malicious threats.
- This is similar to the way most antivirus software detects malware.
- A common strategy for IDS in detecting intrusions is to memorize signatures of known attacks. The inherent weakness in relying on signatures is that the signature patterns must be known first.
- New attacks are often unrecognizable by popular IDS. Signatures can be masked as well. The ongoing race between new attacks and detection systems has been a challenge.
- Also called misuse detection.

Advantages of signature-based detection

1. Signatures are easy to develop.
2. Understand if you know what network behavior you're trying to identify.

Disadvantages of signature-based detection

1. High false positive rate.
2. Largely ineffective at detecting previously unknown threats.
3. Signature database must be continually updated and maintained.

5.3.4.3 Comparison between Signature-based and Anomaly Detection

Parameters	Signature-based detection	Anomaly detection
Technique	Detect patterns of interest	Deviations from learned norms
Generalization	Problematic	Yes
Specific	Yes	No
Sensitivity	High	Moderate
False alarms	Low	Moderate
Adaptation	No	Yes

5.3.4.4 Network based System

- 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.

5.3.4.5 Host-based IDSs (HIDS)

- 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.

5.3.4.6 Differences between HIDS and NIDS

Sr. No.	NIDS	HIDS
1.	Broad in scope, (watching all network activities).	Narrow in scope (watching only specific host activities).
2.	Easier setup.	More complex setup.
3.	Better for detecting attacks from the outside.	Better for detecting attacks from the inside.
4.	Less expensive to implement.	More expensive to implement.

5.	Detection is based on what can be recorded on the entire network.	Detection is based on what any single host can record.
6.	Examines packet headers.	Does not see packet headers.
7.	Near real-time response.	Usually only responds after a suspicious log entry has been made.
8.	OS-independent.	OS-specific.
9.	Detects network attacks as payload is analyzed.	Detects local attacks before they hit the network.
10.	Detects unsuccessful attack attempts.	Verifies success or failure of attacks.

5.3.5 Limitation of IDS

Intrusion detection systems cannot perform the following functions :

1. Compensating for weak or missing security mechanisms in the protection infrastructure. Such mechanisms include firewalls, identification and authentication, link encryption, access control mechanisms, and virus detection and eradication.
2. Instantaneously detecting, reporting, and responding to an attack, when there is a heavy network or processing load.
3. Detecting newly published attacks or variants of existing attacks.
4. Effectively responding to attacks launched by sophisticated attackers.
5. Automatically investigating attacks without human intervention.
6. Resisting attacks that are intended to defeat or circumvent them.
7. Compensating for problems with the fidelity of information sources.
8. Dealing effectively with switched networks.

5.3.6 Difference between IDS and IPS

Sr. No.	IDS	IPS
1.	Installed on network segments (NIDS) and on host (HIDS).	Installed on network segments (NIPS) and on host (HIPS).
2.	Sits on network passively .	Sits inline (not passive).
3.	Cannot parse encrypted traffic.	Better at protecting applications.
4.	Central management control.	Central management control.
5.	Better at detecting hacking attacks.	Ideal for blocking web defacement.
6.	Alerting product (reactive).	Blocking product (proactive).

5.3.7 Intrusion Detection Techniques

- Intrusion detection techniques are as follows :
  1. **Threshold detection :** It records each occurrence of suspicious events and compares it with a threshold number. Threshold detection involves counting no occurrences of a specific event type over an interval of time, if count surpasses a reasonable number, then intrusion is assumed establishing threshold number is difficult.
  2. **Anomaly detection :** It requires little knowledge of the actual system beforehand. Usage patterns are established automatically by means of neural networks.
  3. **Rule based detection :** Observe events on system and apply rules to decide if activity is suspicious or not. Analyze historical audit records to identify usage patterns and auto-generate rules for them. Then observe current behavior and match against rules to see if conforms. Like statistical anomaly detection does not require prior knowledge of security flaws.

5.3.8 Tools for Intrusion Detection

- Audit record is a fundamental tool for intrusion detecting. Two forms of audit records are used.
  1. **Native audit records**

     In all multiuser operating system accounting software collects information about user activity.
  2. **Detective specific audit records**

     A system that collects information need by intrusion detection system.

Audit record format

- Each audit record contains following field.
  1. Subject
  2. Action
  3. Object
  4. Exception - condition
  5. Resource - usage
  6. Time stamp.

Fig. 5.3.1 shows audit record format.

Subject	Action	Object	Exception condition	Resource-usage	Time-stamp

Fig. 5.3.1 Audit record format

5.3.9 Distributed IDS

- A distributed collection of hosts supported by a LAN or internetwork is called distributed intrusion detection system.

Components of distributed IDS

- The distributed IDS consists of three major components.
  1. Host agent module
  2. LAN monitor agent module
  3. Central manager module.

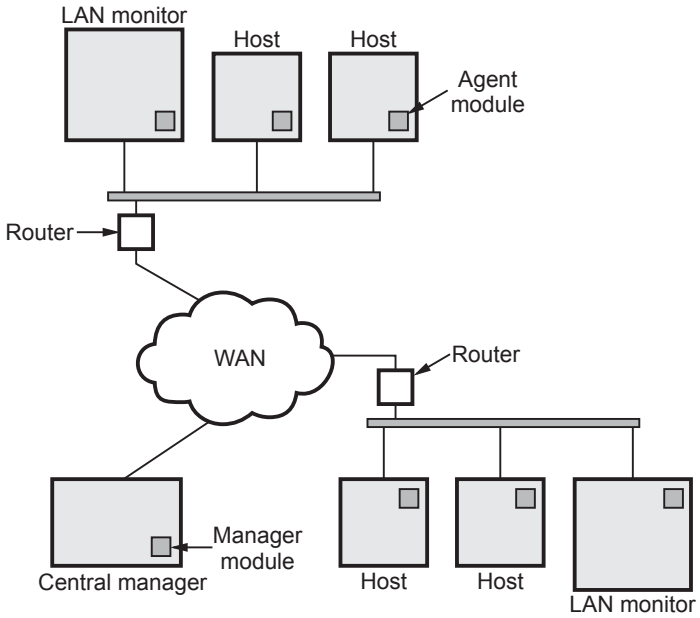


Fig. 5.3.2 Distributed ID architecture

Review Questions

1. *What are the challenges of intrusion detection ?* **SPPU : May-16,17, Marks 6**
2. *Explain anomaly-based intrusion detection system.* **SPPU : May-16,17, Marks 6**
3. *Explain types of Intrusion Detection System (IDS) ?* **SPPU : Dec.-16, Marks 6**
4. *List and explain types of Intrusion Detection System (IDS).* **SPPU : Dec.-17, Marks 9**
5. *Explain operation of anomaly based intrusion detection system in detail.* **SPPU : Dec.-17,18, Marks 8**

6. *Explain the operaton of mis used - based intrusion detection system.*

SPPU : May-18, Marks 8

7. *Explain need and challenges of intrusion detection system. Define signature based IDS.*

SPPU : May-19, Dec.-19, Marks 8

5.4 Honeypot

- honeypot is a system that can detect, monitor, and sometimes tamper with the activities of an attacker.
- When attackers access the system, the honeypot monitors their activity without their knowledge. we might set up a honeypot to provide an early warning system for a corporation, to discover an attacker's methods, or as an intentional target to monitor the activities of malware in the wild.
- Honeypots are designed to :
  a) Divert an attacker from accessing critical systems
  b) Collect information about the attacker's activity
  c) Encourage the attacker to stay on the system long enough for administrators to respond
- Honeypots don't provide security for an organization but if implemented and used correctly they enhance existing security policies and techniques.

5.5 Firewall

SPPU : May-19, Dec.-19

- 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. 5.5.1.

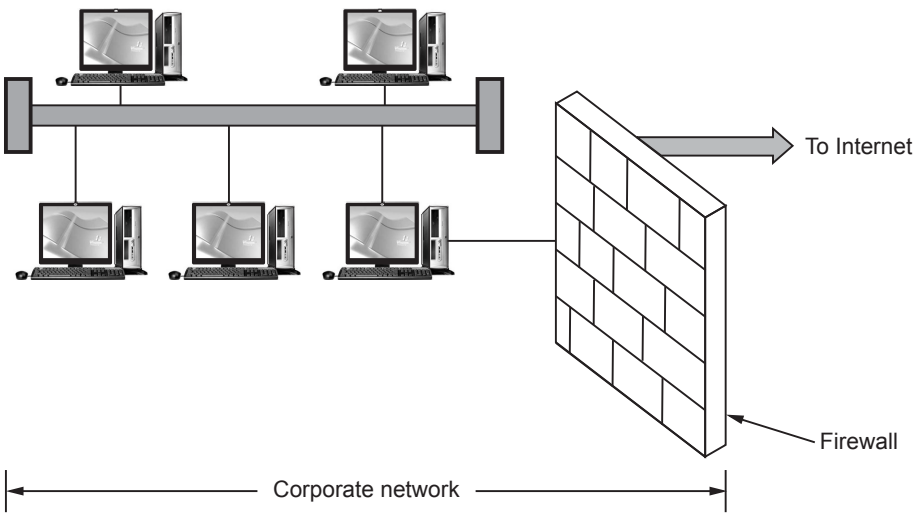


Fig. 5.5.1 Firewall

- 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.

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.

5.5.1 Types of Firewall

- Commonly used firewalls from threats of security are
  1. Packet filtering router
  2. Application level gateways
  3. Circuit level gateways.

5.5.1.1 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. 5.5.2 shows packet filtering router.

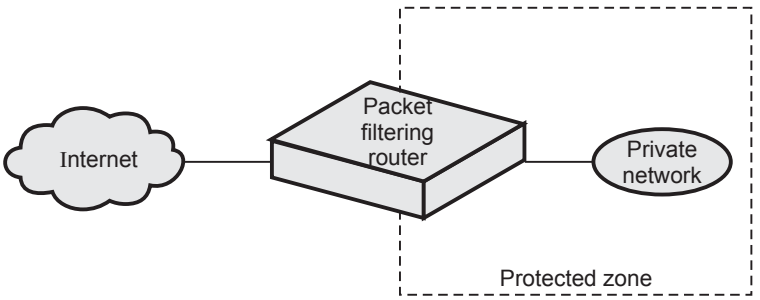


Fig. 5.5.2 Packet filtering router

- 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.
  1) First of course, one must know what should and what should not be permitted.
  2) The allowable types of packets must be specified, in terms of lofical expression on packet fileds.
  3) 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.

5.5.1.2 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. 5.5.3 shows application level gateway.

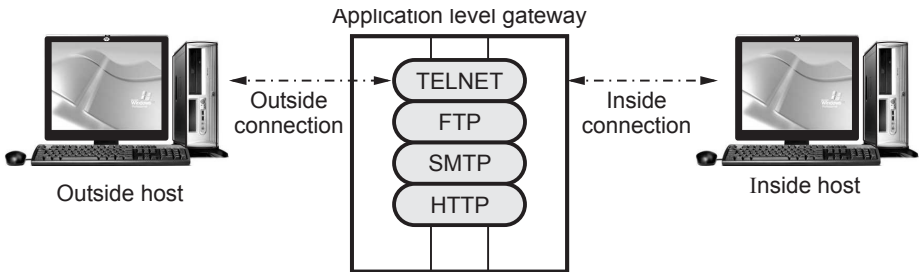


Fig. 5.5.3 Application gateway

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.

5.5.1.3 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.

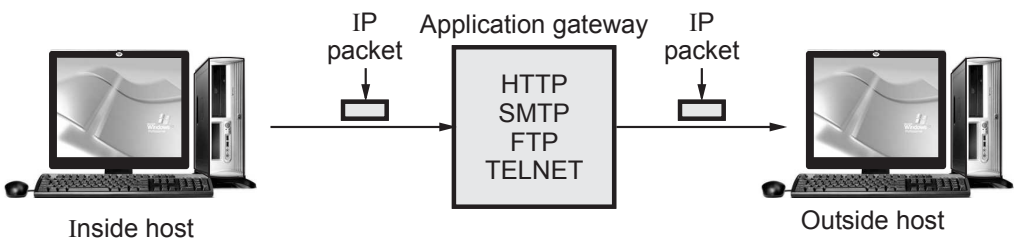


Fig. 5.5.4 Circuit gateway

5.5.1.4 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.

5.5.2 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.

1. DMZ Network (Demilitarized Zone)

- 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. 5.5.5 shows DMZ network.

