Network Security Notes

ICT 7th Semester

by

Mukesh Singh
(ICT 5th batch 2073)

Sukuna Multiple Campus
Sundarharaincha-12, Morang

Page No.
Date

Units	Chapter name / Contents	Page
Unit-1	Introduction	
	1.1 Computer Security Concept	
	1.2 The OSI Security Architecture	
	1.3 Security Attacks	
	1.4 Security Services	
	1.5 Security Mechanism	
	1.6 A Model for Network Security	
	1.7 Classical cryptography	
Unit-2	Symmetric Encryption and message Confidentiality	
	2.1 Computer Security Concept	
	2.2 Symmetric Block Encryption Algorithms	
	2.3 Cipher Block Modes of Operations	
Unit-3	Public-key Cryptography and Message Digest	
	3.1 Secure Hash Functions	
	3.2 Message Digest (MD)	
	3.3 Public-key Cryptography Principles	
	3.4 Public-key Cryptography Algorithms	
	3.5 Digital Signatures	
Unit-4	Network Security Applications	
	4.1 Public Key Infrastructure	
	4.2 Transport layer security: SSL, HTTPS, Secure Shell (SSH)	
	4.3 Wireless Security: WEP, WAP, WPA2	
	4.4 E-mail Security: PGP, S/MIME	
	4.5 IP-Security	

Unit-5 System Security

5.1 Intruders

5.2 Malicious Software

5.3 Firewall

Unit-6 Network Management Security

6.1 Basic Concept of SNMP

6.2 SNMP-v1

6.3 SNMP-v2

Unit-1

Introduction

Ajanta

Page No.
Date

1.1 Computer Security Concept

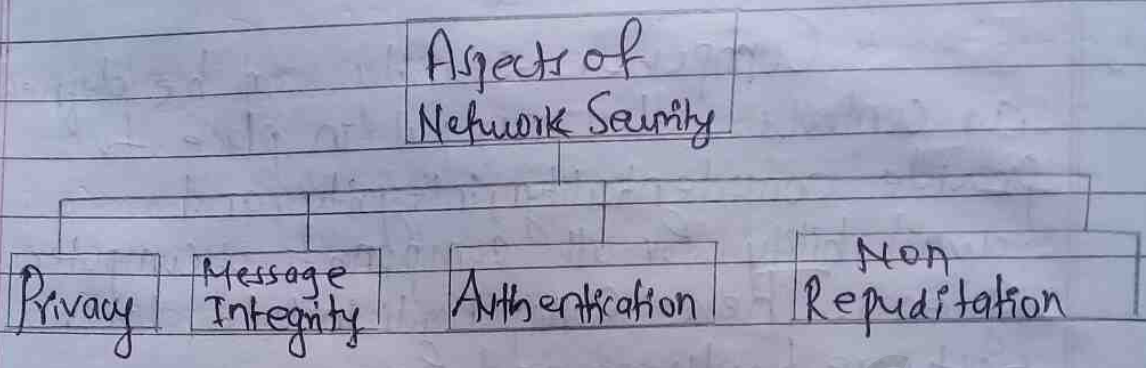
Computer security can be defined as controls that are put in place to provide confidentiality, integrity, and availability for all components of computer systems. These components include data, software, hardware, and firmware.

Computer network security consists of measures taken by buisness or some organizations to monitor and prevent unauthorized access from the outside attackers.

Different approaches to computer network security management have different requirements depending on the size of the computer network. For example, a home office requires basic network security while large buisness require high maintenance to prevent the network from malicious attacks.

Network Administrator controls access to the data and software on the network. A network administrator assigns the user ID and password to the authorized person.

ASPECTS of Network Security:



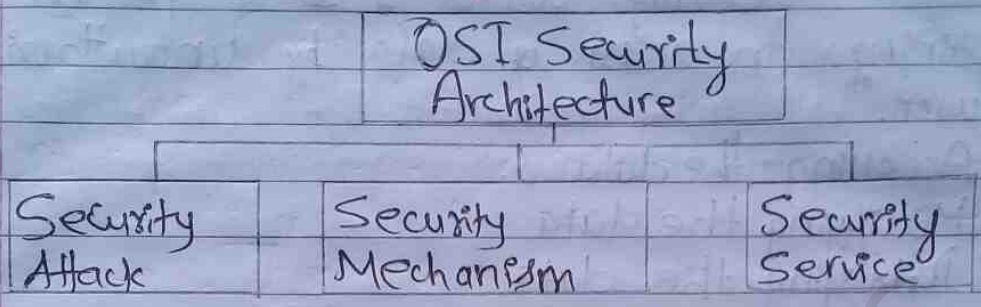
1) Privacy
The transmitted message should be sent only to the intended receiver while the message should be opaque for other users. This aspect of confidentiality is commonly used to achieve secure communication.

2) Message Integrity
There are more and more monetary exchanges over the internet, data integrity is more crucial. The data integrity must be preserved for secure communication.

3) End-point authentication
Authentication means that the receiver is sure of the sender's identity ie no imposter has sent the messages.

4) Non-Repudiation.
Non-repudiation means that the receiver must be able to prove that the received message has come from a specific sender.

1.2 The OSI Security Architecture



The OSI security architecture provides a systematic framework for defining security attacks, mechanism and services.

1) Security attacks → are classified as either passive attacks, which include unauthorized reading of a message of a file and traffic analysis or active attacks, such as modification of message or files, and denial of service.

2) Security mechanism → is any process (or a device incorporating such a process) that is designed to detect, prevent or recover from a security attack. Examples of mechanisms are encryption algorithms, digital signatures, and authentication protocols.

3) Security Services - include authentication, access control, data confidentiality, data integrity, nonrepudiation and availability.

13. Security Attacks

Security attack is a process of gaining an access of data by unauthorized user.

i) Accessing the data
ii) Modifying the data
iii) Destroying the data

Types of Security attacks:

1. Passive attack
2. Active attack

1. Passive attack

In passive attack, no data modification will be done. Passive attack attempts to learn or make use of information from the system but does not affect system resources.

Types of passive attack:

i) Release of message Content

Third party only access the data.

The release of message content is easily understood.

A telephone Conversation, an electronic mail message, and a transferred file may Contain Sensitive or Confidential information.

ii) Traffic analysis

Analyses the traffic and modifies the data that has to be used.

Figure

Suppose that we had a way of ~~Masking~~ masking the contents of messages or other information traffic so that opponents even if they capture the message, could not extract the information from the message.

2. Active attack

In active attack, data modification will be done.

~~It can be~~ It can be subdivided into four categories:

i) Masquerade

Sender sends the message to the receiver but the third party (unauthorized user) accesses the data and modifies the data and sends to the receiver in the name of the sender.

ii) Replay

- Receiver receives the data twice.
- Sender sends the message to the receiver as well as the third party will access the message and modification will be done then the third party sends to the receiver.
- However, the receiver doesn't know the original message.

iii) Data Modification

Third party access the data that is sent by the sender to the receiver, third party modifies

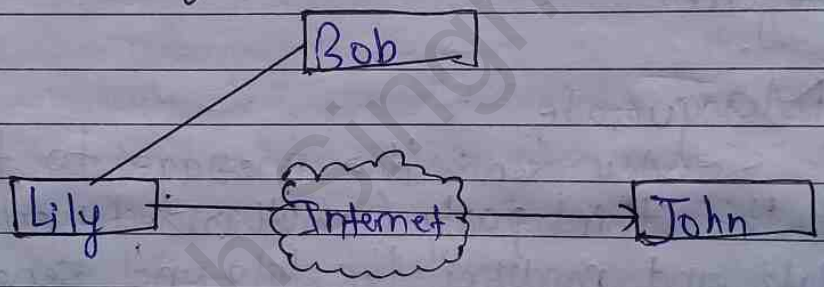
that data and sends to the receiver.

iv) Denial of Service
Third party interrupts the service that is sent by the server.

Remaining figures of Security attacks:

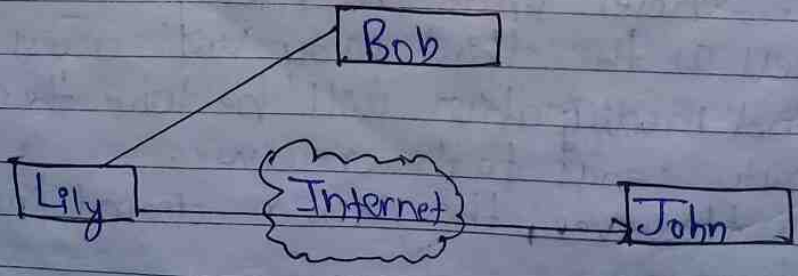
1. Passive Attacks

i) Release of menage content:



Bob reads the content of menage which Lily sends to John.

ii) Traffic Analysis



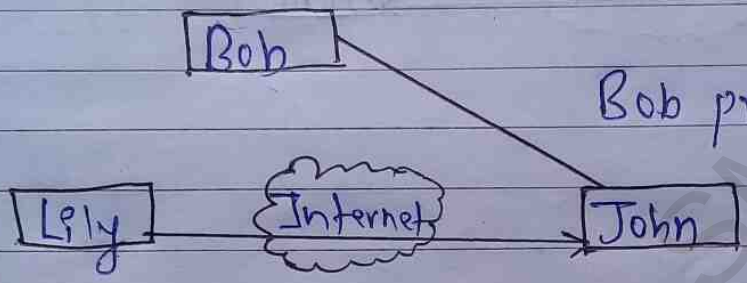
Bob observes the pattern of message exchanged between Lily and John.

Ex

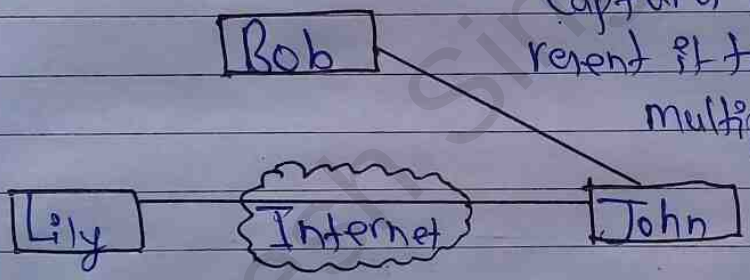
~~2. Passive Attacks~~

2. Active Attacks

i) Masquerade

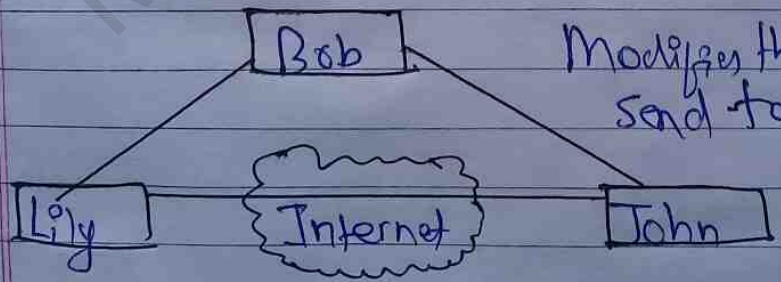


ii) Replay

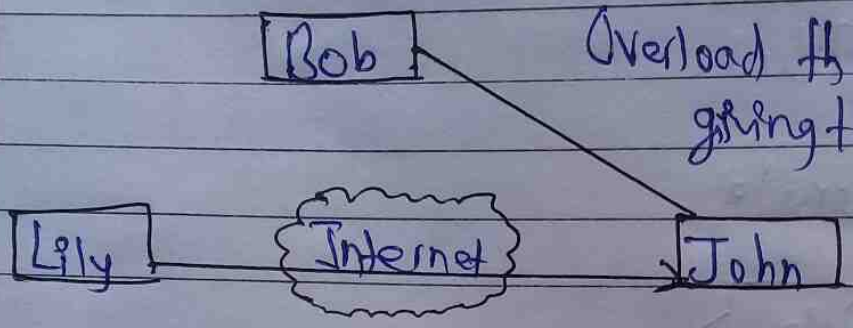


€

iii) Data Modification



iv) Denial of Service



14 Security Services

Security services is a service provided by the protocol layer which ensures the servici-ng of the S/R (or) data transfer.

- X.800 defines a security service as a service that is provided by a protocol layer of communicating open systems and that ensures adequate security of the systems or of data transfers.

- X.800 divides these services into five categories and fourteen specific services.

1. Authentication

Verify the identity who sends and who receives, it varifies the user identity before it sends the data.

i) Peer Entity Authentication

Provides for the corroboration of the identity of a peer entity in association.

It is provided for use at the establishment of or during the data transfer phase of a connection.

ii) Data Origin Authentication

Provides for the corroboration of the source of a data unit.

It does not provide protection against the duplication or modification of data units.

2. Access Control
To prevent unauthorized access to resources only accessed by authorized person.

3. Data Confidentiality
Providing security to the data sent through a network.

i) Connection Confidentiality → The protection of all user data on a connection.

ii) Connectionless Confidentiality → The protection of all user data in a single data block.

iii) Selective field Confidentiality → The confidentiality of selected fields within the user data on a connection or in a single data blak.

iv) Traffic-flow Confidentiality → The protection of information that might be derived from observation of traffic flows.

4. Data Integrity
Modification should not be done either before/after sending the data.

i) Connection integrity with recovery → Provides for the integrity of all user data on a connection.

ii) Connection integrity without recovery → As above

but provides ~~only~~ no recovery.

iii) Selective field Connection Integrity
Provides for the integrity of selected fields within the user data of a data block, transferred over a connection.

iv) Connectionless integrity → Provides for the integrity of a single connectionless data block. ~~and~~ -

v) Selective-field Connectionless Integrity → Provides for the integrity of selected fields within a single connectionless data block.

5. Non-repudiation
Preventing from denial of service attack.

i) Non-repudiation, Origin → Proof that the message was sent by the specified party.

ii) Non-repudiation, Destination → Proof that the message was received by the specified party.

