easy – solutions

Information and Cyber Security

Semester VIII - Computer Engineering
(Savitribai Phule Pune University)

INDEX

- Chapter 1 : Security Basics ICS-1 to ICS-10
- Chapter 2 : Data Encryption Techniques and Standards ICS-10 to ICS-27
- Chapter 3 : Public Key and Management ICS-27 to ICS-47
- Chapter 4 : Security Requirements ICS-47 to ICS-58
- Chapter 5 : Intrusion and Firewall ICS-58 to ICS-63
- Chapter 6 : Confidentiality and Cyber Forensic ICS-63 to ICS-68

8EP2A1

SYLLABUS

Information and Cyber Security

Unit I : Security Basics

Introduction, Elements of Information Security, Security Policy, Techniques, Steps, Categories, Operational Model of Network Security, Basic Terminologies in Network Security. Threats and Vulnerability, Difference between Security and Privacy.

Unit II : Data Encryption Techniques and Standards

Introduction, Encryption Methods : Symmetric, Asymmetric, Cryptography, Substitution Ciphers. Transposition Ciphers, Stenography applications and limitations, Block Ciphers and methods of operations, Feistal Cipher, Data Encryption Standard (DES), Triple DES, DES Design Criteria, Weak Keys in DES Algorithms, Advance Encryption Standard (AES).

Unit III : Public Key And Management

Public Key Cryptography, RSA Algorithm : Working, Key length, Security, Key Distribution,

Deffie-Hellman Key Exchange, Elliptic Curve : Arithmetic, Cryptography, Security, Authentication methods, Message Digest, Kerberos, X.509 Authentication service.

Digital Signatures : Implementation, Algorithms, Standards (DSS), Authentication Protocol.

Unit IV : Security Requirements

IP Security : Introduction, Architecture, IPV6, IPv4, IPSec protocols, and Operations, AH Protocol, ESP Protocol, ISAKMP Protocol, Oakley determination Protocol, VPN. WEB Security : Introduction, Secure Socket Layer (SSL), SSL Session and Connection, SSL Record Protocol, Change Cipher Spec Protocol, Alert Protocol, Handshake Protocol. Electronic Mail Security : Introduction, Pretty Good Privacy, MIME, S/MIME, Comparison. Secure Electronic Transaction (SET).

Unit V : Firewall and Intrusion

Introduction, Computer Intrusions. Firewall Introduction, Characteristics and types, Benefits and limitations. Firewall architecture, Trusted Systems, Access Control. Intrusion detection, IDS : Need, Methods, Types of IDS, Password Management, Limitations and Challenges.

Unit VI : Confidentiality and Cyber Forensic

Introduction to Personally Identifiable Information (PII), Cyber Stalking, PII impact levels with examples Cyber Stalking, Cybercrime, PII Confidentiality Safeguards, Information Protection Law : Indian Perspective.

□□□

Information & Cyber Security

Chapter 1 : Security Basics

Q. 1 What are the security goals ?

Ans. : Security goals

Main goal of information security is to protect data or information which is being transmitted and achieve the confidentiality, integrity and availability of the data.

Following are the main goals of information security :

1. **Confidentiality**

Confidentially is most common aspect of information security. Confidentially is defined as the contents of a message are accessed only by intended person. Aim of confidentially is that only sender and his intended receiver should be able to access the contents of a message.

2. **Integrity**

Principle of integrity states that contents of message should not be modified until it reaches to authorize person. In this case change in the information need to be done only by authorized person and through authorized mechanisms only. Integrity gives assurance that data received exactly as sent by an authorized entity. (No alteration, no modification, no deletion and no intersection etc.). The attack threatening integrity is modification and masquerade.

The two important concepts:

(i) **Data integrity :** Assures information is changed only in authorized manner.

(ii) **System integrity :** Assures that the system performs its intended function properly and free from unauthorized manipulation.

3. **Availability**

Principle of availability states that resources must be available to authorized users at all the time as on when required. It assures that system works correctly and service is available to authorized users. The term resources may refer as confidential information, software and hardware components.

4. **Data Authentication**

Data authentication is important in many applications in networks. Data authentication allows the user or receiver to check whether that data really was sent by the actual sender or not.

In the two - party communication this mechanism is achieved through symmetric cryptography. The sender and receiver share a secret key to calculate a Message Authentication Code (MAC) of all communication data. Receiver knows that the data is send by exact or actual sender, if and only if message arrives with a correct MAC.

It's a technique to validate or verify a human-to-machine data or information transfer to establish the authenticity of the concerned individual. User authentication involves authorizing logins using personal credentials.

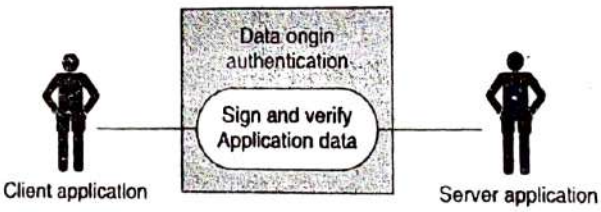


Fig. 1.1 : Data Authentication

Q. 2 List and explain categories of information security. **April 17(In sem.)**

Ans. :

Elements of Information Security are as follows :

1. **Physical Elements :**

Under these elements one can put physical security such as security guard and surveillance cameras which observe the confidential zone 24 × 7. Confidential work of office must be carried out in separate and restricted zone and access to these zones is restricted by biometric authentication system or by proximity cards.

Use of Camera phones, USB ports, portable hard disk are not allowed inside office. Access to the Internet compulsorily passes through the company's firewall and proxy gateway server. All illegal sites offering offensive contents are not accessible also URLs of web based emails are blocked.

Downloading of different types of files such as *.exe, *.mp3, *.3gp etc. is blocked. Access right given to the employee must be revoked on the day when he/she leaves the company or organization.

Data is encrypted format while in transit. A back of all machines should be maintained with the server or every user has to take back of their respective machines frequently. All the rules and regulations defined by the management committee regardless of their security measures has to put on mail for outside visitors.

2. System Elements

The software is updated on a regular basis with license copy of antivirus to protect viruses and malicious software detection solution is installed at all machines. Once virus has been detected there should be provision to remove the infected data and files from the systems. All the user machines have a user account and an administrator account. Changes to the particular software done through the administrator account only.

When user goes on leave his/ her accounts is disabled or even if account is inactive for a specific period of time are also disabled. Disable all the systems USB ports and CD Drives to avoid unwanted data transfer and virus infected programs through such devices. Maintain the logs of network activities or log must be maintained for all network users.

3. Process Elements

Any information stored accessible to authorized user only. Access right of sensitive information given to those who were signed the "Service Level Agreement" and "Non-disclosure / Confidentiality Agreement". A detailed list of all the software and their usage is maintained. Proper monitoring and review of all activities is done on regular basis.

A log entry for every user is maintained and continuously monitored. All log data can be accessed by authorized person only and it is reviewed on a regular basis. Extensive Training is provided to all the members of the organization regarding information security and the measures to be followed.

Q. 3 What are the security approaches used to implement security policy ? **Feb. 16(In sem.)**

Ans. :

The security approaches used to implement security policy

The Security policy is the basic term used to implement effective security solutions. Different security policies are used in the world of Information Security. Many organizations implements different security solutions without the basic groundwork of policies, standards, guidelines, and procedures, which results into unauthorized, unintentional and ineffective security controls.

Security policies are required to control security risks, identify the theft, system misuse detection, system fraud and different service interruptions occurred. Security policy, it is a general statement produced by management committees of specific organization or a selected policy board that dictates what role security plays within that organization.

There are different types of security policies, namely as below :

1. Regulatory

Regulatory policy ensures that the organization is maintaining standards set by specific industry regulations. The organization need to implement this policy because of compliance report, rules and regulations or other legal requirements. These companies can be financial institutions, public utilities, or some other type of organization that operates in the public interest.

2. Advisory

Advisory policy is like standards rules and regulations set by the management to advice their employees on their types of behaviors and on activities which should and should not take place within the organization. If advices rules are not followed by employee he may face series consequences such as termination, a job action warning. The organization/ company with such policies want most employees to consider such type of policies mandatory.

3. User Policies

User policies define how to use your network and organization's computer equipment. It defines the limitations on users to keep the network secure such as whether they can install programs on their workstations, legal software usage, and how they can access data from server or from specific machine.

Some of the User policies include :

Password Policies : To keep user accounts secure password policy is required. User need to change his/her password frequently. Password must be complex such as (types of characters used such as lower case letters, upper case letters, numbers, and special characters), and other items.

Internet Usage : Internet usage must be for informative work. Restrictions on use of your account or password.

System Use : Restriction on illegal usage of system. Only required program installation will be there.

Q. 4 Discuss different standards related to information security. **May 15**

Ans.:

1. Introduction to ISO 27001 security standard

The ISO 27001 security standard was published by International Organization for Standardization (ISO) and International Electro-technical Commission (IEC) in October 2005, having predefined set of rules or terms and conditions in order to maintain and establish an Information Security Management System (ISMS). An Information Security Management System is a systematic way to handle confidential information by keeping it secure and available to authorized users at any time as an when required.

ISO 27001 is a security assessment service that helps organizations (i.e. government agencies, non-profit organizations, commercial enterprises etc.) manage their current information security management system standard against ISO 27001 standard.

2. Objective of ISO 27001 standard

Following are the different objectives that ISO 27001 analyzes against organization to maintain their security standard :

It analyze complete system security standard which include security policies, access control, security monitoring systems, internal and external network activity i.e. traffic analysis, bandwidth analysis. Analysis of whether intrusion detection systems installed, is there any network configuration issues, checks for existing known vulnerabilities, firewall protection policies and virus protection scenario.

It also checks for database security, backup recovery options, data integrity, client and server authentication procedures. ISO 27001 standard helps organization to control security risks, identify the theft, system misuse detection, system fraud and different service interruptions occurred. Finally it checks any security deficiency as per their standard and issue ISO 27001 standard certification to the organization.

3. Evolution of standard

In the beginning of 1990, industry and government took the initiative for better control and to support implementation of information security. The ministry of commerce and industry of United Kingdom form a standard called code of practice (starting point for developing ISMS i.e. best practice guidance) for internal security standard later on in 1995 it was published by the British Standard Institute (BSI) known as BS 7799 part 1 standard.

BS7799 Part 1 standard provided good practice guideline i.e. code of practice for information security management. In 1998, British Standard Institute published BS 7799 part 2 standard as the basis for organization to be registered for audit to their information security management system i.e. specification for information security management systems. In 1999, both BS 7799 part 1 and BS 7799 part 2 were associated and republished the standard called as BS 7799-1 : 1999 and BS 7799-2 : 1999.

In 2000, BS7799 Part 1 was internationally recognized as ISO 17999:2000 which is again revised and renamed in early 2005 known as ISO 27002 : 2005.

ISO 27002 : 2005 is the international standard having structured code of practice for those organizations who seeking for method of implementing security standard to avoid information security risks and achieve confidentiality, integrity and availability their aspects.

In 2005, BS7799 Part 2 was internationally recognized as ISO 27001:2005 the standard helps to establish and audit the information security management system.

ISO 27000 is series of standard in which ISO 27001 just one part all other standards works towards the development and provide the framework for effective implementation of an information security management system.

Following are the ISO 27000 series of standards :

ISO27000 – ISMS introduction and terminology

ISO27001 – ISMS audit and necessary requirements

ISO27002 – Code of Practices for ISMS

ISO27003 – ISMS Implementation Guideline

ISO27004 – Dept analysis or complete measurement

ISO27005 – ISMS Risk Management

ISO27006 – Requirements for Bodies providing Audit and Certification of ISMSs

Q. 5 Explain OSI security architecture in detail.

May 15

Ans. : OSI security architecture

ITU-T International Telecommunication Union Telecommunication Standardization Sector X.800 (It is a service provided by a protocol layer of communicating open systems, to ensure the enough security of the system/ organization or of the data transfer) security architecture for OSI (Open Systems Interconnections) defines a systematic approach for providing security at each layeror it is a standard which provide systematic approach of defining and providing security requirements.

The OSI security architecture focuses mainly on the following three concepts :

Security Attack : An action that may compromise the security of the information that is owned by an organization is called security attack.

Security Techniques/ Mechanism : Security mechanism is the process that designed how to detect, prevent or recover from a security attack.

Categories of Security Service : A processing or communicating service that enhances security of data processing and information transfers of an organization. The services are intended to counter security attacks. The security service can use of one or more security mechanisms to provide security.

Q. 6 What is passive and active attack in information security explain with suitable example.

Feb. 16 (In sem.)

Ans. : Security attacks are as follows :

(a) **Passive Attacks**

The information is only monitored during data transmission between two persons and doesn't involve any modification to the contents of original message is called passive attack. Passive attacks are furthered classified into two subcategories as shown in

Fig. 1.2. A passive attack makes attempt to collect information from the system but does not modify or alter the system data or resources. Eavesdropping or monitoring of information is example of passive attacks. The goal of cryptanalyst is to gain the information that is being transmitted.

The two types of passive attacks are :

1. Release of message contents

Release of message contents attack is quite simple to understand. When we send a confidential email to our friend, our aim is that only intended person should access this mail. If this mail is accessed by unauthorized users then contents of message are released against somewhere else. Such type of attack is called release of message contents. There are different security mechanisms are available to prevent such type of attacks.

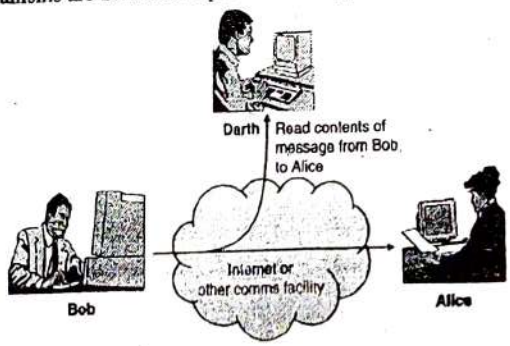


Fig. 1.2 : Release of message contents

For Example

Telephonic conversation between two people, an electronic mail and a file may contents sensitive information sent/ transfer over insecure channel such as Internet. We would like to prevent third person from modification of these type of transmission as shown in Fig. 1.2.

The main goal is to prevent the cryptanalyst from learning sensitive and confidential information through transmissions that take place through telephone calls or email messages or files transferred on network.

2. Traffic analysis

The contents of the message using encryption. The opponent is able to capture the contents of the message but not extract the information from the message. The opponent might observe a pattern of messages to get the location, or any clue regarding the origin of message.

Passive attacks are difficult to detect, because they do not involve modification of the information. The message sent and received is in normal fashion and neither sender nor receiver is aware that a third party has read message or observed pattern of messages as shown in Fig. 1.3. These attacks can be prevented by means of encryption.

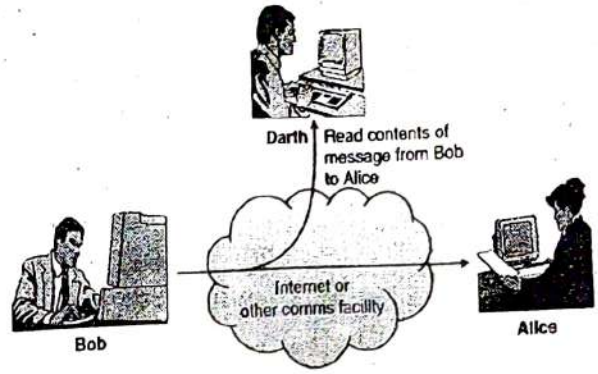


Fig. 1.3 : Traffic analysis

The emphasis when dealing with passive attacks is on prevention rather than detection.

(b) Active Attacks

Active attacks involve modification of a data stream or creation of a false stream of messages. Attacker aim in such type of attack is to corrupt or destroy the data as well as network itself. Active attacks means information is modified or gets altered during transmission between sender and receiver.

Active attacks are divided into four categories as shown in Fig. 1.4.

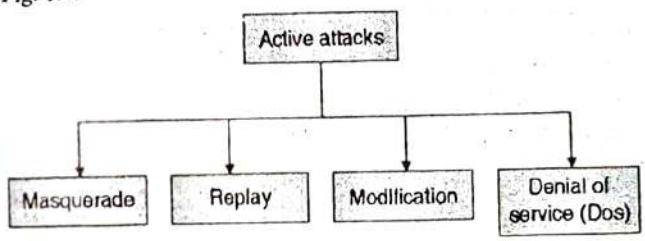


Fig. 1.4 : Types of Active attacks

1. Masquerade

A masquerade takes place when an attacker pretends to be an authentic user. It is generally done to gain access to a system, or steal important data from system. It is generally done by stealing login id and password of authentic user to gain access to a secure network. Once attacker gain access, they get full access to the network for deletion or changing of data or network policies of organization as shown in Fig. 1.5.

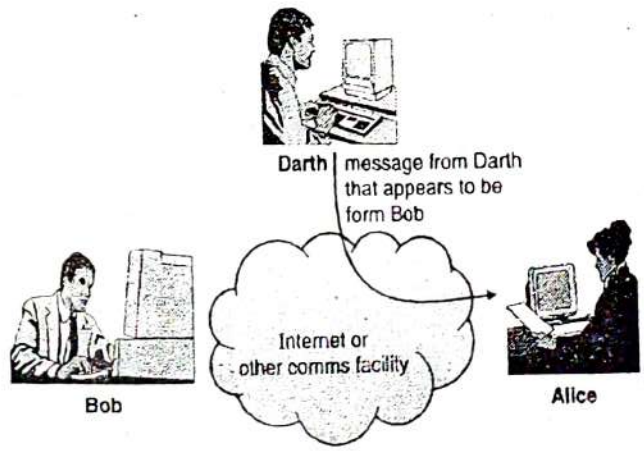


Fig. 1.5 : Masquerade attack

Such type of attack involves pretending the user from accessing authorized information.

2. Replay attack (Rewrite)

It is a network attack in which original data get modified and new malicious code added into valid data, during transmission. The newly generated malicious code retransmitted again and again to receiver called as replay attack (Reusing information). Replay attack involves passive capturing of data and retransmission of subsequent information in order to create unauthorized effect as shown in Fig. 1.6.

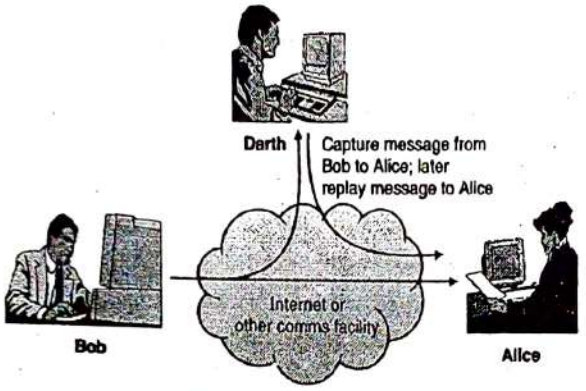


Fig. 1.6 : Replay attack

3. Modification of messages

In modification, the original data that has been sent by the authentic user is been disrupt or modified by the attacker to make it non meaningful for the receiver. Usually the content sequence is been changed. Modification is also called replay attack. When contents of message modified after sender sends it but before it reaches to indented recipients, such type of attack is called modification of message as shown in Fig. 1.7.

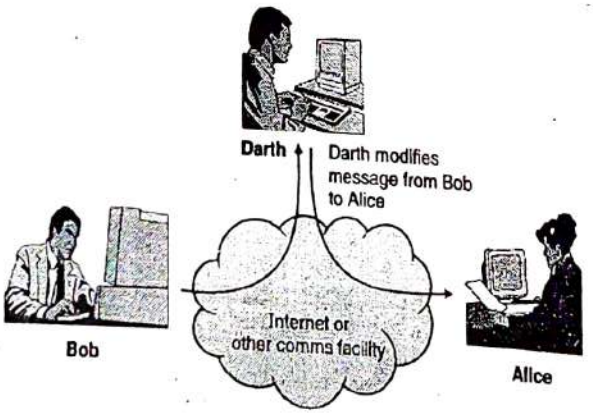


Fig. 1.7 : Modification of messages

For Example

If Bob wants wants to transfer amount of Rs.1000/- into Alice account, during this transmission process an attacker called Darth capture the conversation and modified the actual amount of Rs.1000/- and sends just Rs. of 100/- into Alice account. The case happed here contents of message get altered during transmission process such type of attack called modification. In this case Integrity of original message is lost.

4. Denial of Service (DoS)

Denial of service attack means making the network unavailable for the user to communicate securely. It is generally done by interrupting in the network connection between the users or making some services unavailable for user or disrupts the entire network by overloading with unwanted messages, so that network becomes slow and unavailable for users shown in Fig. 1.8.

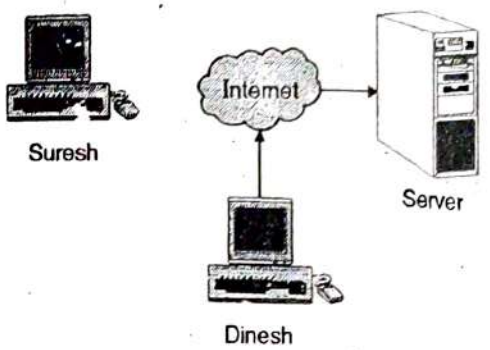


Fig. 1.8 : Denial of service

Due to intentional action of Dinesh, Suresh is unable to access the data from server.

Because of Dinesh intention he denied use or services of sever to Suresh; even if Suresh is authorized user. DoS attack attempt to shut down the network, computer services and deny the use of resources or services to authorized users. Once Dinesh got entire access of network or server he can do the following things :

1. Flood the entire network or server with traffic until shutdown occurs because of overload.
2. Block ongoing traffic which results in a loss of access to network resources to the authorized users. Different security policies like firewall, Intrusion detection system helps to protect such type of attacks.
3. Different security policies like firewall, Intrusion detection system helps to protect such type of attacks.

Q. 7 Differentiate between Active attacks and Passive attacks.

Ans.: Difference between Active attacks and Passive attacks

Sr. No.	Active Attack	Passive Attack
1.	Attacker needs to have physical control of the media or network.	Attacker merely needs to observe the communication in the media or network.
2.	It can be easily detected.	It cannot be easily detected.
3.	It affects the system.	It doesnot affect the system.

Sr. No.	Active Attack	Passive Attack
4.	It involves in modification of data.	It involves in monitoring of data.
5.	Types of active attack are : Masquerade, replay, denial of service, distributed denial of service.	Types of passive attack are : Release of message, traffic analysis.
6.	It does not check for loopholes or vulnerabilities.	It scans the ports and network in search for loopholes and vulnerabilities.
7.	It is difficult to prevent network from active attack.	Passive attack can be prevented.

Q. 8 List and explain different security Techniques. **Feb. 16 (In sem.)**

Ans.:

Following are the eight different security mechanisms.

1. Specific Security Mechanism / Attack Prevention

These mechanisms are incorporated into the appropriate protocol layer in order to provide some OSI security service. It is the security mechanism implemented to prevent against various types of attack before they can actually reach and affect the target systems.

2. Pervasive Security Mechanisms / Attack Detection

These mechanisms are not specific to any of the OSI security service or protocol layer. This technique also called attack detection which is implemented to prevent, if attacker bypass the installed security measures to access the desired target/information. Attack detection technique notifies such incidents happens and takes the responsibility to report someone that something went wrong somewhere in the system. Such type of mechanisms used to inform the administrator or authorized user that something went wrong in the system now its job of administrator or authorized user to take action against detected attack.

3. Attack Avoidance

In these techniques data is sent over an insecure channel such as Internet in encrypted format and decrypted at receiver side using keys under assumptions that attacker may have access to the transmitted data. The encryption and decryption is performed on sending data by using well known cryptographic mechanisms such as :

(i) Private Key Cryptography

(ii) Public Key Cryptography.

(iii) Hash Functions

Q. 9 What are the various security services ? **April 17(In sem.)**

Ans.: Security services are as follows :

X.800 is a service provided by a protocol layer of communicating open systems, to ensure the enough security of the system/ organization or of the data transfer. RFC 2828 defines security service as a communication service provided by a system to give protection to the system resources.

X.800 defines security services into following categories :

1. Authentication

It is assurance of parties that they are authentic user in the communication network. Authentication helps to identify the claimed identity of an entity, such as username password or any other important information such as encryption or decryption keys stolen during transmission between sender and receiver.

It can be further classified as follows :

1. **Peer entity authentication :** It checks that the entities connected in communication network are authentic and do not perform any attack like masquerade and replay of messages in network.
2. **Data origin authentication :** It checks that the data is authentic without any changes received by the receiver.

2. Authorization

Authorization service helps for checking whether the entity has the right to perform action requested. Authorization means providing authority or permission of accessing the system or privilege of accessing data, directories, files etc. of the system.

Authorization is one of the most important security aspects. It provides identification of the user as authorized user. It is a kind of permission given by the network administrator for accessing the network.

For example

Password used for sever login, ATM pin while withdrawing money and biometric machine used in an office for checking employee identification. An authorization principle helps whether server administrator, ATM card user and company employee are valid user or not.

Access Control

Access Control is the ability to limit and control the access to the host systems. It prevents unauthorized use of a resource. The service used to prevent unauthorized use of a resources i.e.

complete control over who can access to resources, under what conditions access can occur and what are different accessing methodology.

For example

It controls the access of resources which is to be made available only to legitimate user. It looks to the conditions of accessing the resource or network and what is allowed to be done to the resources.

3. Non-Repudiation

Principle of non-repudiation states that if sender sends some information and later on he denied that he never sends that information called non-repudiation.

1. **Non-repudiation, Origin** : Proof that the message was sent by the specified party.
2. **Non-repudiation, Destination** : Proof that the message was received by the specified party.

For example

Ramesh sends a request to bank about money transfer into Suresh account but later on Ramesh Denying the money transfer request to bank. Principle of non-repudiation does not allow such type of refuses of sender.

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

4. Auditing

Auditing services helps to trace which user accessed what ? when ? and which way ? In general auditing does not provide protection but can be the tool for analysis of problems. There are different security mechanism are used to provide security services and also helps to prevent all types of attacks.

Q. 10 Draw and explain operational model of security.

April 17(In sem.), May 17

Ans.: Operational model of security

Consider a message/data is to be transferred from sender to receiver or from one party to another across internet. During this data transmission process it is necessary to protect security aspects of this information from an opponent or attacker.

The technique used to provide security is as follows :

The original message is encrypted with the help of a key, which scrambles the message so that it is not readable to any third party. An additional code can be attached to the encrypted data which is based on the contents of the message, which can be used to verify the identity of the sender.

The message is now transmitting through an insecure channel such as Internet. The message when received at the receiver side is unscrambled either using same or different key to obtain the original message. A trusted third party (such as Virtual Private Network) is required for secure transmission. The trusted third party is responsible to distribute the private key and secret information to the sender and receiver while keeping it away from any opponent or attacker.

The model for security is shown in Fig. 1.9.

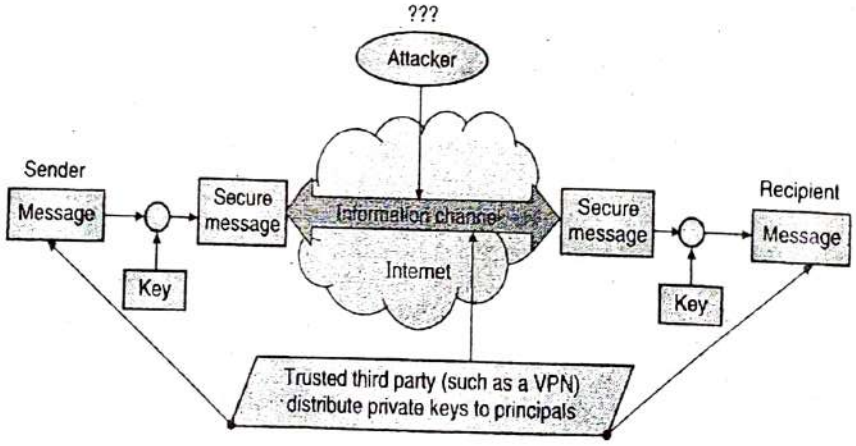


Fig. 1.9 : The model for network security

Q. 11 What are the categories of computer security ? **Dec. 16**

Ans. :

The category of computer security have two types :

(1) Hardware Security

Threat

Even if the computer is not plugged into a network, a person can open its cabinet and gain access to the hard drives, steal them and misuse or destroy the data saved on them or, damage the device altogether. It is also necessary to remember that in case one dissembles his computer hardware, the risk of losing coverage of warranty becomes very high.

Protection

If a stand-alone system contains some important or classified information, it should be kept under constant surveillance. Locking system for a desktop and a security chain for a laptop are basic security devices for your machine. Certain disk locks are available in various sizes, which control the removal of the CPU cover.

(2) Software Security

Denial of Services

Denial-of-service disables a computer or a network and can be executed with limited resources. It is one of the most common forms of attacks by hackers and can effectively disable the whole network of an organization. Denial of service attack makes a computer resource unavailable to its intended user.

Trojan Horse

Trojan horse is common and one of the most potential threats to computer security. They are malicious and security-breaking programs, disguised as something which is considered as non-malicious by the security software. They are a useful tool for hackers who try to break into private networks. Hackers generally attach Trojan horse to a file, which triggers a virus or remotely controlled software, giving the hacker complete control over the computer.

Viruses and Worms

Viruses and worms are well-known for their destructive nature and the property of replicating themselves. They are basically pieces of computer program codes, which are written by hackers and other computer geniuses.

Trapdoor / backdoor

An intruder can enter into the system by bypassing all security services or mechanisms. Thus intruder knows the flaws or loopholes in the system and can get these loopholes to gain access to the computer. Trapdoors are the entry points which are not documented but still inserted during code development for testing purpose, for future extensions or for an emergency access if software fails. These loopholes are purposely kept in the system with good intension.

Major sources of Trapdoors / Backdoors

During testing of the system stubs, drivers are created. These are temporary functions which then further replaced by actual functions. Sometimes some malicious code is intentionally injected into the system for testing purpose.

Poor error checking conditions.

Undefined opcodes in hardware processors.

Firewall - Firewall is one of the most essential type of network security in today's world of Internet. Firewall is a filter that prevents fraud websites from accessing your computer and damaging the data. However, a firewall is not a great option for securing the servers on the Internet because the main objective of a server is granting access to unknown users to connect to various web pages.

Q. 12 Illustrate the cryptanalysis with Dictionary attack. **Dec. 16**

Ans. : The cryptanalysis with Dictionary attack

In **cryptanalysis** and computer security, a **dictionary attack** is a technique for defeating a cipher or authentication mechanism by trying to determine its decryption key or pass phrase by trying hundreds or sometimes millions of likely possibilities, such as words in a **dictionary**.

Two counter measures against dictionary attacks include :

Delayed Response : A slightly delayed response from the server prevents a hacker or spammer from checking multiple passwords within a short period of time.

Account Locking : Locking an account after several unsuccessful attempts (for example, automatic locking after three or five unsuccessful attempts) prevents a hacker or spammer from checking multiple passwords to log in.

Q. 13 Explain various cryptanalysis techniques. **May 17**

Ans. :

Cryptanalysis techniques/attacks

1. A Brute Force Attack

In Brute force attack, cryptanalyst attempt to use all possible permutations and combinations on cipher text message to obtain corresponding plain text message. This attack trying every possible key until the correct translation of cipher text into plain text message is obtained. It is most often used in a known plaintext or cipher text only attack. DES encrypt the block of data using 56 bit key. Now a day it is very easy to crack the encryption key using

specialized hardware called Electronic Frontier Foundation's Deep Crack.

Triple DES (168-bit key) was approved due to DES's weakness to brute force attacks, followed by the Advanced Encryption Standard (AES) in 2001.

2. Meet-in-the-Middle Attack

This attack was introduced by Markel and Hellman. Meet-in-the-middle attacks can be used against cryptographic algorithms that use multiple keys for encryption. An example of a successful meet-in-the-middle attack is the attack against Double DES.

In order to improve the strength of 56 bit DES algorithm double DES concept was introduced having 112-bit key length and two rounds of DES encryption performed as well but still it is vulnerable against attack called as Meet-in-the Middle.

In meet in the middle attack cryptanalyst have access to both plaintext message and its corresponding cipher text message.

For example, assume the plaintext is "Act," and the resulting double DES cipher text is "Dvy." The cryptanalyst wants to recover the two keys (called Key1 and Key2) used for encryption. The cryptanalyst first conducts a brute force attack on Key1 using all 256 different single DES keys to encrypt the plaintext of "Act" and saves each key and the resulting intermediate cipher text into a table.

Q. 14 Explain attacks and counter measures on application and data with example. **May 17**

Ans. :

The attacks and counter measures on application and data with example.

Brute force attacks : Attacks that use the raw computer processing power to try different permutations of any variable that could expose a security hole. For example, if an attacker knew that access required an 8-character username and a 10-character password, the attacker could iterate through every possible combination (256 multiplied by itself 18 times) in order to attempt to gain access to a system. No intelligence is used to shape or filter likely combinations.

Buffer overflows : The maximum size of a given variable (string or otherwise) is exceeded, forcing unintended program processing. In this case, the attacker uses this behaviour to cause insertion and execution of code in such a way that the attacker gains control of the program in which the buffer overflow occurs. Depending on the program's privileges, the seriousness of the security breach will vary.

Cross-site scripting : An attacker is able to inject executable code (script) into a stream of data that will be rendered in a browser. The code will be executed in the context of the user's current session and will gain privileges to the site and information that it would not otherwise have.

Data tampering : An attacker violates the integrity of data by modifying it in local memory, in a data-store, or on the network. Modification of this data could provide the attacker with access to a service through a number of the different methods listed in this document.

Denial of service : Denial of service (DoS) is the process of making a system or application unavailable. For example, a DoS attack might be accomplished by bombarding a server with requests to consume all available system resources, or by passing the server malformed input data that can crash an application process.

Dictionary attack : Use of a list of likely access methods (usernames, passwords, coding methods) to try and gain access to a system. This approach is more focused and intelligent than the "brute force" attack method, so as to increase the likelihood of success in a shorter amount of time.