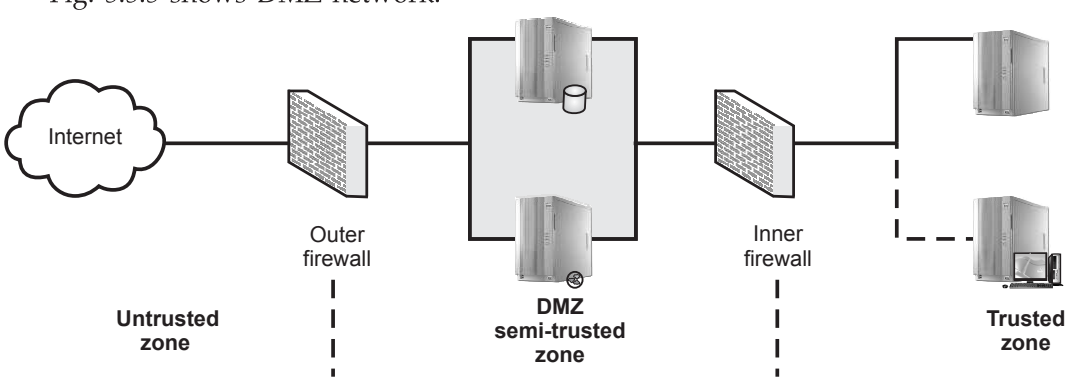


Fig. 5.5.5 DMZ network

- 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 DMZ, they won't gain access to internal network as traffic coming from the DMZ is filtered before being allowed into the internal network.

- To create a DMZ, user 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.
- 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.

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.

5.5.3 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. 5.5.6 shows screened host, single homed bastion host.

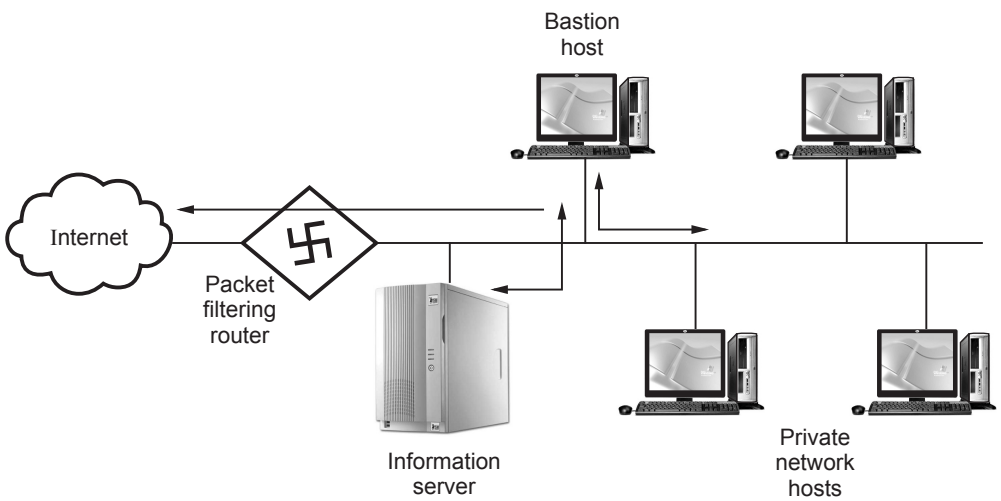


Fig. 5.5.6 Screened host, single homed bastion host

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

2. Screened host, dual homed bastion

- Fig. 5.5.7 shows dual homed bastion.

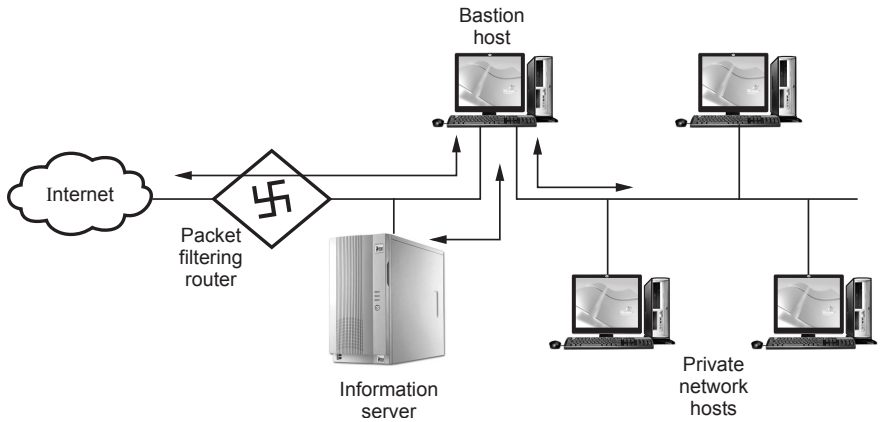


Fig. 5.5.7 Dual homed bastion

- 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. 5.5.8 shows screened subnet

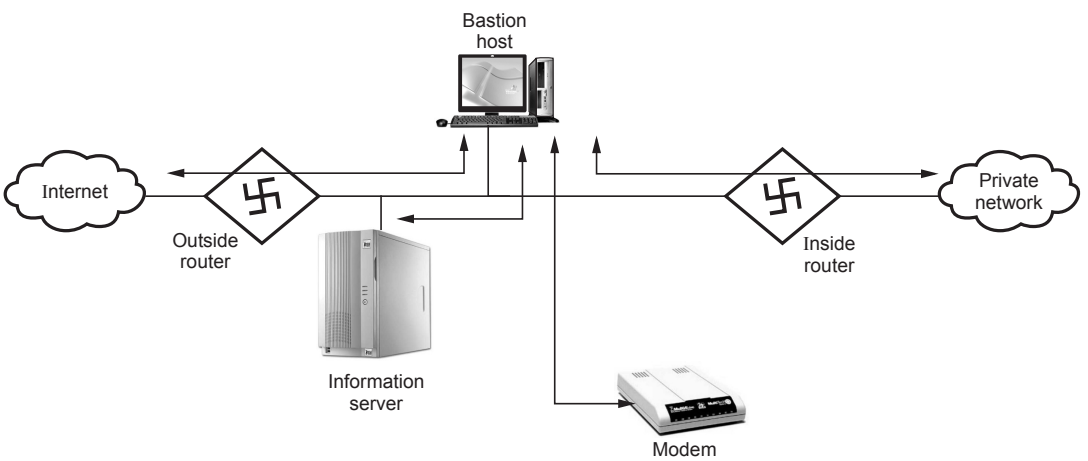


Fig. 5.5.8 Screened subnet

- 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.

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.

Review Questions

1. *What are the various types of firewall. Discuss limitations of firewall.*
   SPPU : May-19, Dec.-19, Marks 9
2. *Explain packet filtering firewall.* **SPPU : May-19, Marks 4**

5.6 Intrusion Prevention System

- Although IDS have been one of the cornerstones of network security, they have covered only one component of the total network security picture since they have been and they a passive component which only detects and reports without preventing.
- A promising new model of intrusion is developing and picking up momentum. It is the Intrusion Prevention System (IPS) which, is to prevent attacks. Like their counterparts the IDS, IPS fall into two categories : Network-based and host-based.
  1. Network-based Intrusion Prevention Systems (NIPSs)
- Because NIDSs are passively detecting intrusion into the network without preventing them from entering the networks, many organization in recent times have been bundling up IDS and firewalls to create a model that can detect and then prevent.
- The bundle works as follows.
  a. The IDS fronts the network with a firewall behind it. On the detection of an attack, the IDS then goes into the prevention mode by altering the firewall access control rules on the firewall. The action may result in the attack being blocked based on all the acces control regimes administered by the firewall.
  b. The IDS can also affect prevention through the TCP resets; TCP utilizes the RST (reset) bit in the TCP header for resetting a TCP connection, usually sent as a response request to a non-existent connection. But this kind of bundling is both expensive and complex, especially to an untrained security team. It suffers

from *latency* - the time it takes for the IDS to either modify the firewall rules or issue a TCP reset command. This period of time is critical in the success of an attack.

2. Host-based Intrusion Prevention Systems (HIPSs)
   a. Most HIPSs work by *sand-boxing,* a process of restricting the definition of acceptable behavior rules used on HIPSs. HIPS prevention occurs at the agent residing at the host. The agent intercepts system calls or system messages by utilizing dynamic linked libraries (dll) substitution.
   b. The substitution is accomplished by injecting existing system dlls with vendor stub dlls that perform the interception.

- Fig. 5.6.1 shows the placement of IDS and IPS.

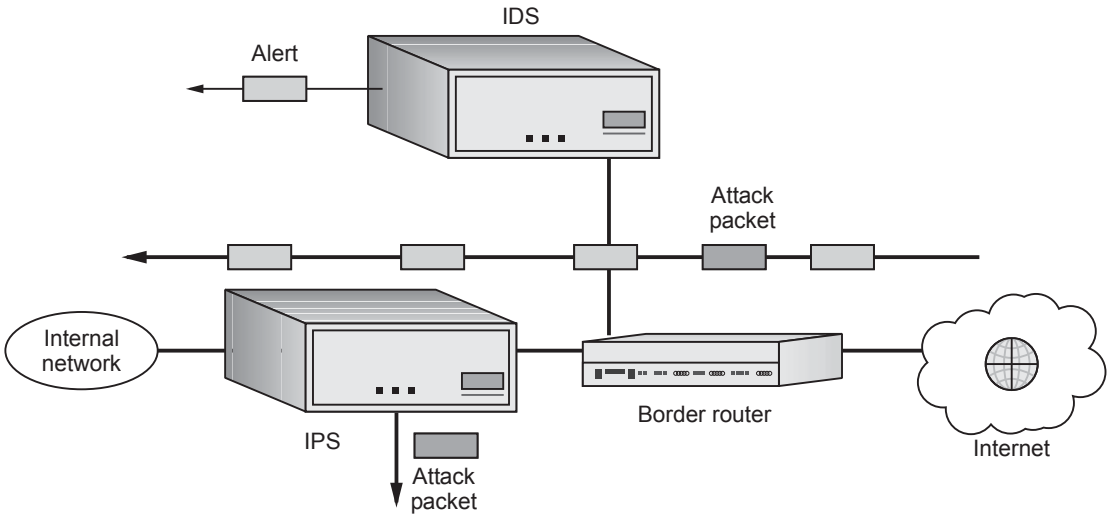


Fig. 5.6.1 IDS and IPS placement

- IDSs are slow and cannot be in-line with the packet stream. IPSs use ASICs for speed; can be in-line with the packet stream. Therefore can stop attacks.

5.7 Operating System Security

- Operating system security (OS 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. OS security encompasses all preventive-control techniques.
- OS hardening refers to the process of securing the operating systems of endpoint devices, such as computers or mobile phones, within network. In computing, an

operating system is a specific type of software that handles a device's basic functions, like enabling programs to launch and run.

- Tactics for performing OS hardening include installing or updating patches and reducing the number of people with the authorization to company's OS.
- Operating system hardening includes :
  a) Apply necessary updates and patches automatically
  b) Remove unnecessary files, libraries, drivers, and functionality
  c) Log all activity, errors, and warnings
  d) Limit sharing and system permissions
  e) Configure file system and registry permissions
- following basic steps that should be used to secure an operating system :
  1. Install and patch the operating system.
  2. Harden and configure the operating system to adequately address the identified security needs of the system by :
     a) Removing unnecessary services, applications and protocols.
     b) Configuring users, groups, and permissions.
     c) Configuring resource controls.
  3. Install and configure additional security controls, such as anti-virus, host based firewalls and intrusion detection systems (IDS), if needed.
  4. Test the security of the basic operating system to ensure that the steps taken adequately address its security needs.

5.7.1 Application Security

- Once the base operating system is installed and appropriately secured, the required services and applications must next be installed and configured.
- Each selected service or application must be installed and then patched to the most recent supported secure version appropriate for the system.
- Any application specific configuration is then performed. This may include creating and specifying appropriate data storage areas for the application and making appropriate changes to the application or service default configuration details.
- Encryption is a key enabling technology that may be used to secure data both in transit and when stored.

5.7.2 Security Maintenance

- Process of security maintenance includes the following steps :
  a. Monitoring and analyzing logging information
  b. Performing regular backups
  c. Recovering from security compromises
  d. Regularly testing system security
  e. Using appropriate software maintenance processes to patch and update all critical software, and to monitor and revise configuration as needed.