1.5 Security Mechanisms

It is a process that is designed to detect, prevent or recover from a security attack.

Types of Security mechanism:

A. Specific Security Mechanism

1) Encipherment

The mathematical algorithm is used to transform data into another form which is not intelligible.

The transformation and subsequent recovery of the data depend on an algorithm and zero or more encryption keys.

a) Reversible encipherment

b) Irreversible encipherment

2) Digital Signature

Data is appended to prove that the source is the one which has sent the data and protect against forgery.

3) Access Control

Provides the access rights to resources.

4) Data Integrity

Assures the integrity of data, no modification is done before/after data transmission.

5) Traffic Padding

Here, bits are padded in the gaps

to give false opinions on traffic analysis.

6) Authentication exchange
A mechanism intended to ensure the identity of an entity by means of information exchange.

7) Routing Control
Enables selection of particular physically secure routes for certain data and allows routing changes specially when a breach of security is suspected.

8) Notarization
This uses the trusted third party to assure the data exchange.

B. Pervasive Security Mechanism
Mechanisms that are not specific to any particular OSI security service or protocol layer.

1) Trusted functionality
That which is perceived to be correct with respect to some criteria (e.g. as established by a security policy.

16. ~~A Model for Network Security~~

2) Security label
The marking bound to a resource (which may be a data unit) that names or designates the security attributes of that resource.

3) Event Detection
Detection of security-relevant events.

4) Security audit trail
Data collected and potentially used to facilitate a security audit, which is an independent review and examination of system records and activities.

5) Security Recovery
Deals with requests from mechanisms, such as event handling and management functions, and takes recovery actions.

1.6 A Model for Network Security

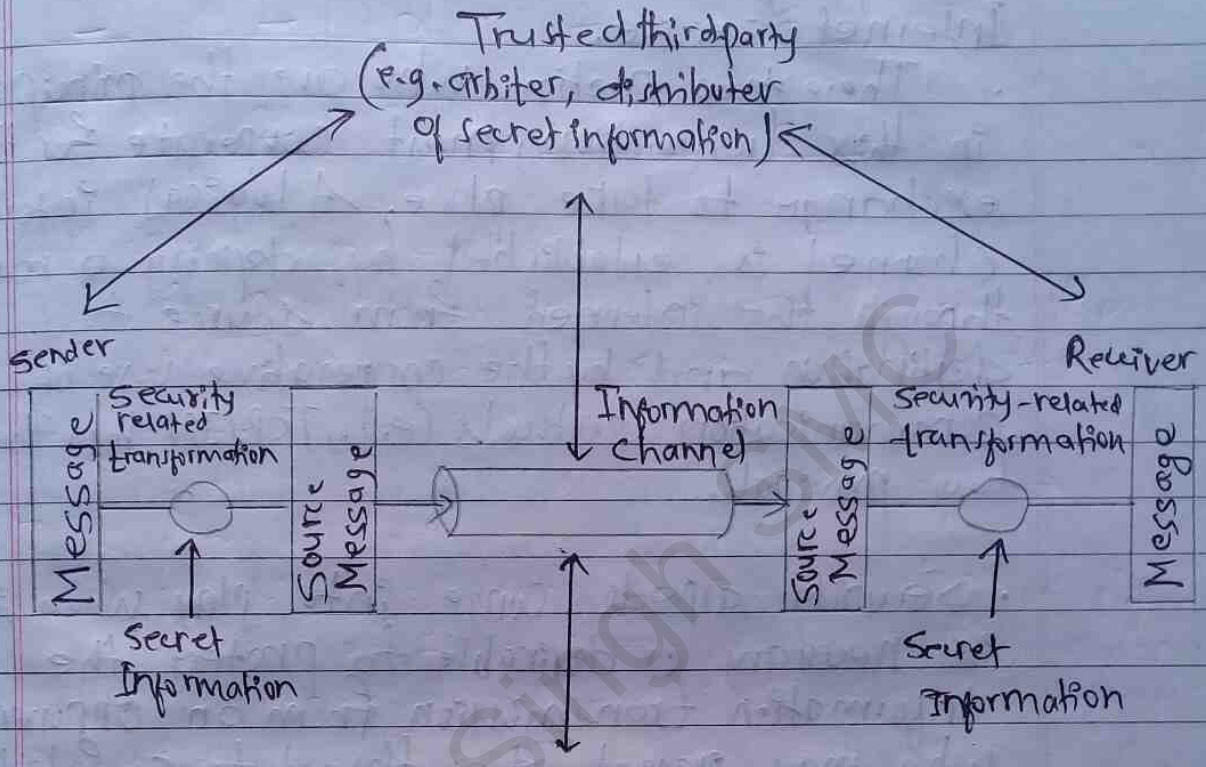
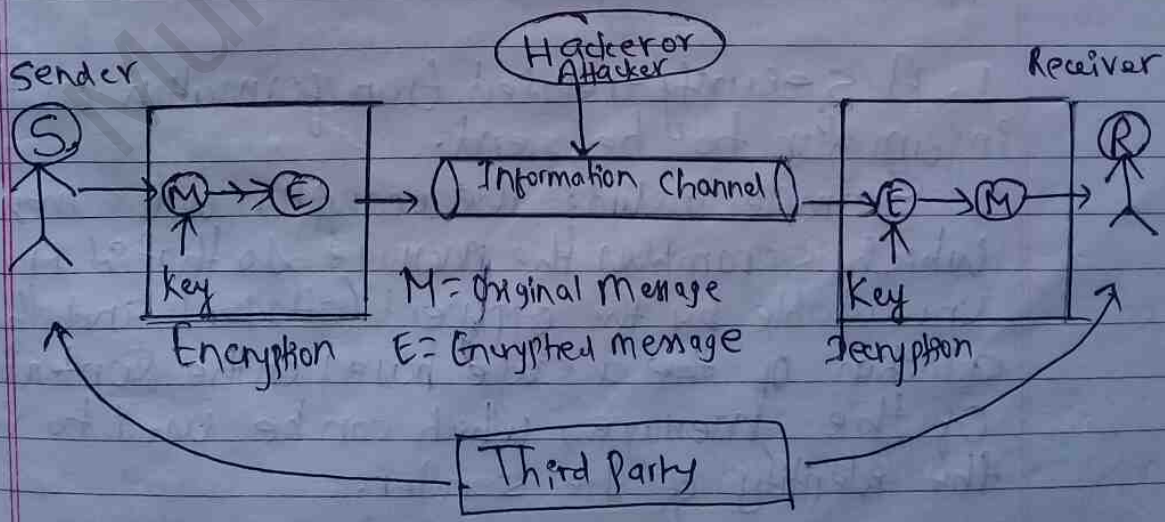


Fig: Model for Network Security

OR



. A message is to be transferred from one party to another across some sort of Internet service.

. These two parties, who are the principals in this transaction, must cooperate for the exchange to take place. A logical information channel is established by defining a route through the internet from source to destination and by the cooperative use of communication protocols (e.g., TCP/IP) by the two principals.

. Security aspects come into play when it is necessary or desirable to protect the information transmission from an opponent who may present a threat to confidentiality authenticity, and so on.

. All of the techniques for providing security have two components:

1. A security-related transformation on the information to be sent.
   Example include the encryption of the message, which scrambles the message so that it is unreadable by the opponent (attacker), and the addition of a code based on the contents of the message, which can be used to verify the identity of the sender.

2. Some secret information shared by the two

principles and it is hoped, unknown to the opponent or attacker.

An example is an encryption key is used in conjunction with the transformation to scramble the message before transmission and unscramble it on reception.

- A trusted third party may be needed to achieve secure transmission.
- For example, a third party may be responsible for distributing the secret information to the two principles while keeping it from any opponent.

This general model shows that there are four basic tasks in designing a particular security service:

1. Design an algorithm for performing the security-related transformation. The algorithm should be such that an opponent cannot defeat its purpose.
2. Generate the secret information to be used with the algorithm.
3. Develop methods for the distribution and sharing of the secret information.
4. Specify a protocol to be used by the two principals that makes use of the security algorithm and the secret information to achieve a

~~parteul~~ → particular security service.

17. Classical ~~Cytography~~ Cryptography

~~Cytography~~ Cryptography is the science of hiding information in plain sight, in order to conceal it from unauthorized parties.

Or, Cryptography is the technique which is used for doing secure communication between two parties in the public environment where unauthorized users and malicious attackers are present.

There are two types of Cryptography techniques:

1. Classical ~~Cytography~~ Cryptography
2. Quantom ~~Cytography~~ Cryptography

We discuss only about Classical Cytography.

~~Classical Cytography~~

Terms used in ~~Cytogr~~ Cryptography:

- Plaintext → This is the original intelligible message or data that is fed into the algorithm as input.
- Ciphertext → This is the scrambled message produced as output. It depends on the plaintext and the secret key.
- Encryption → The process of transforming plaintext into cipher text (also encipher).
- Decryption → The process of transforming ciphertext into plain text (also decipher).

• Encryption algorithm → The encryption algorithm performs various substitutions and transformations on the plain text.

• Secret key → The secret key is also input to the encryption algorithm. The key is a value independent of the plain text and of the algorithm.

• Decryption Algorithm → This is essentially the encryption algorithm run in reverse. It takes the ciphertext and the secret key and produces the original plaintext.

1. Classical Cryptography ~~is based~~.

Classical cryptography is based on the mathematics and it relies on the computational difficulty of factorizing large number. The security of classical cryptography is based on the high complexity of the mathematical problem for the instance factorization of large number.

In the classical cryptography the original data i.e. the plain text is transformed into the encoded format i.e. cipher text so that we can transmit this data through insecure ~~communication~~ communication channels. A data string which known as key is used to control the transformation of the data from plain text to cipher text.

Classical Cryptography has two types of techniques:

1. Symmetric Cryptography:

In the symmetric cytography, a single key is used for the ~~encryption~~ cryption and decryption of the data. The encryption key is private key. This is the limitation of this encryption technique that this private key must be distributed only among the authorized sender and receiver.

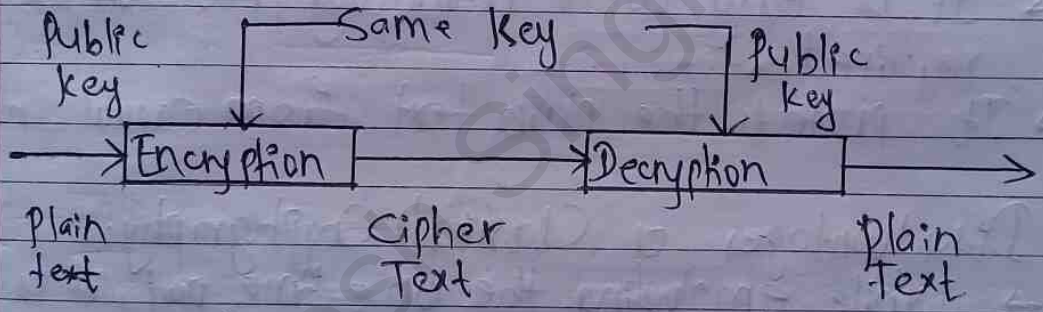


fig: Symmetric Cryptography

2. Asymmetric Cryptography

In the asymmetric cryptography a pair of key i.e. public key and private key is used for encryption and decryption. A sender can use its public key to encrypt the data and on receiver ~~and~~ end receiver can decrypt the data by using its private key. This technique overcomes the problem of key distribution.

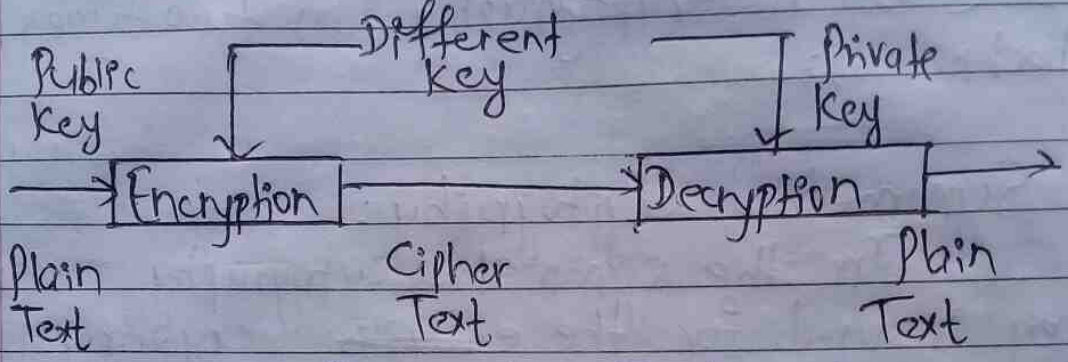


Fig: Asymmetric Cryptography

Advantages of Classical Cryptography:

→ While employing the one-time pad, it is unbreakable.