Disclosure of sensitive/confidential data : Sensitive data is exposed in some unintended way to users who do not have the proper privileges to see it. This can often be done through parameterized error messages, where an attacker will force an error and the program will pass sensitive information up through the layers of the program without filtering it. This can be Personally Identifiable Information (PII) or system data.

Encryption : The process of taking sensitive data and changing it in such a way that it is unrecognizable to anyone but those who know how to decode it. Different encryption methods have different strengths based on how easy it is for an attacker to obtain the original information through whatever methods are available.

Information disclosure : Unwanted exposure of private data. For example, a user views the contents of a table or file that he or she is not authorized to open, or monitors data passed in plaintext over a network. Some examples of information disclosure vulnerabilities include the use of hidden form fields, comments embedded in Web pages that contain database connection strings and connection details, and weak exception handling that can lead to internal system-level details being revealed to the client. Any of this information can be very useful to the attacker.

Man-in-the-middle attacks : A person intercepts both the client and server communications and then acts as an intermediary between the two without each ever knowing. This gives the "middle man" the ability to read and potentially modify messages from either party in order to implement another type of attack listed here.

Network eavesdropping : Listening to network packets and reassembling the messages being sent back and forth between one or more parties on the network. While not an attack itself, network eavesdropping can easily intercept information for use in specific attacks listed in this document.

Password cracking : If the attacker cannot establish an anonymous connection with the server, he or she will try to

establish an authenticated connection. For this, the attacker must know a valid username and password combination. If you use default account names, you are giving the attacker a head start. Then the attacker only has to crack the account's password. The use of blank or weak passwords makes the attacker's job even easier.

Repudiation : The ability of users (legitimate or otherwise) to deny that they performed specific actions or transactions. Without adequate auditing, repudiation attacks are difficult to prove.

Session hijacking : Also known as man-in-the-middle attacks, session hijacking deceives a server or a client into accepting the upstream host as the actual legitimate host. Instead, the upstream host is an attacker's host that is manipulating the network so the attacker's host appears to be the desired destination.

Session replay : An attacker steals messages off of the network and replays them in order to steal a user's session.

Spoofing : An attempt to gain access to a system by using a false identity. This can be accomplished by using stolen user credentials or a false IP address. After the attacker successfully gains access as a legitimate user or host, elevation of privileges or abuse using authorization can begin.

SQL injection : Failure to validate input in cases where the input is used to construct a SQL statement or will modify the construction of a SQL statement in some way. If the attacker can influence the creation of a SQL statement, he or she can gain access to the database with privileges otherwise unavailable and use this in order to steal or modify information or destroy data.

Chap 2 : Data Encryption Techniques and Standards

Q. 1 What are different encryption methods ? Explain along with suitable example.

Ans.:

There are two types of cryptography i.e. symmetric key cryptography and asymmetric key cryptography.

1. Symmetric Key Cryptography

Symmetric key cryptography also called as secret key cryptography. In symmetric key cryptography a single key is used for encryption as well as decryption. As shown in Fig. 2.1 sender encrypt plain text using shared secret key and the resultant cipher text is transmitted through communication medium such as Internet, at the receiver side the cipher text is decrypted using same decryption key to obtain original plain text. Note that encryption and decryption process uses well known symmetric key algorithm called as Data Encryption Standard (DES).

Mathematically it is represented as P = D (K, E(P)).

Where P = Plain Text, E (P) = Encryption of plain text, D (K, E(P)) = Decryption of Plain text using shared key K.

For Example

Stream and block cipher, Data Encryption Standard (DES), Advance Encryption Standard (AES) and BLOFISH.

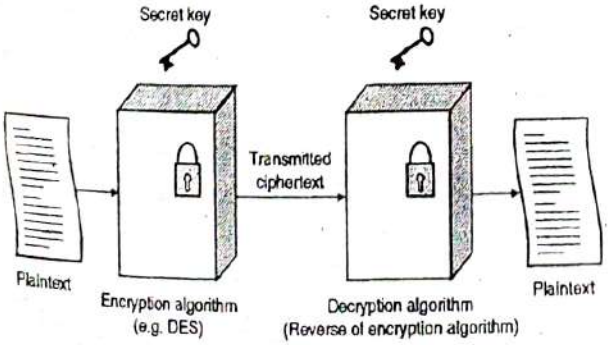


Fig. 2.1 : Symmetric Cipher Model

Here the main aim of cryptography is text into picture. Always sender has to think on applying different encoding technique on plain text message and convert it into cipher text message so that attacker cannot read the actual plain text easily.

Symmetric cipher model convert the plain text message into cipher text by using following techniques.

2. Asymmetric Key Cryptography

Asymmetric key cryptography is also called as public key cryptography. In asymmetric key cryptography two keys are used, one for encryption and other for decryption.

As mentioned asymmetric key cryptography involves use of two keys one is public key that may know to everyone and can be used to encrypt messages, and verify signatures. Other is private key known only to the receiver of the message or verifier, used to decrypt messages, and sign (create) signatures.

It is also called as asymmetric key cryptography because one key is used for encryption only its corresponding key must be used for decryption. No other key can decrypt the message.

The sender and receiver can encrypt messages using encryption key (public) or verify signatures, he cannot decrypt messages or create signatures because he required decryption key (private) which is known only to the receiver of the message. Public key cryptosystem or asymmetric key cryptography as shown in Fig. 2.2.

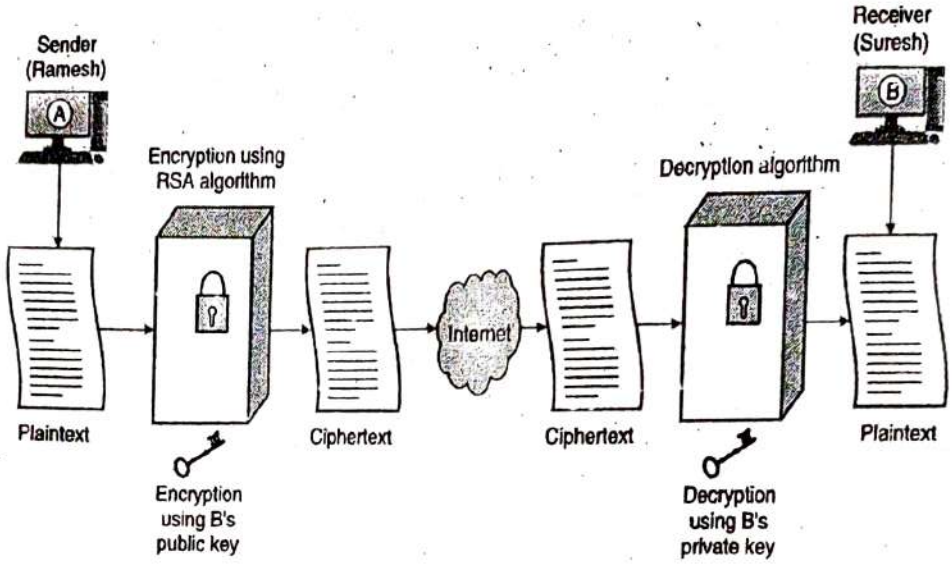


Fig. 2.2 : Asymmetric Key Cryptography

Mathematically it is represented as : P = D(Kd, E (Ke,P))

Where P = Plain Text, E (P) = Encryption of plain text, D = Decryption, Ke = Encryption key, Kd = Decryption Key.

For example, sender Ramesh wants to communicate with the receiver Suresh then they must have each one of this i.e. private key and public key then and then communication will be successful.

Q. 2 Compare between symmetric key encryption and asymmetric key Encryption. **Dec. 16**

Ans.: Difference between symmetric key encryption and asymmetric key encryption

Sr. No.	Symmetric Key Cryptography	Asymmetric Key Cryptography
1.	In Symmetric key cryptography single or same key is used for encryption and decryption.	In asymmetric key cryptography two keys are used, one is for encryption and other is for decryption.
2.	Symmetric key cryptography is also called as secret key cryptography or private key cryptography.	Asymmetric key cryptography is also called as public key cryptography or conventional cryptographic system.
3.	Mathematically it is represented as P = D (K, E(P)). Where K is encryption and decryption key. P = plain text, D = Decryption E(P) = Encryption of plain text	Mathematically it represented as P = D(Kd, E (Ke,P)), Where Ke and Kd are encryption and decryption key. D = Decryption E(Ke, P) = Encryption of plain text using private key Ke.
4.	Symmetric key is faster than asymmetric key cryptography.	Because of two different key used asymmetric key is slower than asymmetric key cryptography.
5.	For encryption of large message asymmetric key cryptography still play an important role.	In asymmetric key cryptography plain text and cipher text treated as integer numbers.
6.	Symmetric key cryptography utilizes less resource as compare to asymmetric key cryptography.	Asymmetric key cryptography utilizes more resource as compare to symmetric key cryptography.
7.	For Example : AES, DES and BLOWFISH	For Example : RSA, Diffie-Hellman Key exchange algorithm.

Q. 3 What is stream Ciphering ? Discuss any one stream ciphering in detail. **Dec. 14**

Ans. :

In stream cipher keys and algorithms are applied to each binary digit in a data stream, one bit at a time, rather than encrypting block of data (a stream cipher operates on plaintext accepting only one bit at a time).

One time pad is the best example of stream cipher in which each bit of plaintext message XOR with each bit of key to obtain cipher text message. It is a symmetric cipher operates on varying time transformation individually on each bit. This is shown in Fig. 2.3.

There is a keystream generator which outputs a stream of bits : $k_1, k_2, k_3, \ldots, k_i$ XOR with a stream of plaintext bits, $p_1, p_2, p_3, \ldots, p_i$, to produce the stream of ciphertext bits $c_1, c_2, c_3, \ldots, c_i$. Broadly it can represented as shown below

$$c_i = p_i \oplus k_i \quad \ldots(1)$$

During decryption, the cipher text bits are XOR with a same key stream to recover the plaintext bits.

$$p_i = c_i \oplus k_i \quad \ldots(2)$$

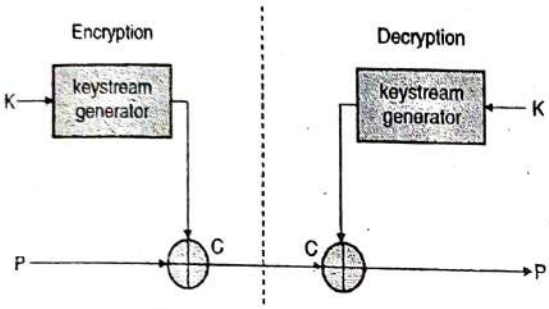


Fig. 2.3 : Stream Cipher

The stream cipher security depends on the simple XOR and one time pad. If the key stream output is random that, it will take harder time for a cryptanalyst to break it. However if it will keep on repeating same stream bits then it can result an attack on the cryptosystem.

For example : Suppose plaintext is pay 100 in ASCII (i.e. text format). When it is converted to binary values let us take that it is translating as 010111001 (hypothetically) also applying XOR logic in encryption algorithm.

In text format	In binary format	
Pay 100	010111001	Plaintext
+	100101011	XOR operation with the key
ZTU91^%D	11010010	Cipher text

XOR Logic is shown in table below

Input 1	Input 2	Output
0	0	0
0	1	1
1	0	1
1	1	0

Rather than divide bit stream into discrete blocks stream cipher convert plaintext message into ciphertext message by encrypting one bit at a time. At receiver side use same key and XOR logic to extract plaintext message. Another interesting property of XOR is that when XORing is done use twice along with key, it produces back the original plaintext described in equation below.

$$p_i \oplus k_i \oplus k_i = p_i \quad \ldots(3)$$

Q. 4 Describe block ciphers.

Ans. : Block ciphers

Block Cipher break plain text message into fixed blocks and encrypt each block with some key size (fixed). Divide each plaintext message into block of 64, 128, 256 bits and apply common key size 40, 56, 64, 80, 128, 168, 192 and 256 bits which generate cipher text message same as size of plaintext block or as per size of plaintext message.

Fig. 2.4 shows encryption of 64-bit plaintext using block cipher with 56-bit key.

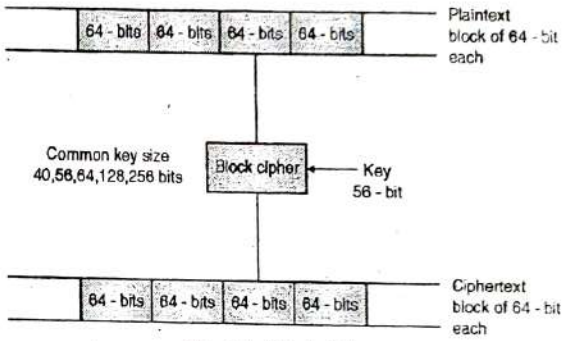


Fig. 2.4 : Block cipher

Block cipher is main method of encrypting text in which keys and algorithm are applied to block of data rather that individual bits like stream cipher. Data Encryption Standard (DES) is the best example of block cipher in which each block of 64-bit get encrypted using 56-bit key and cipher text of 64-bit get generated.

At receiver side decrypt message with same key to generate plaintext.

Like in stream cipher, block cipher also uses the concept of key generator. Block cipher are used in **Chaining mode,** this is because for repeating text pattern, the same cipher block will be generated which can give clue to cryptanalyst regarding what is the original plaintext hence chaining mode is used for block ciphers. We will discuss concept of chaining mode in block cipher modes of operation.

As in chaining method, previous block is mixed with current block to avoid repeats in patterns. Block cipher is little time consuming but secure than stream cipher so generally used in computer based cryptographic algorithms. Stream cipher is faster than block cipher.

Q. 5 What is diffusion and confusion ? Differentiate diffusion and confusion. **Dec. 14**

Ans. :

1. Diffusion

It means any of the character in plaintext is changed, then simultaneously several characters of the cipher text should also be changed. Similarly if the character of cipher text is changed then simultaneously several characters of plaintext should be changed. It is a classical transposition cipher.

"Diffusion" = Transposition or Permutation

Abcd → dacb

Data Encryption Standard is the best example of diffusion.

2. Confusion

Each character of cipher text depends on different part of the key. In confusion the key does not directly related to cipher text. It is a classical substitution cipher.

"Confusion" = Substitution

a → b Caesar cipher

For example

Suppose we have a Hill cipher with an matrix n x n, and suppose we have a plaintext-ciphertext pair of length n^2 with which we are able to solve for the encryption matrix. If change one character of the ciphertext, one column of the matrix can change completely.

It would be more desirable to have the entire key change. When a situation like that happens, the cryptanalyst would probably need to solve for the entire key simultaneously, rather than piece by piece.

Q. 6 Explain Substitution cipher.

Ans. : Substitution cipher

A substitution is a technique in which each letter or bit of the plaintext is substituted or replaced by some other letter, number or symbol to produce ciphertext. Substitution means replacing an alphabet of plaintext with an alphabet of ciphertext. Substitution technique also called confusion. The best example of substitution cipher is Caesar cipher invented by Julius Caesar.

Substitution Cipher techniques are as follows :

1. Caesar Cipher

Julius Caesar introduced the easiest and the simplest use of substitution cipher. In Caesar cipher technique each letter is replaced by the letter /alphabet which is three places next to that letter which is to be substituted. Or In Caesar cipher technique, each alphabet of a plaintext is replaced with another alphabet but three places down the line as mentioned in following table.

For example

Plaintext : Sun rises in the East

Ciphertext : VXQULVHVLQWKHHDVW

Following is the list of possible combination showing the letters 3 places down of each alphabet :

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
Ciphertext	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

The corresponding number equivalent to each alphabet 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

Mathematically the Caesar cipher algorithm can be expressed as

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

$$P = D(3,C) = (C - 3) \bmod 26$$

Where, C = Ciphertext/ or alphabet

P = Plaintext/ alphabet

E = Encryption

D = Decryption

Mod 26 because in English there are total 26 alphabets.

It is very easy to break ciphertext obtained from plaintext message with the help of Brute-Force attack because the attacker will be having only 25 possible keys to decrypt the ciphertext.

Further some more characteristics which lead to easy brute force attacks are :

1. The encryption and decryption algorithms are known.
2. Only 25 possible keys.
3. And plaintext language is easy to recognize with few repetition of alphabet having same ciphertext letter.

2. Monoalphabetic Cipher

In Caesar cipher the attacker can easily guess the plaintext as it is easily recognizable. In Monoalphabetic cipher substitutes one letter of the alphabet with any random letter from the alphabet. It is not necessary that if A is substituted with B then compulsorily B has to be substituted with C. It can be replaced with any other letter

of the alphabet. The only weakness in this algorithm is that if more repetition occurs then attacker can easily guess the plaintext.

This random substitution is just done to have uniqueness. In this the substitution of characters are random permutation of the 26 letters of the alphabet.

For example

Following is the substitution that we are taking :

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
Cipher-text	e o u n a f p v b m W l c q x d g k s y z i T r J H

Plaintext : East or West

Ciphertext : aesy xk taay

Ciphertext obtain with this technique yields completely different text as compare to Caesar cipher. In this method, each letter provides multiple substitutes for a single letter.

For example,

A can be replaced by : d, j, r,y

B can be replaced by : h, u, m,p etc.

Such type of large key space makes this cipher technique extremely difficult to break by brute-force attack. But this can make the cryptanalysis attacker straight forward to guess the pattern.

3. Polyalphabetic Cipher

As in monoalphabetic cipher we use only one fixed alphabet, but draw back in monoalphabetic is these are fairly easy to break. So to make it harder to break the concept of polyalphabetic cipher arises it is a way to use **more than one** alphabet and switching between them systematically.

Procedure of Polyalphabetic Cipher

1. Pick a keyword (for our example, the keyword will be "MEC" as shown in Example 1).
2. Write your keyword across the top of the text you want to encipher, repeating it as many times as necessary.
3. For each letter, look at the letter of the keyword above it (if it was 'M', then you would go to the row that starts with an 'M'), and find that row in the Vigenere table.
4. Then find the column of your plaintext letter (for example, 'w', so the twenty-third column).
5. Finally, trace down that column until you reach the row you found before and write down the letter in the cell where they intersect (in this case, you find an 'I' there).

Example 1

Keyword	MECMECMECMECMECMECMECM
Plaintext	weneedmoresuppliesfast
Ciphertext	IIPQIFYSTQWWBTNUIUREUF

Thus, the urgent message "We need more supplies fast!" comes out :

IIPQIFYSTQWWBTNUIUREUF

Q. 7 Write a short note on Playfair cipher.

Ans.:

It was invented by Charles Wheatstone in 1854 but known by name Playfair because Lord Playfair made this technique popular. It was used by Britisher in World War 1.

It is multiple letter encryption technique, which uses 5 × 5 Matrix table to store the letters of the phrase given for encryption which latter on becomes key for encryption and decryption.

For example : Keyword is FAIR EXAMPLE.

In the first step all letters are to be filled in that matrix from left to right, the letters which are already been placed is not be placed again in that matrix.

After filling up of the given letter, fill rest of the space in the matrix with the remaining letters alphabetically with no repetitions. The letters I and J will be considered as one letter. So If I is already placed then no need to place J in rest of the matrix.

The letters which are already written/ mentioned need not to be placing that letter in given matrix. For in given example A and E are already mentioned in matrix so it is not mandatory to write that letter again in the given matrix.

Table 2.1

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

Encryption using Table 2.1 keyword matrix

1. The plaintext received is to be broken in pair of two letters.
2. For example CYBER can be broken into CY BE R(X).
3. If both letters are same or only one letter is left then put X with that alphabet.
4. If both pair alphabet appears in same row replace the letter with the immediate right alphabet (wrapping around to the left side of the row if a letter in the original pair was on the right side of the row).
5. If both letters appear in same column replace it with alphabet immediate below to that letter (wrapping around to the top side of the column if a letter in the original pair was on the bottom side of the column).
6. If none of the condition explained above meet, then replace them with the letters on the same row respectively but at the other pair of corners of the rectangle defined by the original pair.

For Example : The plaintext CYBER can be encrypted as : CY BE R(X)

1. For pair CY we check that CY does not occur in same row or column so we see step 6.

   The pair CY forms a rectangle, replace it with HU. If pair forms a rectangle, pick same row letter but opposite corners.

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

   So CY will encrypt as H U.

2. Checking for BE both are in same column so replace it with immediate next in that column.

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

   B E will be encrypted as K B (Below to E is B).

3. Checking for R(X)

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

   The pair RX forms a rectangle, replace it with FL. If pair forms a rectangle, pick same row letter but opposite corners.

   R(X) will be encrypted as FL.

Q.8 Use Play fair cipher to encrypt the following message "This is a columnar transposition." Use key APPLE. **Feb. 16(In sem.)**

Ans. :

The key used is APPLE so put it into 5 × 5 matrix.

Draw matrix 5 × 5.

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

The plain text message is "This is a columnar transposition" divide the latter's in to the set of two character.

Message : "This is a columnar transposition".

th is is ac lu mn ar tr an sp os it io n

The first problem is that the message has an odd number of letters. To solve this problem we simply add an extra letter at the end, generally. In this example, the final n becomes a pair nq. The plain text becomes

th is is ac lu mn ar tr an sp os it io nq

Second problem is that plain text have the repeated pair i.e., so that inserts an x. Since that gives an odd number of letter, so adds a q to the final singleton, so that the plaintext becomes

th ix si sa cl um na rt ra ns po si ti on qq

Third problem is that plain text has the repeated pair qq, so that inserts an x at the end

th ix si sa cl um na rt ra ns po si ti on qx

The ciphertext : ug mv qm ql fa so ie su qp mt bk qm qn io sv

Q. 9 Write short note on : Hill Cipher.

Ans.: Hill Cipher

We can work on multiple letters at the same time using hill cipher. Hill cipher techniques were developed by the mathematician lester hill in 1929.

When we use encryption algorithm we take the m successive plaintext letters and substitutor for them in m cipher text latter.

Hill cipher is a polygraphic substitution cipher based on linear algebra. Each letter is represented by a number modulo 26.

Often the simple scheme (A = 0, B = 1, C = 2, ... Z = 25) is used, but this is not an essential feature of the cipher.

To encrypt a plaintext message, each block of m letters (considered as an m-component vector) is multiplied by an invertible m × m matrix, against modulus 26. To decrypt the plaintext message, each block is multiplied by the inverse of the matrix used for encryption.

The technique can be described as following way :

$$\boxed{\begin{aligned} C_{i1} &= (K_{11}, P_{i1} + K_{12} P_{i2} + K_{13} Pi_3) \bmod 26 \\ C_{i2} &= (K_{21}, P_{i1} + K_{22} P_{i2} + K_{23} P_{i3}) \bmod 26 \\ C_{i3} &= (K_{31}, P_{i1} + K_{32} P_{i2} + K_{33} P_{i3}) \bmod 26 \end{aligned}}$$

This techniques uses column vectors and matrices :

$$\begin{bmatrix} C_{i1} \\ C_{i2} \\ C_{i3} \end{bmatrix} = \begin{bmatrix} K_{11} & K_{12} & K_{13} \\ K_{21} & K_{22} & K_{23} \\ K_{31} & K_{32} & K_{33} \end{bmatrix} \begin{bmatrix} P_{i1} \\ P_{i2} \\ P_{i3} \end{bmatrix} \bmod 26$$

We can represented this technique different way like,

$$C_i = KP_i \bmod 26$$

Where,

C_i and P_i are the column vector which is hold length 3 K is used to representing the encryption.key. Which is used 3 × 3 matrix For Example :

$$\text{Key (k)} = \begin{bmatrix} 2 & 5 & 4 \\ 9 & 1 & 2 \\ 3 & 7 & 17 \end{bmatrix}$$

Using the vector we can represent the Key and first three letters of the plaintext HEL as follow.

$$\begin{aligned} C_i &= KP_i \bmod 26 \\ &= \begin{bmatrix} 2 & 5 & 4 \\ 9 & 1 & 2 \\ 3 & 7 & 17 \end{bmatrix} \begin{bmatrix} 7 \\ 4 \\ 11 \end{bmatrix} \bmod 26 \\ &= \begin{bmatrix} 78 \\ 89 \\ 236 \end{bmatrix} \bmod 26 \\ &= \begin{bmatrix} 0 \\ 11 \\ 2 \end{bmatrix} = \text{ALC} \end{aligned}$$

For the given plaintext, we get ciphertext is ALC.

When we get the entire ciphertext it requires to do decryption using the inverse of the matrix K.

Using the general terms in Hill cipher techniques is

Ciphertext $C_i = E_n(K, P_i) = KP_i \bmod 26$

Plaintext $P_i = D_n(K, P_i) = K^{-1} C_i \bmod 26 = K^{-1} KP_i = P_i$

Q.10 Using hill cipher encrypt plain text "COE" use key "ANOTHERBZ". **May 16, 5 Marks**

Ans. :

Plain text (Pi) = COE

By using Hill Cipher

Key = ANOTHERBZ

It is represented as

$$\begin{aligned} Ci &= KPi \bmod 26 \\ &= \begin{bmatrix} A & N & O \\ T & H & E \\ R & B & Z \end{bmatrix} \times \begin{bmatrix} C \\ O \\ E \end{bmatrix} \bmod 26 \\ \text{Cipher Text (Ci)} &= \begin{bmatrix} 0 & 13 & 14 \\ 19 & 7 & 4 \\ 17 & 1 & 25 \end{bmatrix} \times \begin{bmatrix} 2 \\ 14 \\ 4 \end{bmatrix} \bmod 26 \\ &= \begin{bmatrix} 334 \\ 128 \\ 184 \end{bmatrix} \bmod 26 \\ &= \begin{bmatrix} 22 \\ 24 \\ 2 \end{bmatrix} \text{Mod } 26 = \text{WYZ} \end{aligned}$$

For the given plaintext, we get ciphertext is **WYZ.**

Q. 11 What is transposition technique ? **May 16, Dec. 16**

Ans.: Transposition technique

In transposition cipher method plaintext message is hidden by rearranging the order of plain text letters without altering the original letter. In transposition cipher, the letters are written in a row under the key and then arrange the column as per alphabetical order. There are two types of transposition ciphers : single columnar and double columnar transposition ciphers.

In transposition technique, there is no replacement of alphabets or numbers occurs instead their positions are changed or reordering of position of plaintext is done to produce ciphertext. Transposition cipher is a kind of mapping achieved by performing some sort of permutation on the plaintext message. Transposition cipher also called diffusion which performs permutations on plaintext.

Diffusion means permutation of bit or byte positions.

There are two types of transposition techniques

1. Columnar Transposition Technique
2. Keyless Transposition Techniques

Q. 12 Describe the columnar transposition technique in detail.

Ans.:

Columnar transposition technique is very simple to understand having following steps :

(1) Write plaintext message into a rectangle of some predefined size (rows and columns).

(2) Select the random key according to the size of rectangle also called columns. (In this technique order of the columns is the key).

(3) Read the text present in each selected random key columns.

(4) Combine all text present in each column as per selected random key order.

(5) The resultant text called ciphertext shown in Fig. 2.5.

Example 1

Step 1 : Select any **Plaintext :** are you missing somebody.

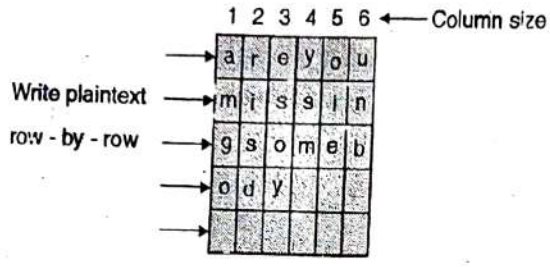


Fig. 2.5 : Columnar transposition technique

Step 2 : Select random key (according to column size) 5 4 2 3 1 6

Step 3 : Read text present in each column according to key.

Step 4 : oieysmrisdesoyamgoumb

Step 5 : Final ciphertext is

Ciphertext : oieysmrisdesoyamgourmb

The ciphertext obtained in step 5 can be made more complicated by performing multiple rounds of such permutations.

A more complex way to encrypt the message would be to write it in a rectangle, row by row, and then read off the message column by column, but to decide the order of the columns. The order of the column will be the key of the algorithm.

Example 2

Plaintext : The book is related to history.

1	2	3	4	5	6	7
T	h	e	b	o	o	k
I	s	r	e	l	a	t
E	d	t	o	h	i	s
T	o	r	y			

Select the order of columns (Key) : 4351267

Ciphertext : beoyertryolhtiethsdooaikts

Q. 13 What is stegnography ? What are applications and limitations of stegnography ? **April 17 (In sem.)**

Ans. : Stegnography

Steganography is a technique of hiding the message, file and image within other message, file or image. Steganography word is of Greek origin that means "covered writing" or "secret writing".

It is the art as well as science of hiding the communication in such way that know body aware the existence of communication. The goal of hiding messages, files and images is to fool attacker and not even allow attacker to detect that there is another message hidden in original message.

The main aim of Steganography is to achieve high security and encode the sensitive data in any cover media like images, audio, video and send it over insecure channel such as Internet. Even if there is small change in stenographic image or data will change complete meaning of the messages.

In Steganography the term called as **Steganalysis** which is similar to cryptanalysis in cryptography. Like cryptanalysis, the goal of steganalysis is to identify suspected messages, files and images, to determine whether any hidden or encoded information is available into those messages, and also to try and gain access to that messages, files and images.

Attacks on steganographic techniques are very similar to attacks on cryptographic techniques/ algorithms and similar techniques apply. The strength of a steganographic algorithm depends on its ability to successfully withstand attacks.

Following are the possible attacks on steganography.

1. **Stego-only attack :** In this type of attack, only the medium (files and images) containing hidden data is available for analysis. This attack also called as Visual attack.

2. **File only attack :** The attacker has access the file he must determine if there is a message hidden information inside that file.

3. **Known carrier attack :** In this type of attack, the steganalyst has access to both the original image and the image containing the hidden information are available and compared to assume the message. The stego object (that contains the hidden information) is compared with the cover object and the differences are detected.

   This attack also called as file an original copy : It might happen that attacker have a copy of both the file i.e. the encoded message and a copy of the original file. If the two files are different, then attacked may guess that there must be some hidden information inside a file. Such type attacks helps attacker to destroy the hidden information by simply replacing it with original message.

4. **Reformat Attack :** Most popular attack on stegnogrephy is reformat attack, in this attack attacker change the format of the file (BMP, GIF, JPEG) because different file formats don't store data in exactly same way.

5. **Destroy Everything Attack :** An attacker could simply destroy the message and all related information. This can works correctly because there are different file formats are used to store data in different ways.

6. **Known message attack :** In this type of attack, the original message prior to embedding and when transmitting over Internet is known to sender. This type of attack analysis can help against attacks in the future.

7. **Multiple Encoding of a Files :** The attacker gets *n* different copies of the files with *n* different messages. It might happen if some companies are inserting different tracking information into each file. If the attacker tracks all the data during transmission then he may try to replace the tracking information with its own available information.

8. **Compression Attack :** One of the simplest attacks is to compress the file. This type of attack tries to remove the unrelated information from a file during compression then what is the use of hiding the data if extraneous information is removed.

Q. 14 What is block cipher? Explain counter mode of block cipher. **April 17(In sem.)**

Ans. : Block cipher

The block cipher is basic building block for providing data security. In Block cipher rather that encrypting one bit at a time, block of bits is encrypted at one go.

The Federal Information Processing Standard (FIPS) defines four methods/modes of operation for block cipher that may be used in a wide variety of applications like symmetric key cryptographic algorithms (DES, AES etc.). The modes specify how data will be encrypted and decrypted.

Q. 15 Describe ECB.

Ans. : ECB

In Electronic Codebook (ECB) mode the given plaintext message is divided into blocks of 64 bits each and each 64-bits blocks get encrypted independently. The plaintext block produces ciphertext of same size (64-bits each). The given plaintext is encrypted using same key and transfers the encrypted data (ciphertext) to receiver.

At the receiver end each block is decrypted independently using same key in order to produce original plaintext message of same size i.e. blocks of 64-bits each.

The Electronic Codebook (ECB) mode encryption and decryption process is shown in Fig. 2.6 and Fig. 2.7.

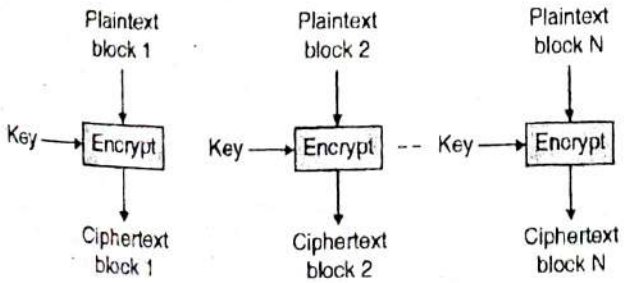


Fig. 2.6 : The Electronic Code Book (ECB) mode encryption process

The drawback of ECB mode is that for the occurrence of more than one plaintext block in the input generates the same ciphertext block in the output, which gives clue to the attacker or cryptanalyst.

Only small messages can be encrypted using ECB mode of operation where the chances of repeating the same plaintext message are quite less.

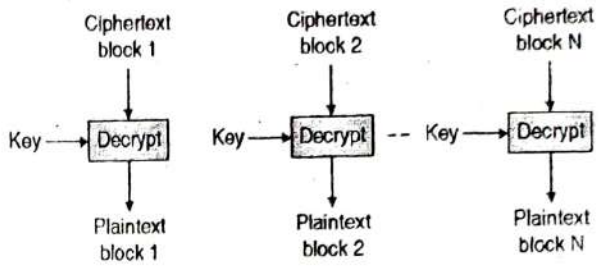


Fig. 2.7 : The Electronic Code Book (ECB) mode decryption process

Q. 16 Explain the operation of cipher Block chaining (CBC) mode. **Feb. 16 (In sem.)**

Ans.:

To overcome the problem of repetition and order independence in ECB even for repeated plaintext the Cipher Block Chaining (CBC) mode is used. In CBC mode the first block of the message (plaintext bolck1) is XORed with an initialization vector (IV) which is then encrypted using key k and produces ciphertext block1.