5.8 Multilevel Security

- When multiple categories or levels of data are defined, the requirement is referred to as multilevel security (MLS).
- A multilevel secure system for confidentiality must enforce the following :
  1. **No read up :** A subject can only read an object of less or equal security level. This is referred to in the literature as the simple security property.
  2. **No write down :** A subject can only write into an object of greater or equal security level. This is referred to in the literature as the *-property.
- In multilateral security, information is placed into compartments and may only flow between them in approved ways. It is an example of mandatory access control systems, where the system administrator sets the policy, in contrast to discretionary access control systems, where the owner of a data item is permitted to choose how access to that item is restricted.
- Multilateral security is concerned with the implementation of security between various actors (users, computer systems, processes) that might very well be on the same MLS clearance level.
- Simple hierarchy of security labels may not be flexible enough therefore Multilevel Security (MLS) enforces.
- Multilateral security enforces access control across by creating compartments. Multilateral security models the relationships of computer systems to each other with respect to security issues.
- The goals of multilateral security can be complex and very different from each other. Thus, multilateral security is sometimes referred to as "policy-based security".
- Bell-LaPadula is a form of multilevel security.

Bell-LaPadula Model (BLP) :

- The Bell-La Padula (BLP) model is a classic mandatory access-control model for protecting confidentiality. It was developed by David Elliott Bell and Leonard J. LaPadula.
- The BLP is a state machine model used for enforcing access control in government and military applications.
- The BLP model is derived from the military multilevel security paradigm, which has been traditionally used in military organizations for document classification and personnel clearance.
- The Bell-LaPadula model focuses on data confidentiality and controlled access to classified information.
- The BLP model has a strict, linear ordering on the security of levels of documents, so that each document has a specific security level in this ordering and each user is assigned a strict level of access that allows them to view all documents with the corresponding level of security or below.

5.9 Concepts of Trusted System

SPPU : May-19

- 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.

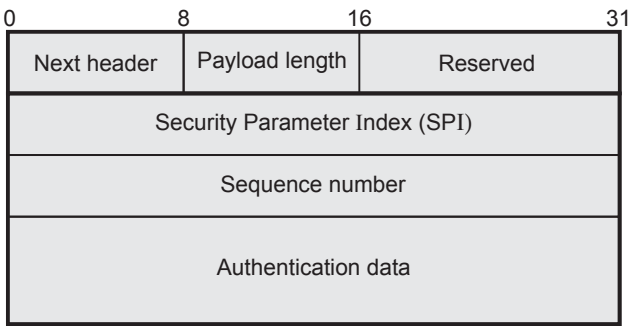


Fig. 5.9.1 IPSec authentication header format

- AH header format is shown in Fig. 5.9.1.
  1. **Next header** - This is 8-bits field and identifies the type of header that immediately follows the AH.
  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.

Review Question

1. *What is trusted system ?* **SPPU : May-19, Marks 4**

5.10 Trusted Computing

- Information security is increasingly important. Trusted Computing is a cluster of proposals and ideas for a locked-down PC architecture which can give guarantees about the application software it is running and which allows applications to communicate securely with other applications and with servers.
- A Trusted Computing Base (TCB) consists of all protection mechanisms within a computer system-including hardware, firmware, and software-that are responsible for enforcing a security policy.
- Hardware support of trusted computing enables hardware encryption keys, memory curtaining, secure execution and tamper resistance.

- TC-capable hardware must be manufactured with a public/private key pair, called the Endorsement Key (EK).
- The private key is held securely by the chip, and is never released. Ideally, the manufacturing process destroys all records of the private key. The chip is tamper-proof (it self-destructs rather than gives up its private key).
- Applications of trusted computing :
  1. Digital rights management
  2. Platform authentication
  3. Distributed firewalls
  4. Rate limitation for DDoS prevention
  5. Preventing cheating in multiplayer games
  6. Third-party computing
  7. Balancing security and privacy.

5.10.1 Software Reverse Engineering

- Software reverse engineering is a process of analysing software with a view to understanding its design and specification. The design and specification of a system may be reverse engineered so that they can be an input to the requirements specification process for the system's replacement.
- The design and specification may be reverse engineered to support program maintenance. Reverse engineering is the process of analyzing a subject system to create representations of the system at a higher level of abstraction.
- The four general reverse engineering objectives :
  1. Improve maintainability 2. Migration
  3. Improve reliability 4. Functional enhancement
- Fig. 5.10.1 shows distinction between forward and reverse engineering.

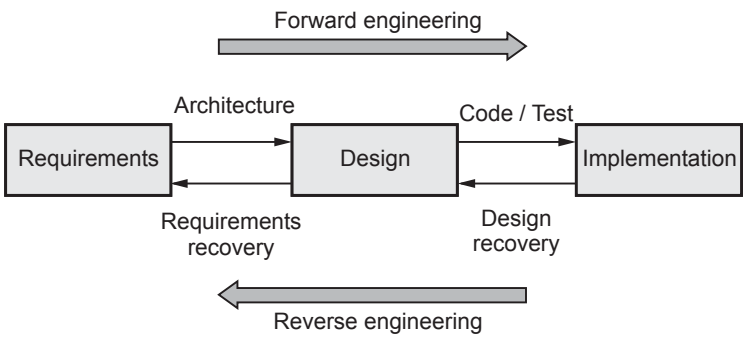


Fig. 5.10.1 Distinction between forward and reverse engineering

- Reverse engineering is beneficial in crime prevention, where suspected malware is reverse engineered to understand what it does and how to detect and remove it, and to allow computers and devices to work together ("interoperate") and to allow saved files on obsolete systems to be used in newer systems.
- Used harmfully, reverse engineering can be used to "crack" software and media to remove their copy protection, or to create a (possibly improved) copy or even a knockoff; this is usually the goal of a competitor.
- Advantages of reverse engineering
  1. Transforming obsolete products into useful ones by adapting them to new systems.
  2. Some features of the system needs to be refined out.
  3. It can be use, if there is no adequate documentation of the original design.
  4. Investigating and correcting errors and limitations in existing programs.
  5. Studying the design principles of a product as part of an education in engineering.
  6. Understanding how a product works.
  7. Malware analysis
  8. Vulnerability analysis
  9. Security assessment of 3rd-party COTS
  10. Evaluation/Breaking of copy-protection schemes
  11. To obtain the lost source code from executable code

5.10.2 Digital Rights Management

- Digital Rights Management (DRM) is "a combination of encryption and Internet validation for protecting vendor copyrights to prevent unauthorised copying of digital content (software, music, books, movies and so on)".
- Digital Rights Management is not security but security and DRM are made of the same blocks.
- Commercial organisations have invested heavily in preventing their work from being copied illegally and distributed over file-sharing mechanisms. This has given rise to many DRM technologies.
- DRM is defined as a broad range of technologies that grant control and protection to content providers over their own digital media. From the content's point of view, there are three key components to its life cycle : The creation of content, the distribution and upkeep of content and the use of content.

- A good DRM scheme should account for all three components, and effectively define the interactions between the user, the permissions and the content itself.
- Fig. 5.10.2 shows digital rights management system. This diagram shows that a rights management system oversees the identification and management of intellectual property items (content), rights assignments, rights transactions, licensing fees and usage monitoring (enforcement).

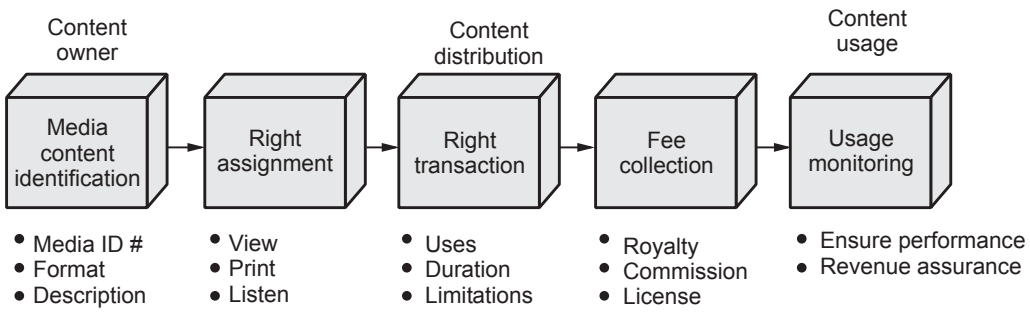


Fig. 5.10.2 Digital rights management system

- Rights management system oversees how content owners can provide access for content to users and how to convert and ensure the usage of content is converted into value for the content owner.
- A content owner is a person or company that owns the rights to intellectual property (content). Rights users can be a person, company or group that receives processes or takes some form of action on services or products.
- Rights may be transferred by the owner of the content or by an agent. A licensor is a company or person who authorizes specific uses or rights for the use of technology, products or services. An agent is a person or a device that performs tasks for the benefit of someone or some other device.

5.11 Multiple Choice Questions

Q.1 Network layer firewall works as a _____.

a frame filter b packet filter

c content filter d virus filter

Q.2 The Bell-La Padula model is a classic mandatory access-control model for protecting _____.

a integrity b availability

c confidentiality d all of these

Q.3 Application-level firewall, also called as _____.

a proxies
b gateways
c router
d distributed firewall

Q.4 What are the different ways to classify an IDS ?

a Anomaly detection
b Signature based misuse
c Stack based
d All of these

Q.5 What are the characteristics of anomaly-based IDS ?

a It models the normal usage of network as a noise characterization.
b It doesn't detect novel attacks.
c Anything distinct from the noise is not assumed to be intrusion activity.
d It detects based on signature.

Q.6 A SYN flood attack works by what mechanism ?

a Exploiting a packet processing glitch in Windows 95.
b Using an amplification network to flood a victim with packets.
c Exploiting the three-way handshake used by TCP/IP.
d Sending oversized ping packets to a victim.

Q.7 Which of the following is a fake network designed to tempt intruders with unpatched and unprotected security vulnerabilities and false data ?

a IDS
b Honey pot
c Padded cell
d Vulnerability scanner

Answer Keys for Multiple Choice Questions :

Q.1	b	**Q.2**	c	**Q.3**	a
Q.4	d	**Q.5**	a	**Q.6**	c
Q.7	b				

❑❑❑

Notes

UNIT VI

6 Cyber Security and Tools

Syllabus

Introduction, Cybercrime and Information Security, Classification of Cybercrimes, The legal perspectives-Indian perspective, Global perspective, Categories of Cybercrime, Social Engineering, Cyber stalking, Proxy servers and Anonymizers, Phishing, Password Cracking, Key-loggers and Spywares, The Indian IT Act-Challenges, Amendments, Challenges to Indian Law and Cybercrime Scenario in India, Indian IT Act.

Contents

6.1 Introduction

- Cyber safety is a common term used to describe a set of practices, measures and/or actions you can take to protect personal information and your computer from attacks.
- There is no standard definition for "**CYBER**". This word is used to describe the virtual world of computers e.g. an object in cyberspace refers to a block of data floating around a computer system or network.
- The word "cyberspace" is credited to William Gibson, who used it in his book, Neuromancer, written in 1984.
- Cyberspace : The impression of space and community formed by computers, computer networks, and their users ; the virtual "world" that Internet users inhabit when they are online.
- The term 'cyber' is derived from the word 'cybernetics' which means science of communication and control over machine and man.
- Cyberspace is the new horizon which is controlled by machine for information and communication between human beings across the world.
- Therefore, crimes committed in cyberspace are to be treated as cyber crimes. In wider sense, cyber crime is a crime on the Internet which includes hacking, terrorism, fraud, gambling, cyber stalking, cyber theft, cyber pornography, flowing of viruses etc.
- Over the past few years, the global cyber crime landscape has changed dramatically, with criminals employing more sophisticated technology and greater knowledge of cyber security.
- Until recently, malware, spam emails, hacking into corporate sites and other attacks of this nature were mostly the work of computer 'geniuses' showcasing their talent.
- Cyber criminals are now moving beyond computers, and attacking mobile handheld devices, such as smart phones and tablet personal computers. In 2010, the number of malicious software programs specifically targeting mobile devices, rose 46 %, according to information technology security group McAfee.
- **Cybercrime** is defined as crimes committed on the internet using the computer as either a tool or a targeted victim.
- **Cybercrime** is defined as a crime in which a computer is the object of the crime (hacking, phishing, spamming) or is used as a tool to commit an offense (child pornography, hate crimes).

- Any criminal activity that uses a computer either as an instrumentality, target or a means for perpetuating further crimes comes within the ambit of cyber crime.