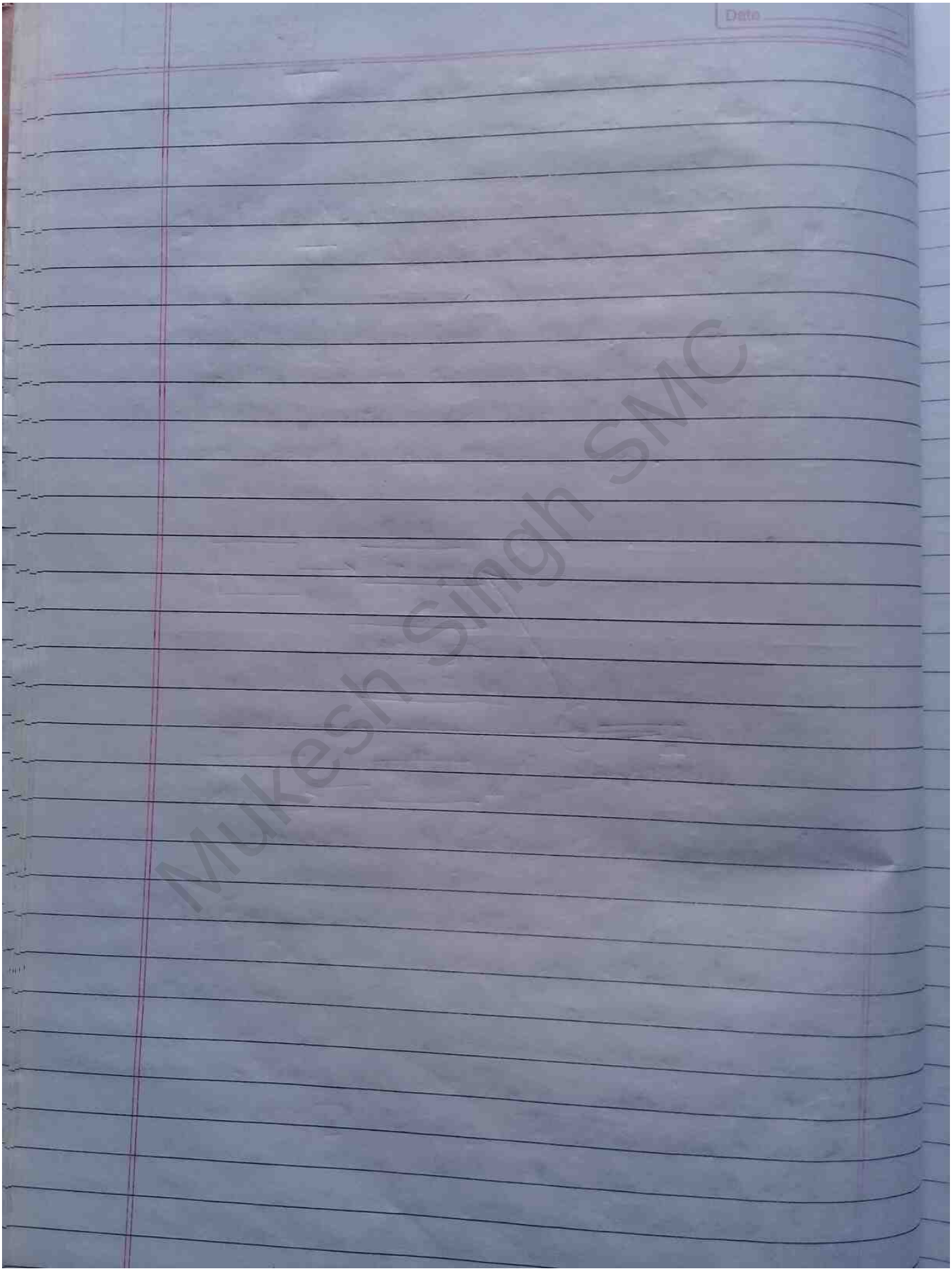
→ It is easy to do manually, no computer required.

→ It protects the plain text from casual snooping.

Disadvantages of Classical Cryptography:

→ While employing the one-time pad, it is cumbersome and requires a personal meetup to exchange the pads.

→ If not employing the OTP, anyone who is even remotely interested in knowing what you wrote and know about cryptography will be able to break the encryption.


Date
Mukesh Singh SMC

Unit-2

Symmetric Encryption and Message Confidentiality

2.1 Symmetric Encryption Principles

Symmetric Encryption

Symmetric encryption is a type of encryption where only one key (a secret key) is used to both encrypt and decrypt electronic information. The entities communicating via symmetric encryption must exchange the key so that it can be used in the decryption process.

Symmetric encryption is a form of cryptosystem in which encryption and decryption are performed using the same key. It is also known as conventional encryption.

Symmetric encryption transforms plain text into Ciphertext using a secret key and encryption algorithm. Using the same key and a decryption algorithm, the plain text is recovered from the Ciphertext.

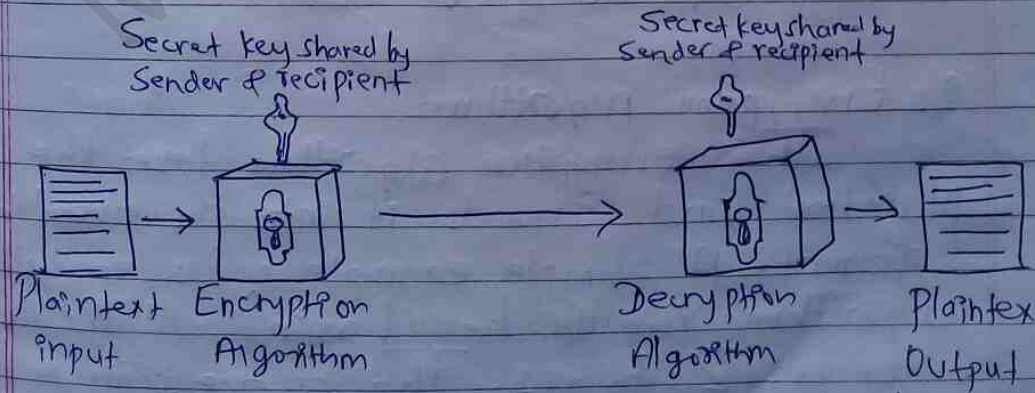
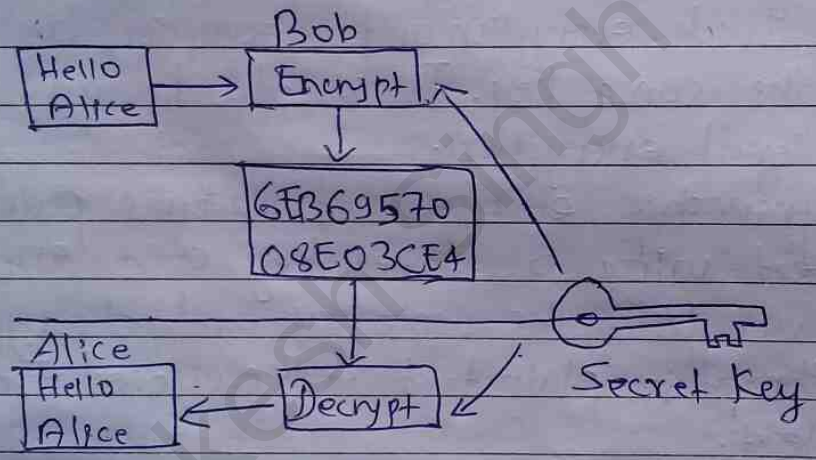


Fig: Symmetric Encryption and description

There are five main components of a symmetric encryption system:

1. Plaintext

The term plaintext refers to the original message that is created and sent into the encryption method. Since you've bothering to encrypt it, the plaintext most likely contains sensitive data that should not be seen by ~~prying~~ prying eyes.



Symmetric Encryption Example

2. Encryption Algorithm

The encryption algorithm takes the plaintext and converts it into an unreadable format. A simple example of an encryption algorithm would be changing all 1s to a 3 or all 2s to a 1. The routine may perform several passes and changes, called permutations, on the plaintext. Once it is encrypted, you'll need a key to unlock it.

3. Key

Think of the key as a decoder ring: the secret of the scrambled text cannot be read without the key. The key holds the information on all the switches and substitutions made on the original plain text.

In symmetric algorithm, the key is actually bundled with the algorithm; in this sense, the decoder ring is not universal. The changes and substitutions depend on the key, and vice versa because the sender and the recipient share the key.

4. Ciphertext

The ciphertext is the text that is now scrambled and ready to be sent. It may look like a random stream of data, and is unreadable.

5. Decryption Algorithm

In the decryption algorithm, the secret key (the decoder ring) is applied to the ciphertext. It converts it back to plaintext, basically performing the encryption in reverse.

2.2 Symmetric Blak Encryption Algorithms

Symmetric-key algorithms are algorithms for cryptography that use the same cryptographic keys for both the encryption of plaintext and the decryption of ciphertext.

Symmetric key encryption can use either stream ciphers or block ciphers.

Stream ciphers encrypt the digits or letters of a message one at a time. For example: Chacha20

Block Ciphers take a number of bits and encrypt them as a single unit, padding the plaintext so that it is a multiple of the book size.

Symmetric key algorithms sometimes referred to as secret key algorithms. There are hundreds of different symmetric key algorithms available. Each has its own strengths and weakness. Some of them are explained below:

1. DES

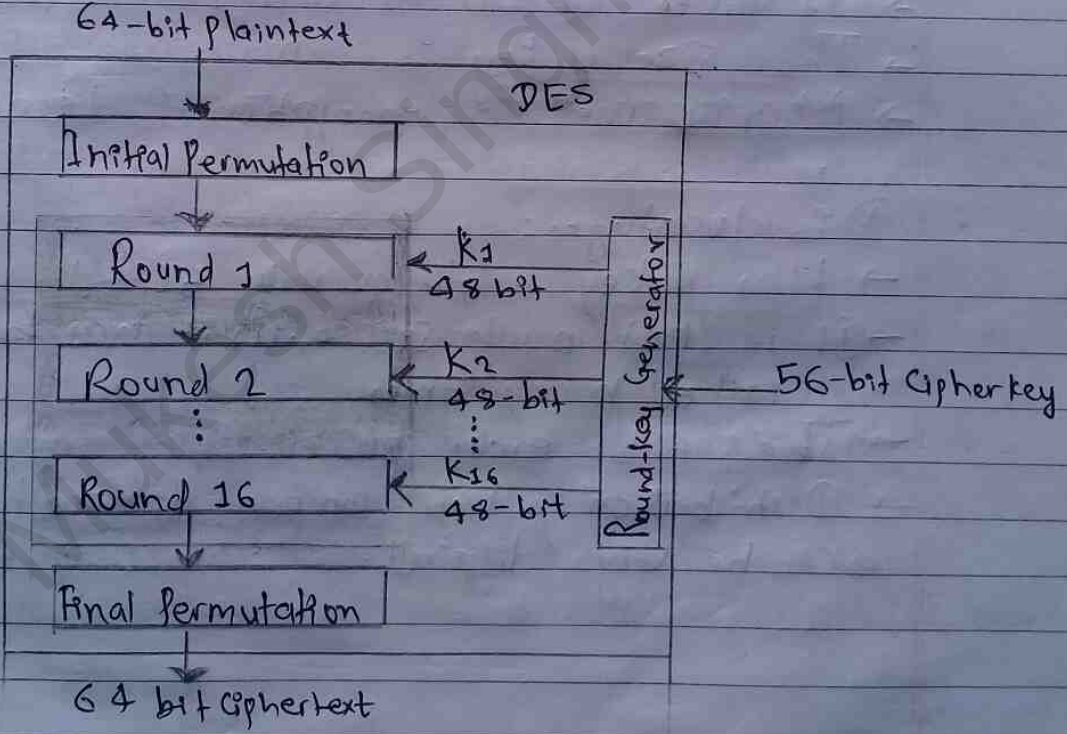
DES (Data Encryption Standard) block cipher algorithm, also known as DEA (Data Encryption Algorithm) was developed by IBM in the early 1970s and published as a standard by the US Government in 1977.

DES is a block encryption algorithm.

The algorithm takes plaintext in 64-bit blocks and converts them into ciphertext using 48-bit keys.

DES is an implementation of a Feistel Cipher. It uses 16 round Feistel structure. The block size is 64-bit. Though key length is 64-bit, DES has an effective key length of 56 bits, since 8 bit of 64 bits of the key are not used by the encryption algorithm (function as check bits only).

General structure of DES is shown in the following illustration:



Initial and Final Permutation

The initial and final permutations are straight permutation boxes (P-boxes) that are inverses of each other. They have no cryptography significance in DES.

Round function:
The heart of this cipher is the DES function, f. The DES function applies a 48-bit key to the rightmost 32 bits to produce a 32-bit output.

Key Generation
The round key generator creates sixteen 48-bit keys of a 56-bit cipher key.

Advantages of DES:
→ It takes less time to encrypt the message.
→ The size of key is small.
→ Mainly used for encryption & decryption.

Disadvantages:
→ Has a key length of only 56-bits.
→ It is not much secure, as it has been cracked many times.
→ Can be easily broken.
→ Distribution of key among different parties can be very difficult.

2) 3DES

~~3DES~~ Triple DES (or TDES, TDEA or, 3DES) was introduced in 1998, using a bundle of 3 keys, giving a nominal strength of 168 bits (i.e. 56x3).