In next step each block of plaintext (plaintext block 2) is XORed with the previous ciphertext block1 before being encrypted and produces output i.e. ciphertext block 2. The procedure is continuing till all plain text block gets encrypted. Initialization Vector doesn't have special meaning it is simply used to make input message more complicated or unique.

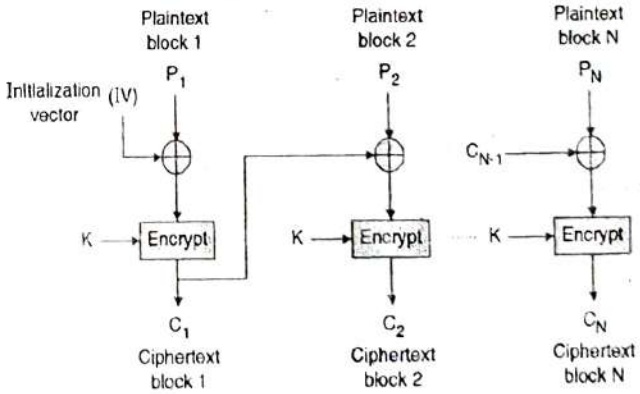


Fig. 2.8 : Cipher Block Chaining (CBC) mode encryption process

Different criteria for IV are fixed-size input value it should be random or pseudorandom. A good initialization vector should be unique and unpredictable. In all modes of operation plaintext blocks are represented by using P_1, P_2, P_3,.....P_n and corresponding ciphertext blocks are represented by using C_1, C_2, C_3,.....C_n.

In case of cipher block chaining mode even if plaintext block repeats in the input, output of CBC mode yields totally different ciphertext blocks as shown in Fig. 2.8. CBC mode is applicable whenever large amounts of data need to be sent securely, provided that all data is available in advance (e.g. email, FTP, web etc.).

In CBC decryption, ciphertext block 1 get decrypted using same key used during encryption process for all plaintext blocks. The output of this step is then XOR with initialization vector (IV) and produces plaintext block 1. In next step the ciphertext block 2 is decrypted and its output is XOR with ciphertext block 1 which results plaintext block 2.

Repeat the process for all ciphertext block in order to produce original plaintext blocks as shown in Fig. 2.9.

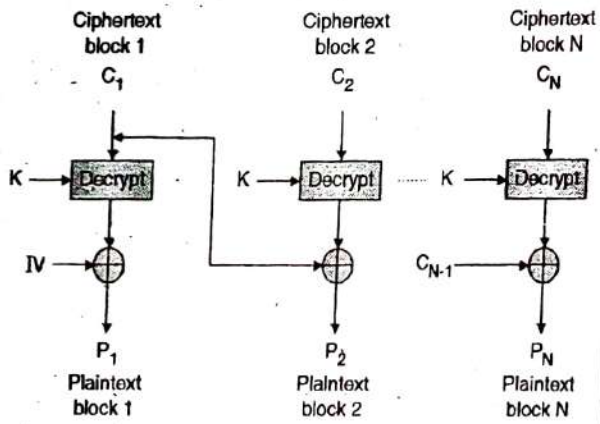


Fig. 2.9 : Cipher Block Chaining (CBC) mode decryption process

Q. 17 Explain Cipher Feedback Mode (CFB) Block cipher. **May 17**

Ans. : Cipher Feedback Mode (CFB) Block cipher

CFB mode uses block cipher as stream cipher meaning is that data is encrypted in smaller units of block say 8-bits rather than predefined size of 64 bits. CFB mode may be used as a stream cipher. In CFB encryption process 64 bits initialization vector is used which is kept in 64 bits of shift register.

The IV (shift register) is then encrypted and produces 64-bits of ciphertext i.e. encrypted IV. Now the leftmost s bits (size of 8 bits) of the encrypted IV are XORed with the first s bits (size of 8 bits) of plaintext P_1 to produce the first s bits of ciphertext C_1, which is then transmitted to next step.

In next step contents of the 64 bit shift register are shifted left by s bits (8 bits) and C_1 is placed in the rightmost s bits of the shift register and which again undergoes to encryption process and XORed with plain text P_2 to produce cipher text C_2 as shown in Fig. 2.7.6. This process continues until all plaintext units have been encrypted. Here same key K is used during encryption and decryption process.

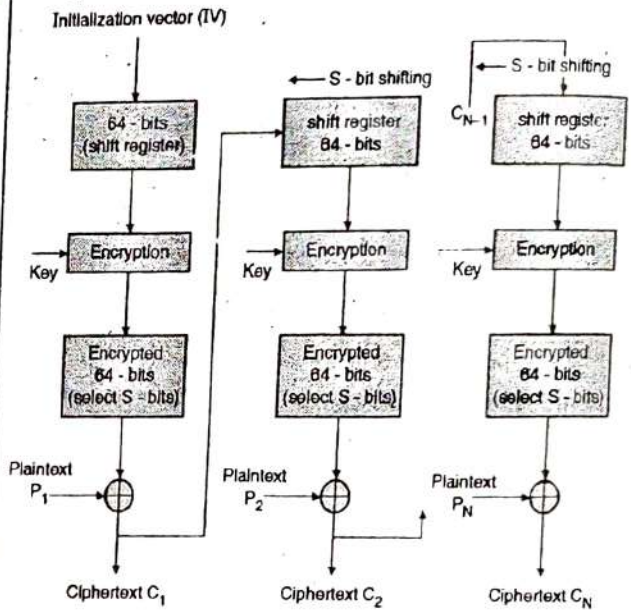


Fig. 2.10: Cipher Feedback (CFB) mode encryption process

Decryption of CBC mode reverse of CBC encryption, the same technique is used, except that the output of encryption process is XOR with the received ciphertext block to produce the original plaintext block as shown in Fig. 2.11.

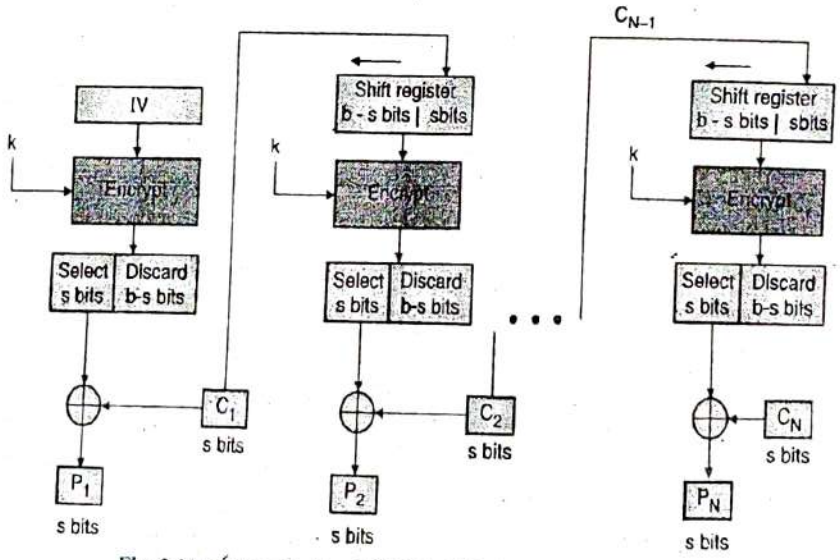


Fig. 2.11: Cipher Feedback (CFB) mode Decryption Process

Q. 18 Describe OFB.

Ans.: OFB

We know the general procedure input to encryption process is 64-bit shift register (IV), select most significant s bits from encrypted IV and XOR with plaintext P_1 to produce ciphertext C_1. Output of encryption process is placed in least significant s bits of shift register (left shift) of next stage and repeat the process until all units encrypted.

In case of OFB having only one difference is that output of encryption process O_1 (instead of generating ciphertext C_1) is directly placed in next stage of shift register without XOR operation to avoid bit errors during transmission as shown in Fig. 2.12.

In OFB mode, if there is a small error in individual bits, it remains an error in individual bits which do not corrupt the whole encrypted message (to avoid bit errors during transmission) which is the biggest advantages of OFB mode over all other mode. In this case Initialization Vector is extracted from a double length encryption key.

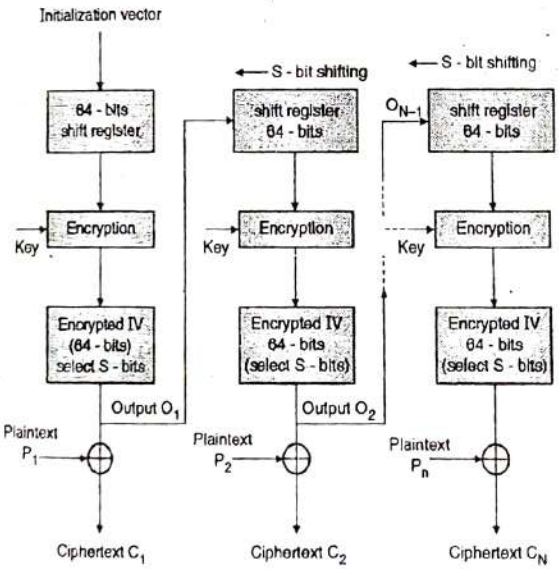


Fig. 2.12: Output feedback (OFB) mode encryption process

Decryption process of OFB is reverse of encryption process as shown in Fig. 2.13.

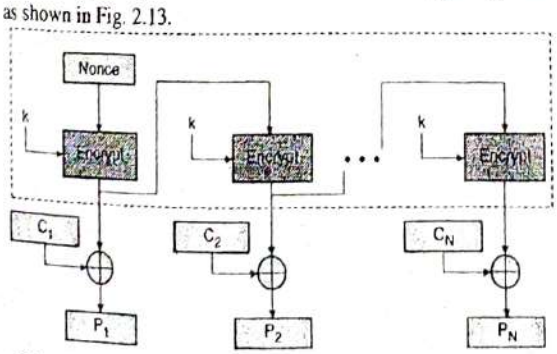


Fig. 2.13 : Output feedback (OFB) mode decryption process

Q. 19 Explain Counter mode of block cipher.

April 17(In sem.)

Ans.: Counter mode of block cipher

This mode is similar to OFB with the difference is that it uses counters or sequence numbers as input to the algorithm. We put a constant value as initial value of counter which will be of same size as that of a plaintext block.

In counter mode, the counter is encrypted and then XOred with the plaintext to produce ciphertext. There is no chaining process is done. CTR Encryption and Decryption Process is shown in Fig. 2.14 and Fig. 2.15.

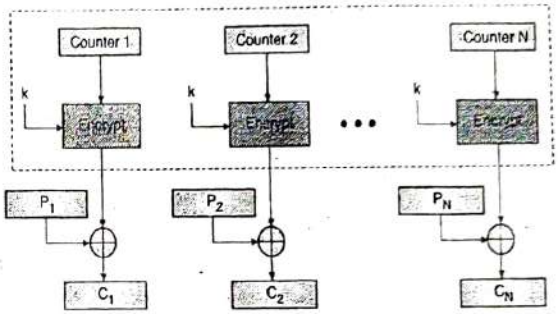


Fig. 2.14 : Counter (CTR) Encryption Process

During decryption process same counter is used as encrypted earlier and later XORed with ciphertext to get the original plain text plaintext.

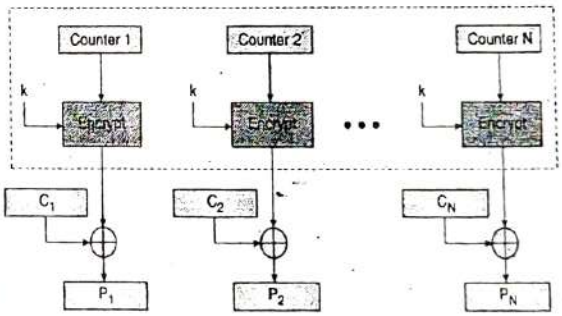


Fig. 2.15 : Counter (CTR) Decryption Process

The advantage of counter mode is that it can make execution speed up which can help in multiprocessing system.

Q. 20 Explain the operation of DES algorithm in detail.

Feb. 16(In sem.)

Ans.: Operation of DES algorithm

DES is block cipher published by National Institute of Standards and Technology (NIST). DES was originally developed by an IBM team formed in early 1970 in response to customer request for a method to secure data.

In 1973, NIST published a request for proposals for a symmetric key cryptography. A proposal from IBM, a change in the project called Lucifer, was accepted as DES. DES was

published in federal register in 1975 as a draft of the Federal Information Processing Standard (FIPS).

This draft was rejected because of small key length (56-bits), which could make ciphertext weaker to many attacks. Later on IBM developer mentioned that internal architecture of DES was designed to prevent cryptanalysis. Finally NIST published DES in January 1977 and defines DES as the standard for use in unclassified applications. The day onwards DES has been proven most widely used symmetric key cryptographic algorithm.

Q. 21 Explain Initial permutation steps in DES.

Ans.: Initial permutation steps in DES

Initial permutation is the process of rearranging or shuffling each bit of original plaintext block with any other random bit of same plaintext message block.

For example

First bit of original plaintext block replace with 48thbit of original plaintext block, the 2nd bit replaces with 57th bit, the 3rd bit replace with 59 and so on of original plaintext message shown in Table 2.2.

Table 2.2 : Initial permutation Plaintext block (64 bits)

48	57	59	63	8	9	43	64
47	42	10	6	4	11	13	18
20	5	16	19	32	1	25	27
2	3	23	29	30	31	34	7

This process called jugglery of bit position of plaintext block which is applied to all original plaintext blocks in a sequence. After initial permutation the 64-bit plaintext block get divided into two halves LPT (32-bit) and RPT (32-bit). Now 16 rounds of encryption process were completed on LPT and RPT.

Q. 22 Explain round function of DES algorithm in detail.

May 15

Ans. :

Step 1 : Key discarding process

We know that 56-bit key is used during encryption process. Here 56-bit key is transformed into 48-bit key by discarding every 8th bit of initial key i.e. 8th, 16th, 32nd ...

From this 56-bit key a different 48-bit sub-key is generated during each round the process called **key transformation**.

Step 2 : Expansion permutation process

As shown in Fig. 2.16 general steps of DES, we had two 32-bit plaintext called as Left Plaintext (LPT) and 32-bit Right Plaintext (RPT). In step 2 Right Plaintext is expanded from 32-bits to 48-bits the process called as **expansion permutation** (During this process bits are permuted hence called as expansion permutation) shown in Fig. 2.16.

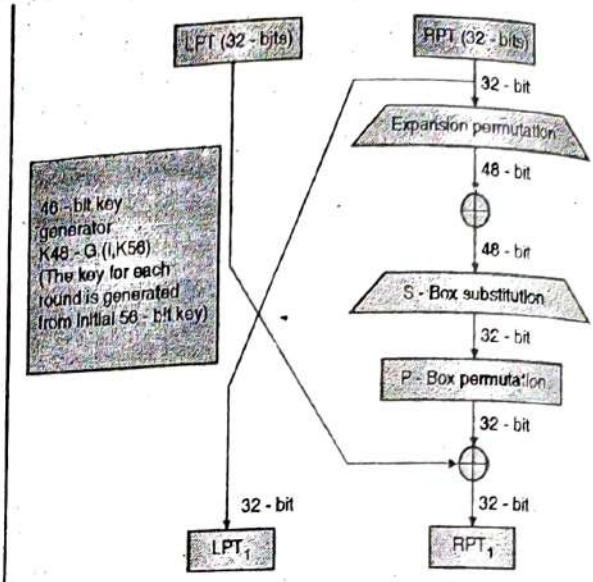


Fig. 2.16 : Expansion Permutation (Details steps of Single Round of DES Algorithm)

So it is clear that 32-bits of RPT get expanded to 48-bit which is XORed with 48-bit key generated during key discarding process. The resulting output of XOR operation is given to next step called as S-box substitution.

Step 3 : S-box substitution

S-box substitution is the process which accepts 48-bit key and expanded right plaintext of 48-bit which get XORed and produces 32-bit output as shown in Fig. 2.17.

S-box performs just jugglery on each bit positions and produces compressed bits. The substitution performed using 8 substitution boxes the reason called as S-boxes. The input for each S-box is 6-bit which produces output of 4-bit each. The output of S-box is then combined to form 32-bit block.

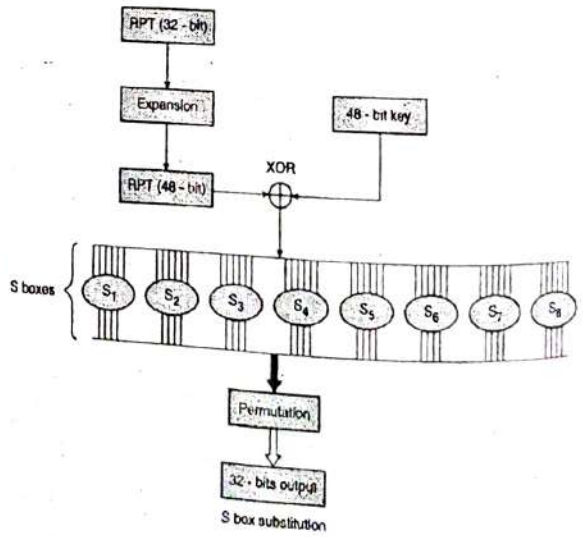


Fig. 2.17 : S-box substitution

Step 4 : P-box permutation

We know that the 32-bit output from eight S-boxes is then permuted, so that on the next round the output from each S-box

immediately affects as many others as possible. The output of S-box is input to P-box in which 32-bits are permuted using straight forward permutation mechanism i.e. replacement of each bit with another bit in the specified table called as P-box permutation.

Step 5 : XOR and swapping

Till this step we have performed all operations on 32-bit right plaintext only left plaintext was not touched yet. Recall step 2 as given in Fig. 2.16 detail steps of each round, output produced by P-box permutation get XOR with the left plaintext (32-bit) to produce the new 32-bit right plaintext. It is quite obvious that output of XOR operation becomes new right plaintext and the old right plaintext becomes new left plaintext, the complete process is called as XOR and swapping operations.

Q. 23 Write a short note on : Multiple DES.

Ans. : Multiple DES

Double performs the same operation as DES only difference is that double DES use two keys K1 and K2.

First it performs encryption on plaintext which is encrypted using K1 obtains first ciphertext again this ciphertext is encrypted by using another key called K2 and converted into final ciphertext.

Mathematically Double DES is represented as

$$Pt \Rightarrow EK1(Pt) \Rightarrow TEMP = EK1(Pt) \Rightarrow EK2(E(K1(P)))$$

$$\Rightarrow Cp = EK2(E(K1(Pt)))$$

Where, Pt = Plaintext

EK1(Pt) = Encrypted plaintext with Key K1

TEMP = EK1(Pt).

= Temporary Variable to store results

EK2(E(K1(P))) = Encrypted Results of first step using K2

Cp = Final Ciphertext.

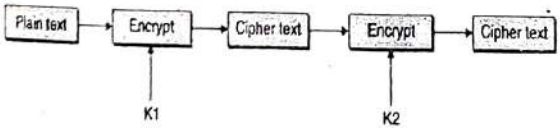


Fig. 2.18 : Encryption of Double DES

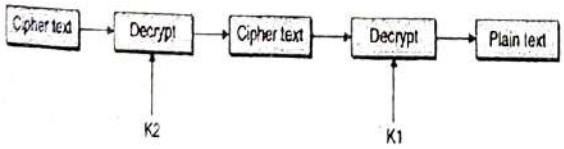


Fig. 2.19 : Decryption of Double DES

Decryption of Double DES is reverse of Encryption. Whatever the ciphertext obtained after double DES encryption process get decrypted using K2 and obtain the first ciphertext, the result of previous step (ciphertext) decrypted using K1 which yields the original plaintext. To decrypt the cipher text Cp and obtain the plain text Pt Double DES need to perform the following operation.

$$Pt = DK2\,(DK1(Cp))$$

Q. 24 Explain 3 DES algorithm in detail. **May 16**

Ans.: 3 DES algorithm

Triple DES performs the same operation as double DES only difference is that triple DES uses three keys K1, K2 and K3 while encrypting plaintext.

First it perform encryption on plaintext which is encrypted using K1 obtains first ciphertext again this ciphertext is encrypted by using another key called K2 which obtains the second ciphertext which is again encrypted using K3 and converted into final ciphertext Cp.

Mathematically, Double DES is represented as,

$$Pt \Rightarrow EK1(Pt) \Rightarrow TEMP = EK1(Pt) \Rightarrow EK2(E(K1(P)))$$

$$\Rightarrow EK3\,(EK2(EK1(Pt)))$$

$$\Rightarrow Cp = EK3\,(EK2(EK1(Pt)))$$

Where Pt = Plaintext

EK1(Pt) = Encrypted plaintext with Key K1

TEMP = EK1(Pt) = Temporary Variable to store results

EK2(E(K1(P))) = Encrypted Results of first ciphertext using K1

EK3 (EK2(EK1(Pt))) = Encrypted Results of second step using K2

Cp = EK3(EK2(EK1(Pt))) Final ciphertext encrypted using K1, K2 and K3

Decryption of Triple DES is reverse of Encryption.

The final ciphertext obtained after Triple DES encryption process get decrypted using K3 which results second ciphertext, second ciphertext decrypted using K2 which results first ciphertext, first ciphertext again decrypted using K1which generate the original plaintext Pt.

To decrypt the cipher text Cp and obtain the plain text Pt, we need to perform following operation.

$$Pt = DK3(DK2\,(DK1(Cp)))$$

DES used the three keys and other uses the two keys, There are two ways :

1. Triple DES with two keys
2. Triple DES with the three keys

Q. 25 Describe linear and differential cryptanalysis with suitable example. **May 16**

Ans. : Linear Cryptanalysis

Linear cryptanalysis first defined by Matsui and Yamagishi in 1992. It was extended by Matsui later in 1993 published a linear attack on DES.

Linear cryptanalysis is a known plaintext attack in which cryptanalyst access larger plaintext and cipher text messages along with encrypted unknown key.

In a linear cryptanalysis the role of cryptanalyst is to identify the linear relation between some bits of the plaintext, some bits of the cipher text and some bits of the unknown key. This relation helps cryptanalyst to understand the logic used during encryption and decryption of messages and to find how many bits of messages undergoes for encryption and decryption.

There are two basic approaches. The first is to use an approximation which relates some bits of plain text with some bits cipher text messages and user defined key in a linear way as mentioned earlier. The second focus on statistical analysis against one round of decrypted cipher text. The cryptanalyst decrypts each cipher text using all possible sub keys for one round of encryption and studies the resulting intermediate cipher text to analyze the random result. The sub key obtained during this process called as candidate key used during encryption and decryption of large amount of data.

Differential Cryptanalysis

Differential cryptanalysis is a method for breaking certain classes of cryptosystems. It was invented in 1990 by Israeli researchers **Eli Biham and Adi Shamir.**

Differential cryptanalysis is available to obtain clues about some bits of the key, thereby shortening an exhaustive search. By analyzing the changes in some chosen plaintexts, and the difference in the outputs resulting from encrypting each one, it is possible to recover some properties of the key.

Differential cryptanalysis is a chosen plaintext attack which identifies a relationship between cipher texts produced by same plain texts.

Differential analysis focuses on statistical analysis of two inputs and two outputs of a cryptographic algorithm. For example assume that the cipher text obtained from one exclusive-or operation of plain text and key.

Without knowing the value of the key, cryptanalyst can easily find the differences between plaintext and cipher text. Plaintext difference is represented by $P1 \oplus P2$ where as cipher text difference represented by $C1 \oplus C2$. The following proves that $C1 \oplus C2 = P1 \oplus P2$.

First cipher text C1 obtained = First plain text $P1 \oplus$ Key K

Second cipher text C2 obtained = Second plain text $P2 \oplus$ Key K if C1 and C2 obtained from XORing P1 and P2 and using Key K can represented by,

$$C1 \oplus C2 = P1 \oplus K \oplus P2 \oplus K = P1 \oplus P2$$

Differential cryptanalysis and linear cryptanalysis attacks are related to each other basically used in symmetric key cryptography. Whatever cipher text produced from same plain text the multiple rounds of encryption applied using sub key for each round.

Cryptanalyst studies changes to the intermediate cipher text obtained between multiple rounds of encryption. The attacks can be combined, which is called differential linear cryptanalysis.

Q. 26 Write a note on Strength of DES.

Ans.:

The strength of DES lies on two facts

1. The DES encryption technique ideally suited for implementation of hardware (bit shifts, lookups etc).
2. Dedicated hardware could run DES at 200 M byte/s.
3. Technique well suited for voice, video encryption.
4. DES uses 56-bit keys so that there are 2^{56} possible key combinations which is roughly equal to 7.2×10^{16} keys required to break DES cipher.
5. A machine performing one DES encryption per microsecond would take more than a thousand year to break the cipher.
6. If a small change in either plaintext or the key, the ciphertext should change markedly
7. The nature of algorithm : Cryptanalyst can perform cryptanalysis by exploiting the characteristic of DES algorithm but no one has succeeded in finding out the weakness.
8. It makes Brute force attack impractical as it use 56 keys during encryption there are 2^{56} possible keys which makes Brute Force attack impractical.

Q. 27 What is weak key in DES algorithm? Explain with example. **May 17**

Ans.:

1. Trying all possible combination of 2^{56} possible keys is not that much hard these days.
2. In an exhaustive search known plaintext attack, the cryptanalyst will obtain the solution after 2^{55} i.e. 3.6029×10^{16} trials on an average.
3. If you spend \$25 K you can build DES password crackers that will successes in few hours.
4. Two chosen input to an S-box can create the same output.
5. The purpose of initial and final permutation is not clear.

(1) A Brute Force Attack

In Brute force attack, cryptanalyst attempt to use all possible permutations and combinations on cipher text message to obtain corresponding plain text message. This attack trying every possible key until the correct translation of cipher text into plain text message is obtained.

It is most often used in a known plaintext or cipher text only attack. DES encrypt the block of data using 56 bit key. It is very easy to crack the encryption key using specialized hardware called Electronic Frontier Foundation's Deep Crack. Triple DES (168-bit key) was approved due to DES's weakness to brute force attacks, followed by the Advanced Encryption Standard (AES) in 2001.

(2) Meet-in-the-Middle Attack

This attack was introduced by Markle and Hellman. Meet-in-the-middle attacks can be used against cryptographic algorithms that use multiple keys for encryption. An example of a successful meet-in-the-middle attack is the attack against Double DES.

In order to improve the strength of 56 bit DES algorithm double DES concept was introduced having 112-bit key length and two rounds of DES encryption performed as well but still it is vulnerable against attack called as Meet-in-the Middle. In meet in the middle attack cryptanalyst have access to both plaintext message and its corresponding cipher text message.

For example, assume the plaintext is "Act," and the resulting double DES cipher text is "Dvy." The cryptanalyst wants to recover the two keys (called Key1 and Key2) used for encryption. The cryptanalyst first conducts a brute force attack on Key1 using all 256 different single DES keys to encrypt the plaintext of "Act" and saves each key and the resulting intermediate cipher text into a table.

Same method cryptanalyst conducts brute force attack on Key2, decrypting "Dvy" up to 2^{56} times. The cryptanalyst takes 2^{56} attempts, or a maximum of 2^{57} total attempts to decrypt the corresponding cipher text "Dvy". This is far easier than 2^{112} attempts as a result of the meet-in-the-middle attack; Double DES has not been widely used.

Q. 28 Draw AES block diagram and explain the steps in detail.

Ans. :

The plaintext given is divided into 128 - bit block as consisting of a 4 × 4 matrix of bytes. Therefore, the first four bytes of a 128 - bit input block occupy the first column in the 4 × 4 matrix of bytes. The next four bytes occupy the second column, and so on.

AES operates on a 4 × 4 column-major order matrix of bytes; called as ***state array*** shown in Fig. 2.20. AES also has the notion of a word. A word consists of four bytes that is 32 bits. The overall structure of AES encryption and decryption process is shown in Fig. 2.20.

The number of rounds are 10, is for the case when the encryption key is 128 bit long. (As mentioned earlier, the number of rounds is 12 when the key is 192 bits and 14 when the key is 256.)

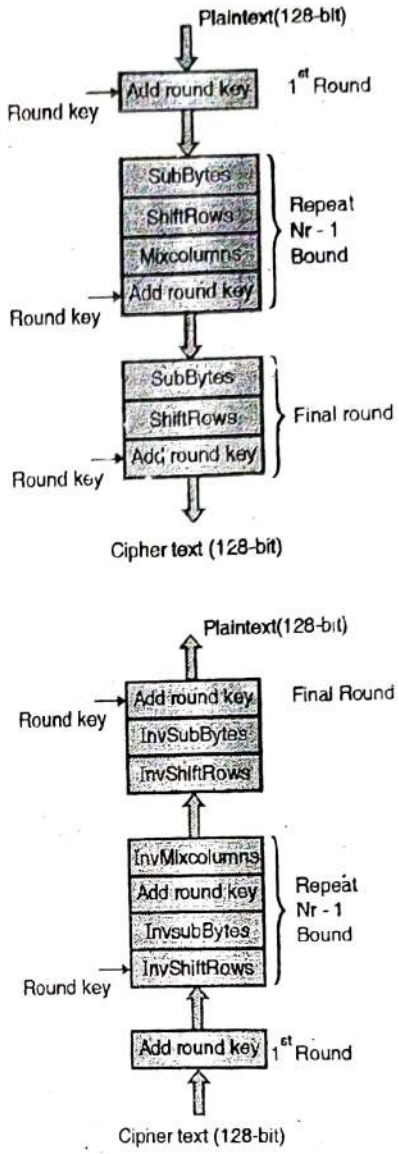


Fig. 2.20 : AES Encryption and Decryption process

Before any round-based processing for encryption can begin each byte of the state (plaintext) is combined with the round key using bitwise XOR operation. Nr stands for number of rounds.

AES divide plaintext into 16 byte (128-bit) blocks, and treats each block as a 4 × 4 State array. It then performs four operations in each round consists of several processing steps like substitution step, a row-wise permutation step, a column-wise mixing step, and the addition of the round key.

Except for the last round in each case, all other rounds are identical. Final Round doesn't have (MixColumns) it includes only SubBytes, ShiftRows and AddRoundKey. The process of transforming the cipher text back into the original plaintext using same encryption key is called as decryption process of AES, during decryption process the set of rounds are reversed.

Detail Steps for AES Encryption

For encryption, each round consists of the following four steps :

1. The SubByte step/Substitute byte

SubBytes() consists of replacement of each byte using a fixed S-box lookup table as shown in Fig. 2.21 to achieve non-linearity into the 4 × 4 state array (16 byte). It performs roughly the same function as the S- BOX in DES. It operates on each byte in the state and performs a non-linear substitution in the Galios Filed GF (2^8) field, which is what makes AES a non-linear cryptographic system.

X \ Y	0	1	2	3	4	5	6	7	8	9	a	b	C	d	e	F
0	63	7c	77	7b	F2	6b	6f	C5	30	1	67	2b	Fe	D7	Ab	76
1	ca	82	C9	7d	Fa	59	47	F0	Ad	D4	A2	Af	9c	A4	72	C0
2	b7	Fd	93	26	36	3f	F7	Cc	34	A5	E5	F1	71	D8	31	15
3	4	C7	23	C3	18	96	5	9a	7	12	80	E2	Eb	27	B2	75
4	9	83	2c	1a	1b	6e	5a	A0	52	3b	D6	B3	29	E3	2f	84
5	53	D1	0	Ed	20	Fc	B1	5b	6a	Cb	Be	39	4a	4c	58	Cf
6	D0	Ef	Aa	Fb	43	4d	33	85	45	F9	2	7f	50	3c	9f	A8
7	51	A3	40	8f	92	9d	38	F5	Bc	B6	Da	21	10	Ff	F3	D2
8	Cd	0c	13	Ec	5f	97	44	17	C4	A7	7e	3d	64	5d	19	73
9	60	81	4f	Dc	22	2a	90	88	46	Ee	B8	14	Be	5e	0b	Db
a	E0	32	3a	0a	49	6	24	5c	C2	D3	Ac	62	91	95	E4	79
b	E7	C8	37	6d	8b	D5	4e	A9	6c	56	F4	Ea	65	7a	Ae	8
c	Ba	78	25	2e	1c	A6	B4	C6	E8	Dd	74	1f	4b	Bd	8b	8a
d	70	3e	B5	66	48	3	F6	0e	61	35	57	B9	86	C1	1d	9e
e	E1	F8	98	11	69	D9	8e	94	9b	1e	87	E9	Ce	55	28	Df
f	8c	A1	89	0d	bf	E6	42	68	41	99	2d	0f	B0	54	bb	16

Fig. 2.21 : S-Box Lookup table for SubBytes

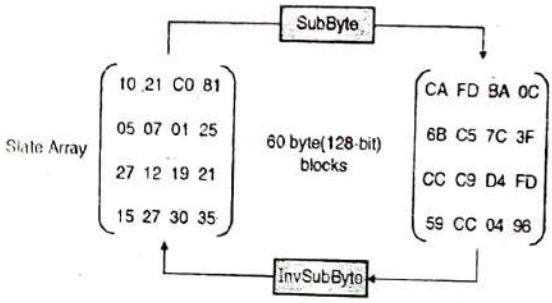


Fig. 2.22 : SubByte transformation

Fig. 2.22 shows the state transformation using SubBytes techniques and if apply reverse called as InvSubBytes transformation which will create original values. For every same two byte value the resulting transformation is also same. It also shows that the InvSubBytes transformation creates the original one. Note that if the two bytes have the same values, their transformation is also the same. The corresponding substitution step used during decryption is called InvSubBytes.

2. ShiftRows

The output of the SubByte transformation is input to the ShiftRows transformation which consists of rotation of each byte of the state array in the order of a row of data matrix (rotation of row byte positions are done in this step). Each byte of the first row remains unchanged. Each byte of the second row is rotate over one byte to the left position. Similarly the third and fourth rows are also rotated left by two and three position as shown in Fig. 2.23.

The corresponding transformation during decryption process is called Inverse shift row transformation (InvShiftRows).