6.1.1 Cybersqatting

- Cybersquatting is registering, selling or using a domain name with the intent of profiting from the goodwill of someone else's trademark. It generally refers to the practice of buying up domain names that use the names of existing businesses with the intent to sell the names for a profit to those businesses
- Internet Corporation for Assigned Names and Numbers (ICANN) coordinates assignment of domain names by various entities, which generally allocate domain names on a first-come, first-served basis for a modest fee.
- A cybersquatter takes advantage of the domain registration companies' 'first come, first served' policy by submitting a large list of very popular words and names all at once.
- While the domain registration company is in the process of entering these names, the cybersquatter uses profits from individual domain resales to finance the required registration fees.
- A cybersquatter can literally sit on a popular domain name for years, causing grief to the actual celebrity or company it represents.
- As the internet started becoming popular, internet users knew businesses would need a website. Some users started buying domains to create sites that looked like they were from reputable companies.
- Example : A cybersquatter could buy Heinz.com if the company hadn't created a website yet, looking to sell the domain to Heinz at a later date for profit, or use the domain name to attract traffic and generate money through advertising.
- If a business has a good reputation but no website, the company either pays the owner of the domain name to transfer the domain or contacts a trademark attorney to start a lawsuit.
- The second way is time- and cost-intensive, so trying to buy the domain directly from the cybersquatter is usually the preferred method.
- Today, opportunities for cybersquatters aren't as common since most businesses make the purchasing of their domain a high priority, especially if they have a strong trademark.
- Cybersquatting is considered to be an "Intellectual Property Right".

6.1.2 Cyber Terrorism

- **Cyber terrorism** is the premeditated, politically motivated attack against information, computer systems, computer programs, and data which result in violence against noncombatant targets by sub national groups or clandestine agents.

What is Terrorism ?

- Most governments in the world cannot agree on one single definition for terrorism. The ambiguity in the definition brings indistinctness in action; as the old maxim goes "one man's terrorist is another man's freedom fighter".
- The US FBI defines terrorism as "The unlawful use of force or violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives."
- The US Department of State defines terrorism as "premeditated politically-motivated violence perpetrated against non-combatant targets by sub-national groups or clandestine agents".
- It is interesting to note that some definitions of terrorism also include targets to computer systems and its services.
- The traditional terrorism and cyber terrorism share the same attributes. One approach of understanding cyber terrorism is by breaking it down to its fundamental elements. The above definitions suggest that there are at least five elements which must be satisfied to construe **cyber terrorism :**
  1. Politically motivated attacks that lead to death or bodily injury;
  2. Cause fear and/or physical harm through attack techniques
  3. Serious attacks against critical information infrastructures such as financial, energy, transportation and government operations;
  4. Attacks that disrupt non-essential services are not considered as terrorism; and.
  5. Attacks that are not primarily focused on monetary gain.
- At the moment, there has been no known publicly reported incident of actual cyber terrorism. Most reported cases are related to cyber threats and the use of the Internet as a tool by terrorists.

Internet as an Ideal Tool for Terrorists

- Several works on cyber terrorism and the Internet have been conducted by researchers including experiments on cyber terrorism activities on major websites and blogs such as YouTube and Second Life.

- The researchers also studied popular hosting service providers such as blogspot.com and wordpress.com. Their findings indicate that :
  1. There have been several cases reported in the media where the Internet has helped terrorists in their activities.
  2. The virtual world is indeed used to promote terrorism activities. Some of the videos published on the Net are related to explosives, attacks, bombing and hostage - taking.
  3. Some terrorist groups use the Internet for the purpose of inter - group communication and inter-networked grouping.
  4. The Internet is used to release manifestos and propaganda statements.
  5. Aside from generating propaganda, the Net is also used to coordinate missions or call meetings and to recruit new members.

Cyber Terrorism in India

- Targeted attacks on military installations, power plants, air traffic control, banks, trail traffic control, telecommunication networks are the most likely targets. Others like police, medical, fire and rescue systems etc.
- Cyber terrorism is an attractive option for modern terrorists for several reasons.
  1. It is cheaper than traditional terrorist methods.
  2. terrorism is more anonymous than traditional terrorist methods.
  3. The variety and number of targets are enormous.
  4. terrorism can be conducted remotely, a feature that is especially appealing to terrorists.
  5. terrorism has the potential to affect directly a larger number of people.

6.1.3 Cybercrime against Property

- Cybercrimes against all forms of property include unauthorized computer trespassing through cyberspace, computer vandalism, transmission of harmful programs, and unauthorized possession of computerized information.
- Property crime is a category of crime that includes, among other crimes, burglary, larceny, theft, motor vehicle theft, arson, shoplifting, and vandalism. Property crime involves the taking of property, and does not involve force or threat of force against a victim.
- Intellectual Property Crimes : Intellectual property consists of a bunch of rights. Any unlawful act by which the owner is deprived completely or partially of his rights is an crime. The most common type of IPR violation may be said to be

software piracy, infringement of copyright, trademark, patents, designs and service mark violation, theft of computer source code, etc.

- The property transaction scams come against a backdrop of instances of con artists pretending to be solicitors, using either fake names or stealing the identities of genuine firms.
- THEFT : A person commits an offense if he unlawfully appropriates property with intent to deprive the owner of property.
- Cybercrime is nothing but where the computer used as an object or subject of crime. Cybercrime is an evil having its origin in the growing dependence on computers in modern life.
- In a day and age when everything from microwave ovens and refrigerators to nuclear power plants are being run on computers. Crime committed using a computer and the internet to steal a person's identity or illegal imports or malicious programs.
- Whoever intentionally Causes damage to any physical property of another without the person's consent is guilty of a Class A misdemeanor.
- Whoever intentionally causes damage to, intentionally marks, draws or writes with ink or another substance on or intentionally etches into any physical property of another, with-out the person' s consent and with knowledge of the character of the property, is guilty of a Class I felony if the property consists of one or more of the following :
  1. Any church, synagogue or other building, structure or place primarily used for religious worship or another religious purpose.
  2. Any cemetery, mortuary or other facility used for burial or memorializing the dead.
- When the individual is the main target of Cybercrime, the computer can be considered as the tool rather than the target. These crimes generally involve less technical expertise as the damage done manifests itself in the real world.
- The ingenuity of cyber criminals is becoming obvious when we look at the clever ways in which online frauds are being perpetrated.
- Phishing, a particularly crafty fraud attack perpetrated by cyber criminals combines elements of forgery, misrepresentation and misplaced trust to obtain sensitive personal data like PIN numbers, credit card details and passwords of victims. The attackers then rob the victim's money by using such personal information.

6.2 Cybercrime and Information Security

- 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.

6.2.1 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.

6.2.2 Information Security Life Cycles

- Fig. 6.2.1 shows information security life cycle.
- Security in development and support processes is an essential part of a comprehensive quality assurance and production control process and usually involves training and continuous oversight by the most experienced staff.
- Rules for system and software development should be developed .
- These rules should incorporate secure software development techniques such as user authentication, session control, logging, and data validation and sanitization.

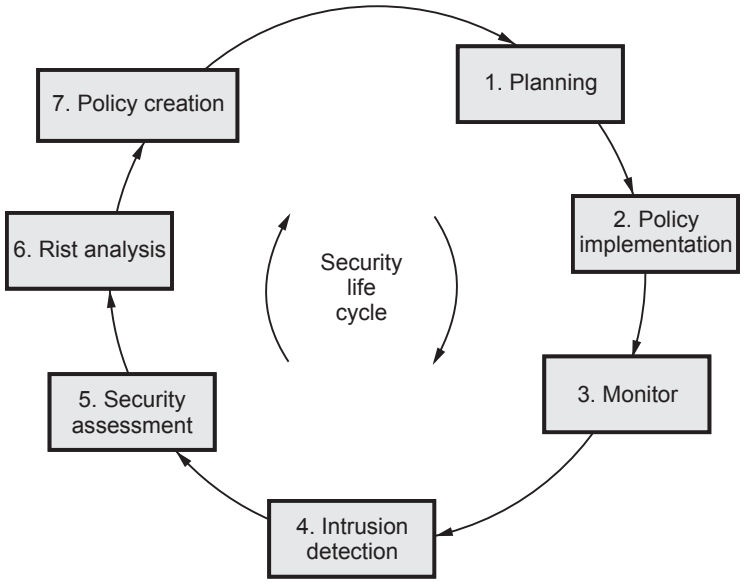


Fig. 6.2.1 Security life cycle

- Security life cycle involves following phases :
  1. Planning
  2. Policy implementation
  3. Monitoring
  4. Intrusion detection
  5. Security assessment
  6. Risk analysis
  7. Security policy creation.

Security categorization standards help organizations make the appropriate selection of security controls for their information systems.

Security planning ensures that user fully document any agreed upon security controls, whether they are just planned or in place.

The security plan also provides a complete characterization or description of the information system and attachments of or references to key documents that support the information security program of the agency.

6.2.3 Botnets

- A botnet is an interconnected network of computers infected with malware without the user's knowledge and controlled by cybercriminals.

- They're typically used to send spam emails, transmit viruses and engage in other acts of cybercrime. Sometimes known as a zombie army, botnets are often considered one of the biggest online threats today.
- Computers in a botnet, called nodes or zombies, are often ordinary computers sitting on desktops in homes and offices around the world.
- Typically, computers become nodes in a botnet when attackers illicitly install malware that secretly connects the computers to the botnet and they perform tasks such as sending spam, hosting or distributing malware or other illegal files, or attacking other computers.
- Fig. 6.2.2 shows botnet.
- Attackers usually install bots by exploiting vulnerabilities in software or by using social engineering tactics to trick users into installing the malware. Users are often unaware that their computers are being used for malicious purposes.

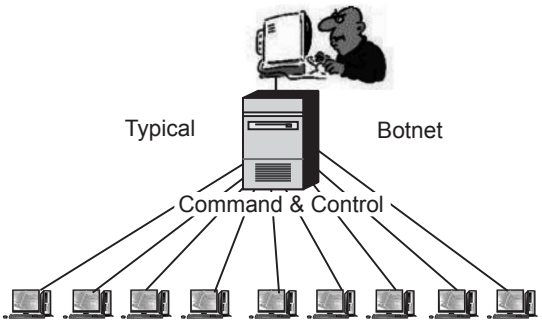


Fig. 6.2.2 Botnet

- The word Botnet is formed from the words 'robot' and 'network'. Cybercriminals use special Trojan viruses to breach the security of several users' computers, take control of each computer, and organize all of the infected machines into a network of 'bots' that the criminal can remotely manage.
- A zombie or bot is often created through an Internet port that has been left open and through which a small Trojan horse program can be left for future activation. At a certain time, the zombie army "controller" can unleash the effects of the army by sending a single command, possibly from an Internet Relay Channel (IRC) site.
- Botnets can be used to :
  1. Send out spam emails
  2. Launch a Distributed Denial of Service Attack
  3. Commit advertising fraud
  4. Distribute malware, or spyware
- Keep phishing websites active and frequently change their domains to remain anonymous and undetected by law enforcement.

6.2.4 Zombie

- Zombie computer is a computer connected to the Internet that has been compromised and controlled by an attacker without user's consent.
- Zombie network (Botnet) refers to a network of zombie computers under the remote control by an attacker. Attackers control their botnets through some command and control centers to perform illegal activities.
- If your computer is infected by malicious code such as Trojan Horse, your computer may be controlled by an attacker and may become a zombie.
- Types of attacks perpetrated by a zombie network include denial of service attacks, adware, spyware, spam and click fraud.
- The following steps are used to create zombie networks :
  1. A zombie network operator uses a bot to infect thousands of computers with worms or viruses that carry a deadly payload.
  2. The bot inside an infected computer logs on to an online server - usually IRC but sometimes Web.
  3. The zombie network operator leases zombie network services to a customer.
  4. The customer provides the zombie network operator with spam or any other material, which is run through the zombie network.
- Another botnet called, Gameover Zeus Botnet, allows cyber criminals to retrieve banking passwords from infected machines, or use the botnet to infect more computers.

How and Why Do Cyber Criminals Use Botnets ?

- The value of bots and botnets to criminals comes from aggregating massive numbers of computers they can control simultaneously to perform malicious activities.
- Cyber criminals may use the botnets to send spam, phishing emails, or other scams to trick consumers into giving up their financial information.
- Cyber criminals may also collect information from the bot-infected machines and use it to steal identities, incurring loans, and purchase charges under the user's name.
- Cyber criminals may use botnets to create Denial - of - Service (DoS) attacks that flood a legitimate service or network with a crushing volume of traffic. The volume may severely slow down, or even shut down, the organization's business operations.
- Revenue from DoS attacks come through extortion and leasing botnets. The criminals will rent botnets to groups interested in inflicting damage to another entity.