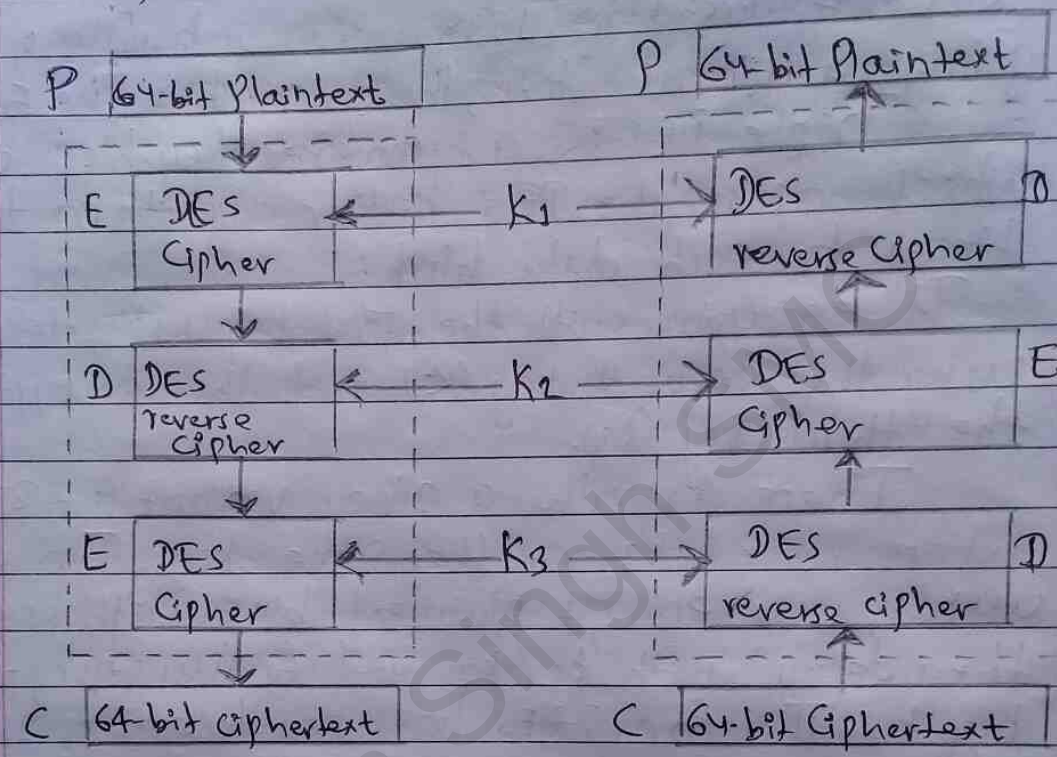
Triple DES is a symmetric key block cipher, which applies the DES cipher algorithm three times to each data block.

It encrypts with the first key (k1), decrypts using the second key (k2) and then encrypts with the third key (k3).

There is also a 2key variant (i.e. 2DES) where k1 and k3 are the same keys. In other words, user encrypt plaintext blocks with key (k1), then decrypt with key k2, and finally encrypt with key k1. Therefore, 2DES has a key length of 112 bits and is no faster and not considered secure.

3DES is still widely used in today, particularly in the financial industry, although many applications skipped Triple DES due to its poor performance and went straight from DES to AES instead. However, even though a 168-bit key is still considered to be strong, it is no longer recommended for new applications because it uses a small block size (64 bits).

The encryption-decryption scheme is as follows:



Encryption

Decryption

① Encrypt the plaintext blocks using single DES with key K_1.
② Now decrypt the output of step 1 using single DES with key K_2.
③ Finally, encrypt the output of step 2 using single DES with key K_3.
④ The output of step 3 is the ciphertext.
⑤ Decryption of ciphertext is a reverse process. User first decrypt ~~key~~ using K_3 then encrypt with K_2 and finally decrypt with K_1.

3. AES

In 2001, NIST (National Institute of Standards and Technology) published an algorithm called Rijndael as AES.

The AES is a fast and secure form of encryption that keeps prying eyes away from our data.

The more popular and widely adopted symmetric encryption algorithm likely to be encountered nowadays is the Advanced Encryption Standard (AES). It is found at least 6 times faster than triple DES.

A replacement for DES was needed as its key size was too small. With increasing computing power, it was considered vulnerable against exhaustive key search attack. Triple DES was designed to overcome this drawback but was found slow.

Features of AES are as follows:

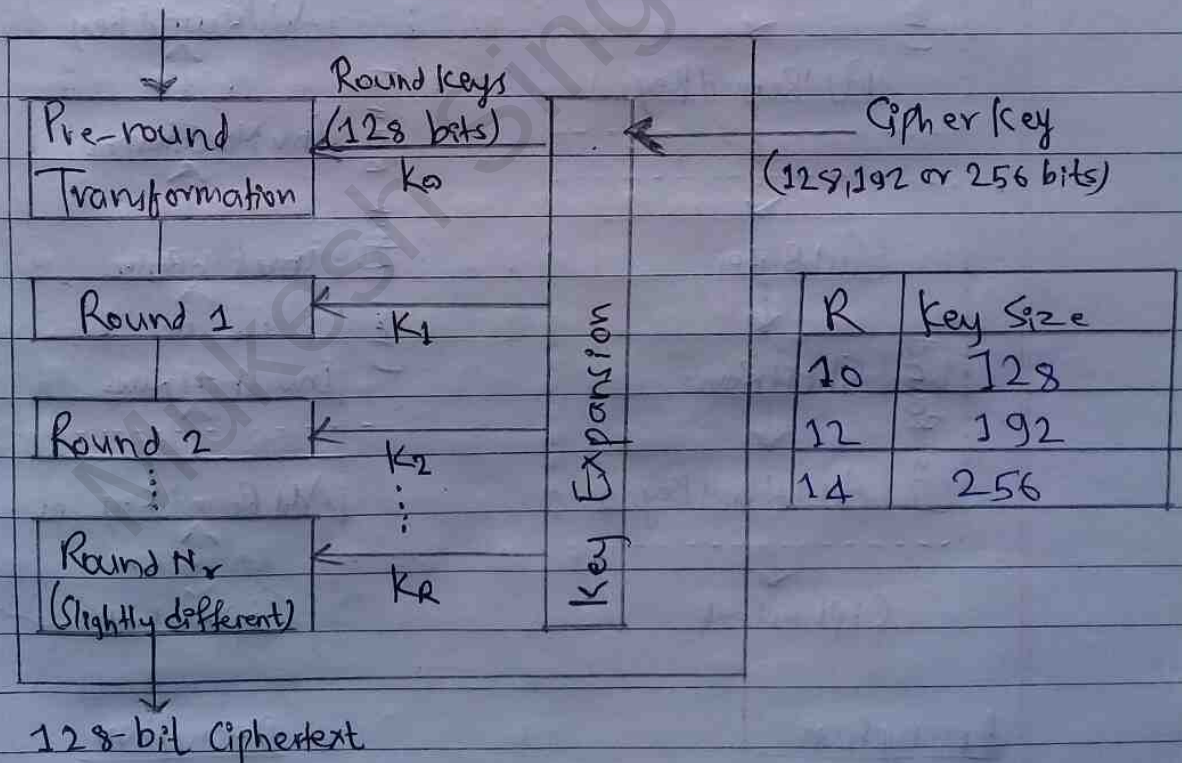
→ Symmetric key symmetric block cipher.
→ 128-bit data, 128/192/256 bit keys
→ Stronger and faster than Triple DES.
→ Provide full specification and design details.
→ Software implementation in C and Java.
→ Block size - 128 bits
→ Rounds: 10, 12 or 14 (depending on key size).

Page No.
Date

Operation of AES:

Unlike DES, the number of rounds in AES is variable and depends on the length of the key. AES uses 10 rounds for 128-bit keys, 12 rounds for 192-bit keys. Each of these round uses a different 128-bit round key, which is calculated from the original AES key.

The schematic of AES structure is given in the following illustration:



R	Key Size
10	128
12	192
14	256

Encryption and decryption process in AES:

Above figure display, the main construction of Encryption and decryption in AES method. Each round Covers four main transformations: SubByte, Shift Row, Mix Column, and Add Round key [14].

1. SubByte ⇒ A non-linear replacement byte that works individually on each state byte by using a table of substitution.

2. Shift Row → Cyclic shifting over different bytes offset numbers.

3. Mix Column → Column with column multiplication.

4. Add Round key → Adding a round key to the state with a simple XOR process [14].

⇒

2.3 Cipher Block Modes of Operations

A block cipher algorithm is a basic building block for providing data security. To apply a block cipher in a variety of applications, four "modes of operation" have been defined by NIST (FIPS 81).

In essence, a mode of operation is a technique for enhancing the effect of a cryptographic algorithm or adapting the algorithm for an application such as applying a block cipher to a sequence of data blocks or a data stream.

The four modes are intended to cover virtually all possible applications of encryption for which a block cipher could be used. These modes are intended for use with any symmetric block cipher, including triple DES and AES.

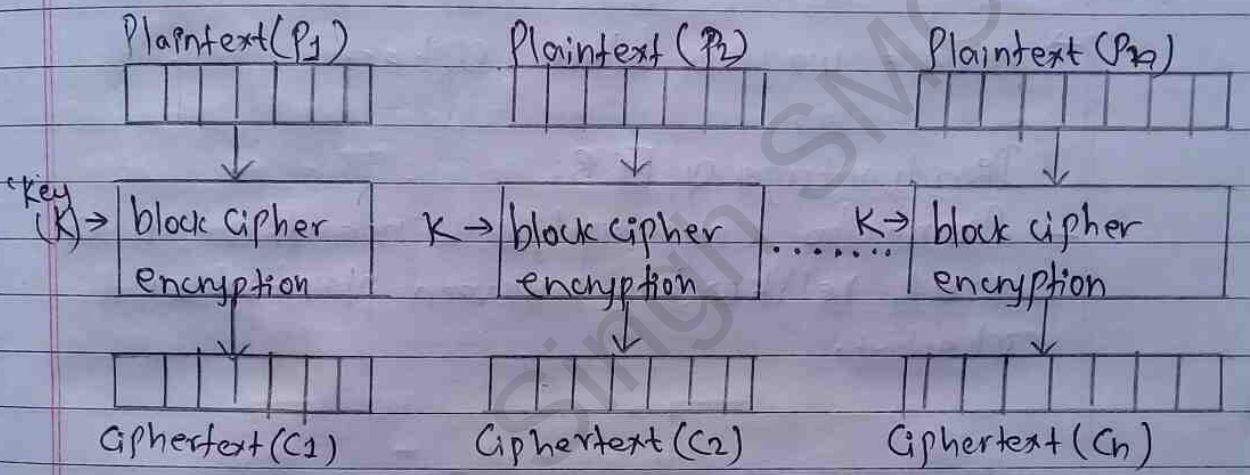
Block cipher modes of operation are explained below:

1. Electronic Codebook Mode

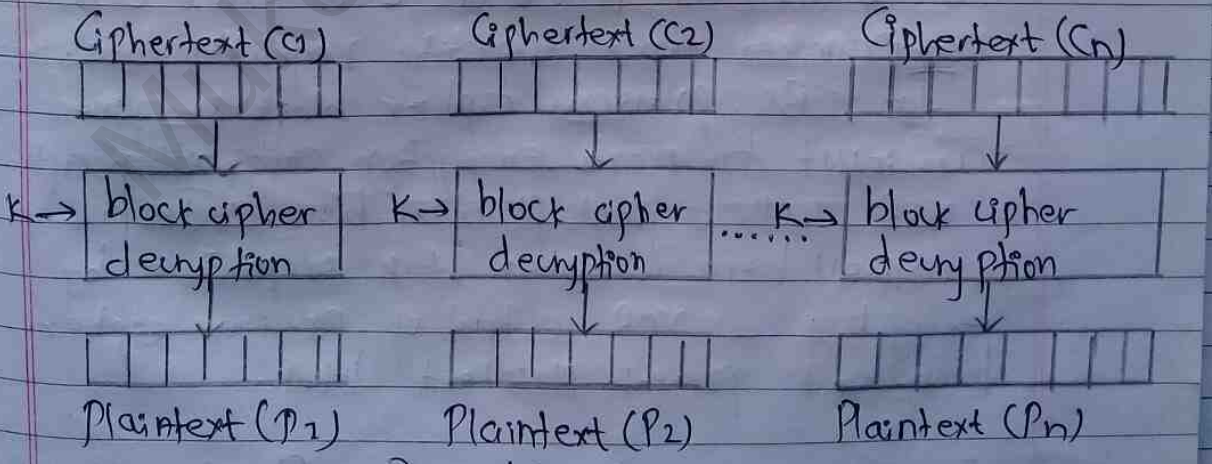
ECB is the simplest block cipher mode of operation. In this mode, each block of plaintext is encrypted separately. ~~The plaintext is encrypted using the same key.~~ The plaintext is handled one block at a time and each block of plaintext is encrypted using the same key. The term codebook

is used because, for a given key, there is a unique ciphertext for every b-bit block of plaintext. Generally if a message is larger than b bits in size, it can be broken down into bunch of blocks and the procedure is repeated.

Procedure of ECB:



Encryption



Decryption

→ The user takes the first block of plaintext and encrypt it with the key to produce the first block of ciphertext.

→ He then takes the second block of plaintext and follows the same process with same key and so on so forth.

Advantages of ECB:

→ Parallel encryption of blocks of bits is possible, thus it is faster way of encryption.

→ Simple way of block cipher.

Disadvantages of ECB:

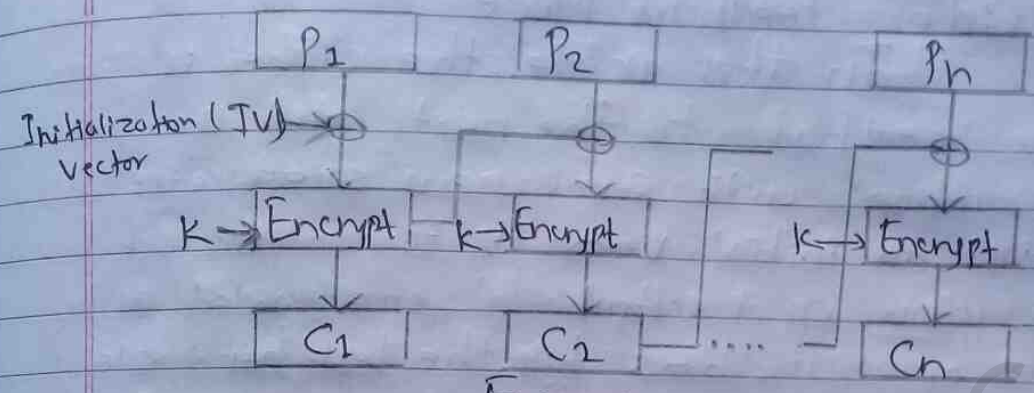
→ Prone to cryptanalysis since there is a direct relationship between plaintext and ciphertext.