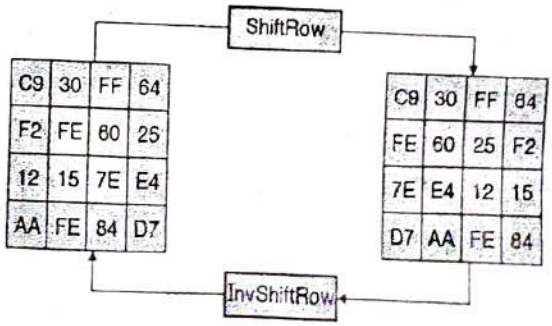


Fig. 2.23 : ShiftRows transformation

3. MixColumns

Mix Columns performs operation on the state array obtained from ShiftRows column-by-column and each column is multiplied with row of a fixed matrix. This step takes four bytes as an input and produces outputs of four bytes (each input byte affects the output bytes). The four numbers of state arrays of first column are modulo multiplied in Rijandeal's Galios Filed (GF) by a given matrix as shown in Fig. 2.24. In AES MixColumn step along with ShiftRows are primary source for providing complete diffusion to the cipher produced.

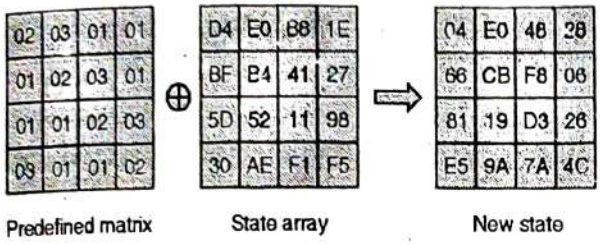


Fig. 2.24 : MixColumns transformation

From Fig. 2.24 on the left hand side, the row of the leftmost matrix is multiply with column of state array (XOR operations) which produces the new state. Perform the same operation on all columns which provides diffusion (mixing data within columns). The 4 bytes of each column in the State are treated as a 4-byte number and transformed to another 4-byte number via finite field mathematics (modulo multiplied in Rijndael's Galois Filed by a given matrix) as shown. MixColumns step is primary source of diffusion in AES.

4. AddRoundKey

In the AddRoundKey step, the Round key one generated using Rijndael's key schedule is combined with the new state obtained from MixColumns transformation state. The round key is added by combining each byte of the state array using bitwise XOR operations. The actual 'encryption' is performed in the AddRoundKey() function, when each byte of state array is XORed with the round key as shown in Fig. 2.25.

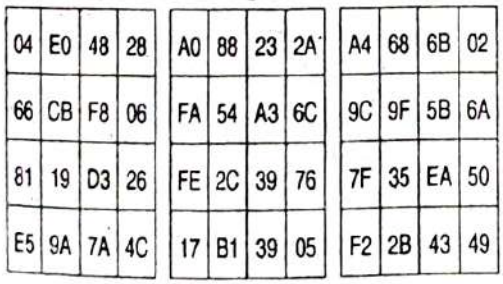


Fig. 2.25 : AddRoundKey

The same process of AddRoundKey is applied for nine rounds i.e Repeat SubByte, ShiftRows, MixColumns step and XOR with Round key 9 more times. Except for the last round in each case, all other rounds are identical. Final Round doesn't have MixColumns step it includes only SubBytes, ShiftRows and RoundKey.

Finally an output cipher text will obtain after performing detail steps of AES. A set of reverse rounds are applied (i.e.InvShiftRows, InvSubBytes, AddRoundKey and InvMixcolumns) to transform cipher text back into the original plaintext using the same encryption key called Decryption process of AES as shown in Fig. 2.25.

Q. 29 Differentiate AES and DES algorithms. **May 15**

Ans. :

Difference between AES and DES algorithms

Sr. No.	DES	AES
1.	Data encryption standard takes 64-bit plaintext as a input and creates 64-bit Ciphertext i.e. it encrypts data in block of size 64-bits per block.	It allows the data length (plain text size) of 128, 192 and 256 bits.
2.	In DES plaintext message is divided into size 64-bits block each and encrypted using 56-bit key at the initial level.	AES divide plaintext into 16 byte (128-bit) blocks, and treats each block as a 4 × 4 State array and supporting three different key lengths, 128, 192, and 256 bits.
3.	The left plaintext and right plaintext goes through 16 rounds of encryption process along with 16 different keys for each rounds.	The number of rounds are 10, is for the case when the encryption key is 128 bit long. (As mentioned earlier, the number of rounds is 12 when the key is 192 bits and 14 when the key is 256.)
4.	DES uses 56-bit keys so that there are 2^{56} possible key combinations which is roughly equal to 7.2×10^{16} keys required to break DES cipher.	AES is stronger than DES because of key size vary from round to round.
5.	Different versions of DES are double DES and triple DES is added.	AES doesn't have any future version.
6.	DES doesn't use Mix Column, Shift Rows method during encryption and decryption process	AES uses Mix Column, Shift Rows method during encryption and decryption process
7.	DES, double DES and Triple DES (168-bit key) are vulnerable to brute force attacks.	AES also are vulnerable to brute force attacks.

Q. 30 Using Playfair cipher encrypt message. "We five in a world full of 'beauty" use key "ANOTHER.

May 2017

Ans. : Keyword is ANOTHER.

In the first step all letters are to be filled in that matrix from left to right, the letters which are already been placed is not be placed again in that matrix. After filling up of the given letter, fill rest of the space in the matrix with the remaining letters alphabetically with no repetitions. The letters I and J will be considered as one letter. So If I is already placed then no need to place J in rest of the matrix.

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

By using Playfair Cipher (Use following steps to encrypt given word or message) we want to encrypt the plain text message **"We five in a world full of 'beauty"** using keyword domestic.

1. The plaintext received is to be broken in pair of two letters, if duplicate letter put x
2. we, fi, ve, in, aw, or, ld, fu, lx, lo, fb, ea, ut, yx
3. If both letters are same or only one letter is left then put X with that alphabet.
4. If both pair alphabet appears in same row replace the letter with the immediate right alphabet (wrapping around to the left side of the row if a letter in the original pair was on the right side of the row).
5. If both letters appear in same column replace it with alphabet immediate below to that letter (wrapping around to the top side of the column if a letter in the original pair was on the bottom side of the column).
6. If none of the condition explained above meet, then replace them with the letters on the same row respectively but at the other pair of corners of the rectangle defined by the original pair.
7. Refer above matrix for the same.

we→ Step 6 →rv

fi→ Step 5 →gk

ve→ Step 5 →af

in→ Step 6→go

aw→ Step 6 →nv

or→ Step 6 →bn

ld→ Step 4 →lu

fu→ Step 4 →lm

lx→ Step 5 →iz

lo→ Step 5 →hi

fb→ Step 6 →ie

ea→ Step 4 →ef

ut→ Step 6 →sh

yx→ Step 6 →zy

The plain text message **"We five in a world full of 'beauty"** encrypted as : rv gkaf go n vbnlu lm izh ii eefshzy.

Chap 3 : Public Key and Management

Q. 1 What is public key cryptography ?

April 17(In sem.)

Ans.: Public key cryptography

Public key cryptography also called as Asymmetric key cryptography. Two different keys are used during encryption and decryption process (one key is for encryption and second key is used at the time of decryption). RSA algorithm is the best example of asymmetric key cryptography. Basics of public key cryptography.

Q. 2 Write short on Principles of public key cryptosystem.

Ans.: Principles of public key cryptosystem

Public key cryptography involves use of two keys one is public key that may known to everyone and can be used to encrypt messages, and verify signatures. Other is private key known only to the receiver of the message or verifier, used to decrypt messages, and sign (create) signatures. It is also called as asymmetric key cryptography because one key is used for encryption only its corresponding key must be used for decryption. No other key can decrypt the message. The sender and receiver can encrypt messages using encryption key (public) or verify signatures, he cannot decrypt messages or create signatures because he required decryption key (private) which is known only to the receiver of the message.

Public key cryptosystem /asymmetric key cryptography is shown in Fig. 3.1.

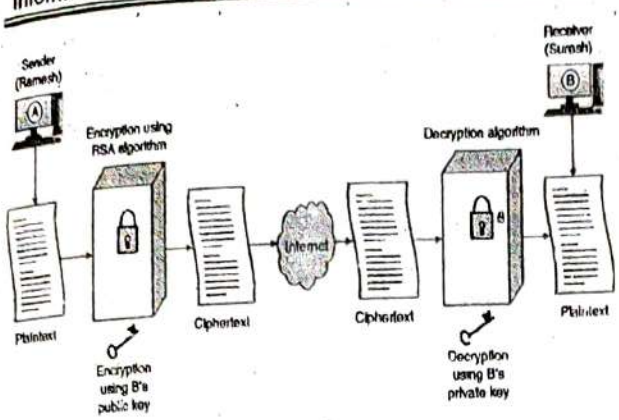


Fig. 3.1 : Public key cryptosystems

For example sender Ramesh wants to communicate with the receiver Suresh then they must have each one of this, i.e. private key and public key then and then communication will be successful.

Table 3.1 shows the possible pair of keys that Ramesh and Suresh must know while communicating with each other.

Table 3.1 : Pair of private and public keys

Key Details	Ramesh (A) Should know	Suresh (B) should know
Ramesh Private Key (A)	Yes A must know	Not known to B
Ramesh Public Key (A)	Yes A must know	Yes it is known to Suresh also
Suresh private key (B)	Not known to Ramesh (A)	Yes Suresh (B) must know
Suresh public key (B)	Yes known to Ramesh (A)	Yes Suresh (B) also known it

Following are the possible cases of public key cryptography as per the Table 3.1.

Case 1

1. When Ramesh wants to send a message to Suresh. Ramesh can encrypt the message using Suresh public key. This is possible because Ramesh and Suresh knows the public key.
2. Ramesh can send this message to Suresh (Keep in mind this it is encrypted using Suresh public key).
3. Suresh can decrypt the Ramesh message by using Suresh own private key. Because only Suresh knows his private key Ramesh is not aware about Suresh private key.
4. It is important to note that the message only decrypted using Suresh private key and nothing else.

Case 2

If Suresh wants send the message to Ramesh, then reverse the above case 1. Suresh can encrypt the message only with Ramesh public key.

The reason only Ramesh can decrypt the message to obtain its original plain text format using his private key.

Public key cryptography achieves authentication (authentication helps to identify the claimed identity of an entity, such as username password or any other important information such as encryption or decryption keys stolen during transmission between sender and receiver) and non-repudiation (it prevents either sender or receiver from denying a transmitted message).

Principles of public key cryptography is explained along with examples using a different technique which uses key pairs like Key Distribution Center, Digital Signatures, RSA (Rivest-Shamir-Aldeman) algorithm, Diffie-Hellman key exchange algorithm.

Q. 3 State Euclid's Algorithm with example.

Ans.:

It is a basic technique or a method for calculation of GCD of two positively integer.

Suppose we have two integers a, b such that d = gcd (a,b) assuming a > b > 0. Now dividing a by b we can state that

$$a = q_1 b + r_1 \qquad 0 \le r_1 < b \qquad ...(1)$$

Where q implies quotient and r implies remainder

Suppose that $r_1 \neq 0$ because b> r1, we can divide b by r_1 and apply division algorithm to obtain :

$$b = q_2 r_1 + r_2 \qquad 0 \le r_2 < r_1$$

if $r_2 = 0$ then $d = r_1$ and if $r_2 \neq 0$ then $d = \gcd(r_1, r_2)$.The division process continues till the remainder is 0.The following equation describes the process.

$$\begin{aligned}
a &= q_1 b + r_1 & 0 < r_1 < b \\
b &= q_2 r_1 + r_2 & 0 < r_2 < r_1 \\
r_1 &= q_3 r_2 + r_3 & 0 < r_3 < r_2 \\
&\vdots & \vdots \\
r_n - 2 &= q_n r_{n-1} + r_n & 0 < r_n < r_{n-1} \\
r_{n-1} &= q_{n+1} r_n + 0 & d = \gcd(a, b) = r_n
\end{aligned}$$

At each stage we have $d = \gcd(r_i, r_{i+1})$ finally $d = \gcd(r_n, 0) = r_n$ Thus, the greatest common divisor of two integers by repetitive can be calculated by repetitive application of the division algorithm. This is known as the Euclidean algorithm.

Euclid's algorithm : EUCLID (x, y)

1. $x \to x$, $y \to y$
2. If y = 0, return x = gcd (x, y)
3. R = x mod y
4. $x \leftarrow y$
5. $y \leftarrow R$
6. Go to 2.

Q. 4 Explain RSA algorithm used for public key cryptography. **April 17(In sem.)**

Ans.:

Ron Rivest, Adi Shamir and Len Aldeman have developed this algorithm (Rivest-Shamir-Aldeman) in 1978. It is a public-key encryption algorithm. It is a block-cipher which converts plain text into cipher text at sender side and vice versa at receiver side.

The algorithm works as follows

1. Select two prime numbers a and b where $a \neq b$.
2. Compute $n = a * b$ (n is used as the modulus for both the public and private keys)
3. Compute $\phi(n) = (a - 1) * (b - 1)$.
4. Select e (public key) such that, e is relatively prime to $\phi(n)$ i.e. gcd $(e, \phi(n)) = 1$ and $1 < e < \phi(n)$.
5. Calculate d (private key) such that, $d = e^{-1} \bmod \phi(n)$ or $ed \bmod \phi(n) = 1$.
6. Public key = {e, n}, private key = {d, n}.
7. Compute cipher text using,

   $C = P^e \bmod n$ where, $P < n$ where C = Cipher text,

   P = Plaintext, e = Encryption key
8. Compute Plaintext P using the given formula.

   $P = C^d \bmod n$.

   Where, d = decryption key.

Both sender and receiver know the value of n. In addition, the sender must know encryption key 'e' and receiver must know decryption key 'd'.

For example

1. Select two prime numbers a = 13, b = 11.
2. $n = a*b = 13 * 11 = 143$.
3. $\phi(n) = (13 - 1) * (11 - 1) = 12 * 10 = 120$.
4. Select e such that, e is relatively prime to $\phi(n)$ i.e. gcd $(e, \phi(n)) = 1$ and $1 < e < \phi(n)$ e is selected as 13, gcd $(13, 120) = 1$.
5. **Finding d**

   $e*d \bmod \phi(n) = 1$; $\quad 13 * d \bmod 120 = 1$

   d is calculated using following method. Do the following procedure till you are not getting a integer numbers

$$d = \frac{(\phi(n) * i) + 1}{e}$$

$$d = \frac{(120 + 1)}{13} = \frac{121}{13} = 9.30 \ (i = 1)$$

where, $i = 1$ to 100

$$= \frac{240 + 1}{13} = \frac{241}{13} = 18.53 \ (i = 2)$$

$$= \frac{360 + 1}{13} = \frac{361}{13} = 27.76 \ (i = 3)$$

$$d = \frac{480 + 1}{13} = \frac{481}{13} = 37$$

Hence $\quad d = 37$

6. Hence public key = {13, 143} and

   Private key = {37, 143}

7. **Encryption**

Plain text message (P) which is in binary format converted into integer.

Here P is selected as 13 such that $P < n$

$\because (13 < 143)$

Now, $\quad C = P^e \bmod n = 13^{13} \bmod 143$

Here to find out 13^{13} mod 143, use the following procedure

$$13 \bmod 143 = 13$$

$$13^2 \bmod 143 = 169 \bmod 143 = 26$$

$$13^4 \bmod 143 = 26^2 \bmod 143 = 104$$

$$13^8 \bmod 143 = 104^2 \bmod 143 = 91$$

$$\therefore C = [(13^8 \bmod 143) * (13^4 \bmod 143) * (13 \bmod 143)] \bmod 143$$

$$= [91 * 104 * 13] \bmod 143 = 52$$

8. **Decryption**

To decrypt given plain text message we must know the C and d.

$$P = C^d \bmod n = 52^{37} \bmod 143$$

Again use above mentioned procedure to find out 52^{37} mod 143. As

$$52 \bmod 143 = 52$$

$$52^2 \bmod 143 = 130$$

$$52^4 \bmod 143 = (130)^2 \bmod 143 = 26$$

$$52^8 \bmod 143 = (26)^2 \bmod 143 = 104$$

$$52^{16} \bmod 143 = (104)^2 \bmod 143 = 91$$

$$52^{32} \bmod 143 = (91)^2 \bmod 143 = 130$$

Hence, $\quad P = 52^{37} \bmod 143$

$$= [(52^{32} \bmod 143) * (52^4 \bmod 143) * (52 \bmod 143)] \bmod 143$$

$$= [130 * 26 * 52] \bmod 143 = 13$$

Q. 5 Prime number p = 3, q = 11, e = 3, m = 00111011 (m-message) then calculate private key d and cipher text C. **May 15**

Soln. : Use RSA Algorithm

Step 1 : Prime numbers $p = 3$, $q = 11$

Step 2 : $n = p * q = 33$

Step 3 : $\phi(n) = (p-1)*(q-1) = (3-1)*(11-1)$

$= 2*10 = 20$

Step 4 : Select e such that it is relatively prime to ϕ (n) i.e. $\gcd(e, \phi(n)) = 1$

$\gcd(e, 20) = 1$

$\gcd(3, 20) = 1$

$e = 3$ is given.

Step 5 : Calculate d such that

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

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

$3 * d \bmod 20 = 1$

$$d = \frac{(\phi(n) * i) + 1}{e}$$

Find d such that it is divisible by e.

Where $i = 1$ to 9

$$d = \frac{(20 \times i) + 1}{3} = \frac{(20 \times i) + 1}{3} = \frac{21}{3} = 7$$

$d = 7$

Step 6 : Public key = $\{e, n\} = \{3, 33\}$

Private key = $\{d, n\} = \{7, 33\}$

Step 7 : Calculate cipher text message for given plain text message.

Plain text message given in binary 00111011 which can be written as 59.

Binary to decimal conversion

$00111011 \Rightarrow 59$ (P = 59)

$c = P^e \bmod n$ where $P < n = 59^3 \bmod 33$

$= [59^2 \bmod 33] * [59 \bmod 33] \bmod 33$

$= 348! \bmod 33 * [59 \bmod 33] \bmod 33$

$c = [16 * 26] \bmod 33$

$c = 20$

Step 8 : Calculate plain text message.

$P = c^d \bmod n = 20^7 \bmod 33$

$P = [20^4 \bmod 33] * [20^3 \bmod 33] \bmod 33$

$= [20^2 \bmod 33] * [20^2 \bmod 33] * [20^2 \bmod 33] * [20^1 \bmod 33] \bmod 33$

$= [400 \bmod 33] * [400 \bmod 33] * [400 \bmod 33] * [20 \bmod 33] \bmod 33$

$= [4] * [4] * [4] * [20] \bmod 33 = 1280 \bmod 33$

$P = 26$

Q. 6 For the given parameters 'P' = 3 and 'Q' = 19 find the value of 'e' and 'd' using RSA algorithm and encrypt message 'M' = 6. **Feb.16(In sem.)**

Soln. :

Step 1 : Prime numbers are P = 3 and Q= 19 we are denoting P and Q as a = 3, b = 19

Step 2 : $n = a * b = 3 * 19 = 57$

Step 3 : $\phi(n) = (a-1).(b-1)$

$= (3-1)*(19-1)$

$= 2*18 = 36$

Step 4 : Select e such that it is relatively prime to ϕ (n) i.e. $\gcd(e, \phi(n)) = 1$ $1 < e < \phi(n)$ e is selected as 5, gcd (5, 36) = 1.

Here gcd(5,36) = 1 One can select e as 7 because 7 is also relatively prime to ϕ (n).

It better if you select large private key therefore we will select e as 7.

$\gcd(7,36) = 1$

Step 5 : Calculate d such that

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

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

$7 * d \bmod 36 = 1$

Using RSA algorithm

$d = ((\phi(n) * i) + 1)/7$ where i = 1 to 100

$= ((36*1) + 1)/7 = 5.28$

d must be completely divisible by 'e'.

$= ((36*2) + 1)/7 = 10.42$

$= ((36*3) + 1)/7 = 15.57$

$= ((36*4) + 1)/7 = 20.71$

$= ((36*5) + 1)/7 = 25.85$

$= ((36*6) + 1)/7 = 31$

$d = 31$

Step 6 : Public key = $\{e, n\} = \{7, 57\}$

Private key = $\{d, n\} = \{31, 57\}$

Step 7 : Calculate cipher text message for given plain text message m = 6.

Plain text denoted as p = 6 (m denoted as p)

$C = P^e \bmod n$

$= 6^7 \bmod 57$

$= 279936 \bmod 57$

$C = 9$

Step 8 : Now calculate plain text P. Once sender sends 9 to the receiver then receiver can calculate plain text p.

$P = C^d \bmod n$

$= 9^{31} \bmod 57 = 6$

Decryption process always yields original message / plain text i.e. = 6

$\therefore P = 9^{31} \bmod 57 = 6$

$P = 6$

Q. 7 Explain the key distribution scenario using public key algorithm.

Ans.:

(1) Simple Secret Key Distribution

If P wants to communicate with Q, following procedure is used shown in Fig. 3.2.

1. P generates a public key/private key pair and transmits a message to Q consists of public key (PU_P) and identifier P (ID_P).
2. Q generates a session key K_s and encrypted using P's public key (PU_P) and transmits to P.
3. P decrypts the session key K_s by using its own private key. Now both P and Q know K_s.
4. P discards public/private key and Q discards P's public key.

At the end of communication both P and Q discards K_s. The communication is secure from eavesdropping. The communication becomes unsafe from man-in-middle attack.

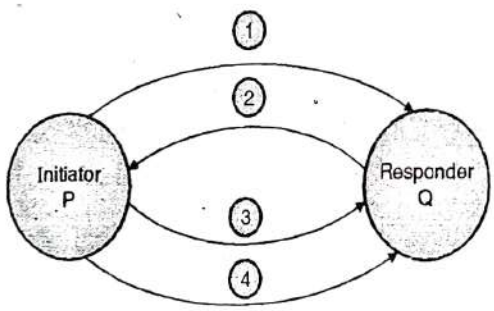


Fig. 3.2 : Distribution of Secret Keys using Public-key Cryptography

(2) Secret Key Distribution with Confidentiality and Authentication

1. P sends encrypted message using Q's public key consists of identifier of P (ID_P) and none N_1.
2. Q sends an encrypted message using P's public key consists of P's nonce N_1 and Q's nonce N_2.
3. P returns N_2, encrypted using Q's public key to Q.
4. P selects a secret key K_S and send a message $M = E(PU_Q, E(PR_P, K_S))$ to Q.
5. Q decrypts it to recover the secret key.

(3) Hybrid Schemes

This technique retains the use of KDC (Key Distribution Center) key Distribution Center that shares a secret master key with each user and distributes secret session keys encrypted with the master key.

Public key is used to distribute the master key.

Q. 8 Which techniques are used for the distribution of public keys?

Ans.:

Following techniques are used for the distribution of public keys :

1. Public Announcement

In a public key cryptography, such as RSA, any user can send his or her key to any other user or broadcast it to the group as shown in Fig. 3.3.

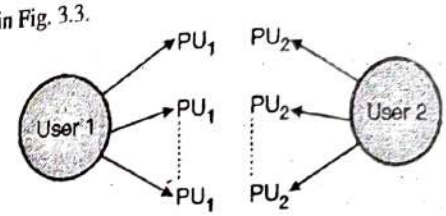


Fig. 3.3 : Public Announcement

This type of approach is having a biggest drawback. Any user can pretend to be a user P and send a public to another user or broadcast it. Until user A has got this thing and alerts to other user, a pretender is able to read all encrypted messages for user P.

2. Publicly Available Directory

A dynamic publically available directory is used to achieve the security. Maintenance and distribution of public directory is controlled by a trusted entity.

This technique is explained as follows and shown in Fig. 3.4.

(a) A trusted entity maintains a directory for each user as < name, public key >

(b) Each user has to register a public key with the directory.

(c) A user can replace the existing key with a new one at any time for any particular reason.

Fig. 3.4 : Publicly Available Directory

It is more secure than public announcement but still having some weaknesses. A hacker can obtain the private key of directory or tamper with the information kept by directory.

3. Public Key Authority

It gives stronger security. As shown in the Fig. 3.5, a central authority keeps a dynamic directory of public keys of all users. Additional, each user knows the public key of authority.

Working of this techniques explained by following steps :

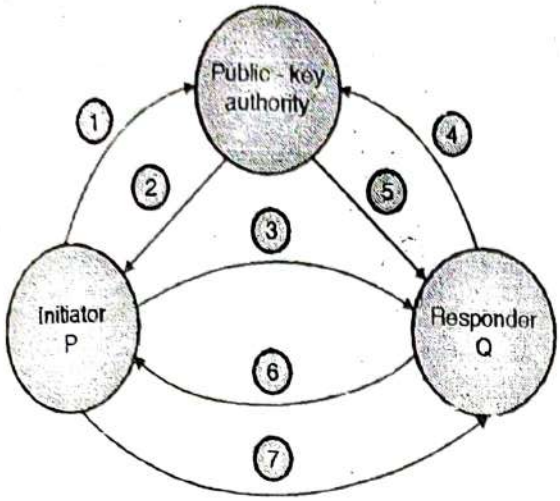


Fig. 3.5 : Public Key Authority

Steps

1. P sends a time stamped request to authority for public key of Q.
2. A authority sends an encrypted message. A message is encrypted using authority's private key, so that P can be decrypt it by using authority's public key. A message includes Q's public key which can be use by P for the encryption, the original request sends by P with the time stamp.
3. P uses Q's public key for an encryption and send an encrypted message to Q. An encrypted message contains the Identity of A (ID_P) and nonce (N_1), which is used to identify the transmission uniquely.

4& 5 Q retrieves P's public key from the authority similarly like 1 and 2. Now P and Q start the communication. Two additional steps may be requiring.

6. Q sends an encrypted message to P. A message encrypted using P's public key which contains P's nonce N_1 and Q's nonce N_2.
7. P in return sent an encrypted message using Q's public key which contains Q's nonce N2, to ensure Q that its correspondent is P.

4. Public - Key Certificates

A public key authority has some drawbacks in the system. If a user has to communicate with authority for a public key for every other user that he wishes to contact. This approach provides certificates to users for exchanging the keys among them without contacting to the authority. The data and public key maintained by authority itself may be vulnerable to the tampering.

The certificate authority shown in Fig. 3.6 is a government agency or trusted agency.

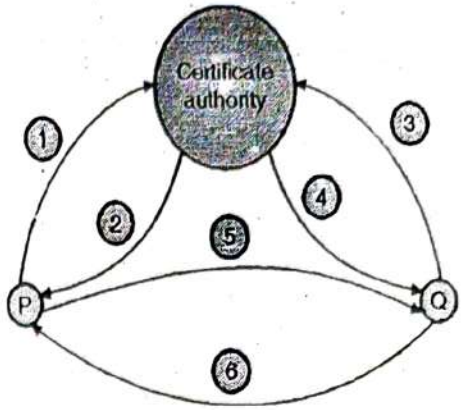


Fig. 3.6 : Public - Key Certificates

Steps

1. User 'P' sends its public key to the certificate authority to get the certificate.
2. A certificate authority sends a certificate in a encrypted form using its private key. A certificate consists of timestamp, identifier of P (ID_P) and public key of P.

3 & 4. Q retrieves its certificate from the authority similarly explained in 1 and 2.

5. P publishes its certificate Cp to anyone (Q) needed P's public key.
6. Similarly Q also publishes its certificate C_Q to anyone (P).

Then the communication between P and Q is started.

Q. 9 Explain the key distribution method.

Ans.: key distribution method

Key Distribution also called as Key Transportation is the process by which keys are securely distributed from the location where they are generated or stored to where there be use of it then transmitted using manual transmission methods (e.g., file transfer, key loaders), automated methods (e.g., key transport and/or key agreement protocols), or a combination of automated and manual methods.

Secure key distribution is the basic aim to achieve the integrity and trust in any cryptographic system.

The goal of any key distribution process is :

To ensure that the keys are distributed to intended recipients only.

To ensure that the keys sent are the correct keys and sent to correct recipient.

To ensure that the keys achieving authentication and protection of recipient.

To ensure that it is not modified during transmission.

To ensure that transmission mechanism is secure and intact.

Q. 10 Explain "Diffie-Hellmen" key exchange algorithm with suitable example. **Feb. 16(In sem.)**

Ans. : "Diffie-Hellmen" key exchange algorithm

The **Diffie Hellman** algorithm was widely known as Key exchange algorithm or key agreement algorithm developed by Whitfield *Diffie* and Martin *Hellman* in 1976. Diffie Hellman algorithm is used to generate same (symmetric) private cryptographic key at sender as well as receiver end so that there is no need to transfer this key from sender to receiver.

Remember that Diffie Hellman algorithm is used only for key agreement not for encryption or decryption of message. If sender and receiver want to communicate with each other they first agree on the same key generated by Diffie Hellman Algorithm later on they can use this key for encryption or decryption.

Steps of Diffie Hellman Algorithm

1. The first step is that if Ramesh wants to communicate with Suresh they must agree on two large prime numbers p and q.
2. Ramesh selects another secret large random integer number a, and calculate R such that

$$R = q^a \bmod p$$

3. Ramesh sends this R to Suresh.
4. Suresh independently selects another secret large random integer number b, and calculate S such that.

$$S = q^b \bmod p$$

5. Suresh sends the number S to Ramesh.
6. Now Ramesh is calculating his secret key by using $R_K = S^q \bmod p$
7. Suresh is calculating his secret key S_K by using

$$S_K = R^b \bmod p$$

8. If $R_K = S_K$ then Ramesh and Suresh can agree for future communication called as key agreement algorithm.
9. We have $R_K = S_K = K$ hence proved. (K is called symmetric key).

For example

1. Ramesh and Suresh are agree on two large prime numbers say p = 17 and q = 7.
2. Ramesh selects another secret large random number 5 i.e. a = 5 and calculate R such that

$$R = q^a \bmod p = 7^5 \bmod 17 = 11$$
$$= (7 \times 7 \times 7 \times 7 \times 7) \bmod 17 = 11$$

3. Ramesh sends number R to Suresh.
4. Suresh selects another secret large random number 3. i.e. b = 3 and calculate s such that

$$S = q^b \bmod p = 7^3 \bmod 17 = 3$$
$$= (7 \times 7 \times 7) \bmod 17 = 3$$

5. Suresh sends number S to Ramesh.
6. Ramesh now calculates its secret key R_K as follows :

$$R_K = S^a \bmod p = S^5 \bmod 17$$
$$\therefore R_K = 3^5 \bmod 17 = 5$$
$$= (3 \times 3 \times 3 \times 3 \times 3) \bmod 17 = 5.$$

7. Suresh is calculating his secret key S_K as follows :

$$S_K = R^b \bmod p = R^3 \bmod 17$$
$$= 11^3 \bmod 17 = 5$$

8. If $R_K = S_K$ then Ramesh and Suresh can agree for future communication.
9. We know that if $R_K = S_K = K = 5$. Hence proved.

Q. 11 Explain man-in-middle attacks.

Ans. : Man-in-middle attacks

Diffie Hellman key exchange algorithm creates one discrepancy called as man-in-the middle attack. Man-in-the middle attack also called as bucket brigade attack.

For example : Ramesh wants to communicate with Suresh using Diffie Hellman key exchange algorithm. First Ramesh and Suresh agree on two large prime no's p = 11, q = 7.

This secure communication between Ramesh and Suresh. If third person is listening this conversation quietly and modifying then original contents of the Message / values, the name of the third person called as attacker / cryptanalyst is Gaffar third person.

Gaffar hacked this conversion which going on in between Ramesh and Suresh and selected prime number p = 11, q = 7 (Because he intercepted the conversions he knows everything) and forwarded it to Suresh.

Ramesh	Gaffar	Suresh
p = 11, q = 7	p = 11, q = 7	p = 11, q = 7

Case 1 : Is of man-in-the middle attack

As per steps mention in Diffie Hellman algorithm. After selection of two large prime numbers, next step is to select random numbers a and b as shown below:

Ramesh	Gaffar	Suresh
a = 3	a = 8, b = 6	b = 9

Case 2 : Is of man-in-the middle attack

As mentioned in step why Gaffar selected two values of a and b. Ramesh and Suresh is calculating value of R and S (The values required to calculate the secret key after selecting random values refer Diffie Hellman algorithm steps) then, similar way Gaffar is also calculating value of R and S at his end.

Refer Diffie Hellman Algorithm to calculate value of R and S(p = 11, q = 7).

$R = q^a \bmod p$ $= 7^3 \bmod 11$ $= 343 \bmod 11$ $= 2$	$= 7^8 \bmod 11$ $= 5764801 \bmod 11$ $= 9$ $S = q^b \bmod p$ $= 7^6 \bmod 11$ $= 117649 \bmod 11$ $= 4$	$S = q^b \bmod p$ $= 7^9 \bmod 11$ $= 40353607 \bmod 11$ $= 8$

Case 3 : Man-in-the middle attack

Here is the actual twists occurs, after calculating values of R and S with Ramesh, Gaffar and Suresh are shown below :

Ramesh	Gaffar	Suresh
R = 2	R = 9 and S = 4	S = 8

Ramesh is sending the value of R = 2, to Suresh during their communication. Gaffar now intercepting the actual Communication between Ramesh and Suresh and sending his own values of R = 9 to Suresh. After receiving value of R = 9 from Gaffar (Suresh doesn't aware that Gaffar has sent it) Suresh sending his value of S = 8 to Ramesh (Actually it was intercept by Gaffar).

In return Gaffar sends his own value of S = 4 to Ramesh, so following are the new values of R and S with Ramesh, Gaffar and Suresh.

Ramesh	Gaffar	Suresh
R = 2, (Original) S = 4 (After Gaffar Interception)	R = 2, S = 8 His own value of R and S	S = 8 (Original Value) R = 9 (After Gaffar interception)

Case 4 : Man-in-the middle attack

Based on above values Ramesh, Gaffar and Suresh calculating secret key R_k and S_k for future communication.