- The "renters" will use the botnet for sending spam and phishing emails or attacking legitimate websites and networks.

6.3 Classification of Cybercrimes

1. Cyber pornography

- Pornography on the internet may take various forms. It may include hosting of website containing some obscene or prohibited material or use of computer for producing obscene materials. Such material tends to pervert the thinking of adolescents and corrupt their mind set.
- A person who publishes or transmits or causes to be published in the electronic form any material which is lascivious, or if its effects in such as to tend to deprave or corrupt the persons who are likely to see, wad or hear the matter contained or embodied in it, is liable to punishment.
- The important ingredients of such an offence are publication and transmission through any electronic medium, of pornographic material in any electronic form.
- Cyber pornography is in simple words defined as the act of using cyberspace to create, display, distribute, import, or publish pornography or obscene materials. With the advent of cyberspace, traditional pornographic content has now been largely replaced by online/digital pornographic content.
- Pornography has no legal or consistent definition. The definition of pornography depends how the society, norms and their values are reacting to the pornographic content.

2. Email spoofing

- A hacker logging in to a computer of under was to his victim often will login under a different identity. This is called spoofing. The hacker able to the by, having previously actual password or having created a new identity by fooling the computer into thinking he is the system's operator.
- A spoofed a may email may be said to be one which the be miss represent its origin. That is, it shows its online to be different from which it actually originates.
- For example, where A sends a threatening a email to the president of the students a union threatening to detente a nuclear sent from the college compos and this email was sent from the account of some other student "A" would a be quality of email spoofing.

3. Identity theft

- Identity theft and fraud is one of the most common types of cybercrime. The term Identity Theft is used, when a person purports to be some other person, with a view to creating a fraud for financial gains.

- When this is done online on the Internet, its is called **online identity theft**.
- The most common source to steal identity information of others, are data breaches affecting government or federal websites.
- It can be data breaches of private websites too, that contain important information such as, credit card information, address, email ID's, etc.

4. Data diddling

- This offence involves changing or reusing of data in sub till of ways which makes of it different to put the data subtitle ways which data back of or be curtain of its accuracy.
- This is resorted to for the purpose of illegal monetary gains or for community of fraud of financial scam. In case of scan the criminal are change of data which is related on the scan.
- In this data are changed of computer system, record are destroy of and alterations of information of and other type of frauds.

5. Email bombing

- This is another form of internet misuse where individuals directs amass numbers of mail to the victim or an address in attempt to overflow the mailbox, which may be an individual or a company or even mail servers there by ultimately resulting into crashing. There are two methods of perpetrating an email bomb which include mass mailing and list linking.

6. Internet time thefts

- This form is kinds of embezzlements where the fraudulent uses the Internet surfing hours of the victim as their own which can be complete by obtaining access to the login ID and the password, an example is Colonel Bajwa's case- in this incident the Internet hours were used up by a unauthorized person.

7. Salami attacks

- This kind of crime is normally consisting of a number of smaller data security attacks together end resulting in one major attack.
- This method normally takes place in the financial institutions or for the purpose of committing financial crimes. An important feature of this type of offence is that the alteration is so small that it would normally go unnoticed.
- This form of cybercrime is very common in banks where employees can steal small amount and it's very difficult to detect or trace.

8. Web jacking

- This is where the hacker obtains access and can control web site of another person, where he or she can destroy or alter the information on the site as they

see fit to them. This type of method of cybercrime is done for satisfying political agendas or for purely monetary means.

9. Hacking

- In other words can be referred to as the unauthorized access to any computer systems or network. This method can occur if computer hardware and software has any weaknesses which can be infiltrated if such hardware or software has a lack in patching, security control, configuration or poor password choice.

10. Software piracy

Software piracy is the illegal copying, distribution, or use of software. It is such a profitable "business" that it has caught the attention of organized crime groups in a number of countries.

- Piracy includes casual copying of particular software by an individual or business.
- Using pirated software is also risky for users. Aside from the legal consequences of using pirated software, users of pirated software forfeit some practical benefits as well. Those who use pirate software :
  a) Increase the chances that the software will not function correctly or will fail completely;
  b) Forfeit access to customer support, upgrades, technical documentation, training, and bug fixes;
  c) Have no warranty to protect themselves;
  d) Increase their risk of exposure to a debilitating virus that can destroy valuable data;
  e) May find that the software is actually an outdated version, a beta (test) version, or a nonfunctioning copy;
  f) Are subject to significant fines for copyright infringement; and
  g) Risk potential negative publicity and public and private embarrassment.
- The software licensure agreement is a contract between the software user and the software developer. Usually, this agreement has certain terms and conditions the software user must follow.
- When the user doesn't follow the rules and regulations, they are guilty of software piracy. Some of these terms and conditions prohibit :
  1. Using multiple copies of a single software package on several computers
  2. Passing out copies of software to others without the proper documentation
  3. Downloading or uploading pieces of software via bulletin boards for others to copy
  4. Downloading and installing shareware without paying for it.

- Examples of documents that support the information security program include a configuration management plan, a contingency plan, an incident response plan, a security awareness and training plan, rules of behavior, a risk assessment, a security test and evaluation results, system interconnection agreements, security authorizations and accreditations, and a plan of action and milestones.
- This step provides the necessary security authorization of an information system to process, store, or transmit information that is required.
- This authorization is granted by a senior organization official and is based on the verified effectiveness of security controls to some agreed upon level of assurance and an identified residual risk to agency assets or operations.
- **Monitoring** ensures that controls continue to be effective in their application through periodic testing and evaluation.
- Security control monitoring, such as verifying the continued effectiveness of those controls over time, and reporting the security status of the information system to appropriate agency officials are essential activities of a comprehensive information security program.
- Assessment may be internal or external. The internal assessment is a controlled network attack simulation that is used to gauge the exposure present on internal systems, applications, and network devices.
- The assessment provides a more structured approach to identifying vulnerabilities that may go undetected.
- The goal of an external assessment is to quantify the security risk that is associated with Internet - connected systems.
- Preliminary risk assessment : This step results in an initial description of the security needs of the system. A preliminary risk assessment should define the threat environment in which the system will operate.

6.4 The Legal Perspectives - Indian Perspective

SPPU : Dec.-19

- The Indian government has created the necessary legal and administrative framework through the enactment of Information Technology Act 2000, which combines the e-commerce transactions and computer misuse and frauds rolled into an Omnibus Act.
- While on the one hand it seeks to create the Public Key Infrastructure for electronic authentication through the digital signatures, on the other hand, it seeks to build confidence among the public that the frauds in the cyber space will not go unpunished.

- The Controller of Certifying Authority (CCA) has been put in place for the effective implementation of the IT Act, 2000.
- The Act also enables e-governance applications for the electronic delivery of services to the public, business and government.
- The Information technology Act, 2000 has been enacted by the legislators with the prime intention of ensuring that the communication through electronic medium is facilitated and all sorts of ambiguity regarding the authenticity of the communication is fixed for once and all.

6.4.1 Indian IT Act

- In May 2000, both the houses of the Indian Parliament passed the Information Technology Bill. The Bill received the assent of the President in August 2000 and came to be known as the Information Technology Act, 2000. Cyber laws are contained in the IT Act, 2000.
- This Act aims to provide the legal infrastructure for e-commerce in India. And the cyber laws have a major impact for e-businesses and the new economy in India. So, it is important to understand the various perspectives of the IT Act, 2000 and what it offers.
- The Information Technology Act, 2000 also aims to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as "electronic commerce", which involve the use of alternatives to paper-based methods of communication and storage of information, to facilitate electronic filing of documents with the Government agencies and further to amend the Indian Penal Code, the Indian Evidence Act, 1872, the Bankers' Books Evidence Act, 1891 and the Reserve Bank of India Act, 1934 and for matters connected therewith or incidental thereto.
- Some highlights of the Act are listed below :
  a. Chapter-II of the Act specifically stipulates that any subscriber may authenticate an electronic record by affixing his digital signature. It further states that any person can verify an electronic record by use of a public key of the subscriber.
  b. Chapter-III of the Act details about Electronic Governance and provides inter alia amongst others that where any law provides that information or any other matter shall be in writing or in the typewritten or printed form, then, notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied if such information or matter is -
  - Rendered or made available in an electronic form; and
  - Accessible so as to be usable for a subsequent reference.

The said chapter also details the legal recognition of Digital Signatures.

c. Chapter-IV of the said Act gives a scheme for Regulation of Certifying Authorities. The Act envisages a Controller of Certifying Authorities who shall perform the function of exercising supervision over the activities of the Certifying Authorities as also laying down standards and conditions governing the Certifying Authorities as also specifying the various forms and content of Digital Signature Certificates. The Act recognizes the need for recognizing foreign Certifying Authorities and it further details the various provisions for the issue of license to issue Digital Signature Certificates.

d. Chapter-VII of the Act details about the scheme of things relating to Digital Signature Certificates. The duties of subscribers are also enshrined in the said Act.

e. Chapter-IX of the said Act talks about penalties and adjudication for various offences. The penalties for damage to computer, computer systems etc. has been fixed as damages by way of compensation not exceeding ₹ 1,00,00,000 to affected persons. The Act talks of appointment of any officers not below the rank of a Director to the Government of India or an equivalent officer of state government as an Adjudicating Officer who shall adjudicate whether any person has made a contravention of any of the provisions of the said Act or rules framed there under. The said Adjudicating Officer has been given the powers of a Civil Court.

f. Chapter-X of the Act talks of the establishment of the Cyber Regulations Appellate Tribunal, which shall be an appellate body where appeals against the orders passed by the Adjudicating Officers, shall be preferred.

g. Chapter-XI of the Act talks about various offences and the said offences shall be investigated only by a Police Officer not below the rank of the Deputy Superintendent of Police. These offences include tampering with computer source documents, publishing of information, which is obscene in electronic form and hacking.

The Act also provides for the constitution of the Cyber Regulations Advisory Committee, which shall advice the government as regards any rules, or for any other purpose connected with the said act.

The said Act also proposes to amend the Indian Penal Code, 1860, the Indian Evidence Act, 1872, The Bankers' Books Evidence Act, 1891, The Reserve Bank of India Act, 1934 to make them in tune with the provisions of the IT Act.

6.4.2 Cyber Laws and Crimes as per the Indian IT Act

- 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.

6.4.3 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.

6.4.4 A Global Perspective on Cybercrimes

- The rapid development of Internet and Computer technology globally has led to the growth of new forms of transnational crime especially Internet related.
- These crimes have virtually no boundaries and may affect any country across the globe.
- Thus, there is a need for awareness and performing of necessary legislation in all countries for the prevention of computer related crime.
- Globally Internet and Computer based commerce and communications cut across territorial boundaries, thereby creating a new realm of human activity and undermining the feasibility and legitimacy of applying laws based on geographic boundaries.
- This new boundary, which is made up of the screens and passwords, separate the "Cyber world" from the "real world" of atoms. Territorially based law- making and law-enforcing authorities find this new environment deeply threatening.

Review Question

1. *Write note on information protection law : Indian perspective.* **SPPU : Dec.-19, Marks 8**

6.5 Categories of Cybercrime

- Cybercrime can be categorized based on the following :
  1. Target of the crime
  2. Whether the crime occurs as a single events or as a series of events
- Three major categories of Cybercrime :
  1. Cybercrimes against a person
  2. Cybercrimes against property
  3. Cybercrimes against the government/organization.

Cybercrimes against a person :

Categories	Remarks
Cybercrimes against a person	• Trafficking of obscene material. • Cyber harassment • Violation of privacy of online citizens • Identity theft (Phishing and Pharming) • Cyberbullying
Cybercrime against property	• All forms of property • Computer vandalism • Transmission of harmful programs • Theft of material on a computer
Cybercrime against the government/organization	• Cyber terrorism is one of the distinct crime against government/organization • Attacker use computer tool and Internet

6.6 Social Engineering

- Social engineering is nothing new in the digital age, of course, but security experts say criminals are using it more as companies have gotten better at securing their networks.
- Social networks are the second most widely used technique is social engineering. Tricking users into collaborating to infect their computers and steal their data is an easy task, as there are no security applications to protect users from themselves.
- In this context, use of social networks (Facebook, Twitter, etc.), places where hundreds of millions of users exchange information (very often personal data), makes them the preferred hunting ground for susceptible users.