2. Cipher Block Chaining Mode

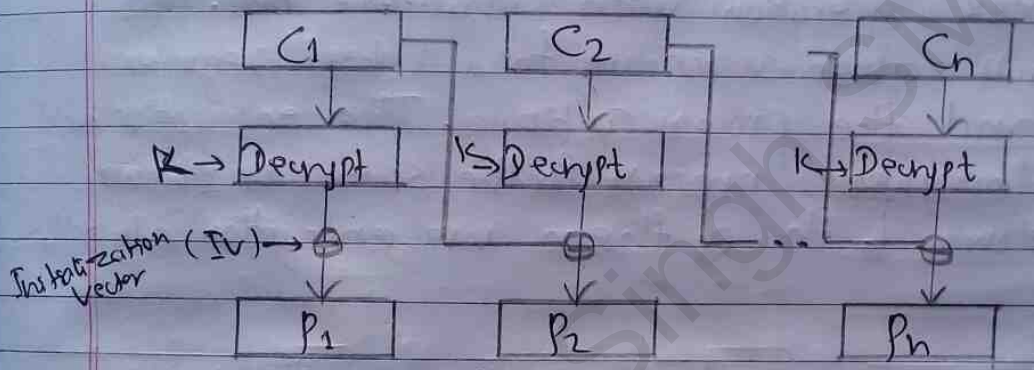
Cipher block Chaining or CBC is an advancement made on ECB since ECB compromises some security requirements. In CBC, previous cipher block is given as input to next encryption algorithm after XOR with original plaintext block. In a nutshell here, a cipher block is produced by encrypting a XOR output of previous cipher block and present plaintext block.

Initialization Vector → IV
Key → K
Encrypt (block cipher encryption)
Decrypt (block cipher decryption)

Plaintext (P_1, P_2, P_n)
Ciphertext (C_1, C_2, C_n)



Encryption



Decryption

Advantages of CBC:

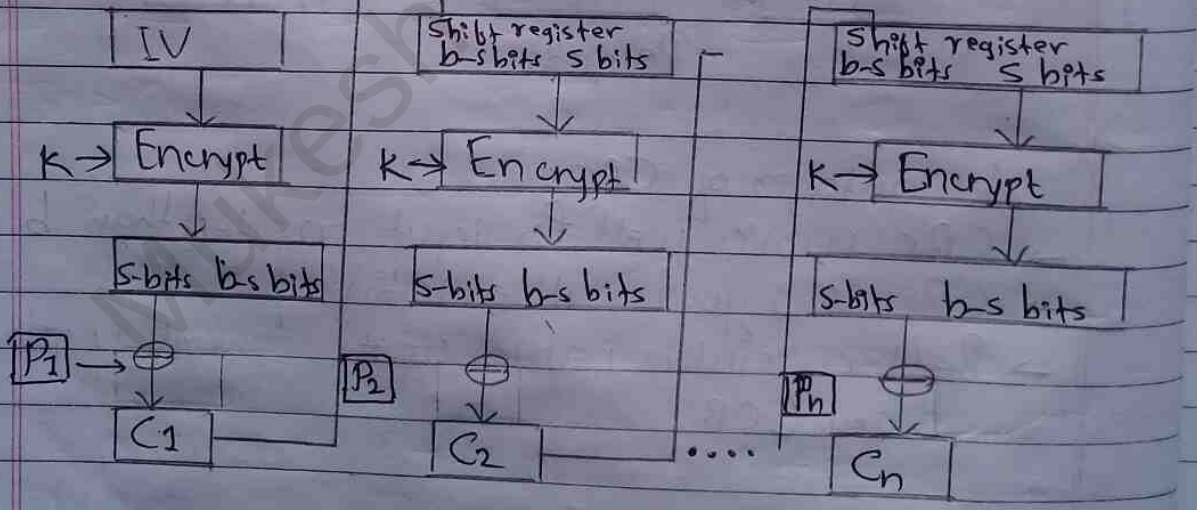
→ CBC works well for input greater than b bits.
→ CBC is a good authentication.
→ Better resistive nature towards cryptanalysis than ECB.

Disadvantages of CBC:

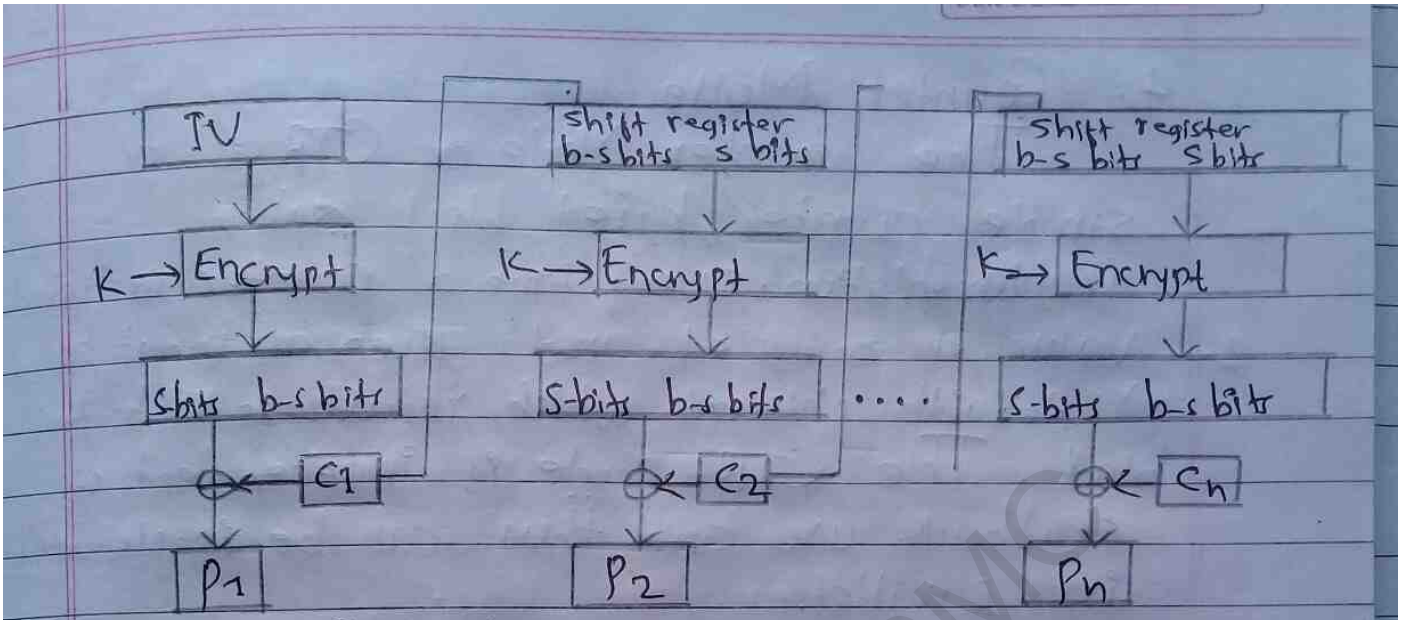
→ Parallel encryption is not possible since every encryption requires previous cipher.

3. Cipher Feedback Mode

In this mode, the cipher is given as feedback to the next block of encryption with some new specifications: First an initial vector IV is used for first encryption and output bits are divided as set of s and b-s bits the left hand side s bits are selected and are applied an XOR operation with plaintext bits. The result given as input to a shift register and the process continues. The encryption and decryption process for the same is shown below, both of them use encryption algorithm.



Encryption



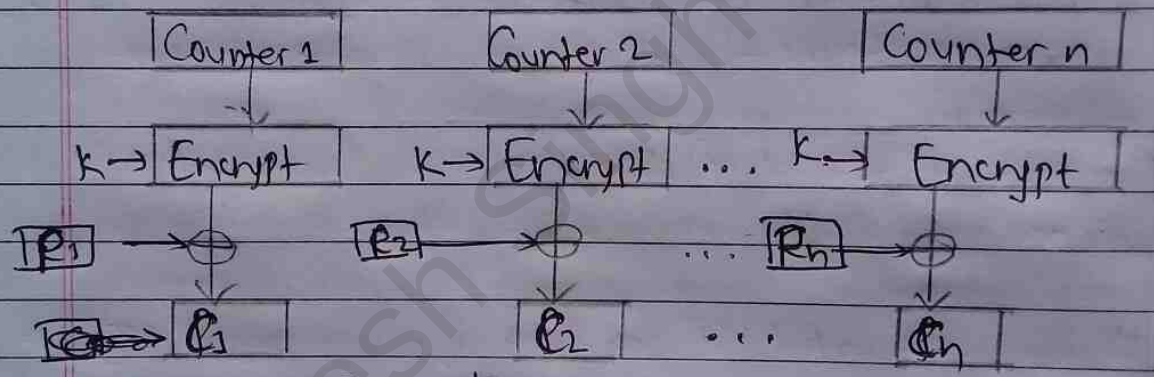
Decryption

Advantages of CFB

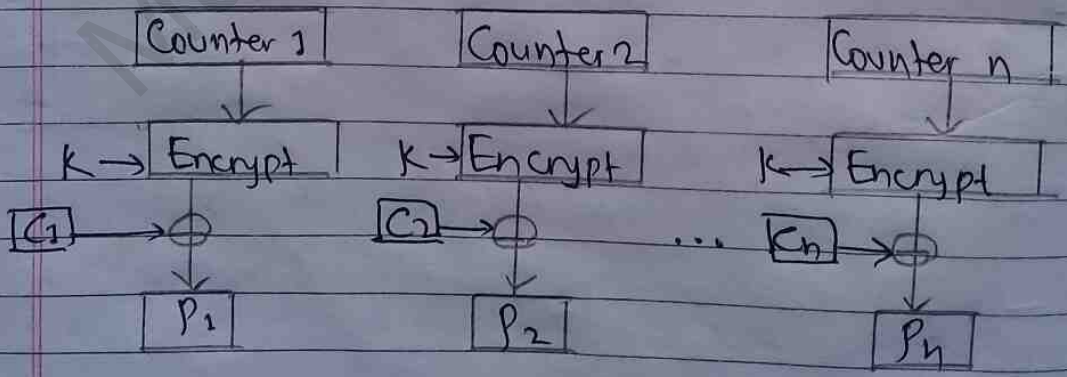
4. Counter Mode

The Counter Mode or CTR is a simple counter based block cipher implementation. Every time a counter initiated value is encrypted and given as input to XOR with plaintext which results in ciphertext block. The CTR mode is independent of feedback use and thus can be implemented in parallel.

Its implementation is shown below:



Encryption



Decryption

Page No.
Date

Summary of Block Cipher Modes of Operation:

Mode	Description	Typical Application
ECB (Electronic Code Book)	Each block of 64 plaintext bits is ~~encoded~~ encoded independently using the same key.	• Secure transmission of single values (e.g. an encryption key).
CBC (Cipher Block Chaining)	The input to the encryption algorithm is the XOR of the next 64 bits of plaintext and the preceding 64 bits of ciphertext.	• General purpose block oriented transmission. • Authentication
CFB (Cipher Feedback)	Input is processed j bits at a time. Preceding ciphertext is used as input to the encryption algorithm to produce pseudorandom output, which is XORed with plaintext to produce next unit of ciphertext.	• General-purpose stream-oriented transmission. • Authentication.
CTR (Counter)	Each block of plaintext is XORed with an encrypted counter. The counter is incremented for each subsequent block.	• General purpose block-oriented transmission. • Useful for high speed requirements.

Q. Differentiate between Cryptography and Cryptanalysis

	Cryptography	Cryptanalysis
1.	Cryptography is the study of conversion of plain text (readable format) to ciphertext (non-readable format) i.e. encryption.	1. Cryptanalysis is the art/study of obtaining plaintext from ciphertext without knowing the encryption key.
2.	It is associated with encryption.	2. It is associated with decryption.
3.	Practitioner of cryptography is called Cryptographer.	3. Practitioner of cryptanalysis is called cryptanalyst.
4.	It takes place on the sender side.	4. It takes place on the receiver side.
5.		

Page No.
Date

8. Differentiate between Symmetric Encryption and Asymmetric Encryption

Symmetric Encryption	Asymmetric Encryption
1. It only requires a single key for both encryption and decryption.	1. It requires two key one to encrypt and the other to decrypt.
2. The size of ciphertext is same or smaller than the original plain text.	2. The sizer of cipher text is same or larger than the original plain text.
3. The encryption process is very fast.	3. The encryption process is slow.
4. It is used when a large amount of data is required to transfer.	4. It is required when used to transfer small amount of data.
5. It only provides confidentiality.	5. It provides Confidentiality, authenticity and non-repudation.
6. Resource utilization is low.	6. Resource utilization is high.
7. Examples: DES, 3DES, AES and RC4.	7. Example: Diffie-Hellman, ECC, DSA and, RSA and EL Gamal.

Q. Explain the Feistel Cipher Structure.

→ A Feistel Cipher is a symmetric structure used in the construction of block ciphers, named after the German-born physicist and cryptographer Horst Feistel.

Feistel Cipher model is a structure or design used to develop many block ciphers such as DES.

Feistel Cipher may have invertible, non-invertible and self-invertible components in its design.

Same encryption as well as decryption algorithm is used.

A separate key is used for each round. However same round keys are used for encryption and as well as decryption.