Ramesh	Gaffar	Suresh
(S = 4, a = 3) $R_k = S^a \bmod p$ $= 4^3 \bmod 11$ $= 64 \bmod 11$ $= 9$	(S = 8, R = 2, a = 8, b = 6) [Gaffar own values $R_k = S^a \bmod p$ $= 8^8 \bmod 11$ $= 16777216 \bmod 11$ $= 5$ $S_k = R^b \bmod p$ $= 2^6 \bmod 11$ $= 64 \bmod 11$ $= 9$	(R = 9, b = 9) $S_k = R^b \bmod p$ $= 9^9 \bmod 11$ $= 387420489 \bmod 11$ $= 5$

Case 5 : Man-in-the middle attack

Ramesh is thinking that secret key value is 9 after sending his secret key to Suresh. Suresh also thinking that the value of secret key is 5 but it is actually intercepted by Gaffar.

During transmission of actual messages, Ramesh sending his secret key $R_k = 9$ to Suresh because of man-in-the middle attack Gaffar sending his secret key 5 to Suresh. In return when Suresh sending his secret key $S_k = 5$, Gaffar is sending his secret key 9 to Ramesh shown in case 5.

Both are not aware the actual communication was done in between Ramesh and Gaffar, Gaffar and Suresh. Here the sender and receiver not aware that the integrity (after sender sends it and before it reaches to intended recipients original contents gets modified) of the message is lost. Because of interception sender and receiver not aware that third person listening their communication such type of attack is called as **man-in-the middle attack.**

Q. 12 Describe elliptic curve cryptography. **Dec. 16**

Ans. : Elliptic curve cryptography

Elliptic Curve Cryptography (ECC) is evolved as an alternative to traditional public-key cryptosystems like Rivest Shamir Adelman, Digital Signature Algorithm and Diffie Hellman. ECC provides equivalent security with smaller key size i.e.160-bits whereas RSA uses 1024 bits.

ECC results in faster computations, lower power consumption, as well as it saves memory and bandwidth utilization. ECC was developed by Neal Koblitz and Victor S. Miller in 1985 which use the elliptic curves in cryptography. The Elliptic curve cryptography (ECC) is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. Since 1985, ECC has received intense scrutiny from cryptographers, mathematicians, and computer scientists around the world. In ECC there is a no significant weaknesses have been found and it also achieves the high confidence in the security of ECC. ECC become more powerful and attractive rather than RSA and DSA.

Top standard agencies such as ANSI, IEEE and ISO certified that ECC has been gaining popularity over past few years.

An elliptic curve is the set of solutions of an equation of the form

$$y^2 = x^3 + ax + b$$

where a, b $\in$ K and $-16(4a^3 + 27b^2) \neq 0$.

The condition that $4a^3 + 27b^2 \neq 0$ implies that the curve has no "singular points", which will be essential for the applications.

Each value of the 'a' and 'b' gives a different elliptic curve. An equation of this kind can be studied over various mathematical structures, such as a ring or a finite field. One interesting property

of elliptic curve is that it forms a group which enables us to do Cryptography.

The public key is a point in the curve and the private key is a random number as shown in Fig. 3.7. The public key is obtained by multiplying the private key with the generator point G in the curve.

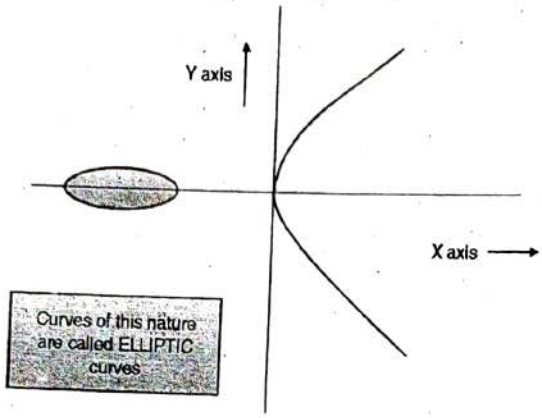


Fig. 3.7 : Graphical representation of Elliptical curve cryptography

Q. 13 What is authentication? Explain various methods for authentication.

Ans.: Authentication

One of the most complex as well crucial areas of the cryptography is message authentication. Message authentication mechanisms help to prove to the identity of the sender of the message.

Authentication mechanisms ensure that who sends the message i.e. origin of an electronic message is correctly identified. Following are possibility of attacks while communication across the network or between sender and receiver.

1. Traffic Analysis

In this type of attack while sending a confidential mail from sender to receiver make size that the original message should be an encrypted form, otherwise it is very easy to attacker to observe the patterns of those message. Such type of attack is called traffic analysis. Passive attacks are very difficult to detect because they do not involve any modification to the actual data. More focus required on such type of attacks are prevention rather than detection.

2. Masquerade Attack

Masquerade is an attack that a user pretends identification such as showing himself as a legitimate user to gain the access of personal computer. Such type of attack involves pretending the user from accessing authorized information.

3. Replay attack (Rewrite)

It is a network attack in which original data get modified and new malicious code added into valid data, during transmission. The newly generated malicious code retransmitted again and again to receiver called as replay attack (Reusing information).

Replay attack involve the passive capture of data and it's subsequent retransmission to produce an unauthorized effect. Proper authentication mechanism helps here to prove user identity.

4. Modification

Modification is also called replay attack. When contents of message modified after sender sends it but before it reaches to indented recipients, such type of attack is called modification of message.

For Example

Ramesh wants to transfer amount of Rs.1000/- into Suresh account, during this transmission process an attacker called Deepesh eavesdrop the conversation and modified the actual amount of Rs.1000/- and sends just Rs. of 100/- into Suresh account. The case happened here contents of message get altered during transmission process such type of attack called modification. In this case Integrity of original message is lost.

5. Replay Attack

Replay attack involve passive capturing of data and retransmission of subsequent information in order to create unauthorized effect. This is network type of attack in which valid data transmission is fraudly repeated or delayed.

For example

Ramesh sending confidential information to Suresh an attacker called Deepesh capturing confidential information and retransmitting it to Suresh after a long time. Here Deepesh can mismatch the confidential information and later on replay to Suresh (Deepesh reusing information). Proper authentication mechanism helps here to prove user identity.

6. Non-Repudiation

Principle of non-repudiation states that if sender sends some information and later on he denied that he never sends that information called non-repudiation.

For example

Ramesh sends a request to bank about money transfer into Suresh account but later on Ramesh denying the money transfer request to bank. Principle of non-repudiation does not allow such type of refuses of sender. Non-repudiation prevents either sender or receiver from denying a transmitted message.

Q. 14 Explain various methods for authentication.

Ans. : Authentication Methods

1. Hash Function

The process of transforming input message m into a fixed size string (called as hash value h) is called as hash function and it is denoted by H. Fixed size hash value act as a authenticator.

2. **Message encryption**

The cipher text produced after encryption act a authenticator.

3. **Message Authentication Code (MAC)**

MAC ensures that only receiver can identify the original message. The Message Authentication Code (MAC) is a small fixed-size block of data that is generated based on a message M of variable length using secret key K. The fixed size block that serves as the authenticator. Following sections introduces the details on above three functions.

Q. 15 Explain cryptographic hash function.

Ans. : Cryptographic hash function

In **hash function H** accepts a variable length block of input data called as 'M' and produces the fixed size hash value can be represented as :

$$h = H(M)$$

A good has function provides a property that hash function is applied on large amount of data input (M) and then it produces the fixed amount of output data. If any bit or bits changes in the data, then whole hash function output data will also change.

When hash function provides security application this is called cryptographic hash functions. Cryptographic has function is one of the algorithm which is computationally infeasible. Input is padded with some fixed out of length (For e.g. 1024 bits). It includes original message in bits and padding bits.

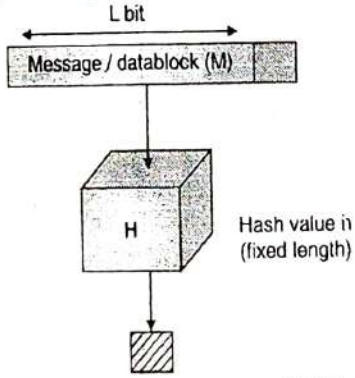


Fig. 3.8 : Block Diagram of Cryptographic Hash Function

Because of these securities will provided, the length field produces difficulty for the attacker to create alternative message with the same hash value. Cipher Block chaining is mostly used for to implementing cryptographic Hash function, whirlpool is another popular cryptographic hash function.

Cryptographic hash algorithm is applied on original message when padding is done. In padding fix variable length input is added like 1024 bits. After this hash function algorithm is applied so it creates a Hash value h.

Q. 16 How message authentication code can be used to achieve message authentication and confidentiality ?

Ans. :

Most adaptable cryptographic algorithm is the cryptographic hash function. It is mostly used in Internet protocol and security application.

Following are some application which are used in Cryptographic Hash Function :

1. **Message Authentication**

Message Authentication is a nothing but service that verify or checks the integrity of that message. Message Authentication checks that the data received from sender which is exactly same as sent to receiver. (i.e. content of the data will be same no modification will have done or insertion deletion or updation).

Some authentication provides a mechanism that checks identity of sender is valid or not. When Hash Function provides a value, which is used for message authentication purpose then that value is invoked as Message Digest (MD). The Fig. 3.9(a), describes how many approaches in which a hash code can be helps to provide the message authentication.

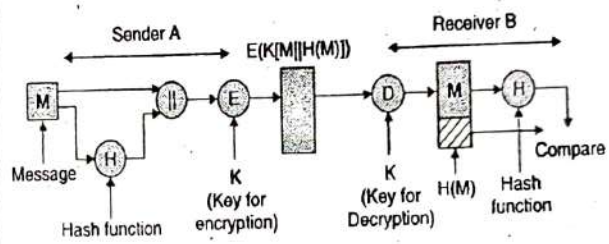


Fig. 3.9(a)

(a) Message added with hash code that encrypted using symmetric encryption. Sender A and receiver B shares the same secret key, A message is come from sender A that must not be changed. After that hash code provides a security or structure to active authentication.

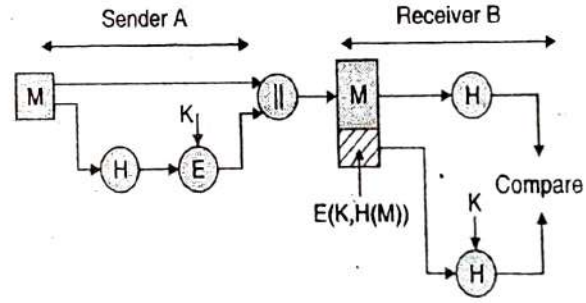


Fig. 3.9(b)

(b) Hash code is encrypted using symmetric key encryption. This minimizes the load for those applications that don't required any confidentiality.

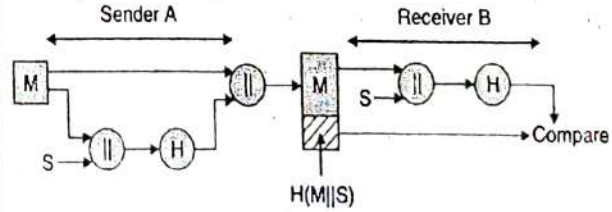


Fig. 3.9(c)

(c) No encryption required for message authentication only use hash function. In this process two person shares the same secret key when they communicate with each other.

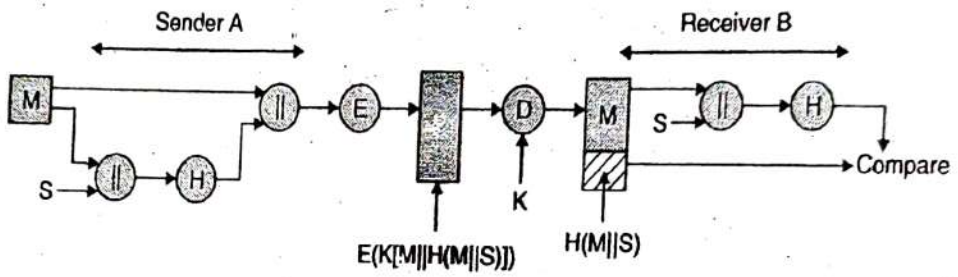
Sender A calculates the hash value over adding the original message M and S and attach the result of hash value to message M.

Because receiver B processes S and it can recalculate the hash value to check it.

(d) Confidentiality is added to this process and process (c) is encrypted with entire message concatenate with hash code.

Process (b) has more advantage over process (a) and process (d) which encrypts the whole data or message.

Minimum calculation is required in process(b). Using message authentication code (MAC) message authentication is achieved. This is also called as a keyed hash function. MAC are used between two persons for communication that shares the same secret key to authenticate information transfer between two users. A MAC function takes input as data block and secret key and produce output as hash value. MAC function is applied to the original message and the produced result will be check or compare with stored MAC value.



(d)

Fig. 3.9 : Simplified Examples of the use of a Hash Function for Message Authentication

Q. 17 Write the properties of hash functions.

Ans.:

There are four main properties of has function :

1. It is quick to compute the hash value for any given message.
2. It is infeasible to generate a message from its has value except by trying all possible messages.
3. A small change to a message should change the hash value so extensively that the new hash value appears uncorrelated with the old hash value.
4. It is infeasible to find two different message with the same has value.

Q. 18 What characteristics are needed in a secure hash function ?

Ans.:

Characteristics are needed in a secure has function are as follows :

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 sometime referred to in the literature as the one-way property.
5. For any given block x, it is computationally infeasible to find $y \neq x$ with H (y) = H (x).
6. It is computationally infeasible to find any pair (x, y), such that H (x) = H (y).

Q. 19 Explain in brief "Security of Hash functions.

Ans.: Security

Before taking any action, we need to define the two points. For a hash value h = H (m), we can say that m is the preimage of the h. That is m data block whose hash function, using function H, is h. Here, the collision occurs if $A \neq y$ and H (A) = H (B).

For region, we use here hash function the data, integrity and also the collisions are clearly undesirable. Assume, suppose the length of hash code is n bit, and function H use as input messages or the block of length of bits with b > n. Here, the total number of possible messages is 2b. Total number of hash values is 2^h.

Q.20 Explain operation of MD5 message digest algorithm. **Feb. 16 (In sem.)**

Ans.: Operation of MD5 message digest algorithm

It was developed by Ron Rivest. This algorithm takes an input of arbitrary length and 128 - bit message digest is produced. The input message is produced in 512 - bit blocks.

Fig. 3.10 shows processing of a message to produce message digest. Following steps explains the procedure of MD5.

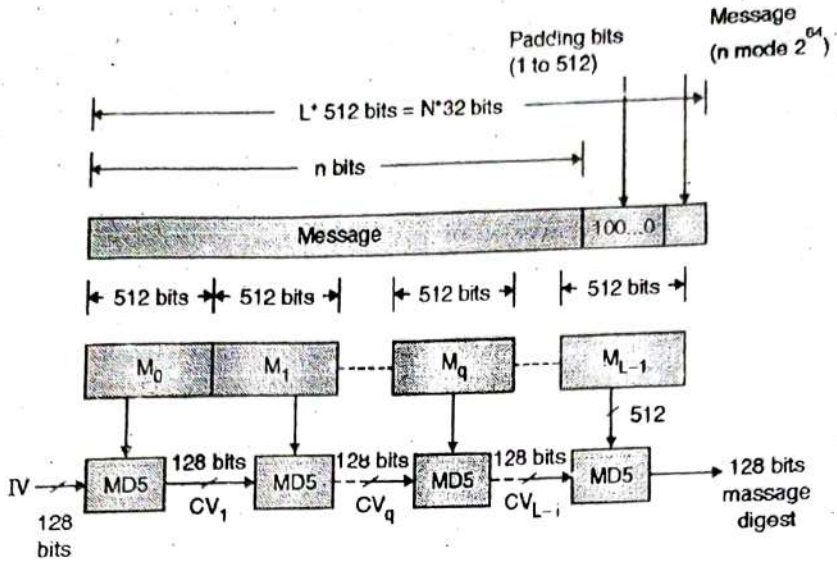


Fig. 3.10 : Detail steps of Message Digest 5 Algorithm

Steps MD5 Message Digest Algorithm

(1) Append Padding Bits

The message is padded to make the length of message is 448 mod 512. The length of the padded message is 64 bits less than an integer multiple of 512. The padding message consists a single 1-bit followed by 0 bits. The length of padding bits is in between 1 to 512.

(2) Append Length

64 bits of original message is appended to the result of above step 1. It is appended such that least significant bytes to most significant byte. The output of step 2 yields a message of integer multiple of 512 bits. As $M_0, M_1, \ldots M_q \ldots M_{L-1}$. The total length of expanded message is L * 512 bits.

(3) Initialize MD Buffer

A 128 - bit buffer is used to store the intermediate as well as final result. A buffer is represented as four 32-bit registers as P, Q, R, S.

P = 67452301

Q = EFCDA1389

R = 98BADCFE

S = 10325476.

It used a little-endian methods. Hence initial values (IV) are represented as,

P = 01 23 45 67

Q = 89 AB CD EF

R = FE DC BA 98

S = 76 54 32 10.

(4) Process Message in 512-bit (16 word of 32 bit) Blocks

It consists of four rounds of processing as shown in Fig. 3.11. These four rounds have similar structure but differ in primitive logical function referred as A, B, C, D.

Each round takes input 512-bit block, processed it and produces 128 bit output. The output of fourth round is added to the first round CV_q to produce CV_{q+1} using addition modulo 2^{32}.

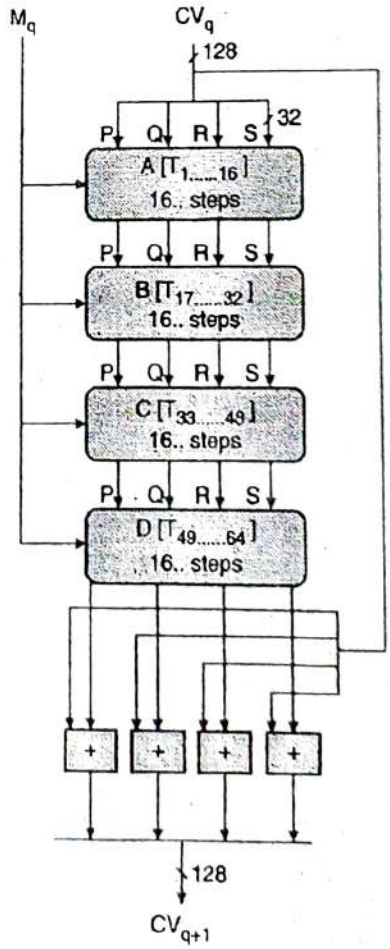


Fig. 3.11 : Four rounds of MD5 algorithm

(5) Output

After processing all L 512-bit blocks, the 128 bit message digest is produced as a output.

The entire MD5 process can be summarized as follows :

CV0 = IV

CVq+1 = Sum32(CVq, RFd [Mq,RFc [Mq,,RFb [Mq, RFa [Mq, CVq]]]])

MD5Sum = CVL

Where,

IV = the initial value of the PQRS buffer, mentioned in step 3

Mq = the qth 512-bit block of the message

CVq = the chaining variable processed with the q-th block of message

RF = the round function using primitive logical function a, b, c, d.

MD5Sum = the final hash result or message digest

Sum32 = addition modulo 232

Q. 21 Explain the operation of secure hash algorithm on 512 bit block.

Ans. :

The operation of secure hash algorithm on 512 bit block.

The SHA was developed by NIST in 1993. It is referred as Secure Hash Algorithm-1. SHA - 1 takes an input message of a maximum length less than 2^{64} bits and produced an output of 160 bit message digest. The overall processing of SHA-1 is much similar to MD5. The processing is explained as follows.

(1) Append Padding Bits

Padding means addition of bits to the original message. To make length of original massage to a value 64 bits less than multiple of 512. The message is padded to make the length of message 448 mod 512.

The length of the padded message is 64 bits less than an integer multiple of 512. The padding message consists of a single 1-bit, followed by many 0 bits as required. The length of padding bits is in between 1 to 512.

(2) Append Length

A block of 64-bit is appended to a message. 64 bits of original message is appended to the result of above step 1 (Original message + Padding). It is appended such that least significant bytes to most significant byte.

(3) Initialize MD5 Buffer

A 160-bit buffer is used to store the intermediate as well as final result. The buffer is represented as five 32-bit registers as P, Q, R, S, T, as.

P = 67452301

Q = EFCDAB89

R = 98BADCFE

S = 10325476

T = C3D2E1FO

It uses a big-endian method. First four registers are same as MD5. These five registers P, Q, R, S, T are represented as,

P = 67 45 23 01

Q = EF CD AB 89

R = 98 BA DC FE

S = 10 32 54 76

T = C3 D2 E1 FO

(4) Process Message in 512-bits (32 bit 16 word) Block

It consists of four rounds of 20-step each as shown in Fig. 3.12. These rounds referred as F1, F2, F3, F4 have similar structure. These rounds used different primitive logical function.

Each round takes input 512-bit block processed it and produced 160 bit output. The output of fourth round is added to the first round CV_q to produce CV_{q+1}.

Each round also uses an additive constant k_t, where $0 \le + \le 79$.

K_1 = 5A 827999

K_2 = 6E D9 EB A1

K_3 = 8F 1B BC DC

K_4 = CA 62 C1 D6

(5) Output

After processing all L 512 bit blocks, the 160 bit message digest is produced as output. The SHA compression function uses a feed forward operation where the chaining variable CVq input of the first round is added to the output obtained (last step) after execution of 80 steps to produce the next chaining variable CVq+1 as shown in Fig. 3.12.

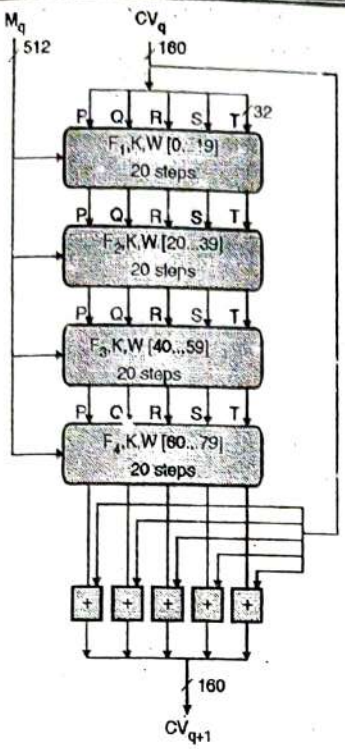


Fig. 3.12 : Four rounds of Secure Hash Algorithm

Q. 22 Compare MD5 with SHA-1. **April 17(In sem.)**

Ans.:

Both are derived from MD4. Both are quite similar. They differs from each other in design goals.

Sr. No.	SHA-1	MD5
1.	It uses a 160-bit message digest. Hence it is stronger against Brute - force attacks than MD5.	It uses a 128 bit message digest. Hence it is weaker than SHA1 against Brute - force attacks.
2.	SHA-1 is not vulnerable against cryptanalysis.	MD5 is vulnerable against cryptanalysis
3.	SHA-1 is slower than MD5.	MD5 is faster than SHA-1.
4.	It uses big - endian method to represent the message.	It uses a little endian method to represent the message.
5.	SHA has 20 rounds.	MD5 has 64 rounds.
6.	Bit rotation counts for SHA - 1 are the same for all rounds.	In MD5 each round has its own bit rotation counts.

Q. 23 Define MAC. **May 15, 2 Marks**

Ans.: MAC

The Message Authentication Code (MAC) is a small fixed-size block of data that is generated based on a message M of variable length using secret key K as follows. MAC is also called cryptographic checksum.

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

Q. 25 Explain the operation of Kerberos. **May 16**

Ans. : Operation of Kerberos

Kerberos is also called as authentication protocol. Like when to start in journey we need a confirm ticket then only we can do our journey safely. Kerberos uses the concept of the ticket as a token to prove the identity of the user. Microsoft introduced Kerberos in Windows 2000 server as a default authentication protocol. Kerberos uses the concept of a ticket as a token that proves the identity of a user. Tickets are digital documents that store session keys. Instead of password, tickets are issued during login session and then can be used in any Kerberos services. For client authentication phase requires two tickets:

Ticket Granting Ticket (TGT), which act a identifier for user and session key. A service ticket to authenticate user to gain access to user for particular service.

The same concept of ticket is used likewise we use railway tickets it has time duration, expiration dates after that ticket become invalid. In Kerberos these ticket includes different contents like time stamps to indicate an, start and expiration time, after time expiration the ticket become invalid. The timestamp is the time set by Kerberos administrator depending upon how much time service is required to the client.

1. Kerberos Servers

To accomplish the task of secure authentication, Kerberos uses a trusted third party is called a Key Distribution Center (KDC).

The Key Distribution Center uses two techniques for authentication :

Authentication Server (AS), which performs user authentication

Ticket Granting Server (TGS), which permits/ grants tickets to users

The role of an Authentication server is to store a database like secret key of the users and its services. The secret key of a user is generated using one-way hash of user provide password. The main aim of the Kerberos is provide centralize authentication of entire network rather than storing the sensitive information at each user machine, the sensitive information will be maintained at particular secure location only.

2. Kerberos Authentication

This phase is called as Authentication phase because during this phase only authentication can be done between authentication server, ticket-granting server and service provider. As shown in Fig. 3.13 first client and authentication server authenticate themselves to each other.

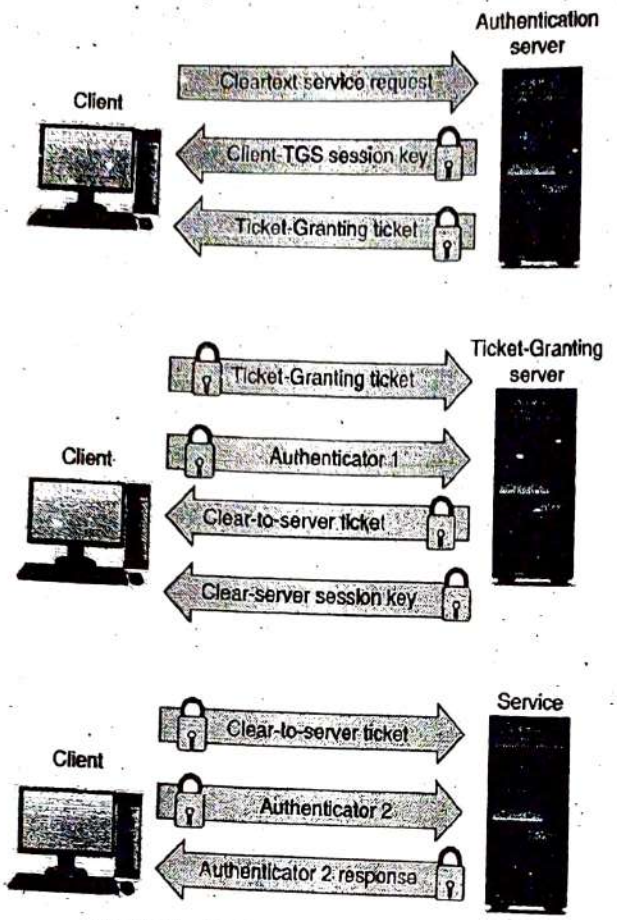


Fig. 3.13 : Kerberos athentication process

Client and Ticket granting server authenticate themselves. Finally client and requested service provider authenticate themselves to each other regarding which information/ service client wants.

3. Authentication Details

During authentication phase user has to provide username and password on the client machine which cryptographically hashed to create a secret key for the client.

After client verification done with authentication server, AS will replies the following details to clientas shown in Fig. 3.13.

1. The client Ticket Granting Sever (TGS) session key Kt, encrypted using clients secrets key Kc (which now stored in authentication server).
2. The Ticket Granting Ticket (TGT) encrypted using the secret key of the Ticket granting server. The ticket granting ticket includes the client ticket granting sever session key Kt and its validity period.

The client now decrypt the Ticket Granting Server session key Kt using his secret key Kc. To request as service client sends following two message to Ticket Granting Server (TGS).

1. The Ticket Granting Ticket and the name of the service Sr that client wants to request.
2. Authentication token which includes client ID and time stamp, encrypted using client ticket granting server session key Kt.

Upon receiving all the details from client Ticket Granting Server decrypts the Ticket Granting Ticket using Kt, thus retrieving the client Ticket granting server session key Ktand the validity of the ticket granting ticket. If it is valid then Ticket granting Server sends following messages to the client.

1. New client server session key Ksc, encrypted using TGS session key Kt.
2. Client to server ticket, encrypted using specific services key Ks, known to Ticket Granting Server only. (Client to server ticket contains the client ID, network address, validity period and the client server session key Ksc).

Upon receiving all the details from Ticket Granting server client decrypt the client server session key Ksc, and authenticate him to service Sr by sending following messages :

1. The client server ticket sent by the ticket granting server in previous step.
2. The client ID and the time stamp encrypted suing client server session key Ksc.

The service provider decrypts the client to server ticket using secret key Ks and obtains the client server session key Ksc. With the help of client server session key Ksc, service provider decrypt the client ID and time stamp information. To prove the final identity service providers increment the time stamp by 1 and send it back to the client.

The client decrypts and verifies this response using client to server session key Ksc. Once this verification get succeed, now client - server can start. Kerberos protocol was specially design to check the authentication of the client over insecure network. Two types Kerberos versions are exits i.e. Kerberos 4 and 5.

Q. 26 What are the difference between Kerberos version 4 and version 5 ?

Ans.:

Difference between Kerberos version 4 and version 5

Sr. No.	Kerberos version 4	Kerberos version 5
1.	Kerberos v4 was released prior to the version 5 in the late 1980's.	The version 5 was published in 1993, years after the appearance of version 5.
2.	Ticket support is Satisfactory in this version	Ticket support is well extended. Facilitates forwarding, renewing and postdating tickets.
3.	It uses the "receiver-makes-right" encoding system.	It uses the ASN.1 coding system.

Sr. No.	Kerberos version 4	Kerberos version 5
4.	Since the same key is used repeatedly to gain a service from particular server, there is a risk that an attacker can replay messages from an old session to the client or server.	in V5 this is avoided by requiring a sub session key which is used only for one connection.
5.	Kerberos V4 uses DES encryption techniques	In Kerberos V5 the cipher text is tagged with an encryption type identifier hence any type of encryption can be used.
6.	Kerberos uses IP addressing	Kerberos V5 can use any address since the address is now tagged with type and length.
7.	In V4 the ticket lifetime has to be specified in units of 5 minutes.	In V5 ticket lifetime one can specify an explicit start and finish times allowing arbitrary lifetimes.
8.	It contains only a few IP addresses and other addresses for types of network protocols.	Kerberos V5 tickets can now contain multiple IP addresses and addresses for different types of networking protocols.

Q. 27 Explain with the help of diagram X.509 certificate format. **Dec. 13, May 15**

Ans. :

The diagram of X.509 certificate format is :

Digital certificate is an electronic file that is used to identify people and resources over a insecure channel or a networks called Internet. Digital certificate also enable secure, confidential communication between sender and receiver using encryption.

For example when we travel to another country, our passport provides a way to establish our identity and gain entry. Digital certificate provide similar identification in the electronic world.

The role of Certification Authority (CA) is to issue certificates with authorized digital signature. Much like the role of the passport office, the role of the CA is to validate the certificate owner's identity and to "sign" the certificate so that it cannot be tampered by unauthorized user. Once a CA has signed a certificate, the owner can present their certificate to people, web sites and network resources to prove their identity for confidential communications over insecure channel.

A standard called as **X.509** defines structure of digital certificate. The International Telecommunication Union (ITU) permitted this standard in 1998. Fig. 3.14 shows structure of X.509 digital certificate.

Digital Certificate contents
Certificate version number
Certificate serial number
Algorithm for signature identifier
Certificate Issuer name
Validity Details
Name of the certificate owner Public key of certificate owner
Issuer unique identifier
Owner unique identifier
Extensions to certificate
Certification Authority (CA) Digital Signature

Fig. 3.14 : Structure of X.509 Digital certificate

A standard digital certificate typically includes a variety of information pertaining to its owner and to the Certification Authority (a trusted agency that can issue digital certificate) such as:

Certificate version number

Identifies a particular version of the X.509. Current version is X.509 v3.

Certificate serial number

Unique integer number generated by certification authority.

Algorithm for signature identifier

Identifies algorithm used by the certification authority to sign the certificate.

Certificate Issuer name

The name of the Certification Authority that issued the certificate.

Validity Details

The validity period (or lifetime) of the certificate (a start and an end date).

Name of the certificate owner

The name of the owner and other identification information required for identifying the owner such as email id and contact details.

Public key of certificate owner

Certificate owner's public key, which is used to encrypt confidential information of the certificate owner.

Issuer unique identifier

Indentify the CA uniquely i.e. whether single CA signed it or is any CA using same details.

Owner unique identifier

Indentify the owner uniquely if two or more owner has used the same name over a time.

Extensions to certificate

This is an optional field which allows a CA to add additional private information to a certificate. These additional fields are called as extensions of version 2 or 3, respectively.

Certification Authority (CA) Digital Signature

In creating the certificate, this information is digitally signed by the issuing CA. The CA's signature on the certificate is like a tamper-detection seal on packaging any tampering with the contents is easily detected.

Q. 28 What is digital signature ? **April 17(In sem.)**

Ans. : Digital signature

Digital signatures are essential in today's modern world to verify the sender of a document's and his identity. A digital signature is represented in a computer as a string of binary digits and computer is using a set of rules and regulations (algorithm) to identify the person signing the document as well as the originality of the data can be verified.

A digital signature is defined the signature generated electronically from the digital computer to ensure the identity of the sender and contents of the message cannot be modified during transmission process. Digital signature techniques achieve the authenticity, integrity and non-repudiation of the data over Internet.

Concept of digital signature is that sender of a message uses a signing key (Private Key) to sign the message and send that message and its digital signature to a receiver over insecure communication channel.

The receiver uses a verification key (Public Key) of the sender only to verify the origin of the message and make sure that it has not been tampered with while in transit as shown in Fig. 3.14.