- Social engineering is the art of manipulating people so they give up confidential information.
- The types of information these criminals are seeking can vary, but when individuals are targeted the criminals are usually trying to trick user into giving them user passwords or bank information, or access user computer to secretly install malicious software that will give them access to passwords and bank information as well as giving them control over user computer.
- Criminals use social engineering tactics because it is usually easier to exploit natural inclination to trust than it is to discover ways to hack software.
- For example, it is much easier to fool someone into giving their password than it is for user to try hacking their password.

Common Types of Attacks

- Most users today get updates from social networking websites such as Facebook, Twitter and LinkedIn. These updates arrive on an almost daily basis and are reviewed by many users.
- All these social networking sites include multiple links in their emails, and it's very common for users to click on these links.
- We all know that fraudsters actively use fake messages from social networking websites in order to install malware on victims' computers.
- As a security best practice, users are told that if something calls for immediate action or looks uncommon, too good to be true or unlikely, it is most likely an attack.
- For example, phishing emails that encourage users to click on a link in order to unlock their bank account meet most of these criteria. It is unlikely for a bank to contact customers this way, and it calls for immediate action.
- Similarly, an email from tax authorities on a pending refund is probably too good to be true and such information would likely not be conveyed via email.
- **Response to a question you never had.** Criminals may pretend to be responding to your 'request for help' from a company while also offering more help. They pick companies that millions of people use like a software company or bank. If you don't use the product or service, you will ignore the email, phone call, or message, but if you do happen to use the service, there is a good chance you will respond because you probably do want help with a problem.
- **The message may notify you that you are a 'winner'.** Maybe the email claims to be from a lottery, or a dead relative, or the millionth person to click on their site, etc. In order to give you your 'winnings' you have to provide information about your bank routing so they know how to send it to you, or give your address and

phone number so they can send the prize, and user may also be asked to prove who are often including user Aadhar card number and PAN number. These are the 'greed phishes' where even if the story pretext is thin, people want what is offered and fall for it by giving away their information, then having their bank account emptied, and identity stolen.

6.7 Cyber Stalking

SPPU : May-19, Dec.-19

Definition of stalking : *Threatening behavior or unwanted advances directed at another using the Internet and other forms of online and computer communications.*

- Cyber stalking is defined as the repeated use of the Internet, e-mail, or related digital electronic communication devices to annoy, alarm, or threaten a specific individual or group of individuals.
- Stories of criminal intimidation, harassment, fear, and suggestive violence where individuals use the Internet as a tool to stalk another person.
- Stalkers use victim information like mobile numbers, telephone numbers, addresses, and personal preferences to impinge upon their normal life. Some time cyber stalkers can learn what sorts of things upset their victims and can use this knowledge to harass the victims further.
- Stalkers target victims through chat rooms, WhatsApp, Hangouts, e-mail, facebook etc.
- Different forms of cyber stalking : Threatening e-mails, spam, and online verbal abuse, inappropriate messages on message boards, computer viruses, tracing internet activity, and identity theft.
- Effects of cyber stalking on person :
  1. Changes in sleeping and eating patterns
  2. Nightmares
  3. Hyper vigilance
  4. Anxiety
  5. Helplessness
  6. Fear for safety
  7. Shock and disbelief.
- Cyber stalking damages multiple aspects of victims' lives, from study to professional activity to their relationships with others. Survey respondents reported changing or losing jobs, isolating themselves by giving up social activities, and having important relationships break up.

- The Delhi police registered India's first case of cyber stalking. A case was registered under section 509 of the Indian Penal Code. One Mrs. Neha (Name changed) complained to the police against a person who was using her identity to chat over the Internet. She also complained that the person was chatting on the Net, using her name and giving her address and was talking obscene language. The same person was giving her telephone number to other chatters encouraging them to call her at odd hours.
- Stalkers usually make harassing phone calls, leave written messages or objects, or vandalize a person's property. Cyber stalkers meet or target their victims by using different search engines, bulletin and discussion boards, and online forums.
- Cyber stalkers use different social network sites and self publishing media such as Facebook, Twitter, Friendster, Bebo, Myspace and Indymedia etc. They try to damage the reputation of their victims by posting false information on websites, blogs or user pages. Many cyber stalkers use third parties to encourage them to join in their pursuit.
- They may order pornographic materials and sex toys, having them sent to their victim's address. Some cyber stalkers may arrange to meet their victims, especially young people who are at high risk of becoming their victims.
- Most stalking behavior is not a crime, at least not by itself. Calling someone over and over, texting numerous messages and leaving gifts are common behaviors that, on their own, do not constitute a crime.
- Section 354D says that anyone who monitors an individual's electronic communication and causes fear or distress is guilty of stalking, just as they are if they follow or attempt to contact them in the real world. The offender could get a fine and three years in jail.
- India is finally waking up to cyber stalking with the Criminal Law (Amendment) Bill, 2013, saying that stalking includes monitoring of a person's use of internet, email and electronic communication.
- Section 66A of the IT Act deals with cyber stalking. "A person who repeatedly sends emails can be booked under 66A, but not many know this,"
- Two different kinds of cyber stalking situations which can occur.
  1. Online harassment and cyber stalking that occurs and continues on the internet.
  2. Online harassment and stalking that begins to be carried on offline too. This is when a stalker may attempt to trace a telephone number or a street address. Always be careful what details you give out over the web and to whom.

- The increasing use of the Internet and the ease with which it allows others unusual access to personal information, have made this form of stalking ever more accessible. Potential stalkers may find it easier to stalk via a remote device such as the Internet rather than to confront an actual person. You cannot stop the contact with a request. In fact, the more you protest or respond, the more rewarded the cyber stalker feels. The best response to cyber stalking is not to respond to the contact.

6.7.1 Motivates of Cyber Stalker

1. **Sexual harassment :** Sexual harassment is also a very common experience offline. The internet reflects real life and consists of real people. It's not a separate, regulated or sanctified world. A common form of sexual harassment on the Internet occurs when a harasser sends unwanted, abusive, threatening, or obscene messages to a victim via e-mail or instant messaging.
2. **Obsession for love :** This category is characterized by stalkers who develop a love obsession or fixation on another person with whom they have no personal relationship. It could also be an online romance that moves to real life, only to break-up once the persons really meet.
3. **Ego and power trips :** stalkers online showing off their skills to themselves and their friends. They do not have any grudge against you - they are rather using you to 'show-off' their power to their friends or doing it just for fun and you have been unlucky enough to have been chosen.

- Some other forms of cyber stalking are listed below :
  1. Sending inappropriate electronic greeting cards.
  2. Sending viruses.
  3. Sending harassing messages to the victim's.
  4. Hacking into the victim's computer.
  5. Posting personal advertisements in the victim's name.

6.7.2 Types of Stalkers

- There are three main types of stalkers :
  1. Simple obsessional
  2. Delusional
  3. Vengeful.

Simple obsessional stalkers or domestic

- This is the most common type of stalker.

- Stalker, usually male, knows victim as an ex-spouse, ex-lover, or former boss, who they attempt to establish a relationship with and when rebuffed begin a campaign of harassment.
- This category represents 70 - 80 % of all stalking cases and is distinguished by the fact that some previous personal or romantic relationship existed between the stalker and the victim before the stalking behavior began.
- This kind of stalker may or may not have psychological disorders, all clearly have personality disorders. They refuse to believe that the relationship is over despite being told several times. They may have a history of other criminal behaviors.
- The love - obsessional stalker, who is typically a psychotic stalker targeting famous people or total strangers; and, most common. Stalker is a stranger to the victim but is obsessed with the victim and when rejected mounts a campaign of harassment to make the victim aware of the stalker's feelings.

Delusional stalkers

- Often have little contact with their victims
- Could have a mental disorder
- Often are unmarried, socially immature, isolated loners
- Typically choose a victim that is unattainable or who has shown them kindness in some way…a therapist, celebrity, clergy, teacher, doctor, etc.
- Can be dangerous and usually the rarest category of stalker.
- False belief that the victim shares the stalker's feelings and desire for a relationship.
- Here relationship based on stalker's psychological fixation. It also based on idealized love or spiritual union rather than sexual attraction.
- Target is usually a person with high visibility and a higher status.
- The danger period for a delusional is when they are falling out of love with one victim and in love with another victim.

Vengeful stalkers

- **Vengeful stalkers** may or may not have contact with their victims. They become angry with their victims over some real or perceived event or insult.
- They are as dangerous as delusional stalkers and are violent
- Vengeful stalkers thinks you did them wrong and they want to make you pay for it.
- These stalkers may be stalking to get even and take revenge and believe that "they" have been victimized. Ex-spouses can turn into this type of stalker.

6.7.3 Typology of Cyber Stalking

- The typology of the stalker is defined by what the relationship is/was between the suspect and the victim. Stalker, usually female, falsely believes that the victim, usually someone famous or wealth is in love with them. The target is usually unobtainable by the suspect.
- Primarily, there are three ways of cyber stalking :
  1. E-mail stalking : Direct communication through e-mail
  2. Internet stalking : Global communication through internet
  3. Computer stalking : Unauthorized control of another person's computer
- Cyber stalkers use email as the primary means to harass and threaten victims, far more than any other electronic communication device.
- Emailing allows an offender to repeatedly transmit harassing, threatening, hateful, or obscene messages, including pictures, videos, or audio.

Preventing cyber stalking

1. Do not post your personal information online.
2. Do not use your real name as a screen name.
3. Find out if your chat client or ISP network has a policy against cyber stalking.
4. Be careful about meeting friends that you have talked to online.

6.7.4 Types of Stalkers

1. **The resentful / rejected stalker :** The rejected suitor is when someone stalks their ex lover because in their mind they think that it is the only relationship they will ever have and believe that there is no other possibility except for that one relationship. In some cases these types of stalkers have some type of psychological disorder.
2. **The intimacy** seeker is similar to the rejected suitor except that this stalker is trying to create a relationship with what he or she believes is their one and only and the rejected suitor is a person that is trying to get back an old recent relationship.
3. **The incompetent** suitor is usually a man that has been turned down by a woman that they would like to develop a relationship with. After being turned down the stalker begins to repeatedly bother her and hope that his actions with let the women see that he is willing to work for the relationship and she will change her mind.
4. **The perdatory stalker** is a stalker that usually chooses victims at random with intent to commit a sexual crime with their victim. The initial motivation is to

gather information about the potential victim and gain access to their life. This is to most dangerous type of stalker.

6.7.5 Investigating Cyber Stalking

- Following are the some of the methods for investigating the cyber stalking :
  1. Take interview of victim person
  2. Take interview of other persons
  3. Check Risk assessment
  4. Find out any other additional digital evidence
  5. Purpose of the crime or characteristics
  6. Motivation
  7. Repeat the steps until.
- **Take interview of victim person :** Victim has to submit the proof about cyber stalking. The investigator has to check proof before taking any action. Collect the initial information from victim and develop victimology.
- After gathering all information, investigation will move forward. The whole story needs to be heard from the perspective of the complainant's history with the suspect in order to properly.
- **Take interview of other persons :** If suppose other persons involved in this case, investigator will take interview of all that peoples. It will help to understand the case.
- **Check risk assessment :** Check the relationship between victim and an offender.
- **Find out any other additional digital evidence :** What is known about the victim and cyber stalker to perform a thorough search of the Internet ? Aim of this stage is to collect detail information about victim, cyber stalker and crime.
- **Purpose of the crime or characteristics :** Find out the depth of crime scenes. Find the location where the cyber stalker and victim meet. There is any physical location and over the internet they meet without knowing to each other.
- **Motivation :** Determine personal interest of cyber stalker.
- Repeat the steps until you reach to the cyber stalker.