~~Feistel Cipher Algorithm:~~

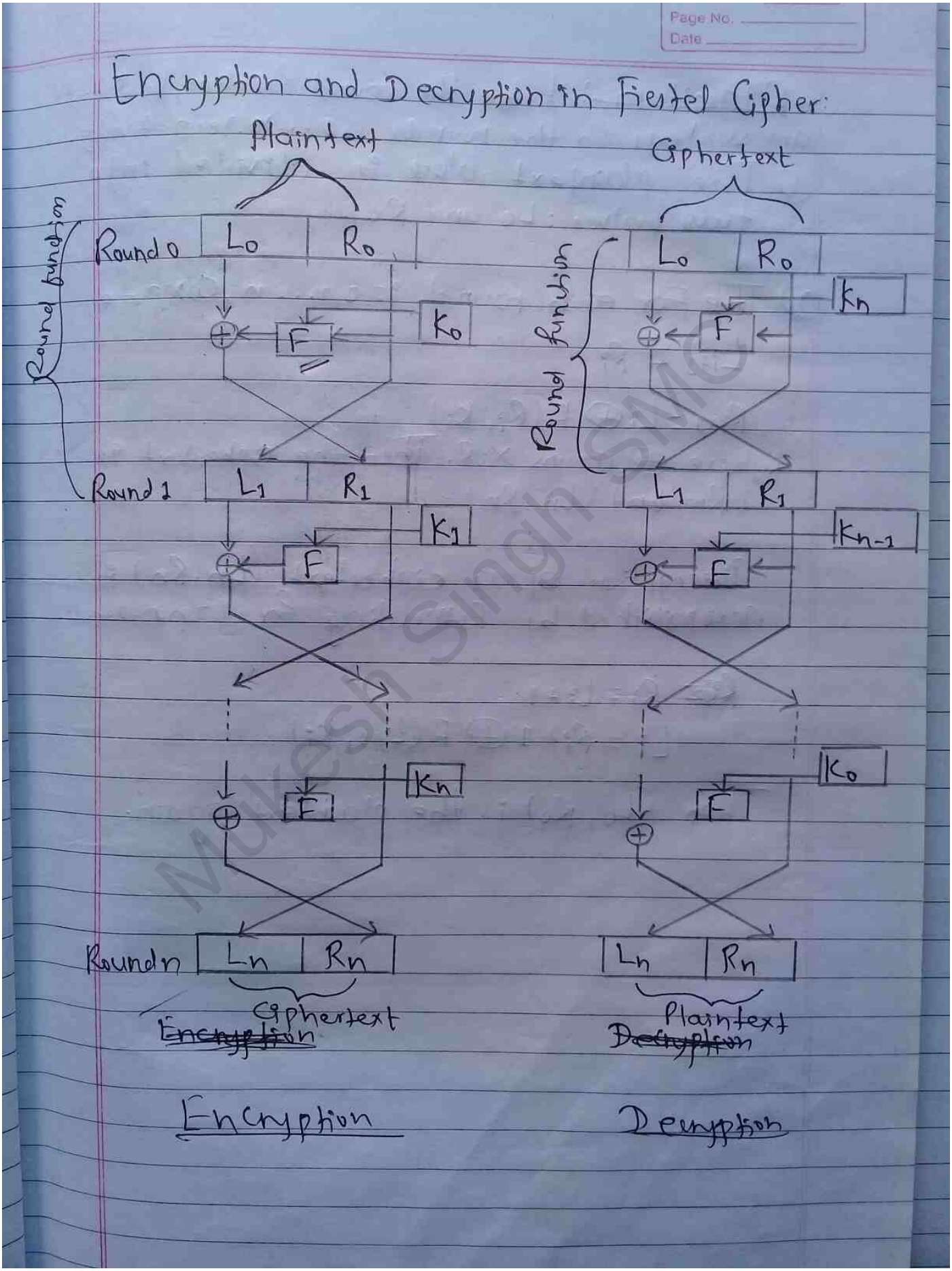
i) Create a list of all plaintext characters.

ii) Convert the plaintext into ASCII and then 8-bit binary format.

iii) Divide the binary plaintext string into two halves. Left half (L_1) and right half (R_1).

Page No.
Date

Encryption and Decryption in Fiestel Cipher:



Encryption

Decryption

Algorithm: F be the round function, $k_0, k_1 \ldots k_n$ are subkeys for the rounds $0, 1 \ldots n$ respectively.

① The plaintext block is divided into two halves: L_0 and R_0.

② For each round $i = 0, 1 \ldots n$, compute

$$L_{i+1} = R_i$$

$$R_{i+1} = L_i \oplus F(R_i, K_i)$$

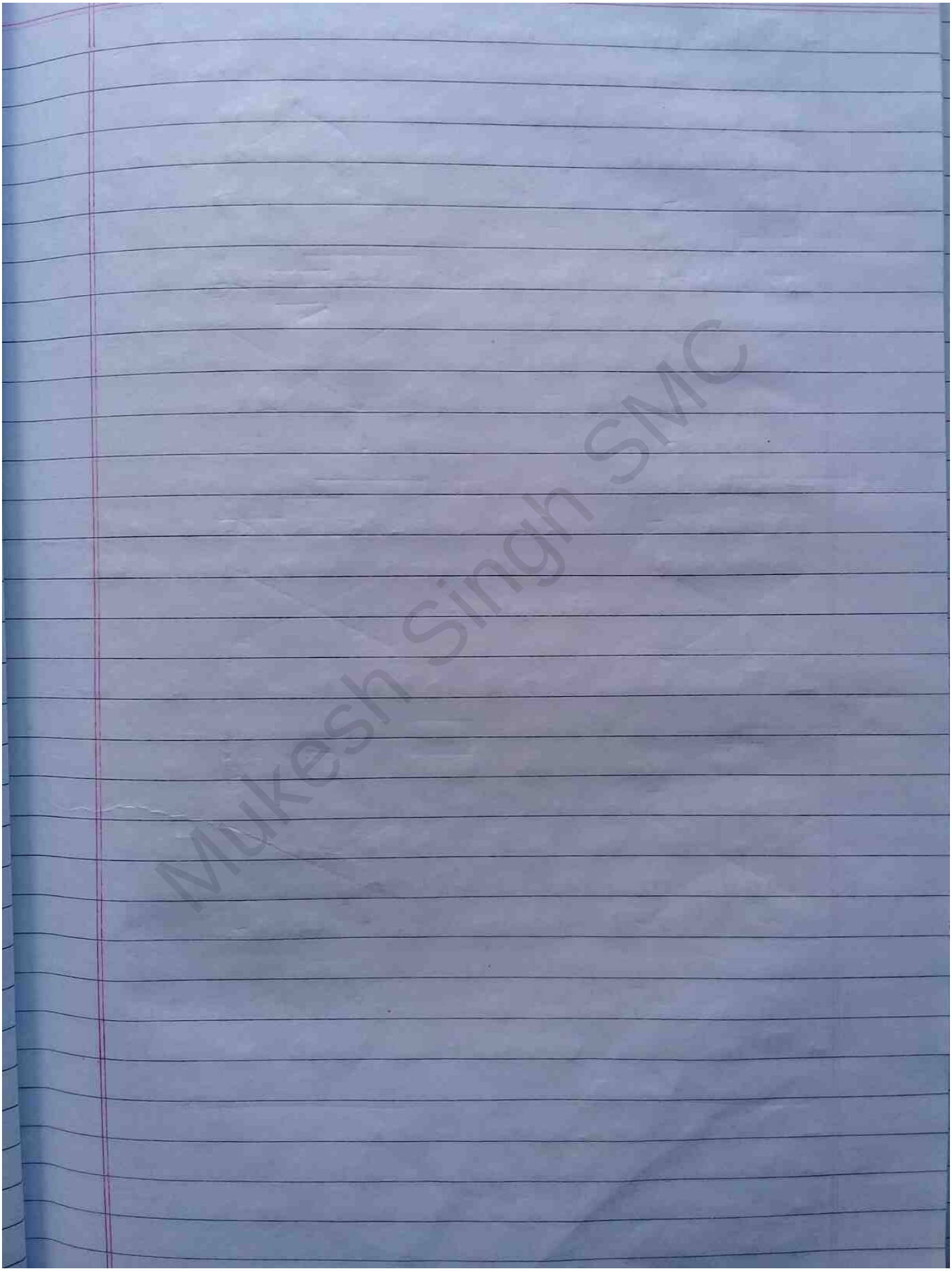
Where $\oplus$ means XOR. Then the ciphertext is (L_n, R_n).

Decryption of a ciphertext (L_n, R_n) is accomplished by computing for $i = n, n-1 \ldots 0$.

$$R_i = L_{i+1}$$

$$L_i = R_{i+1} \oplus F(L_{i+1}, K_i)$$

Then (L_0, R_0) is the plaintext again.

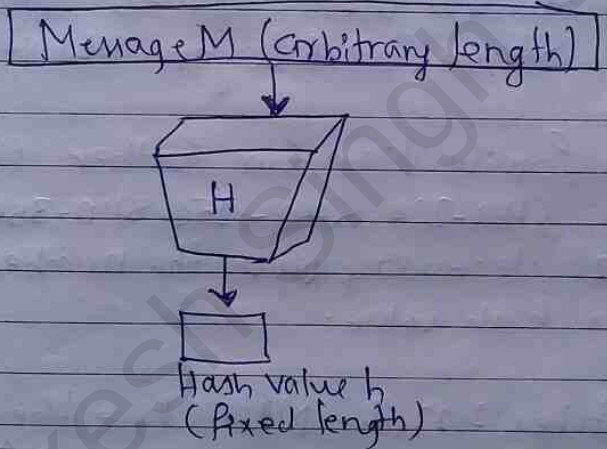


Unit-3

Public Key Cryptography and Message Digest

3.1. Secure Hash functions

A hash function is a mathematical function that converts a numerical input value into another compressed numerical value. The input to the hash function is of arbitrary length but output is always of fixed length.



Secure Hash Function (SHA)

The Secure Hash Algorithm (SHA), are a family of cryptographic hash functions published by NIST which is designed to keep data secured. It works by transforming the data using a hash function: an algorithm that consists of bitwise operations, modular additions and compression functions.

Family of SHA comprises of four SHA algorithms : SHA-0, SHA-1, SHA-2 and SHA-3. Though from the same family, they are structurally different.

→ The original version is SHA-0, a 160-bit hash function, was published by the NIST in 1993. It had a few weakness and did not become very popular. Later in 1995, SHA-1 was designed to correct alleged weakness of SHA-0.

→ SHA-1 is the most widely used of the existing SHA has functions. It is employed in several widely used applications and protocols including Secure Socket Layer (SSL) security.

→ SHA-2 family has four further SHA variants, SHA-224, SHA-256, SHA-384 and SHA-512 depending upon the number of bits in their hash value.

→ In October 2012, the NIST chose the Keccak algorithm as the new SHA-3 standard. It supports the same hash lengths as SHA-2 and its internal structure differs ~~from~~ significantly from the rest of the SHA family. It has many benefits such as efficient performance and good resistance for attacks.

Characteristics of SHA

→ They have variable input length and fixed output length.
→ They are one-way functions.
→ Produces 160 bit message digest.
→ Same message digest is to be produced from both sender and receiver.

→ Purpose : Authentication, not Encryption
→ It is not possible to generate the same hash value using two different input values. This is called "Collision resistance".
→ A small change in the input value, even a single bit, completely changes the resultant hash value. This is called the "avalanche effect".
→ If the same input message is fed to the SHA function, it will always generate the resultant hash.

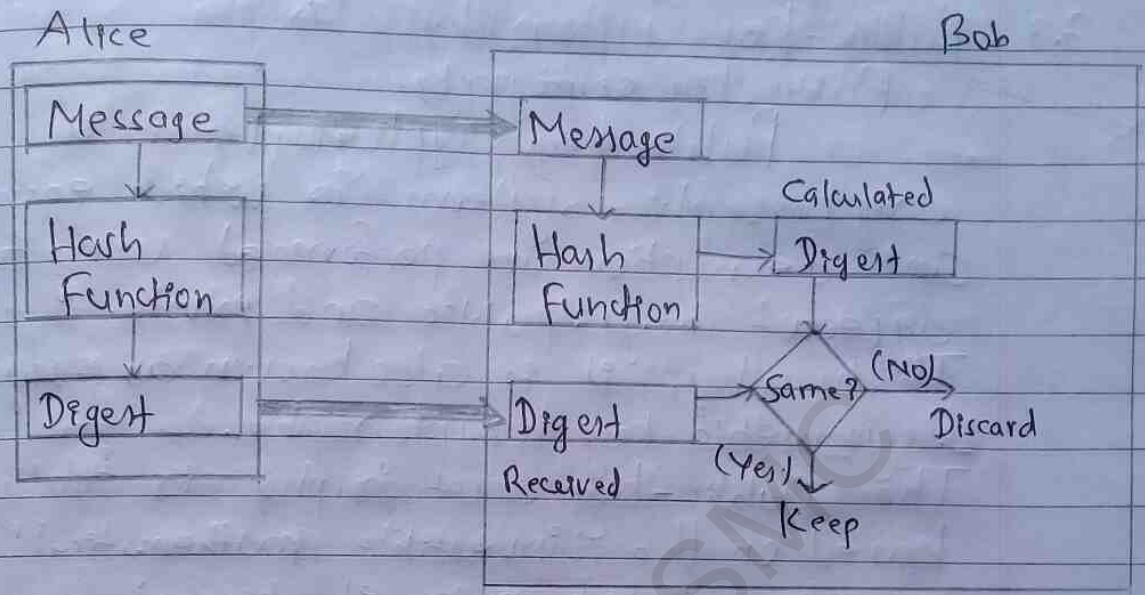
3.2 Message digest (MD)

A message digest is a cryptographic hash function containing a string of digits created by a one-way hashing formula. Message digest is used to ensure the integrity of a message transmitted over an insecure channel (where the content of the message can be changed). The message is passed through a cryptographic hash function. This function creates a compressed image of the message called Digest.

Working Principle of MD:

Lets assume, Alice sent a message and digest pair to Bob. To check the integrity of the message Bob runs the cryptographic hash function on the received message and gets a new digest. Now, Bob will compare the new digest and the digest sent by Alice. If, both are same then Bob is sure that the original message is not changed.