Hash value of a message when encrypted with the private key of a person is, his digital signature on that e-Document. Digital signature is an example of asymmetric key cryptography which uses three different algorithms to complete the process.

1. First step is key generation algorithm which generates private key and a corresponding public key.
2. Next step signing algorithm which selects sending message and a private key generated in step 1, to produce a signature.
3. Third step is signature verifying algorithm which verifies the authenticity of sending message and public key.

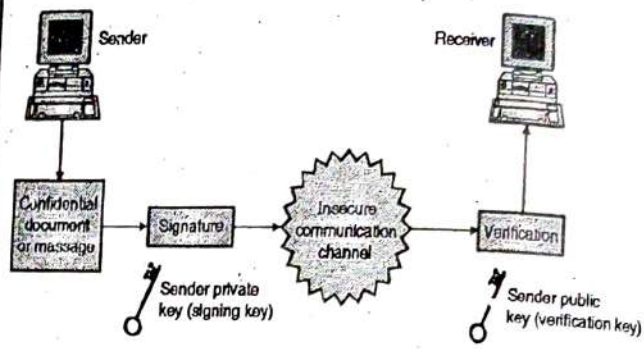


Fig. 3.14 : Digital Signature block diagram

As mentioned above the signature is generated with the help of private key. The private key, which is never shared, is used in signature generation, known to sender only.

Public keys, which are known by everyone, can be used to verify the signature of a sender. Every sender and receiver having a private and public key pair, the reason digital signature called public-key cryptography.

Q. 29 Explain Digital Signature Standard.

May 16, Dec. 16, April 17(In sem.)

Ans. : Digital signature standard

The National Institute of Standards and Technology (NIST) has published Federal Information Processing Standard FIPS 186, known as the Digital Signature Standard (DSS) algorithm to generate a digital signature to correctly identify (authentication) the electronic documents.

It is Public-key cryptosystem technique. User applies the Secure Hash Algorithm (SHA) and MD5 to the message to produce message digest. User's private key is applied to message digest using *DSA* to generate signature.

Public-Key components

1. Select prime number a of L bits where L is a multiple of 64 bits and $512 \le L \le 1024$
2. Select b (A 160 – bit s prime factor of a – 1)

   b = a prime divisor of a – 1, where $2^{159} < b < 2^{160}$
3. g is generator of subgroup of order a mod b such that $1 < g < a$ [$g = h^{(a-1)/b}$ mod a, where h is any integer].
4. x the private key that must be secrete ; x is randomly or pseudo randomly generated integer, such that $0 < \infty < b$.
5. y the public key where $y = g^x$ mod a.
6. k a secret key that is unique to every message where k is randomly or pseudo randomly generated integer, such that 0 < k < b.

7. Signature generation.

The signature of message m is pair of numbers q_r and s computed using following equation,

$$gr = (g^k \bmod a) \bmod b$$

$$s = [k^{-1} (H(M) = xgr)] \bmod b$$

$$\downarrow$$

SHA-1

Where,

gr and s are generated signature.

signature = (gr , s)

k^{-1} = Multiplicative inverse of k, mod b,

The value of SHA-1 (m) is a 160-bit string output by secure Hash Algorithm,

8. DSA signature verification

To verify the signature of signal message verifier requires a, b and g along with senders private key and identity are made available in authenticated manner.

Let, m', q_r' and s' be the received copies of m, qr and s. Let y be the public key of receiver. To verify the signature following equations are required.

$$\omega = (s^{-1})^{-1} \bmod b$$

$$V_1 = (1 \text{ SHA} - 1 \ (m')\ \omega) \bmod b$$

$$V_2 = (gr')\ w \bmod b$$

$$V_r = ((g)^{V_1} (y)^{V_2} \bmod a) \bmod b$$

If $V_r = q_r$ then signature is verified and receiver can identify that message was send by intended sender with secrete key x corresponding to y.

If $V_r \neq gr$ then message may be modified or may be incorrectly signed by sender.

Q. 30 Explain how ElGamal scheme generate and verify the digital signature.

Ans. :

The word cryptography is incomplete without mathematics. Cryptography is based on specific areas of mathematics like finding greatest common divisor using Euclidean algorithms. Finally most important concept called prime numbers used in different cryptography algorithms.

1. This scheme is variant of digital signature algorithm.
2. This scheme is based on computing assumption of discrete logarithms over finite field with a large prime factor.
3. It is computationally infeasible to compute q_r and s.

ElGamal scheme is based on difficulty of computing discrete logarithms. This scheme assures that the authenticity of message m sent by sender/ signer to verifier.

System parameters

Let H be the hash function.

Let a be the prime number.

Let g < a be a randomly chosen generator.

Key generation

Chose randomly a secret key x with $1 < x < p - 1$.

Compute $y = g^x \bmod a$.

The public key (a, g, y).

These steps are performed by signer of documents.

Signature generation

To sign a message m, signer needs to perform following steps.

Chose random integer i such that

$(i : a - 1) = 1$; $1 < i < a - 1$

$$gr = g^i \bmod (a)$$

Compute

$$s - (H(m) - xgr)\, k^{-1} \bmod (a - 1)$$

If s = 0 then repeat above step.

The pair (qr, s) is called as Digital signature of message m. The signer has to repeat all these steps during every signature generation.

Verification

Digital signature (gr, s) of message m was verified as follows,

$0 < q_r < a$ and $0 < s < a - 1$

$$g^{H(m)} = y^{qr} q_r^{s} \bmod a.$$

If $g^{H(m)} = y^{qr} q_r^{s} \bmod a$ is equal then verifier accept the signature otherwise he reject it.

Where,

$$H(m) = x\, q_r + Si \bmod a - 1$$

According to format s little theorem

$$g^{H(m)} = g^{xqr}\ g^{is}$$

$$= (g^x)^{qr} \times (g^i)^{s}$$

We know that $y = q^{\xi} \bmod a$

Above equation can be rewrite as follows,

$$g^{H(m)} = (y)^{qr} \times (gr)^{s} \bmod a$$

Hence proved.

Here, H(m) = SHA – 1 (m) is 160-bit string output produced by secure Hash Algorithm.

Q. 31 Explain different authentication methods and protocol.

Ans. :

Authentication Methods and Protocol are as follows :

1. One Way Authentication

Authentication mechanisms ensure that who sends the message i.e. origin of an electronic message is correctly identified. One-way authentication refers to the authentication of only one end of communication users.

For example, One-way authentication follows the flow : If there are two users, user A and B wants to communicate with each other user B authenticates user A, but user A cannot authenticate user B. This process called one-way authentication. Finally the integrity and originality of message is confirmed.

There are different factors of authentication mechanisms used to give strength for authentication. First method is known as **one-factor authentication**. Password is the example of one-factor authentication because it is something that we know. Any operating system first ask for a user name and then for a password. It then looks up the name in a password table and sees if the passwords match. This is known as a **reusable password** since the same password is used for each login.

Second method of authentication is known as **two-factor authentication.** Withdrawing cash from an ATM machine is an example of two-factor authentication. For authentication present the ATM card (something we have) and enter PIN (something we know) or use of **one-time passwords** – a new password must be used for each login.

2. Mutual Authentication

Mutual authentication also called as two-factor authentication. Mutual Authentication is a security mechanism used to authenticate sender with the receiver. Sender must prove its identity to a receiver, and the receiver must prove its identity to the sender, before any unwanted threat sent between the sender and receiver.

For example : If sender wants to communicate with the receiver over networks they must first mutually authenticate each other.

Meaning is that when sender A sends confidential message which is intended to receiver B. If B can decrypt the message using A's public key, then B has verified that the message originated from A. Both communicating users (sender and receiver) are verifying each other i.e. mutual authentication mechanisms helps to verify identity of the sender. The most important application of mutual authentication is that communication between client machine and server machine over a network must be secure before performing any data sending and receiving process.

Q. 32 Explain role of key distribution centre in symmetric system.

Ans. :

Role of key distribution centre in symmetric system

In order to achieve mutual authentication there must be certain provision of some protocols which suppose to verify identity of the sender over an insecure communication channel.

To achieve this goal most of the protocols depends on an authentication server also called **Key Distribution Center (KDC).**

If sender A wants to establish a secure communication with receiver B, then A can request for **session key** from Key Distribution Center for communicating with B. If group of people wants to securely communicate with Key Distribution Center then providing every group member a single key called a **master key or secret key**. Authentication servers are capable to delivers good quality session keys and distribute securely to client who requested it.

Authentication server also maintains a table containing a name and a **master key or secret key** of each client.

The secret key is used to authenticate client to the authentication server and then for securely transmission of data between client and the authentication server. There are different protocols are used to perform this task but among this the well known protocol called as Needham-Schroeder Protocol.

Q. 33 Draw sequence diagram of Needham Schroeder protocol and explain.

Ans. : Sequence diagram of Needham Schroeder protocol

The first mutual authentication protocol was published in 1978 by Needham and Schroeder. This approach was proposed for various purposes that includes secret-key and public key generation and distribution of those keys between sender and receiver.

Needham and Schroeder protocol uses a secret key known to the sender and also to an authentication server. Sender and receiver share a secret key and use it for secure communication with authentication server.

Detail steps of Needham-Schroeder Secret-key Protocol

Step 1 : Sender A requests for a session key to authentication server for communication with receiver B as shown in Fig. 3.15. The message sent by A to authentication server includes A's secret key Ka, A's network address Na, B's network address Nb and a nonce. A nonce is basically a random number used to demonstrate the freshness of a request denoted by N. The request sent by A to authentication server which is in encrypted format E denoted by,

$$E(Ka, [Na, Nb, N])$$

Step 2 : Authentication server returns a message, containing a newly generated key Kab (used to encrypt communication between sender and receiver), nonce N (to match the response received from authentication server with the request sent), ticket (contains the same shared secret key Kab , as well as the name of the sender A) encrypted with B's secret key Kb and whole these message encrypted with senders private key or secret key Ka to ensure that no one else can read it. The message that authentication server sends back to A can be expressed as :

$$E(Kab, N, \{A, Kab\} Kb, B_{|}Ka$$

Step 3 : After receiving replay from authentication server, sender decrypt the ticket and sends the ticket {A, Kab} to the receiver B. A sends the ticket to B which is not in encrypted format because it was previously encrypted by authentication server using B's secret key Kb.s

$$(A, Kab) Kb$$

Step 4 : B decrypts the ticket received from A using the secret key Kb and compares sender identity. B is again encrypting the ticket using shared secret key Kab and generates nonce N1 and sends it back to receiver. This can be represented as

$$E(N1) Kab$$

In this step B got the **session key**(Kab) for communicating securely with A.

Step 5 : Sender is decrypting the nonce N1; using the shared secret key Kab this proved the senders identity. The sender sends response N1+1 encrypted using the shared secret key Kab.

$$E(N1+1) Kab.$$

Step 6 : Now sender A and receiver B can securely communicate with each other using session key generated.

The main weakness of this protocol is that for large networks it is not possible for single authentication server to generate and distribute number of session key which is practically not possible.

Another weakness is that if session key between sender A and receiver B is stolen, and the ticket to B is recorded, attacker can easily copy the contents of a sender A by performing last 3 steps.

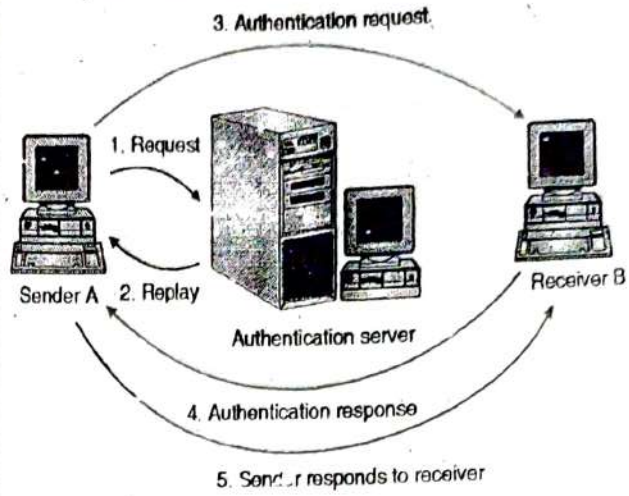


Fig. 3.15 : Needham - Schroeder Secret-key Protocol

Q. 34 Use RSA algorithm to encrypt the plaintext "3" use following parameters p = 11, q = 3, e = 13.

May 17

Soln. :

1. Select two prime numbers p = 11, q = 3.
2. n = p*q = 11 * 3 = 33.
3. $\phi(n) = (11 - 1) * (3 - 1) = 10 * 2 = 20$.
4. Select e such that, e is relatively prime to $\phi(n)$ i.e. gcd $(e, \phi(n)) = 1$ and $1 < e < \phi(n)$ e is selected as 13, gcd (11, 20) = 1.
5. Finding d

   e*d mod $\phi(n) = 1$

   13 * d mod 20 = 1

   d is calculated using following method. Do the following procedure till you are not getting a integer numbers

$$d = \frac{(\phi(n) * i) + 1}{e}$$

$$d = 20 + 1/13 = 1.61 = 1.61$$

where, i = 1 to 100

$= 40 + 1/13 = 3.15$ (i = 2)

$d = 60 + 1/13 = 4.69$ (i = 3)

$d = 80 + 1/13 = 6.23$ (i = 4)

$d = 100 + 1/13 = 7.76$ (i = 5)

$d = 120 + 1/13 = 9.30$ (i = 6)

$d = 140 + 1/13 = 10.84$ (i = 7)

$d = 160 + 1/13 = 12.38$ (i = 8)

$d = 180 + 1/13 = 13.92$ (i = 9)

$d = 200 + 1/13 = 15.46$ (i = 10)

$d = 220 + 1/13 = 17$ (i = 11)

Hence **d = 17**

6. Hence public key = {13, 33} and Private key = {17, 33}
7. Encryption

Plain text message (P) which is in binary format converted into integer.

Here P is selected as 3 such that $P < n$

$\because (3 < 33)$

Now, $C = P^e \bmod n = 3^{13} \bmod 33$

Here to find out $3^{13} \bmod 33$, use the following procedure

$3 \bmod 33 = 3$

$3^2 \bmod 33 = 9$

$3^4 \bmod 33 = 15$

$3^8 \bmod 33 = 27$

$\therefore C = [(3^8 \bmod 33) * (3^4 \bmod 33) * (3 \bmod 33)] \bmod 33$

$= [27 * 15 * 3] \bmod 33 = 27$

$C = 27$

Chapter 4 : Security Requirements

Q. 1 Define IP sec. **May 15**

Ans. : IP sec

Internet Protocol security (IPSec) is a framework of open standards for protecting communications over Internet Protocol (IP) networks through the use of cryptographic security services. The most important feature of IPsec is that it can authenticate and encrypt all on-going traffic at the IP level.

In terms of cryptography Internet Protocol support for sending and receiving encrypted information of any kind without any modification. IPSec provides different kinds of cryptographic services like confidentiality integrity and authentication.

Q. 2 Discuss IP sec protocols in detail. **May 15**

Ans. : IP sec protocols are as follows :

1. IPv4

IPv4 is a Network Layer Protocol. IPv4 Stands for Internet Protocol Version 4. An IPv4 address is a 32-bit :

Address that uniquely identifies host or a computer to the Internet. Length of IPv4 address is a 32-bit IPv4 Address are unique and all nodes connecting Internet must have IPv4. The address space of IPv4 is 2^{32} or 4,294,967, 296. Dotted decimal notation of IPv4 is representing as 192.168.0.1 (each single byte separated. (dot) symbol)

Packets in the network layer is called as datagram's, which consist of two parts : header and data. The header is 20 to 60 bytes in length and contains necessary information about delivery of the packet from one router to another as shown in Fig. 4.1.

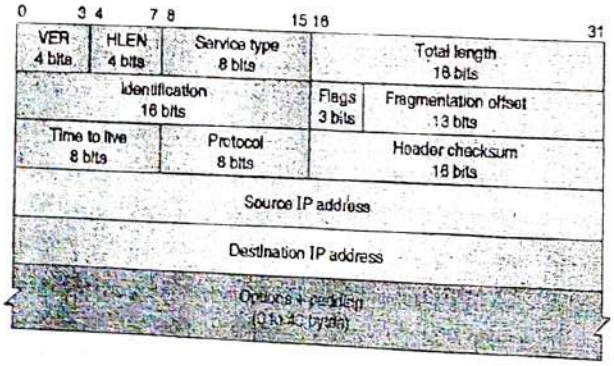


Fig. 4.1 : IPv4 Packet Format

Detail explanation about of each field is given below.

Version (4 bits)

Indicates the version of IP and is set to 4.

Internet Header Length (4 bits)

Indicates the number of 4-byte blocks in the IPv4 header (Length of entire IP header). Because an IPv4 header is a minimum of 20 bytes in size, the smallest value of the Internet Header Length (IHL) field is 5.

Type of Service (8 bits)

Indicates the desired service expected by this packet for delivery through routers across the IPv4 internetwork.

Total Length (16 bits)

Indicates the total length of the IPv4 packet (IPv4 header + IPv4 payload) that is up to 65,535 bytes long

Identification (16 bits)

Identifies this specific IPv4 packet. The Identification field is selected by the originating source of the IPv4 packet. If the IPv4 packet is fragmented, all of the fragments retain the

Identification field value so that the destination node can group the fragments for reassembly.

Flags (3 bits)

Identifies flags for the fragmentation process. There are two flags one to indicate whether the IPv4 packet might be fragmented and another to indicate whether more fragments follow the current fragment.

Fragment Offset (13 bits)

Indicates the position of the fragment relative to the original IPv4 payload.

Time to Live (8 bits)

Indicate the maximum number of links on which an IPv4 packet can travel before being discarded. Therefore, the TTL becomes a maximum link count with the value set by the sending node.

IPv4 packet if checksum verification fails. Therefore, the Header Checksum is recomputed at each hop between source and destination.

Source Address (32 bits)

Stores the IPv4 address of the originating host.

Destination Address (32 bits)

Stores the IPv4 address of the destination host.

Options (multiple of 32 bits)

Stores one or more IPv4 options.

2. IPv6

IPv6 stands for Internet Protocol version 6. As discussed earlier the Internet addresses are 32 bits in length; this gives us a maximum of 2^{32} addresses. IPv6 is a new design which has 128-bit address that give much greater flexibility in address allocation.

IPv6 address format (128 bits)

2031:0000:130F:0000:0000:09C0:876A:130B

8 groups of 4 hexadecimal digits

Each group represents 16 bits

Separator is ":"

Case-independent

Leading zeros in a field are optional:
2031:0:130F:0:0:9C0:876A:130B

IPv6 Header Format

Fig. 4.2 shows format of IPv6.

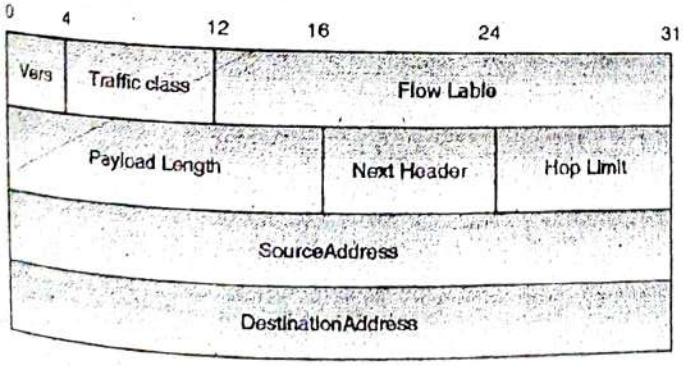


Fig. 4.2 : IPv6 Header Format

distinguish between different classes or priorities of IPv6 packets.

Flow Label (20 bits)

Identifies a flow and it is intended to enable the router to identify packets that should be treated in a similar way without the need for deep lookups within those packets. This label is used to maintain the sequential flow of the packets belonging to a communication. Set by the source and should not be changed by routers along the path to destination.

The source labels the sequence to help the router identify that a particular packet belongs to a specific flow of information. This field helps avoid re-ordering of data packets. Unique and powerful tool to IPv6.

Payload Length (16 bits)

With the header length fixed at 40 bytes, it is enough to indicate the length of the payload to determine the length of the entire packet.

Next Header (8 bits)

Indicates either the first extension header (if present) or the protocol in the upper layer (such as TCP, UDP, or ICMPv6). When indicating an upper layer protocol above the Internet layer, the same values used in the IPv4 Protocol field are used here.

Hop Limit (8 bits)

In IPv6, the IPv4 TTL was appropriately renamed Hop Limit because it is a variable that is decremented at each hop, and it does not have a temporal dimension.

Source IPv6 Address (128 bits)

Stores the IPv6 address of the originating host.

Destination IPv6 Address (128 bits)

Stores the IPv6 address of the current destination host.

Q. 3 Explain Authentication Header.

Ans.: Authentication Header

It is designed for authentication, integrity of payload which is carried in IP Packet. It is first protocol of IPSec called Authentication Header (AH) protocol designed to provide data authentication (to identify source host), data integrity (if data get modified while in transit) and non-repudiation but doesn't provide data confidentiality (if attacker able to access the contents of a message) because Authentication Header does not encrypt the data/ IP packet. The main functionality of this protocol is protection

against replay attacks (sending same data to receiver again and again) and protection against tampering of data over a network.

Authentication Header is also used to protect the upper-layer or the entire IP packet, with the help of message authentication code (MAC - used to generate fixed length value from message and secret key to provide authentication) using well known hashing algorithms like MD5 or SHA1.

By using Hash function and symmetric key algorithm, message digest is calculated and inserted in authentication data as shown in Fig.4.3 because of this AH protocol provides data authentication and data integrity, but not confidentiality or privacy.

The internal fields of authentication header format are shown in Fig. 4.3. This protocol uses cryptographic checksum which is similar to hash function or message digest, the checksum is inserted in authentication header and placed in location depends on which mode it is using (tunnel mode or transport mode).

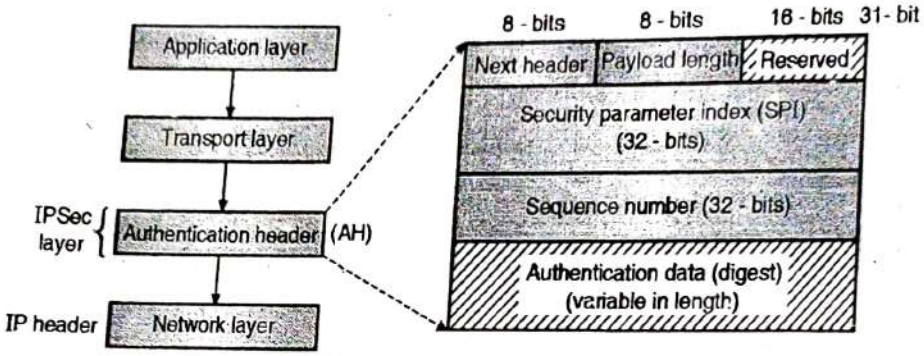


Fig. 4.3 : Authentication Header

A brief description of each field

Next header (8 bits) : The next header is an 8 - bit filed which is used to identify the type of payload/ data carried by IP packet.

Identifies the type of header immediately following this header.

Payload length (8 bits) : The payload header is also an 8 - bit filed which defines length of the authentication header.

Length of the AH in 32-bit words minus 2.

Reserved (16 bits) : AH contains 16 - bit field which is reserved for future use and always set to zero.

Security Parameter Index (SPI) (32 bits) : SPI is a 32-bit field used in combination with source IP address, destination IP address and AH security protocol to uniquely identify a security association (SA) for the traffic to which IP packet belongs, we will discuss SA it next bit. This field also defining which different security algorithms and keys were used to calculate the message authentication code (MAC).

Sequence number (32 bits) : It is also a 32 bit field. It prevents the retransmission of datagram which is also known as Replay attack.

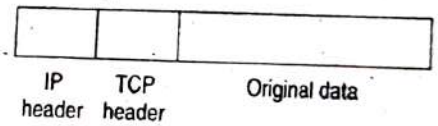
A monotonically increasing counter value.

Authentication Data : This is variable length field whose length depends upon encryption algorithm used. Authentication data field of AH protocol is the output of hashing algorithm or message digest algorithm. AH protocol performs the Integrity Check Value (ICV) on packet header or MAC is computed over the complete IP packet including the outer IP header to ensure that the data has not been changed during transmission process. As mentioned earlier AH doesn't encrypt the data the reason it doesn't provide confidentiality during transmission.

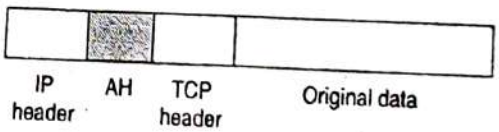
Modes of Operation

(i) AH Transport Mode

In Transport mode the authentication header is placed between original IP Header and original TCP header as shown in Fig. 4.4.



(a) Before applying AH



(b) After applying AH

Fig. 4.4 : AH transport mode

(ii) AH Tunnel Mode

In Tunnel Mode the AH is inserted between the new IP header and original IP header. The inner IP address contain source and destination address of sender and receiver and the out IP address contain the address of security gateway or firewall as shown in Fig. 4.5.

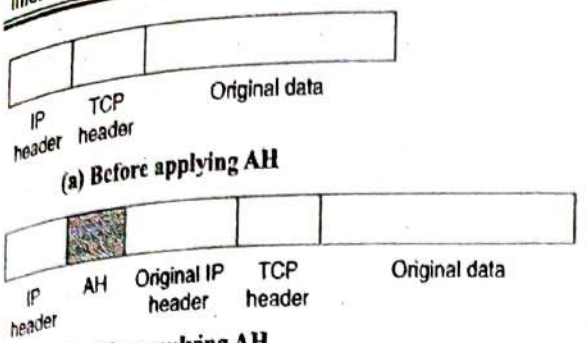


Fig. 4.5 : AH tunnel mode

Q. 4 Explain in detail IPSec ESP format.

Ans. : IPSec ESP format

One of the most important feature that Authentication Header was unable to provide called data confidentiality (if attacker able to access the contents of a message).

An Encapsulating Security Payload is primarily designed to provide encryption, authentication and confidentiality for the data or payload that is being transferred in an IP network. As defined earlier ESP is used to encrypt the entire payload of an IPSec packet the reason ESP alone can provide data authentication, protection against replay attacks and data integrity by adding ESP header, ESP trailer and MAC to the packet.

ESP has the same fields as defined in AH, but it integrates these fields in a different way instead of having just a header, it divides these fields into three components: An ESP header, ESP trailer and ESP authentication block as shown in Fig. 4.6.

It is designed for confidentiality and integrity of messages. ESP can be used alone or with combination of AH.ESP adds a header and a trailer to the payload. Following are the steps for adding ESP header and trailer.

Step 1 : In the initial step, ESP trailer is added to IP payload.

Step 2 : Payload and trailer or encrypted

Step 3 : After the encryption ESP header is added to the encrypted packet.

Step 4 : ESP header, payload and ESP trailer are used to create authenticated data.

Step 5 : This authentication data is added at the End of Trailer.

Step 6 : Lastly the IP header is added.

The main functionality of ESP is to provide the confidentiality to IP packet by encrypting them. Encryption algorithms (Triple DES, Blowfish, and IDEA etc.)used to combines the data in the packet with a key and transform it into an encrypted form. The encrypted packet now then transmitted to the destination, and decrypts it using the same algorithm.

The detail description of Encapsulating Security Payload (ESP) fields is given below :

ESP Header : This contains two fields, Security Parameter Index (SPI) of 32 bits and Sequence Number of 32 bits, as defined in AH protocol SPI is a 32-bit field used in combination with source IP address, destination IP address and ESP security protocol to identify a security association (SA) for the traffic to which IP packet belongs.

Sequence number : It is also a 32 bit field. It prevents the retransmission of data gram which is also known as **Replay attack** as defined earlier. This field is not encrypted but it's authenticated to perform anti-replay checking before decryption.

Encrypted data : This is variable length filed contains transport layer segment or IP packet which is protected by performing ESP encryption.

ESP Trailer : ESP trailer field contains padding (0-255 bytes), pad length 8- bits and next header 8 - bits.

Padding (0-255 bytes) : Padding filed used to expand plain text message to required size or to align the encrypted data by adding padding bits to the actual data which provides confidentiality to traffic flow.

If an encryption algorithm requires the plaintext to be a multiple of some number of bytes (e.g., the multiple of a single block for a block cipher), the Padding field is used to expand the plaintext (consisting of the Payload Data, Padding, Pad Length, and Next Header fields) to the required length.

Pad Length (8 bits) : This is mandatory field in ESP protocol which used to indicate the number of pad (protection) bytes added into the packet.

Indicates the number of pad bytes immediately preceding this field.

Next Header (8 bits) : The same bit length as of pad length used to identifies the type of encrypted data in the Payload Data field. Identifies the type of data contained in the Payload Data field (an upper-layer protocol - TCP, UDP, or an IPv6 extension header).

ESP Authentication Data : This is variable length field whose length depends upon encryption algorithm used.

A variable-length field (must be an integral number of 32-bit words) that contains the Integrity Check Value computed over the ESP packet minus the Authentication Data field. As mentioned earlier ESP encrypts the data the reason it provide data confidentiality during transmission.

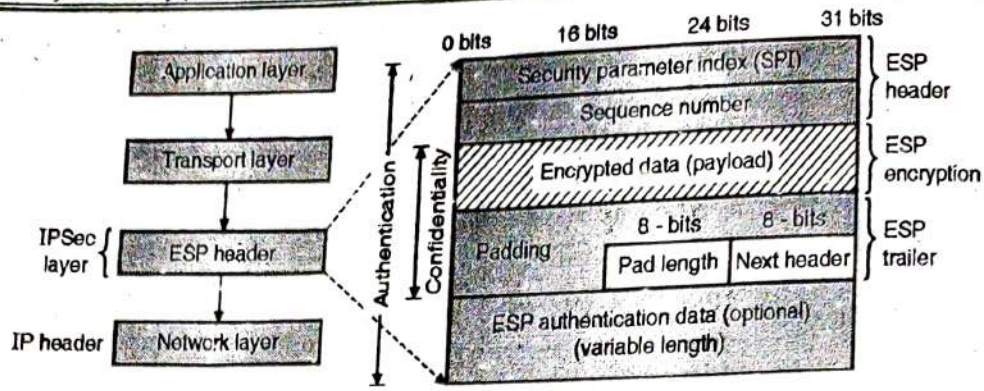
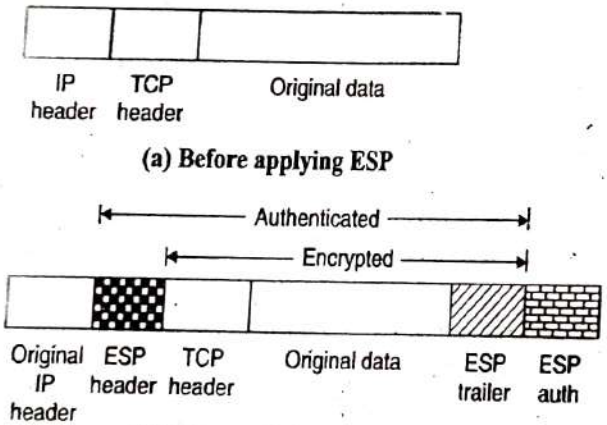


Fig. 4.6 : ESP header, trailer and encryption

Modes of Operation

(i) ESP Transport mode

In this case ESP header is added before the transport layer header (like TCP,UDP) and trailer is added after the IP Packet whereas if authentication is required then authentication data is added after the ESP trailer. Fig. 4.7 shows transport mode in ESP.



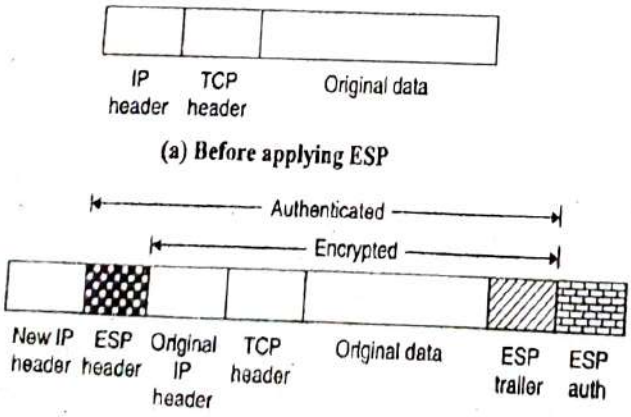
(a) Before applying ESP

(b) After applying ESP

Fig. 4.7 : Transport mode in ESP

(ii) ESP tunnel mode

In this case ESP header is added before original IP header and ESP trailer after the original data.



(a) Before applying ESP

(b) After applying ESP

Fig. 4.8 : Tunnel mode in ESP

The whole packet is encrypted. As whole packet is encrypted so New IP header will be added, which will contain information for routing from on network to another, so that packet can be transmitted.

Fig. 4.8 shows tunnel mode in ESP.

Q. 5 Explain ISAKMP protocol for IP sec.

Dec. 16, May 17

Ans. : ISAKMP protocol for IP sec

The internet security association and key management protocol is a framework that defines the formats of payload, the mechanics of implementation of a key exchange protocol, and the exchange of a security association between the parties. ISAKMP protocol defines the mechanics of implementing a key exchange protocol, and agreement between communicating parties i.e. which are the different features of IPSec protocol has to use etc. and all (simply its negotiation of security association).

ISAKMP features

It is used to authenticate of remote entity. It manages the secure session between communicating parties by applying different cryptographic techniques.

Exchanging required information about key sharing. Negotiation over all data transmission by applying security policies. The reasons ISAKMP establish secure communicating channel between two parties and authenticate them for secure key exchange and negotiation on certain security terms and condition.

ISAKMP header

1. **Initiator cookie** (64 bit) : The cookie of the entity that initiated SA establishment, SA notification, or SA deletion.
2. **Responder cookie (64 bit)** : The cookie of the entity that is responding to an SA establishment request, SA notification, or SA deletion.
3. **Next payload (8 bits)** : Indicates the type of the first payload in the message.
4. **Major version (4 bits)** : The major version of the ISAKMP protocol in use.