Review Question

1. *What is cyber stalking ? How to identify and detect cyber stalking.*

SPPU : May-19, Dec.-19, Marks 8

6.8 Proxy Servers

- The second broad category of firewall technology is application level technology. Devices in this category are called application gateways, which are computers running *proxy server* software.
- A proxy server is software that acts on behalf of an application that is trying to communicate from one network to another. Proxy server software can run on a machine by itself or along with other software such as packet filtering.
- A proxy server is like a border checkpoint between the internal network and the external world. Applications on both sides can communicate with proxy server, but they can not communicate beyond it. The proxy server receives communication from one side, checks to make sure the communication is authorised to proceed. If someone initiates a contact from the Internet to a site on your intranet, proxy server receives the contact, checks the rules, and makes the connection on the intranet side if the contact is authorised.
- Application gateways have additional capabilities. They can log information about what passes through them, such as what users connected with what sites at what times. Some application gateways also store pages from the internet that are requested frequently. When a user requests a page that is in the server's cache, the server can supply the page itself rather than having to go out to the server on the internet. That makes for much faster service for the user. Application level proxy servers are written for specific services. It's a disadvantage because the proxy server is limited in the application protocols it handle, it's a advantage because the proxy server can look into the application protocol information to find out where the connection is supposed to go. The proxy server can even go so far as to inspect the contents of the packet and accept or reject the connection based on that the user trying to do. For example, a proxy server for FTP can be set to reject a connection if the packet contains the "put" command.
- There is one more proxy server called a *circuit-level gateway*.
- A circuit level gateway doesn't know anything about the application protocol. It's just set up a connection from one network to other, if the connection meet is permissible under it's rule, and gets out of the way. That's an advantage because it can handle any protocol that comes along. That's an disadvantage because it can't inspect the application protocol information to find out where the connection is supposed to go. The application that is using the circuit-level proxy server has to tell server what to do with the connection.

6.9 Anonymizers

- Using a proxy server is the most common method of anonymous surfing. However, not all web proxy servers are anonymous or secure.
- An anonymizer is a proxy server that makes Internet activity untraceable. An anonymizer protects personally identifying information by hiding private information on the user's behalf. An anonymizer may also be known as anonymous proxy.
- When users anonymize their personal electronic identification information it can enable :
  1. Risk minimization
  2. Taboo electronic communications
  3. Identity theft prevention
  4. Protection of search history
  5. Avoidance of legal and/or social consequences.
- A number of free proxy anonymizers use proxy servers from free, open, proxy lists.
- Although some proxies are anonymous, a number of them aren't. Many of these lists do indicate whether a proxy is anonymous or not, but sometimes they are not accurate or up-to-date.
- A problem is that malicious hackers (crackers) and spammers set up proxies in the free proxy lists. They hijack the details of users, who may be open to ID theft or hacking and spamming attacks.
- If we use a commercial or free proxy anonymizer that does not use SSL or SSH encryption, then we are anonymous when connecting to standard unsecured (http) sites, but when we visit a secure, https link, then our real IP address will appear in that Website's server logs.

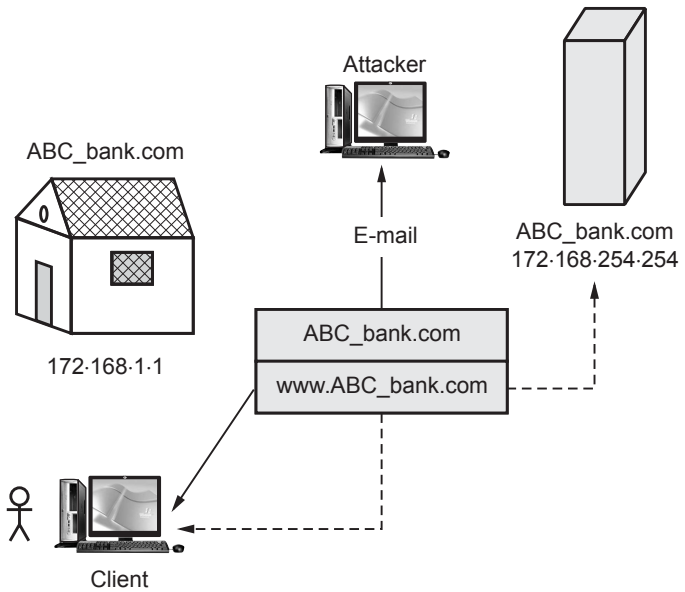
6.10 Phishing

- Phishing and pharming attacks have become sophisticated and are being used to cause real harm to a wide range of organizations.
- Attackers' objectives are both to steal confidential information and to gain access to and control over sensitive systems, whether for political or financially-motivated reasons. Phishing and pharming attacks are increasingly being used as a means of delivering malicious software into target organizations, with this malware then used to achieve the attackers' ultimate goals.
- **Phishing :** Attempting to criminally acquire sensitive information, such as usernames and passwords, by masquerading as trustworthy entities

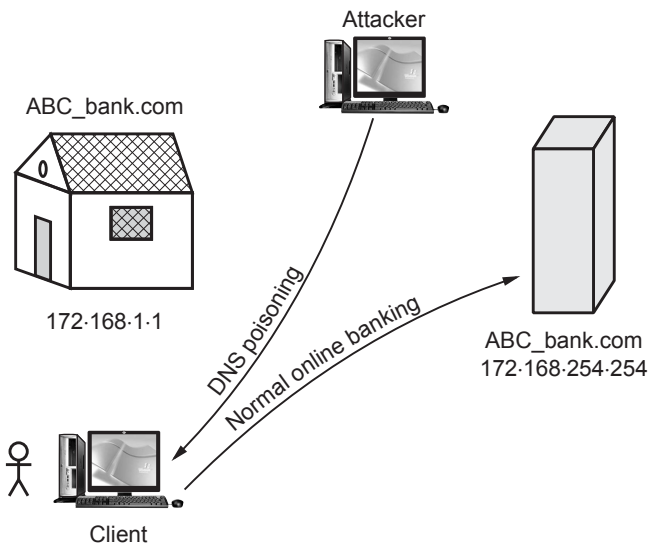
- **Pharming** is an attack on network infrastructure that results in a user being redirected to an illegitimate website despite the user having entered the correct web address.

Difference between phishing and pharming :

- Fig. 6.10.1 shows phishing and pharming attacks.



(a) Phishing



(b) Pharming

Fig. 6.10.1

- Phishing attacks usually will involve an email that appears to be from a company with which user do business prompting user to take action and log in to account with the link provided in the email. The Web site user visit is not the real site but a cleverly designed imposter site that may seem real to you, so user will enter your username and password, which is then captured by the attacker.
- Pharming is different in that it can happen when you are going to a legitimate Web site, even when user have typed the URL of the Web site yourself. In a pharming attack, the criminal "hijacks" the intended site's DNS server. The result is that users are redirected an imposter site that looks like your intended site. Many won't notice any difference, will enter their username and password as usual and the attacker captures it.

6.10.1 Phishing Attacks

- **Phishing** is a type of deception designed to steal your valuable personal data, such as credit card numbers, passwords, account data, or other information by masquerading as a trustworthy entity in an electronic communication. Communications purporting to be from popular social web sites, auction sites, online payment processors or IT administrators are commonly used to lure the unsuspecting public.
- Phishing is typically carried out by e-mail or instant messaging and it often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one.
- Phishing is an example of social engineering techniques used to fool users and exploits the poor usability of current web security technologies. The purpose of a phishing message is to acquire sensitive information about a user. For doing so the message needs to deceive the intended recipient.

How to avoid being a phishing victim ?

1. Phishing e-mail messages are usually sent out in bulk and often do not contain user first or last name. Never respond to requests for personal information via email. When in doubt, call the institution that claims to have sent the email.

   For example, "Dear Sir or Madam" rather than "Dear Dr. Phatak".

2. If you suspect the message might not be authentic, don't use the links within the email to get to a web page. Retype the address in a new window.
3. Never fill out forms in email messages that ask for confidential information.
4. Always ensure that you're using a secure website when submitting credit card or other sensitive information via your web browser.

   - Check the beginning of the Web address in your browsers address bar

- It should be 'https://' rather than just 'http://'
- Look for the locked padlock icon on your URL bar.

5. Regularly check bank, credit and debit card statements to ensure that all transactions are legitimate and if anything is suspicious, contact bank and all card issuers immediately.
6. Ensure that browser and OS software is up-to-date and that latest security patches are applied. Keep antivirus definitions updated.
7. Verify the real address of a website. Phishers also use Uniform Resource Locators (URLs) that resemble the name of a well-known company but are slightly altered by adding, omitting, or transposing letters. For example, the URL "www.microsoft.com" could appear instead as :

   www.micosoft.com ?

   www.mircosoft.com ?

   www.verify-microsoft.com

6.10.2 Buffer Overflow

- A buffer overflow occurs when a program or process tries to store more data in a buffer (temporary data storage area) than it was intended to hold. Since buffers are created to contain a finite amount of data, the extra information - which has to go somewhere - can overflow into adjacent buffers, corrupting or overwriting the valid data held in them.
- It may occur accidentally through programming error, buffer overflow is an increasingly common type of security attack on data integrity. In buffer overflow attacks, the extra data may contain codes designed to trigger specific actions, in effect sending new instructions to the attacked computer that could, for example, damage the user's files, change data, or disclose confidential information.
- Buffer overflow attacks are said to have arisen because the C programming language supplied the framework, and poor programming practices supplied the vulnerability.
- In July 2000, a vulnerability to buffer overflow attack was discovered in Microsoft Outlook and Outlook Express. A programming flow made it possible for an attacker to compromise the integrity of the target computer by simply it sending an e-mail message.
- Unlike the typical e-mail virus, users could not protect themselves by not opening attached files; in fact, the user did not even have to open the message to enable the attack.

- The programs message header mechanisms had a defect that made it possible for senders to overflow the area with extraneous data, which allowed them to execute whatever type of code they desired on the recipient's computers. Because the process was activated as soon as the recipient downloaded the message from the server, this type of buffer overflow attack was very difficult to defend. Microsoft has since created a patch to eliminate the vulnerability.
- Buffer overflow vulnerabilities are one of the most common vulnerabilities. These kinds of vulnerabilities are perfect for remote access attacks because they give the attacker a great opportunity to launch and execute their attack code on the target computer.
- A buffer overflow attack occurs when the attacker intentionally enters more data than a program was written to handle. The data runs over and overflows the section of memory that was set aside to accept it.
- The extra data overwrites on top on another portion of memory that was meant to hold something else, like part of the program's instructions. This allows an attacker to overwrite data that controls the program and can takeover control of the program to execute the attacker's code instead of the program.
- In exploiting the buffer overflow vulnerability, the main objective is to overwirte some control information in order to change the flow of control in the program. The usual way of taking advantages of this is to modify the control information to give authority to code provided by the attacker to take control.
- The stack is a section of memory used for temporary storage of information. In a stack-based buffer overflow attack, the attacker adds more data than expected to the stack, overwriting data. For example, "Let's say that a program is executing and reaches the stage where it expects to use a postal coder or zip code, which it gets from a Web-based form that customers filled out."
- The longest postal code is fewer than twelve characters, but on the web form, the attacker typed in the letter "A" 256 times, followed by some other commands. The data overflows the buffer allotted for the zip code and the attacker's commands fall into the stack. After a function is called, the address of the instruction following the function call is pushed onto the stack to be saved so that the function knows where to reutrn control when it is finished.
- A buffer overflow allows the attacker to change the return address of a function to a point in memory where they have already inserted executable code. Then control can be transferred to the malicious attack code contained with the buffer, called the payload.
- The payload is normally a command to allow remote access or some other command that would get the attacker closer to having control of the system.

- The best defense against any of these attacks is to have perfect programs. In ideal circumstances, every input in every program would do bounds checks to allow only a given number of characters. Therefore, the best way to deal with buffer overflow problems is to not allow them to occur in the first place.

6.10.2.1 Exploitation

- The techniques to exploit a buffer overflow vulnerability vary per architecture, operating system and memory region.

1. Stack - based exploitation

- A technically inclined and malicious user may exploit stack-based buffer overflows to manipulate the program in one of several ways :
  1. By overwriting a local variable that is near the buffer in memory on the stack to change the behaviour of the program which may benefit the attacker.
  2. By overwriting the return address in a stack frame. Once the function returns, execution will resume at the return address as specified by the attacker, usually a user input filled buffer.
  3. By overwriting a function pointer or exception handler, which is subsequently executed.

2. Heap - based exploitation

- A buffer overflow occurring in the heap data area is referred to as a heap overflow and is exploitable in a different manner to that of stack-based overflows. Memory on the heap is dynamically allocated by the application at run-time and typically contains program data.
- Exploitation is performed by corrupting this data in specific ways to cause the application to overwrite internal structures such as linked list pointers. The canonical heap overflow technique overwrites dynamic memory allocation linkage (such as malloc meta data) and uses the resulting pointer exchange to overwrite a program function pointer.