This message and digest pair is equivalent to a physical document and fingerprint of a person on that document. Unlike the physical document and the fingerprint the message and the digest can be sent separately.



Examples / Types of MD:

The MD family comprises of hash functions MD2, MD4, MD5 and MD6. It was adopted as Internet Standard RFC 1321. It is a 128-bit hash function.

The hash algorithm MD5 is widely used to check the integrity of messages. MD5 divides the message into blocks of 512 bits and creates a 128-bit digits (typically, 32 Hexadecimal digits). It is no longer considered reliable for use as researchers have demonstrated techniques capable of easily generating MD5 collisions on commercial computers.

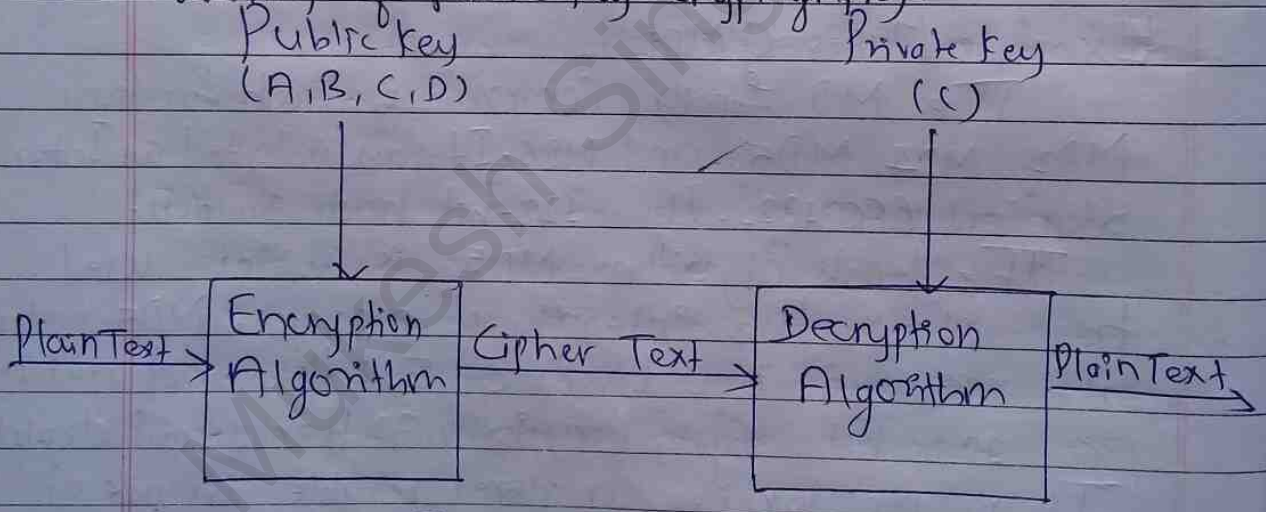
The weakness of MD5 have been exploited by the flame malware in 2012.

3.3 Public-Key Cryptography Principles

Public key cryptography

Public key cryptography is a cryptographic system in which encryption and decryption are performed using two different keys: public and private. That is why, it is also known as Asymmetric-key cryptography. The public-key cryptography is totally based on the 'invertible mathematical' function which makes it different from the conventional symmetric key cryptography.

Working of Public key Cryptography:



Public keys of every user are present in the public key register. If B wants to send a confidential message to C, then B encrypt the message using C public key. When C receives the message from B then C can decrypt it using its own Private key. No other than C can decrypt the message because only C know C's private key.

Public-key Cryptography principles:

→ 1) Public-key cryptography algorithms rely on one key for encryptions and a different but related key for decryption.

2) It is completely infeasible to determine the decryption from encryption key and encryption algorithm.

3) The use of two keys has consequences in: key distribution, confidentiality and authentication.

4) Public key ~~etc~~ encryption has following 6 key ingredients (components):

i) Plaintext → This is a readable message or data which is given to the encryption algorithm as input.

ii) Ciphertext → The ciphertext is produced as an output of Encryption algorithm. We cannot simply understand this message.

iii) Encryption Algorithm → It performs various ~~operations on~~ transformations on plain text. It is used to convert plaintext into cipher text.

iv) Decryption Algorithm → This algorithm accepts the Ciphertext and the matching key to produce original plaintext.

v) Public and Private key → They is a pair of keys that has been selected to so that if one is used for encryption then the other is used for decryption.

Steps in public key cryptography:

1.) Each user has to generate two keys one of will be used for encryption and other for decryption of messages.

2) Each user has a pair of keys, among which one has to be made public by each user. And the other has to be kept secret.

3) If a user has to send a message to a particular receiver then the sender must encrypt the message using the intended receivers public key and then send the encrypted message to the receiver.

4) On receiving the message, the receiver has to decrypt the message using his private key.

Page No.
Date

Applications for Public-key Cryptosystem

We can classify the applications of the public key cryptosystem as below:

a) Encryption/Decryption → The sender encrypts a message with the recipient's public key and only the receiver can decrypt the message using her own private key.

b) Digital Signature → Content/menage is digitally signed with a sender's private key and is verified by the sender's public key.

c) Key Exchange → Two sides cooperate to exchange a sesion key (secret key). This secret key is valid for short period only.

Applications for Public Key Cryptography table:

Algorithm	Encryption / Decryption	Digital Signature	Key Exchange
RSA	Yes	Yes	Yes
Elliptic Curve	Yes	Yes	Yes
Diffie-Hellman	No	No	Yes
DSS	No	Yes	No

Requirements for Public Key Cryptography:

→1) It is easy for party B to generate a pair of keys (public key PU_b, private key PR_b).

2) It is easy for sender A, ~~too~~ knowing the public key and message M to be encrypted, to generate the ciphertext.

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

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

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

4) It is computationally infeasible for an opponent, to known the public key PU_b to determine the private key PR_b.

5) It is infeasible for any ~~person~~ opponent to known the public key PU_b and a ciphertext C to recover the original message M.

6) Two keys: public and private key can be applied/implemented in both/any orders for encryption and decryption.

$$D[PU, E(PR, M)] = D[PR, E(PU, M)].$$

3.4 Public-key Cryptography Algorithms

Public-key cryptography algorithms (also known as an asymmetric algorithm) is one where the keys used for encryption and decryption are different and the decryption key cannot be calculated from the encryption key. This allows someone to keep a public-key/private-key pair. The public key is used to encrypt and the private key is used to decrypt. The public key can be distributed to allow others to encrypt menage. But the private key is not shared with anyone, and is the only way to decrypt menage that have been encrypted with the public key.

Some public key algorithms provide key distribution and secrecy (e.g. Diffie-Hellman key exchange), some provide digital signatures (e.g. Digital Signature Algorithm) and some provide both (e.g. RSA).

Some public key cryptography algorithms are described below:

1. RSA public-key Encryption Algorithm

The acronym RSA comes from the surnames of Ron Rivest, Adi Shamir and Leonard Adleman, who publicly described and developed the algorithm in 1977. It is a public key cryptosystem that is widely used for secure data transmission. It is also known as asymmetric cryptographic algorithm because two different keys: public and private, are used for encryption and decryption. Public key is given to everyone

and the private key is kept private.
Both public and private keys are interchangeable.
RSA keys can be typically 512, 1024 or 2048 bits long.

RSA Algorithm

1. Choose two large prime numbers p & q.
2. Compute $n = pq$ and $z = (p-1)(q-1)$
   $z = \phi(n)$
3. Choose number e, less than n, which has no common factor (other than 1) with z.
   $1 < e < \phi(n)$ and $gcd(\phi(n), e) = 1$
4. find the number d, such that ed-1 is exactly divisible by z keys, are generated using n, d, e.

	where,
• Public key is (n, e)	$d = e^{-1} \bmod \phi(n)$
• Private key is (n, d)	i.e. $ed = 1 \bmod \phi(n)$

5. Encryption :
   $C = m^e \bmod n$
   m is plain text
   C is cipherfext.

6. Decryption:
   $m = C^d \bmod n$

Public key is shared and private key is hidden.

Example of RSA:

1)

- $p = 5$ & $q = 7$
- $n = pq = 5 \times 7 = 35$ and $z = (p-1)(q-1) = 4 \times 6 = 24$
- $e = 5$
- $d = 29$, $(29 \times 5 - 1)$ is exactly divisible by 24

$d = (k*z+1)/e$ for some integer k let's suppose $k = 6$

Keys generated are:

Public key $(n, e) = (35, 5)$

Private key $(n, d) = (35, 29)$

- Encrypt the word love using $(C = m^e \bmod n)$

(Assume that the alphabets are between 1 & 26)

Plain Text	Numeric Representation	m^e	Cipher Text $(C = m^e \bmod n)$
l	12	248832	17
o	15	759375	15
v	22	5153632	22
e	5	3125	10

Decrypt the word love using $(m = c^d \bmod n)$, $n = 35$, $c = 29$

Cipher Text	C^d	$(m = m^e \bmod n)$	Plain Text
17	48196857210675091509141182522307200O	17	l
15	127834039488589391117232757568359400	15	o
22	852643319098653770195619449972111000000O	22	v
10	10000000000000000000000000000000	10	e

Example 2

Let $p=3, q=11$

$n = p*q = 3\times11 = 33$ and $z = 2\times10 = 20$

So, let $e=7$ as $1<7<20$ and $\gcd(7,20)=1$

Now,

$d \equiv e^{-1} \bmod z$

$de \equiv 1 \bmod z \rightarrow de \bmod z = 1$

$7\times d \equiv 1 \bmod z$

$(7\times d) \bmod 20 = 1$ $\therefore d=3$

Keys generated are:

public key $(n, e) = (33, 7)$

private key $(n, d) = (33, 3)$

Encryption:

Let $m=31$

$c = M^e \bmod n$

$c = 31^7 \bmod 33 = 4$ $\therefore c=4$

(C is cipher text)

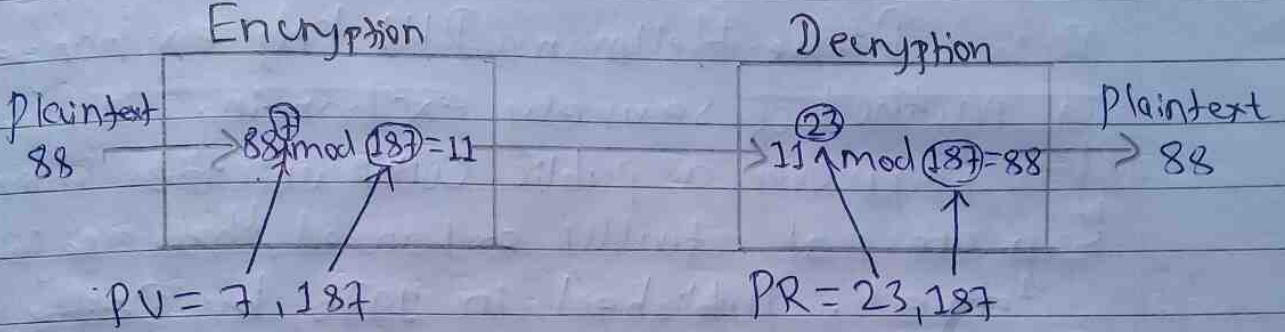
Decryption:

$M = c^d \bmod n = 4^3 \bmod 33 = 31$

$\therefore m=31$

(m is plaintext).

~~2. Diffie Hellman key Exchange Algorithm~~



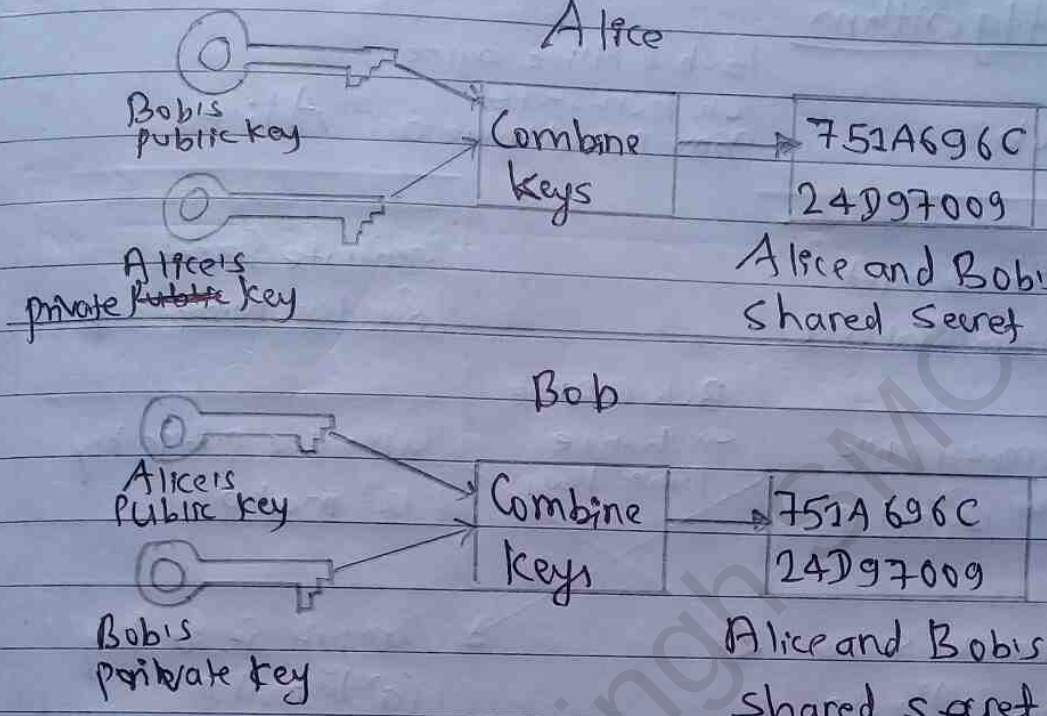
RSA

2. Diffie-Hellman Key Exchange Algorithm

Diffie-Hellman (DH) key exchange is a method of securely exchanging cryptographic keys over a public communication channel. Keys are not actually exchanged, they are jointly derived. Published in 1976 by ~~Diffie~~ Ralph Diffie and Martin Hellman, this is the earliest publicly known work that proposed the idea of ~~public~~ private key and a corresponding public key.