5. **Minor version (4 bits) :** The minor version of the ISAKMP protocol in use.
6. **Exchange type (8 bits) :** Indicates the type of exchange being used. This dictates the message and payload orderings in the ISAKMP exchanges.
7. **Flags (8 bits) :** Indicates the options that are set for the ISAKMP exchange.
8. **Message ID (32 bit) :** A unique value used to identify the protocol state during Phase 2 negotiations. It is randomly generated by the initiator of the Phase 2 negotiation.
9. **Length (32 bit) :** The total length of the ISAKMP header and the encapsulated payloads in bytes.

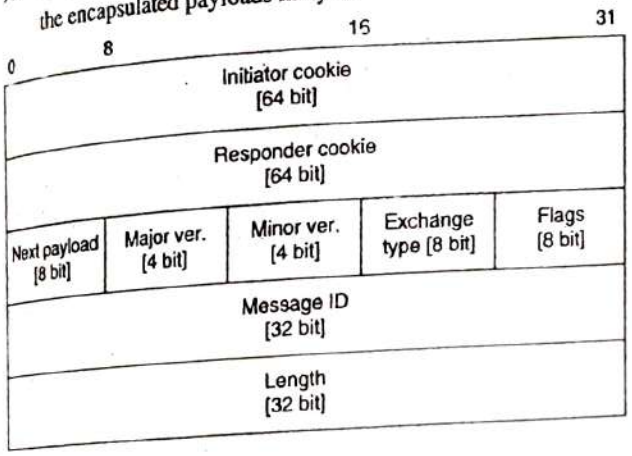


Fig. 4.9 : ISAKMP header format

Q. 6 Explain OAKLEY key determination protocol.

May 16

Ans. :

OAKLEY key determination protocol

It is a key Determination Protocol proposed by Hilarie K. Orman in 1998, which is a firm base for broadly used Internet Key Exchange protocol.

Diffie-Hellman key exchange algorithm is used in between authenticated parties', so on insecure connection also both the parties can exchange the keying material over the network. Hence it is also known as Key agreement protocol.

This protocol was proposed to increase the cryptographic strength where it allows two organizations to agree on a shared value without requiring encryption. The shared value is immediately available for use in encrypting subsequent conversation, e.g. data transmission and/or authentication.

OAKLEY is a generic key exchange protocol, because the keys that it generates might be used for encrypting data with a long privacy lifetime, 20 years or more.

For distribution of keys there are some options laid down. Along with Diffie-Hellman key exchange, OAKLEY protocol can be used to generate a new key from an existing key and before distributing the newly (externally) derived key encryption is performed.

As per the security requirements and performance requirement of two parties protocol allows using some of the forward secrecy features and anti-clogging features. It also gives an authority to use encryption and non-encryption algorithms.

Q. 7 Explain different phases of IKE protocol.

Ans.:

IKE has two phases of operations :

1) **IKE phase 1 :** Aggressive mode of exchange : Uses to negotiate IKE SA

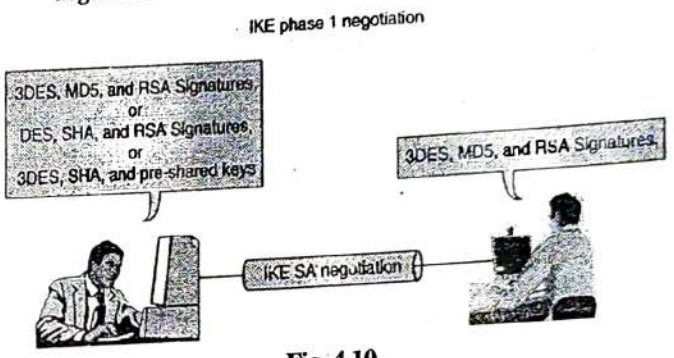


Fig. 4.10

For instance

As shown in Fig. 4.10 user A and user B want to talk IKE, They must agree on a common IKE protection suite. The initiator (user A) proposes several protection suites and the responder (user B) chooses one of the offered protection suite. The selection is made according to the priorities and the configuration of the responder.

In the Fig. 4.11, user A proposes three protection suites out of which user B chooses the second protection suite. Both must agree on the same protection suite. If they do not, no common policies may exist and the IKE session may be terminated.

2) **IKE Phase 2 :** Quick mode of exchange : Uses to negotiate IPSec's SA

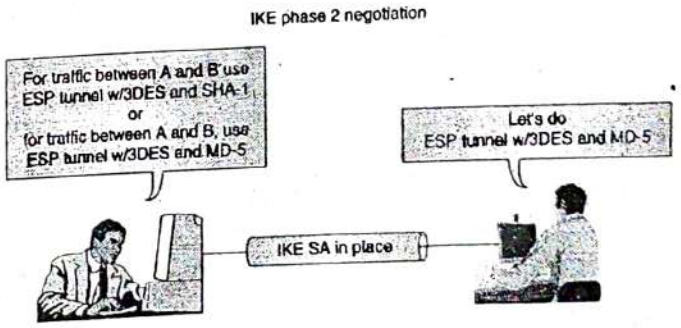


Fig. 4.11

For instance

As shown in Fig. 4.11 user A and user B wish to protect the traffic with IPSec and the IKE SA is already established between them. User A proposes various IPSec security policies and user B

chooses one of them (with highest priority according to configuration). After successful negotiation, keying material is exchanged and IPSec SAs are established to protect network traffic

Q. 8 What are the benefits of IPSec ? **Dec. 14**

Ans. : Benefits of IPSec

For secure access of remote computer over Internet IPSec is used. For securely connecting all branches of bank sectors over internet IPSec protocol is used. For secure communication between same organization which are located at different places. For connecting to college server any time from any location IPSec protocol is used.

Most of the corporate sector allowing employees to performed their task from home and update it to company server at any time from any location or secure access of company server at any time. IPSec now-a-days called as one of the standard of Virtual Private Networks that allow low cost connectivity, secure data transmission between various locations over insecure communication channel.

If IPSec is implemented in a *firewall or router*, can provide strong security to the ongoing traffic crossing the network.

Q. 9 What is VPN ? Explain types of VPN. **Dec. 16**

Ans. : VPN

VPN stands for Virtual Private Network. The network technology VPN extends the private network (LAN) over a public network (Internet).

The computer (or network) can be connected securely using VPN if they are physically connected. The companies use VPN, which allows remote workers to connect securely to their private network over public network. Also it is used to interconnect remote offices with a head office. VPN is creating secure tunnel between two more devices. It also helps to protect the web traffic from snooping and interference.

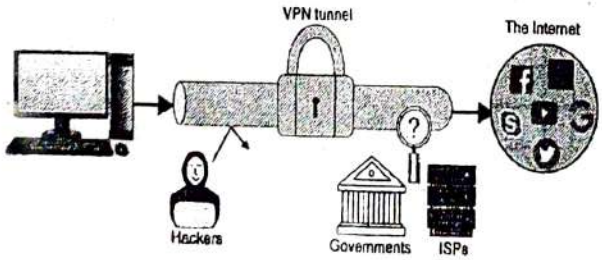


Fig. 4.12 : Virtual Private Network

Q. 10 Explain the operation of Secure Socket Layer (SSL) protocol in detail. **May 17**

Ans.:

Secure Socket layer invented by Netscape communications in 1994. Secure Socket layer is an internet protocol used for securely exchanging the information between client's web browser and the web server.

Secure socket layer ensure the authentication, data integrity and data confidentiality between web browser and web server i.e. it creates a secure tunnel between client and server. The main role of SSL is to provide the security to web traffic in all the way.

The current version of SSL is 3.0. The position of SSL in TCP/ IP protocol suite is shown in Fig. 4.13. SSL is works in between application layer and transport layer the reason SSL is also called as **Transport Layer Security (TLS).**

Transport Layer Security (TLS) protocol is used to ensure security between communicating applications and their users on the Internet. Main function of transport layer protocol is to protect attacker when a server and client communicate, it ensures that attacker or third party should not modify or tamper with any message.

TLS is the successor to the Secure Sockets Layer (SSL). Will discuss TLS in section 4.13.

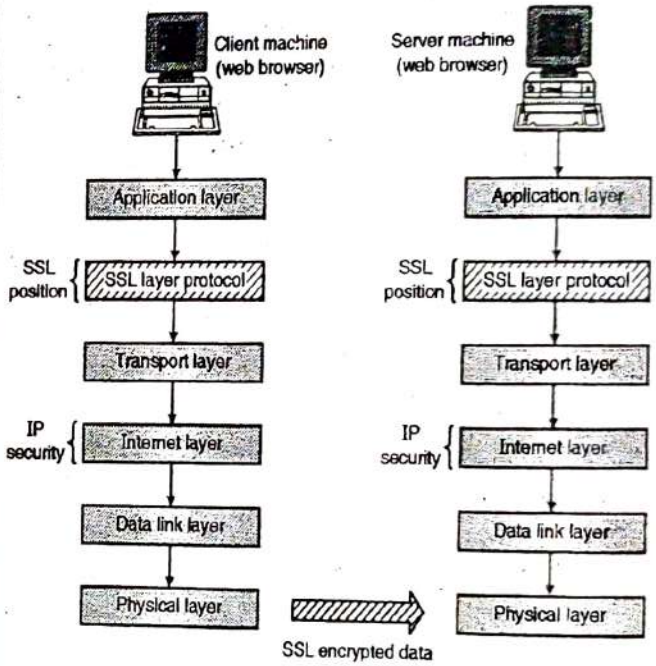


Fig. 4.13 : Position of SSL in TCP/ IP protocol suite

The data will not be passed directly to transport layer instead it will passed to secure socket layer. Secure Socket Layer will perform encryption to the data received by application layer and add its own encryption information header called SSH i.e. Secure Socket Layer Header. In the receiver's end SSL will remove the SSH header and then pass data to application layer.

The Fig. 4.14 shows position of SSL protocol in TCP/ IP protocol suite. SSL protocol uses digital certificate and digital signature for securely communication between client machine and server machine. SSL encrypt the data received from application layer of client machine and add its own header (SSL Header) into the encrypted data and send encrypted data to the server side.

Upon receiving encrypted data, server removes the SSL header and decrypts the data and sends the decrypted data to application layer. SSL is composed of four protocols in two layers, which support SSL as shown in Fig. 4.14. Out of the four, the two

most important protocols that are at the heart of SSL are the SSL Handshake Protocol and the SSL Record Protocol, The other two protocols such as SSL Change Cipher Specification and the SSL Alert Protocol play a minor role relatively to previous two protocols.

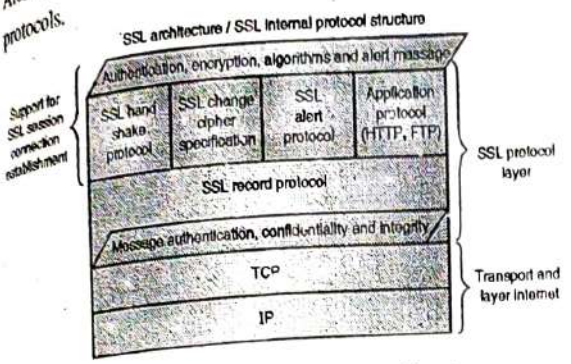


Fig. 4.14 : SSL protocols internal architecture

The role of these higher-level protocols is the connection establishment, use of required cipher techniques for data encryption and alert (warning, error if any) generation before starting actual data transmission process between client and server.

The SSL Record Protocol is responsible for encrypted data transmission and encapsulation of the data sent by the higher layer protocols (handshake, alert, HTTP) also to provide basic security services to higher layer protocols. SSL was designed to make use of TCP protocol to provide a reliable secure process-to-process delivery of entire message/packets. We will discuss how client machine securely communicate with the server machine by using underlying network architecture.

Q. 11 Explain Secure Socket Layer handshake protocol in brief.

Ans. :

Secure Socket Layer handshake protocol

As the name suggests when we meet to our friend/colleagues, we have habit to say hi/hello and do the *shake-hands* with each other before starting our actual communication. SSL handshake protocol uses somewhat same ideology but in terms of client and server.

The first sub-protocol of SSL called handshake protocol used for secure communication between client and the server using an SSL enabled connections. In this protocol client authentication to the server is more important that server authentication because server has different options available for client authentication. The details steps of SSL **handshake protocol** are shown in Fig. 4.15.

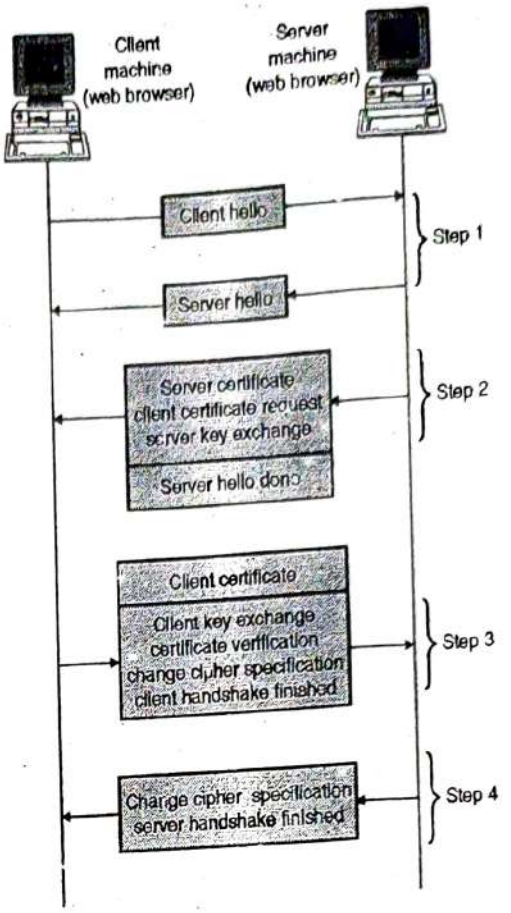


Fig. 4.15 : SSL handshake protocol

1. It is used by client and server to start communication using SSL enabled connection.
2. The handshaking is done 4 phases :

Q. 12 Explain TLS.

Ans.: TLS

It is an extension of secure socket layer. The main aim of TLS is to provide security and data at the transport layer between two web applications. Almost all web browsers and web servers support TLS. It ensures no eavesdropping and tampering of the message.

The TLS protocol consists of two main components : Handshake protocol, to start session and share private key, and Record protocol, to transmit data securely using the shared keys.

Handshake protocol : In the Handshake protocol, both sending and receiving parties acknowledge their protocol versions, agree on cryptographic and compression algorithms, optionally authenticate each other through certificates, and use public-key encryption techniques to generate shared private keys.

Following are the steps

Step 1 : Clients sends message publicly to containing version of TLS,32-byte random number r_A consisting of a 4-byte timestamp and a 28-byte random number.

A Cipher Suite list in decreasing order of preference for each of the following algorithm families : Public-Key Algorithm (PKA), encryption algorithm used in the Cipher Block Chaining, and compression algorithm (COMPRESS).

Step 2 : Server informs the client about the decided algorithms (after examining the Cipher Suite list sent by the client) along with a 32-byte random number r_B constructed similarly as r_A.

Step 3 : Client replies with a number called pre-master secret s_{pm} using the public key algorithm PKA with public keys retrieved from the server's certificate signed by a Certifying Authority (CA).

Step 4 : Both parties independently calculate the 48-byte long master secret, s_m, to further obtain the keys to exchange data. The master secret is calculated using Pseudorandom Function

$$PRF: s_m = PRF(s_{pm}, \text{"master secret"}, r_A \| r_B)$$

It is worth mentioning that in the previous version of TLS the master secret was computed as follows, before MD5 proven to be insecure :

$$MD5(s_{pm} \| SHA\text{-}1(A \| s_{pm} \| r_A \| r_B)) \| MD5(s_{pm} \| SHA\text{-}1(BB \| s_{pm} \| r_A \| r_B)) \| MD5(s_{pm} \| SHA\text{-}1(CCC \| s_{pm} \| r_A \| r_B))$$

Where A, BB, and CCC are strings added for padding.

Step 5 : At this stage, both parties know s_m, s_{pm}, r_A, and r_B, they independently compute the Key Block (KB) that contains all needed private shared keys for this session : $KB = P\ RF(s_m, \text{"key expansion"}, r_A \| r_B)$ KB is then broken into six pieces and labeled as K1, K2, ..., and K6, before terminating the Handshake phase

Record protocol : Now the client and the server are ready to communicate securely using the key block as a set of security parameters obtained by the Handshake protocol. The Record protocol takes data to be transmitted in one endpoint, fragments the data into manageable blocks, compresses the data, applies a MAC, encrypts by block cipher, and transmits the result. Received data is then decrypted, verified, decompressed, reassembled, and then delivered to higher-level application on the other endpoint. In short, Record protocol ensures that the connection is private via symmetric encryption by session unique keys and reliable via integrity check. Suppose the client wants to send data chunk, d.

The client

1. Compresses the data using the agreed algorithm :
   $d' = COMPRESS(d)$.
2. Hashes the compressed data for data integrity using K_2: $d'' \{d', HMAC_{K2}(d')\}$.
3. Encrypts the data along with its MAC using CBC mode block cipher BCA where the secret key is K_1 and the initialization vector is K_3:
   $d''' = BCA_{K1}(d'' K_3)$.
4. Sends d''' over the public channel.

And the server retrieves d from d'''

1. Decrypts the data along with its MAC using BCA_{K1}.
2. Verifies data integrity by computing HMAC of data using K_2 and comparing it with the HMAC computed on the client side.
3. Decompresses to retrieve d.

The process is reversed when server wants to send data to the client while the last three pieces of the key block is used instead.

Q. 13 What is PGP? Explain operations of PGP. May 15

Ans.: PGP

We all are aware that most popular use of Internet is to send the email and chatting with the friend's, partner etc. But have you ever think that if we are sending mail to intended person is going in his inbox only?

Security concerns have estimated that only about one in every 100 messages is secured against interception and modification attacks. Are we aware that sending an email to business partner or friends in clear text message is going through thousands of machines (between sender and receiver before it reaches to intended recipients?) these machines might read and saved the contents of email for future use? Many people think that name given in sender of the mail identifies who actually sends it.

When you send a message through email, we cannot guarantee that it will be deliver to correct destination or received exactly what you sent. And even there is a no way of knowing that the message is received read and forwarded by attacker.

Because of wide spared problem of email modifications, sending it to wrong destination by intermediate parties, email spoofing, we need a competing solution to overcome and address the issues of authentication, integrity and reliability of the messages between sender and receiver. The public key cryptography play an important role because of two keys used, only intended sender can decrypt the message using his public key as message encrypted using private key of the sender.

The solution is called as Pretty Good Privacy (PGP) program/ software which provide the secrecy and non-repudiation of data sent over Internet especially by email. Pretty Good Privacy (PGP) is a popular open-source freely available software package/ techniques used to encrypt and decrypt email messages over the Internet.

PGP is an e-mail security program written by Phil Zimmermann in 1991, PGP program become a de facto standard for e-mail security used to store the encrypted files so that it can be non-readable by other users or intruders. This program also be used to send an encrypted digital signature, let the receiver verify the sender's identity and know that the message was not changed or modified while transmission.

Once the file is encrypted using PGP program only the intended recipient can decrypt it. Once message content digitally singed by sender, the sender guarantee to the recipients that message or file comes from valid sender and not by attacker. Digital signature functionality of PGP guarantees that the message or file come from the sender and not from an intruder.

Q. 14 What is Backdoors and Key Escrow in PGP ? **May 16**

Ans.: Backdoors

A **Backdoor** is a method for bypassing normal authentication in a system and thus, provide unauthorized remote access to the system to malicious users. A backdoor is a "feature" in the software of PGP like an utility functions but not in the encryption algorithm that allows an outside party to decrypt which is encrypted by PGP. A Backdoor may be implemented as a hidden part of a program or a separate program or even be implemented by hardware.

An example, in 2003 a Backdoor was planted in Linux Kernel. In a conditional statement for checking root access permission, '==' was replaced with '='. As a result, it gave unauthorizd access to malicious callers. Even very recently, in 2015, **Juniper Networks** have warned about a malicious Backdoor in their firewalls that automatically decrypts VPN traffic.

There are two types of Backdoors – **Object Code Backdoors** and **Asymmetric Backdoors**.

In **Object Code Backdoors**, software source code remains unchanged, but the object code gets modified maliciously. As the object code is designed to be machine readable, it becomes much more difficult to detect. These type of Backdoors are inserted in the on-disk object code or inserted at some point during compilation, linking or loading.

Recompiling the software source code may get rid of the Backdoors. So, malicious users sometimes change the compiler source code in such a way that, whenever it compiles, links and loads the source code, the Backdoor is inserted. These Backdoors can be fixed by recompiling the compiler and removing the Backdoor inserting codes.

Normally, Backdoors are symmetric. Anyone who finds the Backdoor, can in turn use it. But, **Asymmetric Backdoors** can be exploited only by the attacker who plants it, even if the Backdoor implementation becomes public. This type of attacks are termed as **Kleptography** and they can be carried out in software, hardware or in combination of both. The theory of Asymmetric Backdoors is a part of a larger field named **Cryptovirology**.

Key Escrow

Key escrow is a cryptographic key exchange process in which a key is held in escrow, or stored, by a third party. A key that is lost or compromised by its original user(s) may be used to decrypt encrypted material, allowing restoration of the original material to its unencrypted state.

Key escrow systems provide a backup source for cryptographic keys. Escrow systems are somewhat risky because a third party is involved. The Clipper Chip was a U.S. government encryption chipset introduced in 1993. The chipset was promoted as an encryption device with a government-held (escrow) master key to facilitate encryption in the face of security threats. The controversial Clipper Chip was defunct by 1996, but the concept evolved into the Pretty Good Privacy (PGP) encryption tool, which is used worldwide.

Key escrow (also known as a "fair" cryptosystem) is an arrangement in which the **keys** needed to decrypt encrypted data are held in **escrow** so that, under certain circumstances, an authorized third party may gain access to those **keys**.

Q. 15 Write a short note on S/MIME. **May 15**

Ans. : S/MIME

S/MIME stands for Secure/Multipurpose Internet Mail Extensions provides a de facto standard to send and receive secure Multipurpose Internet Mail Extensions (MIME) data.

S/MIME developed by RSA Data Security, S/MIME version 3 is now being maintained by the S/MIME Working Group of the Internet Engineering Task Force (IETF). As explained in PGP, because of large number of increasing Internet usage for sending and receiving emails over an insecure communication channel increases the risk of data modification, confidentiality, authentication and non-repudiation.

We need our mail should be safe from unauthorized users. It should reach to intended recipients only. Based on the popular Internet usage, S/MIME provides the different cryptographic security services to secure electronic messaging applications: authentication, message integrity and non-repudiation and data security. Traditional mail user agents (MUAs) uses S/MIME to add cryptographic security services to mail that is sent, and to interpret cryptographic security services in mail that are received.

S/MIME uses both symmetric as well as asymmetric key cryptographic techniques to sign and encrypt e-mail. Sender as well as receiver of the mail has two keys: A private key, which is kept secret and a public key, which is available to everyone. Mails encrypted using senders private key can only be decrypted using his public key and vice versa.

Mail signing concepts

Generally when sender sends a message he could just encrypt the message using his private key at the receiver side. If the message decrypted using senders public key then we can say that the message came from authenticated user and its content cannot be modified, because a message, that can be decrypted using senders public key must have been encrypted using senders private

key only. To increase the performance S/MIME uses the following concepts.

The message is not encrypted using receivers public key instead of that it is encrypted using a randomly created symmetric session key because symmetric key is faster than asymmetric key cryptography. The generated session key is encrypted using receiver's public key so that only receivers can retrieve the session key and thus decrypt the original message.

The following steps are taken in order to create an encrypted message :

1. The user writes the message in plain text.
2. Triple DES algorithm is used to create random session key
3. The message is being encrypted using the random session key.
4. For every recipient, the session key is being encrypted using the recipient's public key.

S/MIME-e-mail software must support Secure Hash Algorithms (SHA-1) standard and Message Digest Algorithm (MD5) in order to provide backward-compatibility with MD5-digested S/MIME v2 messages.

Digital signatures : To encrypt the message digest, the S/MIME client must support DSS (Digital Signature Standard) and should support RSA (Rivest, Shamir, Adleman)

Content Encryption: To encrypt the message content (symmetrically, using a random session key), Triple DES must be supported

Key encryption and management : To encrypt the session key, Diffie-Hellmann algorithm must be supported. Key S/MIME uses X.509v3 certificates to determine whether a public key used to verify a signature is trustworthy. The certificate signed by Certificate Authority (CA) for claiming that public key belongs to the person.

S/MIME (Secure/Multipurpose Internet Mail Extensions) is a specification for secure electronic mail providing authentication and confidentiality. It is not a particular software product but a standard designed to be implemented by various e-mail vendors, so that any two S/MIME-supporting mail clients can communicate securely.

Q. 16 What is secure electronic transaction ? **May 16**

Ans. :

Secure electronic transaction

SET stands for Secure Electronic Transaction. It is an encryption and security specification protocol designed to protect credit card transactions over an insecure channel such as Internet.

SET is not a payment system it is set of rules and regulations designed to protect credit card payments of users, employee over an open network such as Internet in a secure way.

SET was developed in 1996 by VISA and MasterCard, with participation from different leading technology companies, which includes Microsoft, IBM, Netscape, RSA, Teresa Systems and VeriSign.

After testing of the SET in 1998 it declares as a standard for safeguarding credit card purchases made over open networks and made it available to users with following requirements.

SET create a secure communications channel among all parties involved in a transaction.

SET provides privacy because the information is only available to sender, receiver and bank or the communication parties' involved in transaction.

SET provides confidentially, only sender and his intended receiver should be able to access the contents of a message. It assures to card holder is that is safe and accessible only to the intended recipient.

SET provides integrity of the message. Integrity gives assurance that data received exactly as sent by an authorized entity. (No alteration, no modification, no deletion and no intersection etc.).

Q. 17 List and explain various participants involved in Secure Electronic Transaction (SET). **May 17**

Ans.:

Following are the components of the Secure Electronic Transaction (SET) which involves in the electronic payment as shown in Fig. 4.16.

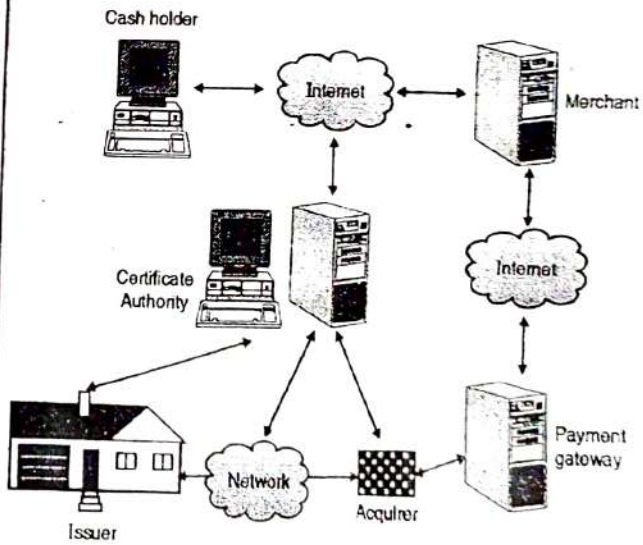


Fig. 4.16 : SET Participants

The cardholder : called as buyer in the transaction who initiates the transaction.

The merchant : Also called seller of goods and services which maintains an account with a bank or acquirer.

The acquirer : Also known as bank or financial institution. The financial institution that establishes an account with a

merchant and processes payment card authorizations and payments.

The issuing bank : Bank that maintains the account of the buyer and issues a credit card to the buyer and also sets limit on the amount of purchases.

Certification Authority (CA) : Certification Authority (CA) is a trusted unit that helps to issue certificates.

A CA takes the certificate request from owner, verifies the requested information according to the terms and conditions of the CA, and uses its private key to apply digital signature to the certificate. Responsibility of the CA is to identify the correct identity of the person who asks for a certificate to be issued, and make sure that the information contained within the certificate is legal and later digitally sign on certificate.

This is an entity that is trusted to issue X509v3 public-key certificates for cardholders, merchants, and payment gateways.

Payment gateways : It is designated third party that processes merchant payment messages. The merchant exchanges Secure Electronic Transaction messages with the payment gateway over the Internet, while the payment gateway has some direct or network connection to the acquirer's financial processing system.

Following are the steps of interactions used in SET protocol :

1. **The customer opens the account :** Once the customer obtains a credit card account, such as MasterCard or Visa, from the bank which supports electronic payment and Secure Electronic Transaction then customer may proceed for future communication over network.
2. **The customer receives a certificate :** After suitable verification of identity, the customer receives an X.509v3 digital certificate, which is signed by the bank which verifies the customers RSA public key and its expiration date.
3. **Merchants have their own certificates :** A merchant have two public keys one for signing message and another for key exchange The merchant also needs a copy of the payment gateway's public-key certificate.
4. **The customer places an order :** Here customer first browsing through the merchant's Web site to select items and determine the price. The customer now sends its list of items to be purchased to the merchant. Upon receiving list of items from customer merchant returns an order from containing the list of items, their price, a total price, and an order number to the customer.
5. **The merchant is verified :** Along with order number, the merchant sends a copy of its certificate, so that the customer can verify that he or she is dealing with a valid merchant store.
6. **The order and payment is verified :** The customer sends both order and payment information to the merchant, along with the customer's certificate (approved by CA). Customer also confirms the purchase of the items in the order form. The payment contains credit card details. The payment information is encrypted in such a way that it cannot be read by the merchant. The customer's certificate enables the merchant to verify the customer.
7. **The merchant requests payment authorization:** The merchant sends the payment information to the payment gateway for authentication as well as to check whether customer's available credit is sufficient for this purchase.
8. **The merchant confirm the order :** Upon receiving payment confirmation from customers credit, the merchant sends confirmation of the order to the customer.
9. **The merchant provides the goods or service :** After all verification the merchant provides the goods or service to the customer.
10. **The merchant request payment :** This request is sent to the payment gateway, which handles all of the payment processing.

Chap 5 : Intrusion and Firewall

Q. 1 What is firewall ?

Ans.:

Firewall

Firewall is called as barrier place between inside and outside network to protect organization from inside and outside hackers. It also filters all traffic between intranet and extranet which runs through it. The main purpose of the firewall is to keep attackers outside the protected environment. For that policies are set in the firewall to decide what is allowed and what is not allowed.

Moreover we can decide the allowed places, allowed users, allowed sites, can provide different access rights to different category of the users.

Example : Cyber am through which only educational sites are allowed through college internet and non-educational sites like facebook, twitter can be blocked using firewall.

Q. 2 What are the various characteristics of firewall ?

May 16, Dec. 16, May 17

Ans.:

Following lists the characteristics as well as design goals for a firewall :

1. All inside and outside traffic must pass through the firewall. This is possible only because of physically blocking of all access to the local network except via the firewall.
2. The traffic defined by the local security policy will only allowed to pass through the network. Different types of firewall are used to define the policies as per the norms decided.
3. The firewall itself is immune to penetration. Different techniques are used to control access and enforce the site's security policy.

Q. 3 What are the disadvantages of firewalls ?

Ans. :

Following are the disadvantages of firewall :

1. **Viruses**

Not all firewalls have full protection against computer viruses because virus uses different encoding techniques to encode files and transfer them over Internet.

2. **Attacks**

A firewall cannot prevent users or attackers with modems from entering in to or out of the internal network, thus bypassing the firewall and its protection completely.

3. **Architecture**

Firewall architecture depends upon single security mechanism failure. If that security mechanism has a single point of failure, affects on entire firewall programs which opens the loop falls for intruders.

4. **Configuration**

Firewall doesn't have mechanism to tell administrator about incorrect configuration. Only trained professionals in the field of network security can configure firewall properly.

5. **Monitoring**

Firewall doesn't give notification about hacking. It will notify only about threat occurrences. The reason is, organization demands additional hardware, software and different networking tools as per there requirement hence there is no control on it.

6. **Encryption**

Firewall and Virtual Private Networks (VPNs) don't encrypt confidential documents and E-mail messages sent within the organization or to outsiders. Dignified procedures and tools are needed to provide protection against confidential documents.

7. **Masquerading**

Firewalls can't stop hacker those who steal login id and password of authentic user to gain access to a secure network. Once attacker gains full access of the entire network, attacker can delete or change the network policies of organization.

8. **Vulnerabilities**

Firewall can't tell other venerability that might allow a hacker access to your internal network.

Q. 4 Describe types of firewall in detail.

Dec. 16, May 17

Ans.:

A firewall is a kind of reference monitor. All network traffic passes through firewall. That's why it is always in invoked condition. A firewall is kept isolated and cannot be modified by anybody other than administrator. Generally it is implemented on a separate computer through which intranet and extranets are connected.

Following are the common architectural implementations of firewalls :

1. **Packet Filtering Gateway**

It is the most simple and easy to implement firewall. Packet filtering is done on the basis of packets source or destination address or based on some protocol type like HTTP or HTTPs. If the firewall is placed just behind the router then the traffic can be analyzed easily. In the Fig. 5.1 it is shown that how packet filtering gateway can block traffic from network 1 and allow traffic from network 2.

Also the traffic using telnet protocol is blocked. Packet filters do not analyze the contents of the packet rather they just check IP address of the packets as shown in Fig. 5.1. The biggest disadvantage of the packet filtering gateway is that it requires lot of detailing to set policies.

Example

If port 80 is blocked. If some applications essentially need use of port 80 then in this case we have to provide all the details of those applications for which port 80 is needed.

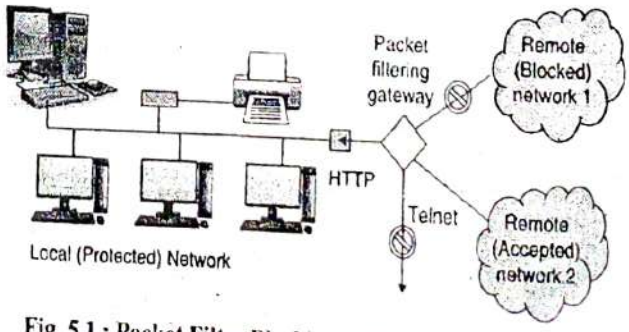


Fig. 5.1 : Packet Filter Blocking Addresses and Protocols

2. Stateful Inspection Firewall

Packet filtering is done one packet at time. Sometimes attacker may use this technique for their attack. Attacker can split the script of attack into different packets so that the complete script of attack cannot be identified by packet filtering firewall. To avoid this stateful inspection firewall keeps record of states of the packets from one packet to another. Thus sequence of packets and conditions within the packets can be identified easily.