6.11 Password Cracking

- A password is the secret word or phrase that is used for the authentication process in various applications. It is used to gain access to accounts and resources. A password protects our accounts or resources from unauthorized access.
- Password cracking refers to various measures used to discover computer passwords.
- This is usually accomplished by recovering passwords from data stored in, or transported from, a computer system.

- Password cracking is done by either repeatedly guessing the password, usually through a computer algorithm in which the computer tries numerous combinations until the password is successfully discovered. This results in cybercrime such as stealing passwords for the purpose of accessing banking information
- In penetration testing, it is used to check the security of an application.
- In the past few years, programmers have developed many password cracking tools. Every tool has its own advantages and disadvantages.

6.12 Keyloggers and Spywares

SPPU : Dec.-15, May-16

- A keylogger is a technology that tracks and records consecutive key strokes on a keyboard. Because sensitive information such as usernames and passwords are often entered on a keyboard, a keylogger can be a very dangerous technology.
- Keyloggers are often part of malware, spyware or an external virus.
- There are many different kinds of keyloggers based on diverse keylogging methods. These include hardware and software keyloggers.
  1. Software keyloggers can be built into rootkits or other less detectable forms, and can infiltrate a computer in various ways.
  2. Hardware keyloggers can be fitted into the line from a keyboard to a device.
- Other more esoteric forms of keyloggers are based on electromagnetic emanations from hardware, which are addressed by emissions security protocols.

6.13 The Indian IT Act - Amendments

- The IT Amendment Act was passed by the Indian Parliament in October 2008 and came into force a year later. The Amendment was created to address issues that the original bill failed to cover and to accommodate further development of IT and related security concerns since the original law was passed.
- Provisions under IT act 2000 and amendment act 2008.
  1) Section 66E : Capturing, publishing or transmitting the image of a private area of any person is an punishable offence.
  2) Section 67 & 67A : Sending obscene material is an punishable offence.
  3) Section 67B : Transmitting material depicting children, including nude or sexually explicit pictures of self (Child Sexual Abuse Material - CSAM).
  4) Section 66C : Hacking of account or creating a fake account (identity theft) in someone else's name is an offence
  5) Section 66D : Impersonation; assumes the identity of someone else with the intention of fooling or deceiving the person is an offence

6) Section 66B : Stolen Computer; receiving or retaining any stolen computer resource or communication device is an punishable offence

6.14 Challenges to Indian Law and Cybercrime Scenario in India

- Cybercrime is not clearly defined under the Information Technology Act 2000, the amendment of the I.T. Act of 2008 or in the legislation in India.
- Un - authorized access to computer.
- Breach of confidentiality and privacy
- Securing access or attempting to secure access to a protected system.
- Publication of digital signature certificates for fraudulent purposes

6.15 IT Act

- The present laws governing Information and Communication Technology have been derived from the Indian Telegraph Act 1885, Indian Wireless Telegraphy Act 1933, The Telegraph Wire Unlawful Possession Act 1950 and the Cable Television Networks (Regulation) Act 1995.
- In the recent past the Telecom Regulatory Authority of India Act 1997 (TRAI Act) was enacted, paving way for the constitution of the first ever telecom regulatory body in India, known as Telecom Regulatory Authority of India (TRAI).
- The TRAI apart from telecom has recently been entrusted with the task of regulating and drafting of policies relating to broadcasting sector.
- The growth of IT industry and e-commerce, lead the government to enact the Information Technology Act 2000 (IT Act 2000).
- The issues relating to cyber crimes, data security, digital signatures, electronic commerce etc are covered under the IT Act 2000.
- The IT Act 2000 grants legal sanction to e-commerce transactions and also prohibits breach of confidentiality and privacy.

6.15.1 Aim and Objectives of IT Act, 2000

- The important aims and objectives of the IT Act, 2000 are :
  1. To suitably amend existing laws in India to facilitate e-commerce.
  2. To provide legal recognition of electronic records and digital signatures.
  3. To provide legal recognition to the transactions carried out by means of Electronic Data Interchange (EDI) and other means of electronic communication.

4. To provide legal recognition to business contacts and creation of rights and obligations through electronic media.
5. To establish a regulatory body to supervise the certifying authorities issuing digital signature certificates.
6. To create civil and criminal liabilities for contravention of the provisions of the Act and to prevent misuse of the e-business transactions.
7. To facilitate e-governance and to encourage the use and acceptance of electronic records and digital signatures in government offices and agencies. This would also make the citizen-government interaction more hassle free.
8. To make consequential amendments in the Indian Penal Code, 1860 and the Indian Evidence Act, 1872 to provide for necessary changes in the various provisions which deal with offences relating to documents and paper based transactions.
9. To amend the Reserve Bank of India Act, 1934 so as to facilitate electronic fund transfers between the financial institutions.
10. To amend the Banker's Books Evidence Act, 1891 so as to give legal sanctity for books of accounts maintained in the electronic form by the banks.
11. To make law in tune with Model Law on Electronic Commerce adopted by the United Nations Commission on International Trade Law (UNCITRAL) adopted by the General Assembly of the United Nations.

6.15.2 Importance of IT Act

- From the perspective of e-commerce in India, the IT Act 2000 and its provisions contain many positive aspects.
  a) Firstly, the implication of these provisions for the e-businesses is that email is now a valid and legal form of communication in our country that can be duly produced and approved in a court of law.
  b) Companies are now able to carry out electronic commerce using the legal infrastructure provided by the Act.
  c) Digital signatures have been given legal validity and sanction in the Act.
  d) The Act opens the doors for the entry of corporate companies in the business of being Certifying Authorities for issuing Digital Signature Certificates.
  e) The Act now allows Government to issue notification on the web thus heralding e-governance.
  f) 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.

g) The IT Act also addresses the important issues of security, which are 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 be passed through a system of a security procedure, as stipulated by the Government at a later date.

Under the IT Act, 2000, it is possible for corporate 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 ₹ 5 crores.

6.16 Multiple Chioce Questions

Q.1 A computer crime is _____.

a any activity in which the thief uses computer technology

b an illegal action in which the perpetrator uses special knowledge of computer technology

c an immoral action in which the thief uses special knowledge of computer technology without the other person knowing

d any threat to computer or data security

Q.2 Theft can take many forms of hardware, software, data or computer time. White - collar computer crime involves the theft of _____.

a applications b spikes

c data d property

Q.3 People who gain unauthorized access to computers for the purpose of doing damage are called _____.

a employees b hackers

c members of organized crime d crackers

Q.4 Why would a hacker use a proxy server ?

a To create a stronger connection with the target.

b To create a ghost server on the network.

c To obtain a remote access connection.

d To hide malicious activity on the network.

Q.5 Which of the following is considered as cyber crime ?

a Virus attack b Worm attack

c Hacking d All of these

Q.6 Which of the following techniques do not help prevent computer crime ?

a Firewalls b Cryptography

c Computer forensics d Intrusion prevention systems

Answer Keys for Multiple Choice Questions :

Q.1	b	**Q.2**	c	**Q.3**	d
Q.4	d	**Q.5**	d	**Q.6**	c

❑❑❑

SOLVED MODEL QUESTION PAPER (In Sem)

Information Security

T.E. (Computer) Semester - VI (Elective - II) (As Per 2019 Pattern)

Time : 1 Hour] **[Maximum Marks : 30**

N.B. : i) Attempt Q.1 or Q.2, Q.3 or Q.4.

ii) Neat diagrams must be drawn wherever necessary.

iii) Figures to the right side indicate full marks.

iv) Assume suitable data, if necessary.

Q.1 **a)** *Define security mechanism and security policy.* **(Refer section 1.6)** **[3]**

b) *Explain model for network security.* **(Refer section 1.7)** **[4]**

c) *Explain passive and active attack with example.* **(Refer section 1.4)** **[8]**

OR

Q.2 **a)** *What is difference between passive and active attack ?* **(Refer section 1.4.3)** **[3]**

b) *Describe elements of information security.* **(Refer section 1.2.4)** **[5]**

c) *Explain security services.* **(Refer section 1.5)** **[7]**

Q.3 **a)** *What is block cipher ? Explain advantages and disadvantages of block cipher.* **(Refer section 2.6)** **[4]**

b) *Using hill cipher encrypt the message 'ESSENTIAL'. The key for encryption is 'ANOTHERBZ'.* **(Refer example 2.4.5)** **[4]**

c) *What is DES ? Explain single round of DES.* **(Refer section 2.9.1)** **[7]**

OR

Q.4 **a)** *Explain the operation of polyalphabetic cipher.* **(Refer section 2.4)** **[3]**

b) *Use play fair cipher to encrypt the following message "This is a columnar transposition" use key - APPLE.* **(Refer example 2.4.2)** **[5]**

c) *What is stream cipher ? Explain its advantages and disadvantages. Compare stream cipher with block cipher.* **(Refer section 2.3)** **[7]**

SOLVED MODEL QUESTION PAPER (End Sem)

Information Security

T.E. (Computer) Semester - VI (Elective - II) (As Per 2019 Pattern)

Time : $2\frac{1}{2}$ Hours] **[Maximum Marks : 70**

N.B. : i) Attempt Q.1 or Q.2, Q.3 or Q.4, Q.5 or Q.6, Q.7 or Q.8.
ii) Neat diagrams must be drawn wherever necessary.
iii) Figures to the right side indicate full marks.
iv) Assume suitable data, if necessary.

Q.1 a) *Explain with example Diffie-Hellman key exchange.* **(Refer section 3.10)** **[8]**

b) *Explain the following :*
1) Divisibility **(Refer section 3.1.1)**
2) Testing for primality **(Refer section 3.3)** **[10]**

OR

Q.2 a) *Explain chinese reminder theorem.* **(Refer section 3.4)** **[5]**

b) *Perform encryption and decryption using RSA algorithm. p = 7, q = 11, e = 17 and M = 8.* **(Refer example 3.8.5)** **[6]**

c) *What is public key cryptography ? Explain its advantages and disadvantages.* **(Refer section 3.7)** **[7]**

Q.3 a) *What is IPSec ? Explain tunnel mode and transport mode.* **(Refer section 4.13)** **[8]**

b) *What is SHA ? List the features of SHA1. Explain SHA-3 secure hash crypto engine.* **(Refer section 4.3)** **[9]**

OR

Q.4 a) *What is HTTPS ? What are the problems with HTTP ? Explain working of HTTPS.* **(Refer section 4.10)** **[8]**

b) *What is cryptography hash function? Explain properties of hash function. What is one way hash function.* **(Refer section 4.1)** **[9]**

Q.5 a) *What is intrusion detection? Explain function of intrusion detection system.* **(Refer section 5.3)** **[6]**

b) *What is firewall ? Explain design goal of firewall.* **(Refer section 5.5)** **[6]**

c) *Explain multilevel security.* **(Refer section 5.8)** **[6]**

OR

Q.6 **a)** *Explain difference between HIDS and NIDS.* **(Refer section 5.3.4.6)** **[6]**

b) *Describe in detail trusted computing.* **(Refer section 5.10)** **[6]**

c) *Explain flooding attacks ?* **(Refer section 5.2)** **[6]**

Q.7 **a)** *Explain the following :*
1) Cyber terrorism **(Refer section 6.1.2)**
2) Cybersqatting **(Refer section 6.1.1)**
3) Cybercrime against property. **(Refer section 6.1.3)** **[9]**

b) *What is cyber stalking ? Explain motivates of cyber stalker.* **(Refer section 6.7)** **[8]**

OR

Q.8 **a)** *Explain proxy server and anonymizers.* **(Refer sections 6.8 and 6.9)** **[8]**

b) *What is cyber crime ? Explain types of cyber crime.* **(Refer section 6.2)** **[9]**

❑❑❑

Notes

Made in India

TEXT BOOKS FOR T.E. (COMP) SEM VI

Compulsory Subjects

1. Web Technology *(A. A. Puntambekar)*
2. Data Science and Big Data Analytics *(I. A. Dhotre, Dr. Kalpana V. Metre)*
3. Artificial Intelligence *(Anamitra Deshmukh-Nimbalkar, Dr. Vaishali P. Vikhe)*

Elective Subjects

4. Information Security *(V. S. Bagad, I. A. Dhotre, Dr. Swati Nikam)*
5. Augmented and Virtual Reality *(Dr. Ninad More, Sunita Patil)*
6. Cloud Computing *(I. A. Dhotre)*
7. Software Modeling and Architecture *(A. A. Puntambekar)*