3. Application Proxies

Packet filters cannot see inside the packets. From the packet headers they just get IP addresses for filtering. Application proxy is also known as a bastion host. Fig. 5.2 shows firewall proxies.

Example

A college wants to publish a list of selected students. Then they just want students to read that list. No student can change that list. Moreover students cannot access more data than the list.

Application proxy helps us in this regard. Here it helps us to check only list is displayed on the screen and not more than that. That list should not have any modified contents. Proxies on the firewall can be customized as per the requirements.

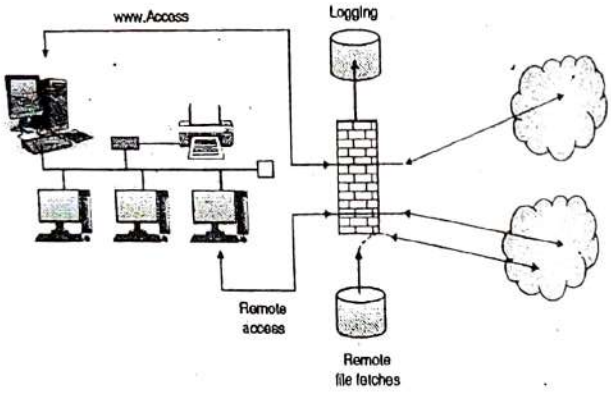


Fig. 5.2 : Firewall Proxies

4. Guard

A guard is kind of complex firewall. It works similar to proxy firewall. Only difference is that guard can decide what to do on behalf of the user by using available knowledge. It can use knowledge of outside users identity, can refer previous interactions, blocked list etc.

Example

In order to increase the speed of the internet a school can set download limit for the students.

A student can download only 20mb data per day etc.

5. Personal Firewalls

For a personal use to keep separate firewall on a separate machine is quite difficult and costly. So personal users need a firewall capability on lower cost. An application program which can have capabilities of a firewall can solve this problem.

It can screen incoming and outgoing traffic on a single host. Symantec, McAfee, Zone alarm are the examples of personal firewalls. Personal firewalls can be combined with antivirus systems.

Q. 5 How firewalls are configured and managed ?

Dec. 13

Ans. : Firewall Configurations

1. Firewall with screening router

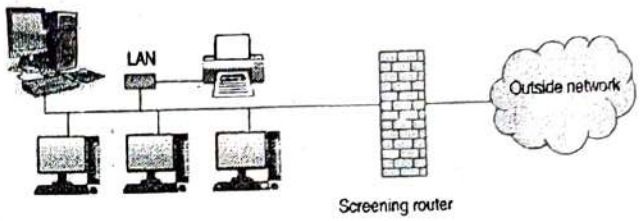


Fig. 5.3

The screening router is placed in between intranet and extranet. Another name for screening router firewall is network level or packet-filter firewall. Protocol attributes are used for performing the screening of incoming packets. The attributes like source or destination address, type of protocol, source or destination port, or some other protocol-specific attributes plays a vital role. A screening router performs packet-filtering and is utilized as a firewall. In a few cases a screening router may be utilized as perimeter assurance for the internal network or as the whole firewall solution.

2. Firewall on Separate LAN

Unauthorized internet users from accessing private networks connected to the internet are prevented by firewall, especially intranets. All messages entering or leaving the intranet (i.e., the local network to which you are connected) must pass through the firewall, which examines each message and blocks those that do not meet the specified security constraint.

To overcome the problem of the exposure of LAN, a proxy firewall can be installed on its own LAN.

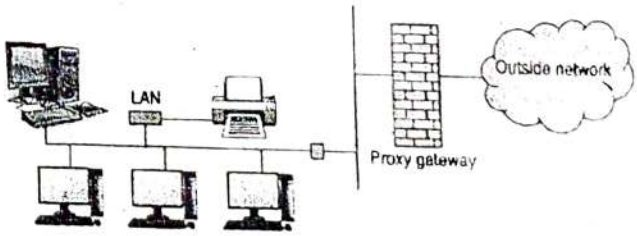


Fig. 5.4

3. **Firewall with Proxy and Screening Router**

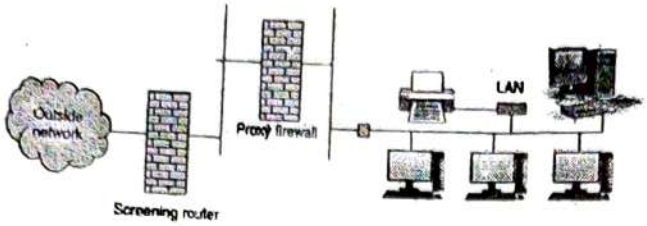


Fig. 5.5

If screening router is installed behind the proxy firewall, then it ensures the correct address to proxy firewall. In other words it is a double guard protection. If anyone fails LAN is not exposed.

Q. 6 What is Trusted System ? **May-16, May 17**

Ans.: Trusted System

Trusted system is level base security system where protection is provided and handled according to the different levels. This is commonly found in military, where information is categorized as unclassified (U), confidential (C), secret (S), top secret (TS), or beyond.

This concept is equally applicable in other areas, where information can be organized into categories and users can be granted clearances to access certain categories of data. When multiple categories or levels of data are defined, the requirement is referred to as **multilevel security**.

The general statement of the requirement for multilevel security is that a subject at a high level may not convey information to a subject at a lower or non-comparable level unless that flow accurately reflects the will of an authorized user. For implementation purposes, this requirement is in two parts and is simply stated. A multilevel secure system must enforce the following :

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.**

No write-down : A subject can write into an object of greater or equal security level. This is referred to as the ***-property** (pronounced star property)

These two rules, if properly enforced, provide multilevel security. For a data processing system, the approach that has been taken, and has been the object of much research and development, is based on the **reference monitor** concept. The reference monitor is a controlling element in the hardware and operating system of a computer that regulates the access of subjects to objects on the basis of security parameters of the subject and object. The reference monitor has access to a file, known as the security kernel database that lists the access privilege (security clearance) of each subject and the protection attributes (classification level) of each object. The reference monitor enforces the security rules (no read-up, no write-down) and has the following properties:

Complete mediation : The security rules are enforced on every access, not just, for example, when a file is opened (requires high performance overhead).

Isolation : The reference monitor and database are protected from unauthorized modification (requires impossibility for attacker to change database).

Verifiability : The reference monitor's correctness must be provable. That is, it must be possible to demonstrate mathematically that the reference monitor enforces the security rules and provided complete mediation and isolation. If provided, system is referred to as a trusted system. These are stiff requirements. Important security events, such as detected security violations and authorized changes to the security database, are stored in the audit file.

These are the systems whose failure may break a specified security policy. The base of the trusted system is as follows :

It combines software and hardware portions with respect to security.

1. It can act as a mediator. 2. It is tamperproof.
3. It is validated.

Q. 7 What is Access control security service?

Dec. 16

Ans. : Access control security service

Access Control is the ability to limit and control the access to the host systems. It prevents unauthorized use of a resource. The service used to prevent unauthorized use of a resources i.e. complete control over who can access to resources, under what conditions access can occur and what are different accessing methodology.

For example

It controls the access of resources which is to be made available only to legitimate user. Secondly it looks to the conditions of accessing the resource or network and what is allowed to be done to the resources.

Database administrator decides what should be stored in a database and to whom access rights can be given based on the needs of different users. Database administrator takes these decisions on the basis of access policies.

Following are the factors that the DBMS may consider for deciding access policies :

1. **Availability of Data :** While updating proper blocking and locking should be used so that other processes cannot interfere and can get correct data also.
2. **Acceptability of Access :** DBMS must protect sensitive data from unauthorized users.

3. **Assurance of Authenticity** : Sometimes database may permit some users to access sensitive data.

Example : During auditing of a failure database may give permission to auditor/administrator also to access the sensitive data in order to resolve the problem after looking at the severity of the things.

Q. 8 What is intruder and intrusion detection system ?

Ans. :

Intruder and intrusion detection system

An Intruder is a person who intercepts system availability, confidentiality and data integrity. Intruder's gains unauthorized access to a system with criminal intensions. Intruder may damage that system or disturbs data.

When an attacker or intruder attempts to break into an information system or performs an illegal action such as denial of service attacks, scanning a networks, ping scan, sending many request for connection setup using fake IP address, etc. which is legally not allowed, that is called as an intrusion.

Intrusion detection is an important technology that monitors network traffic, events and identifies network intrusions such as abnormal network behaviours, unauthorized network access and malicious attacks to computer systems.

The general example of intrusion detection is when we suffer from some disease and asking doctor what happen to me. Doctor suggests for blood checking and sends blood sample to laboratory for detection. The blood report given by pathologies is just detection of disease (number of platelets count, WBC, RBC, haemoglobin, etc.) then after checking the entire history of blood report doctor suggests medicine to cure the disease.

Here blood report is intrusion detection where as medicine given by the doctor after checking blood report is called intrusion detection system. Finally how fast patient get relief depends upon the doctor's education, experience and knowledge, joke apart let us move towards technical definition of IDS.

Q. 9 What are the challenges of intrusion detection ? May 16, May 17

Ans. : Challenges of intrusion detection

In order to better understand intrusion detection systems, it is important to realize that threats to networked computer systems come in a number of forms. According to the source of threats, potential intruders can be roughly classified into two categories :

1. **Outside Intruders** : The attack is launched by an unauthorized computer user. The attacker will stole or broken passwords, using system vulnerabilities or improper configurations, human engineering techniques, to gain access to computers.

2. **Inside Intruders** : Internal intruders, who have permission to access the system with some restrictions, In this case, the intruder already has legitimate access to a computer system, but utilizes any of the previously mentioned techniques to gain additional privileges and misuse the computer system. Sometimes inside intruders are more harmful than outside intruders. It is observed that 80% of intrusions and attacks come from within organizations.

Following are the possible type of attacks that intrusion detection needs to face :

Q.10 Explain Anomaly-based Instruction Detection System. May 16, May 17

Ans. : Anomaly-based Instruction Detection System

It is the process of comparing activities which are supposed to be normal against observed events to identify deviation.

An IDPS uses Anomaly based detection techniques, which has profiles that represent normal activities of user, host, connections or applications.

For example : Web activities are a normal activity done in a network. Anomaly based IDS works on the notation that "attack behavior" enough differ from "normal behavior" (IDS developer may define normal behavior).

Normal or acceptable behaviours of the system (e.g. CPU usage, job execution time etc.) if the system behaviour looks abnormal i.e. increasing CPU speed, too many job execution at a time then it is assumed that the systems is out of normal activity. Anomaly based detection is based on the abnormal behaviour of a host or network.

Database for such type of IDS is the events generated by user, host and network, and the "normal" behaviour of the systems. These events (historical data) are collected from the research laboratories which continuously work on normal and abnormal behaviour systems over a period of time.

Anomaly based IDS checks ongoing traffic, host activities, transactions and behaviour in order to identify intrusions by detecting anomalies. Host - based IDS generally uses anomaly based techniques.

This can be done in two ways:

1. **Threshold detection**

   Threshold is defined for all users for all groups and frequency of all events is measured comparing with threshold.

2. **Profile Based detection**

   Profiles of individuals are created and they are matched against the collected statistics for checking the irregular patterns.

Q. 11 Explain types of Intrusion detection systems (IDS). Dec. 16

Ans. :

There are four types of IDS.

1. **Network based**

The IDS monitors network traffic. It analyzes the network activities and protocol activities to identify suspicious activity of the network.

2. **Wireless**

The IDS monitors the wireless network traffic. It analyzes the network activities and protocol activities of wireless network.

3. **Network Behaviour Analyse**

These network behavior analyze identify the treats that create unusual traffic overflow, DDOS (Distributed Denial of Service) attacks, malwares, and policy violations.

4. **Host Based**

These IDS monitors the host and the event occurs within that host. Among above four types of IDS two are important and most commonly used to monitor the networks and hosts.

Chapter 6 : Confidentiality and Cyber Forensic

Q. 1 Explain Personally Identifiable information (PII).

Ans. :

Personally Identifiable information (PII)

Personally Identifiable Information (PII) is any data that could potentially recognize a specific individual. Any information that can be used to tell apart one person from another and can be used for deanonymizing anonymous data can be considered PII.

PII can be sensitive or non-sensitive. Non-sensitive PII is in order that can be transmitted in an unencrypted form without resulting in harm to the individual. Non-sensitive PII can be simply gathered from public records, phone books, corporate directories and websites.

Sensitive PII is in turn which, when disclosed, could result in harm to the individual whose privacy has been breached.

Sensitive PII should therefore be encrypted in transfer and when data is at rest. Such information adds biometric information, medical information, in Person Identifiable Financial Information (PIFI) and unique identifiers such as passport or Social Security numbers.

Q. 2 What is Cyber stalking ? Explain with example.

Ans. : Cyber stalking

Cyber stalking is a crime in which the attacker harasses a victim using electronic message, such as e-mail or Instant Messaging (IM), or messages posted to a Web site or a discussion group. A cyber stalker relies upon the secrecy afforded by the Internet to allow them to stalk their victim without being detected.

Cyber stalking messages differ from ordinary spam in that a cyber stalker targets a specific victim with often threatening messages, while the spammer targets a multitude of recipients with merely annoying messages. WHOA (Working to Halt Online Abuse), an online organization committed to the cyber stalking problem, reported that in 2001 58% of cyber stalkers were male and 32% female (presumably in some cases the perpetrator's gender is unknown). In a difference known as corporate cyber stalking, an organization stalks an individual.

Corporate cyber stalking (which is not the same thing as corporate monitoring of e-mail) is usually initiated by a high-ranking company official with a grudge, but may be conducted by any number of employees within the organization. Less frequently, corporate cyber stalking involves an individual pestering a corporation.

WHOA reported that, in 2001, cyber stalking began with e-mail messages most frequently, followed by message boards and forums messages, and less frequently with chat. In some cases, cyber stalking develops from a real-world stalking incident and continues over the Internet. However, cyber stalking is also sometimes followed by stalking in the physical world, with all its assistant dangers. According to former U.S. Attorney General Janet Reno, cyber stalking is often "a prologue to more serious behaviour, including physical violence".

In 1999, a New Hampshire woman was murdered by the cyber stalker who had endangered her in e-mail messages and posted on his Web site that he would kill her. There are a number of effortless ways to guard against cyber stalking. One of the most useful protection is to stay anonymous yourself, rather than having an identifiable online presence: Use your primary e-mail account only for communicating with people you trust and arrangement an anonymous e-mail account, such as Yahoo or Hotmail, to use for all your other communications.

Set your e-mail program's filtering options to avert delivery of unwanted messages. When choosing an online name, make it different from your name and gender-neutral. Don't put any identifying particulars in online profiles. Should you become the victim of a cyber stalker? The most effective course of action is to report the criminal to their Internet service provider (ISP). Should that option be impossible, or unproductive? The best thing is to change your own ISP and all your online names. WHOA news that over 80% of cases reported in 2001 and 2002 were resolved by

these methods, while 17% were reported to law enforcement officials. Cyber stalking, cyber squatting, and cyber terrorism are among the rising number of new computer and internet-related crimes, sometimes referred to collectively as cybercrime.

Q. 3 Distinguish Cyber stalking from other acts.

Ans. :

Distinguishing cyber stalking from other acts

It is important to draw a distinction between cyber-trolling and cyber-stalking.

Research has shown that actions that can be supposed to be harmless as a one-off can be considered to be trolling, whereas if it is part of a persistent campaign then it can be considered stalking.

Sr. No.	Motive	Mode	Gravity	Description
1	Playtime	Cyber-bantering	Cyber-trolling	In the moment and quickly regret
2	Tactical	Cyber-trickery	Cyber-trolling	In the moment but don't regret and continue
3	Strategic	Cyber-bullying	Cyber-stalking	Go out of way to cause problems, but without a sustained and planned long-term campaign
4	Domination	Cyber-hickery	Cyber-stalking	Goes out of the way to create rich media to target one or more specific individuals

Q. 4 List out the key factors in identifying Cyber stalking.

Ans.:

Cyber Angels has written about how to identify cyber stalking :

When identifying cyber stalking "in the field," and mostly when considering whether to report it to any kind of legal authority, the following features or combination of features can be considered to characterize a true stalking situation : malice, premeditation, repetition, distress, obsession, vendetta, no legitimate purpose, personally directed, disregarded warnings to stop, harassment and threats.

A number of key factors have been identified in cyber stalking :

False accusations : Many cyber stalkers try to harm the reputation of their victim and turn other people against them. They post fake information about them on websites. They may set up their own websites, blogs or user pages for this purpose. They post allegations about the victim to newsgroups, chat rooms, or other sites that allow public contributions such as Wikipedia or Amazon.com.

Attempts to gather information about the victim : Cyber stalkers may advance to their victim's friends, family and work colleagues to obtain personal information. They may publicize information on the Internet, or hire a private detective. Monitoring their target's online activities and attempting to trace their IP address in an attempt to gather more information about their victims.

Encouraging others to annoy the victim : Many cyber stalkers try to involve third parties in the annoyment. They may say the victim has harmed the stalker or his/her family in some way, or may post the victim's name and telephone number in order to encourage others to join the pursuit.

False victimization : The cyber stalker will claim that the victim is annoying him or her. Bocij writes that this fact has been noted in a number of well-known cases.

Attacks on data and equipment : They may try to harm the victim's computer by sending viruses.

Ordering goods and services : They order items or subscribe to magazines in the victim's name.

These frequently involve subscriptions to pornography or ordering sex toys then having them delivered to the victim's workplace.

Arranging to meet : Young people face a particularly high risk of having cyber stalkers try to set up meetings between them.

The posting of defamatory or derogatory statements: Using web pages and message boards to incite some response or reaction from their victim.

Q. 5 Write a short note on : Prevalence and impact.

Ans. : Prevalence and impact

According to Law Enforcement Technology, cyber stalking has increased exponentially with the expansion of new technology and new ways to stalk victims. Disgruntled employees pose as their bosses to post open messages on social network sites, spouses use GPS to track their mates' every move. Even police and prosecutors find themselves at risk, as gang members and other organized criminals come across where they live - frequently to intimidate them into dropping a case.

In January 2009, the Bureau of Justice Statistics in the United States released the study "Stalking Victimization in the United States", which was sponsored by the Office on Violence Against

Women. The report, based on supplemental data from the National Crime Victimization Survey, showed that one in four stalking sufferers had been cyber stalked as well, with the perpetrators using internet-based services such as email, instant messaging, GPS, or spyware.

The final report stated that around 1.2 million victims had stalkers who used technology to find them. The Rape, Abuse and Incest National Network (RAINN) in Washington D.C. has released statistics that there are 3.4 million stalking sufferer each year in the United States. Of those, one in four reported experiencing cyber stalking.

According to Robin M. Kowalski, a social psychologist at Clemson University, cyber bullying has been shown to cause higher levels of anxiety and depression for sufferer than normal bullying. Kowalksi states that much of this stems from the anonymity of the perpetrators, which is a common feature of cyber stalking as well. According to a study by Kowalksi, of 3,700 bullied middle-school students, a quarter had been subjected to a form of annoyment online.

Q. 6 Enlist the different types of Cyber stalker attacks.

Ans. : Types of Cyber stalker attacks

1. Stalking by strangers

According to Joey Rushing, a District Attorney of Franklin County, Alabama, there isn't a lone definition of a cyber stalker - they can be either strangers to the prey or have a former/present relationship. "Cyber stalkers come in all shapes, sizes, ages and backgrounds. They tour Web sites looking for an opportunity to take advantage of people".

2. Gender-based stalking

Annoyment and stalking because of gender online is common, and can include rape threats and other threats of violence, as well as the posting of the sufferer's personal information. It is blamed for limiting sufferer activities online or driving them offline entirely, thereby impeding their participation in online life and undermining their autonomy, dignity, identity, and opportunities.

3. Of intimate partners

Cyber stalking of intimate partners is the online annoyment of a current or former romantic partner. It is a form of domestic violence, and experts say its purpose is to control the victim in order to encourage social isolation and create dependency.

Annoyers may send repeated insulting or threatening e-mails to their sufferer, monitor or disrupt their sufferer' e-mail use, and use the victim's account to send e-mails to others posing as the victim or to purchase goods or services the victim does not want. They may also use the Internet to research and compile personal information about the victim, to use in order to annoy him or her.

4. Of celebrities and public persons

Profiling of stalkers shows that about always they stalk someone they know or, via delusion, think they know, as is the case with stalkers of celebrities or public persons in which the stalkers feel they know the celebrity yet the celebrity does not know them. As part of the risk they take for being in the public eye, celebrities and public figures are frequently targets of lies or made-up stories in tabloids as well as by stalkers, some even seeming to be fans.

In one noted case in 2011, actress Patricia Arquette quit Facebook after suspected cyber stalking. In her last post, Arquette explained that her security warned her Facebook friends to never accept friend requests from people they do not really know. Arquette stressed that just because people seemed to be fans did not mean they were safe. The media issued a statement that Arquette planned to communicate with fans entirely through her Twitter account in the future.

5. By anonymous online mobs

Web 2.0 technologies have enabled online groups of anonymous people to self-organize to target individuals with online defamation, fear of violence and technology-based attacks. These include publishing lies and doctored photographs, threats of rape and other violence, posting sensitive personal information about sufferer, e-mailing damaging statements about sufferer to their employers, and manipulating search engines to make damaging material about the victim more prominent. Sufferer frequently respond by adopting pseudonyms or going offline entirely.

Experts attribute the destructive nature of anonymous online mobs to group dynamics, saying that groups with homogeneous views tend to become more extreme. As members reinforce each others' beliefs, they fail to see themselves as individuals and lose a sense of personal responsibility for their destructive acts. In doing so they dehumanize their sufferer, becoming more aggressive when they believe they are supported by authority figures. Internet service providers and website owners are sometimes blamed for not speaking out against this type of annoyment.

A notable example of online mob annoyment was the experience of American software developer and blogger Kathy Sierra. In 2007 a group of anonymous individuals attacked Sierra, threatening her with rape and strangulation, publishing her home address and Social Security number, and posting doctored photographs of her. Frightened, Sierra cancelled her speaking engagements and shut down her blog, writing "I will never feel the same. I will never be the same".

6. Corporate cyberstalking

Corporate cyberstalking is when a company annoyes an individual online, or an individual or group of individuals annoyes an organization. Motives for corporate cyberstalking are ideological, or include a desire for financial gain or revenge.

Q. 7 Define Cybercrime and discuss its types.

Ans. : Cybercrime

The crime that involves and uses computer devices and Internet is known as cybercrime. Cybercrime can be committed in opposition to an individual or a group; it can also be committed against government and private organizations. It may be planned to harm someone's reputation, physical harm, or even mental harm.

Cybercrime can cause direct harm or indirect harm to whoever the sufferer is. However, the largest threat of cybercrime is on the financial security of an person as well as the government.

Cybercrime causes loss in billions each year.

Types of Cybercrime

1. **Hacking**

It is an unlawful practice by which a hacker breaches the computer's security system of someone for personal interest.

2. **Unwarranted mass-surveillance**

Mass surveillance means surveillance of a considerable fraction of a group of people by the authority especially for the security purpose, but if someone does it for personal interest, it is considered as cybercrime.

3. **Child pornography**

It is one of the most atrocious crimes that is brazenly practiced across the world. Children are sexually abused and videos are being made and uploaded on the Internet.

4. **Child grooming**

It is the practice of establishing an emotional connection with a child mainly for the purpose of child-trafficking and child prostitution.

5. **Copyright infringement**

If someone infringes someone's protected exclusive rights without permission and publishes that with his own name, is known as copyright infringement.

6. **Money laundering**

Unlawful possession of money by an individual or an organization is known as money laundering. It typically involves transfers of money through foreign banks and/or legal business. In added words, it is the practice of transforming illegitimately earned money into the legitimate financial system.

7. **Cyber-extortion**

When a hacker hacks someone's email server, or computer system and load money to reinstate the system, it is known as cyber-extortion.

8. **Cyber-terrorism**

Normally, when someone hacks government's security system or intimidates government or such a big organization to move forward his political or social objectives by invading the security system through computer networks. it is known as cyber-terrorism.

Q. 8 Discuss PII confidentiality safeguards.

Ans.: PII confidentiality safeguards

Personally Identifiable Information (PII) is any information that can be used to recognize, contact, or locate an individual, either alone or combined with other easily accessible sources. It includes information that is connected or linkable to an individual, such as medical, educational, financial and employment information. Examples of data elements that can identify an individual contain name, fingerprints or other biometric (including genetic) data, email address, telephone number or social security number.

Safeguarding university-held PII (and other sensitive information) is the accountability of each and every member of the University's workforce. Regardless of your role, you should know what PII is and your accountability in ensuring its protection. Although society has always relied on personal identifiers, essential and protecting PII has recently become much more important as a component of personal privacy, now that advances in computing and communications technology, including the internet, has made it easier to collect and process vast amounts of information.

The protection of PII and the on the whole privacy of information are concerns both for individuals whose personal information is at stake and for organizations that may be liable or have their reputations spoiled should such PII be inappropriately accessed, used, or disclosed. Examples of laws related to different types of PII are listed below :

HIPAA/HITECH - Health related information.

GLBA - Financial information.

Privacy Act - Fair Information Practices for PII held by Federal Agencies.

COPPA - Protects children's privacy by allowing parents to control what information is collected.

FERPA - Student's personal information.

FCRA - Collection and use of consumer information.

Such laws attempt to restrict corporations from incorrectly sharing PII and impose requirements for appropriately protecting such information. Legally collecting and selling PII has become lucrative, but PII can also be exploited by criminals to steal a person's identity or commit other crimes.

According to FBI statistics, identity theft continues to be one of the nation's fastest growing crimes and can cause both financial

and emotional damage to its sufferer. Due to this threat, many governments have enacted legislation to bound the distribution of personal information.

The following list contains examples of information that may be considered PII :

1. Name, such as full name, maiden name, mother's maiden name, or alias
2. Personal identification number, such as social security number (SSN), passport number, driver's license number, taxpayer identification number, patient identification number, and financial account or credit card number
3. Address information, such as street address or email address
4. Asset information, such as Internet Protocol (IP) or Media Access Control (MAC) address or other host-specific persistent static identifier that consistently links to a particular person or small, well-defined group of people
5. Telephone numbers, including mobile, business, and personal numbers
6. Personal characteristics, including photographic image (especially of face or other distinguishing characteristic), x-rays, fingerprints, or other biometric image or template data (e.g., retina scan, voice signature, facial geometry)
7. Information identifying personally owned property, such as vehicle registration number or title number and related information
8. Information about an individual that is linked or linkable to one of the above (e.g., date of birth, place of birth, race, religion, weight, activities, geographical indicators, employment information, medical information, education information, financial information)

Q. 9 What are different types of attacks by Hackers?

Ans. : Types of Attacks By Hackers

Hacker is computer expert who uses his knowledge to get unauthorized access to the computer network. He is not any person who intends to break through the system but also includes one who has no intention to damage the system but intends to learn more by using ones computer. Crackers on other hand use the information cause disruption to the network for personal and political motives. Hacking by an insider or an employee is pretty prominent in present date. Section 66(b) of the Information Technology Act 2000, provides punishment of imprisonment for the period of 3 years and fine which may extent to two lakhs rupees, or with both.

Banks and other financial institutions are threatened by the terrorist groups to use their sensitive information resulting in deep loss and in turn ask for ransom amount from them. There are various methods used by hackers to gain unauthorised access to the computers distant from use of viruses like Trojans and worms etc.

Therefore if anyone secures access to any computer without the permission of the owner shall be likely to pay damages of 1 crore rupees under Information Technology Act, 2000. Computer system here means a device including input and output support devices and systems which are capable of performing logical, arithmetical, data storage and reclamation, communication control and other functions but excludes calculators.

Unauthorised access under Section 43 of the Information Technology Act 2000 is punishable regardless of the intention or purpose for which unauthorised access to the computer system was made. Owner needn't prove the facto of loss, but the fact of it been used without his authorisation.

Case of **United States v. Rice** would be important in this consider where defendant on the request of his friend (who was been beneath investigation by IRS officer) tried to find the status of his friends case by using officers computer without his approval. Though it didn't cause any spoil/loss to the plaintiff (officer) but was convicted by the Jury for accessing the computer system of a Government without his authority and his sincerity was later on confirmed. Even if one provides any help to the other to gain any unauthorised access to the computer he shall be liable to pay damages by way of compensation of Rupees 1 crore.

Does turning on the computer leads to unauthorized access? The mensrea under section 1 of the Computer misuse Act, 1990 comprises of two elements there must be an intent to secure an access to any programme or data held in any computer, and the person must know that he intends to secure an unauthorized access.

Though section 1 (1) (a) requires that second computer must be involved but the judiciary in the case of R v. Sean Cropp, believed that the Parliament would have intended to limit the offence even if single computer system was involved.

(A) Computer Viruses

Viruses are used by Hackers to contaminate the user's computer and dent data saved on the computer by use of payload in viruses which carries damaging code. Person would be liable under I.T Act only when the consent of the owner is not taken before inserting virus in his system.

The contradiction here is that though definite viruses causes temporary interruption by showing messages on the screen of the user but still its not punishable under Information Technology Act 2000 as it doesn't cause tangible damage. But, it must be made punishable as it would plunge under the ambit of unauthorised access though doesn't cause any damage. Harmless viruses would also plunge under the expression used in the provision to unsurp the normal operation of the computer, system or network. This ambiguity needs reconsideration.

(B) Phishing

By using e-mail messages which entirely resembles the original mail messages of customers, hack...

verification of certain information, like account numbers or passwords etc. Here customer might not have knowledge that the e-mail messages are unreliable and would fail to identify the originality of the messages. This results in huge financial loss when the hackers use that information for fraudulent acts like withdrawing money from customers account without him having knowledge of it.

(C) Spoofing

This is carried on by use of unreliable Websites or e-mails. These sources copy the original websites so well by use of logos, names, graphics and even the code of real banks site.

(D) Phone Phishing

Is done by use of in-voice messages by the hackers where the customers are asked to disclose their account identification, and passwords to file a complaint for any problems regarding their accounts with banks etc.

(E) Internet Pharming

Hacker here aims at redirecting the website used by the customer to another fake website by hijacking the sufferer DNS server (they are computers responsible for resolving internet names into real addresses - signposts of internet), and changing his I.P address to fake website by manipulating DNS server. This redirects user's original website to a false deceptive website to gain unauthorised information.

(F) Risk Posed On Banks and Other Institutions

Wire transfer is the means of transferring money from one account another or transferring cash at cash office. This is most convenient way of transfer of cash by customers and money laundering by cyber terrorists. There are many guidelines issued by Reserve Bank of India (RBI) in this view, one of which is KYC (Know Your Customer) norms of 2002. Main objective of which is to :

1) Ensure appropriate customer identification, and
2) Monitor the transaction of suspicious nature and report it to appropriate authority every day bases.

(G) Publishing Pornographic Material in Electronic Form

Section 67 of the Information Technology Act, 2000 in parallel to Section 292 of Indian Penal Code, 1860 makes publication and broadcast of any material in electronic that lascivious or appeals to the prurient interest a crime, and punishable with captivity which may extend to 5 years and fine of 1 lakh rupees and subsequent offence with an captivity extending to 10 years and fine of 2 lakhs.

Various tests were laid down slowly in course of time to determine the actual crime in case of obscene material published in electronic form on net. Hicklin test was adopted in America in the case of Regina v. Hicklin wherein it was seized that if the material has tendency is to deprive and corrupt those whose minds are open to such immoral influences, and into whose hands a publication of this sort may fall.

In Indian situation the case of Ranjeet D. Udeshi v. State of Maharashtra the Supreme Court admitted that Indian Penal Code doesn't term obscenity though it provides punishment for publication of obscene matter. There are very thin line existing between a material which could be called obscene and the one which is artistic. Court even strained on need to maintain balance between fundamental right of freedom of speech and expression and public decency and morality. If matter is likely to degrade and corrupt those minds which are open to influence to whim the material is likely to fall. Where both obscenity and artistic matter is so mixed up that obscenity falls into shadow as its insignificant then obscenity may be overlooked.

In the case of Miller v. California it was held that local community standard must be applied at the time of determination of the offence. As it can traverse in many jurisdictions and can be accessed in any part of the globe. So wherever the material can be accessed the community standards of that country would be applicable to determine the offence of publication of obscene material posted in electronic form. Though knowledge of obscenity under Information Technology Act 2000 and Indian Penal Code may be taken as justifying factor but doesn't take the case out of the provision.

Section 72 of Information Technology Act, 2000 provides punishment for an unauthorised access or, exposé of that information to third person punishable with an captivity upto 2 years or fine which may extend to 1 lakh rupees or with both.

English courts have also dealt with an issue as to what activities would form crime under existing legislation, in the case of R. v. Fellows and Arnold it was held that the legislation before the 1994 amendment would also facilitate computer data to be considered a copy of an indecent photograph and making images available for downloading from the website would constitute material being distributed or shown. Statute is wide enough to deal with the use of computer technology.

(H) Investment Newsletter

We usually get newsletter providing us free information recommending that investment in which field would be lucrative. These may sometimes be a fraud and may origin us huge loss if relied upon. False information can be spread by this method about any company and can cause massive inconvenience or loss through junk mails online.

(I) Credit Card Fraud

Huge loss may reason to the victim due to this kind of fraud. This is done by publishing false digital signatures. Most of the people misplace credit cards on the way of delivery to the recipient or its damaged or defective, misrepresented etc.