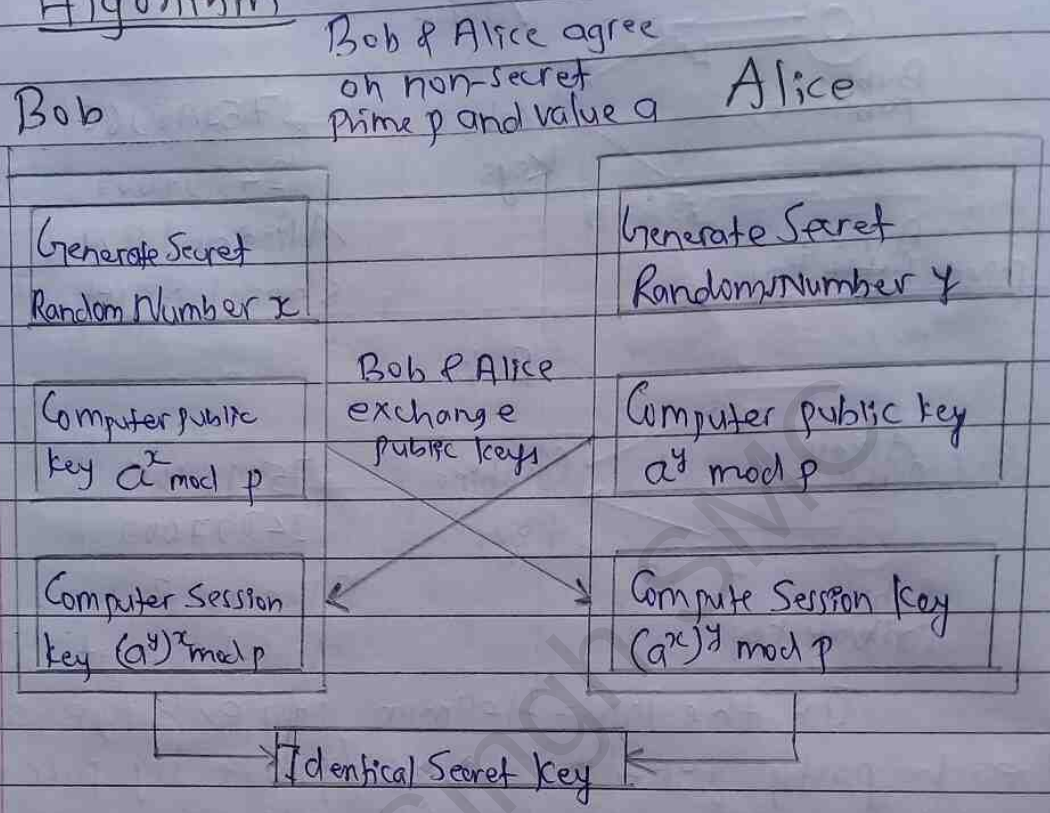
The purpose of the algorithm is to enable two users to securely exchange a key that can then be used for subsequent encryption of messages. The algorithm itself is limited to the exchange of secret values.

The Diffie-Hellman key exchange is method allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure communication channel. This key can be used to encrypt subsequent communication using a symmetric key cipher.



In the Diffie-Hellman key exchange algorithm, each party generates a public/private key pair and distributes the public key. After obtaining an authentic copy of each other's public keys, Alice and Bob can compute a shared secret offline. The shared secret can be used, for instance, as the key for symmetric cipher.

Algorithm



Alice	Bob
Public keys available = P, G	Public keys available = P, G
Private key selected = a	Private key selected = b
Key generated = $x = G^a \bmod P$	Key generated = $y = G^b \bmod P$
Exchange of generated keys takes place	
Key received = y	Key received = x
Generated Secret key = $k_a = y^a \bmod P$	Generated secret key = $k_b = x^a \bmod P$

Algebraically it can be shown that

$k_a = k_b$

Page No.
Date

Users now have symmetric secret keys to exchange.

Example

Step 1: Alice and Bob get public numbers P=23, G=9

Step 2: Alice selected a private key a=4 and
Bob selected a private key b=3

Step 3: Alice and Bob Compute public values
Alice: $x = G^a \bmod P = (9^4 \bmod 23) = (6561 \bmod 23) = 6$
Bob: $y = G^b \bmod P = (9^3 \bmod 23) = (729 \bmod 23) = 16$

Step 4: Alice and Bob exchange public numbers.

Step 5: Alice receives public key, y=16 and
Bob receives public key, x=6

Step 6: Alice and Bob compute Symmetric keys
Alice: $K_a = y^a \bmod p = 65536 \bmod 23 = 9$
$K_b = x^a \bmod p = 216 \bmod 23 = 9$

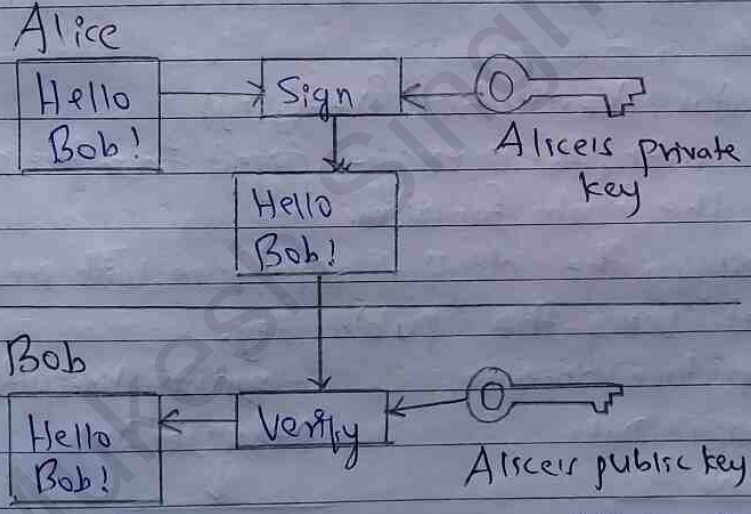
Step 7: 9 is the secret.

3.5 Digital Signatures

A Digital signature is a mathematical scheme/technique used to validate/verify the authenticity and integrity of digital messages or documents.

It's the digital equivalent of a handwritten signature or stamped seal, but it offers far more inherent security.

A digital signature may be used to detect whether or not the information was modified after it was signed.

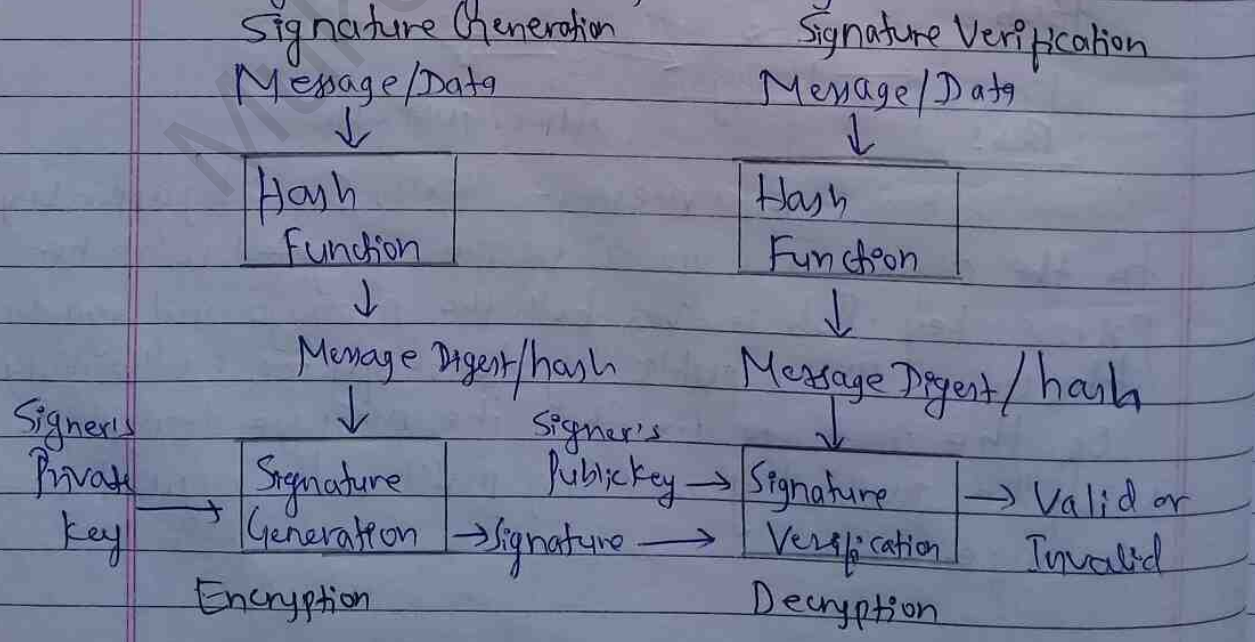


Alice signs a message, "Hello Bob!" by appending to the original message a version encrypted with her private key. Bob receives both the message and signature. He uses Alice's public key to verify the authenticity of the message i.e. that the message, decrypted using the public key, exactly matches the original message.

The digital signature process can be divided into 2 parts:

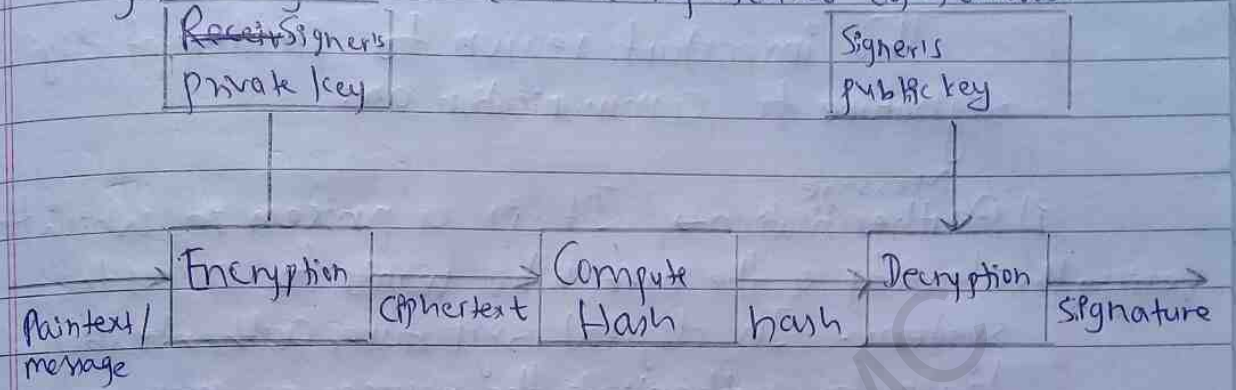
1. Signature Generation (Signing)
→ Generating a pair of public key and private key by the Sender of the message.
→ Generating the message digest from the message using a hash function.
→ Generating the digital signature from the message digest with the private key.
→ Sending the message, the digital signature and the public key to receiver.

2. Signature Verification (Verifying)
→ Generating the message digest from the message using the hash function.
→ Verifying the digital signature with message digest using the public key.



OR

Digital Signature process can be represented as follows:



1. Select a file/message to be digitally signed.

2. The hash value of the message is calculated. The message is encrypted by using a private key of a sender to form the digital signature.

3. Now, the original message along with the digital signature is transmitted.

4. The receiver decrypts the digital signature by using a public key of Sender.

5. The receiver now has the message ~~of the~~ and can compute it.

6. Comparing these computed message or file content with the original computed message. The comparison needs to be the same for ensuring integrity.

Applications of Digital Signature

The important reason to implement digital signature to communication are:

i) Authentication (Message) → It is a process in which ~~the~~ verifies the identity of the user who wants to access the system. In digital signature, authentication helps to authenticate the sources of messages.

ii) Integrity (Data) → It ensures that the message is real, accurate and safeguards from unauthorized ~~users~~ modification during the transmission.

iii) Non-repudiation → It means assurance of something that cannot be denied. It ensures that someone to a contract or communication cannot later deny the authenticity of their signature on a document or sending of message that they originated.

Page No.
Date

Algorithms in digital Signature:

A digital signature consists of three algorithms:

1. Key generation algorithm

The key generation algorithm selects private key randomly from a set of possible private keys. This algorithm provides the private key and its corresponding public key.

2. Signing algorithm

A signing algorithm produces a signature for the document.

3. Signature verifying algorithm

A signature verifying algorithm either accepts or rejects the document's authenticity.

Types of digital signature:

1) Certified Signature
2) Approval Signature
3) Visible Digital Signature
4) Invisible Digital Signature

Unit-4

Network Security Applications

Ajanta
Page No.
Date

4.1 Public-key Infrastructure

→ A public key infrastructure (PKI) is a set of roles, policies, hardware, software and procedures needed to create, manage, distribute, use, store and revoke digital certificates and manage public-key encryption (RFC 2822).

→ ~~RFC 2822 (Internet Security Glossary) defines public-key infrastructure (PKI)~~

→ The purpose of PKI is to facilitate the secure electronic transfer of information for a range of network activities such as e-commerce, internet banking and confidential email.

→ The principle objective for developing a PKI is to enable secure, convenient and efficient acquisition of public keys.

→ The Internet Engineering Task Force (IETF), Public Key Infrastructure X.509 (PKIX) working group has been the driving force behind setting up a formal (and generic) model based on X.509 that is suitable for deploying a certificate-based architecture on the Internet. This section describes the PKIX model.

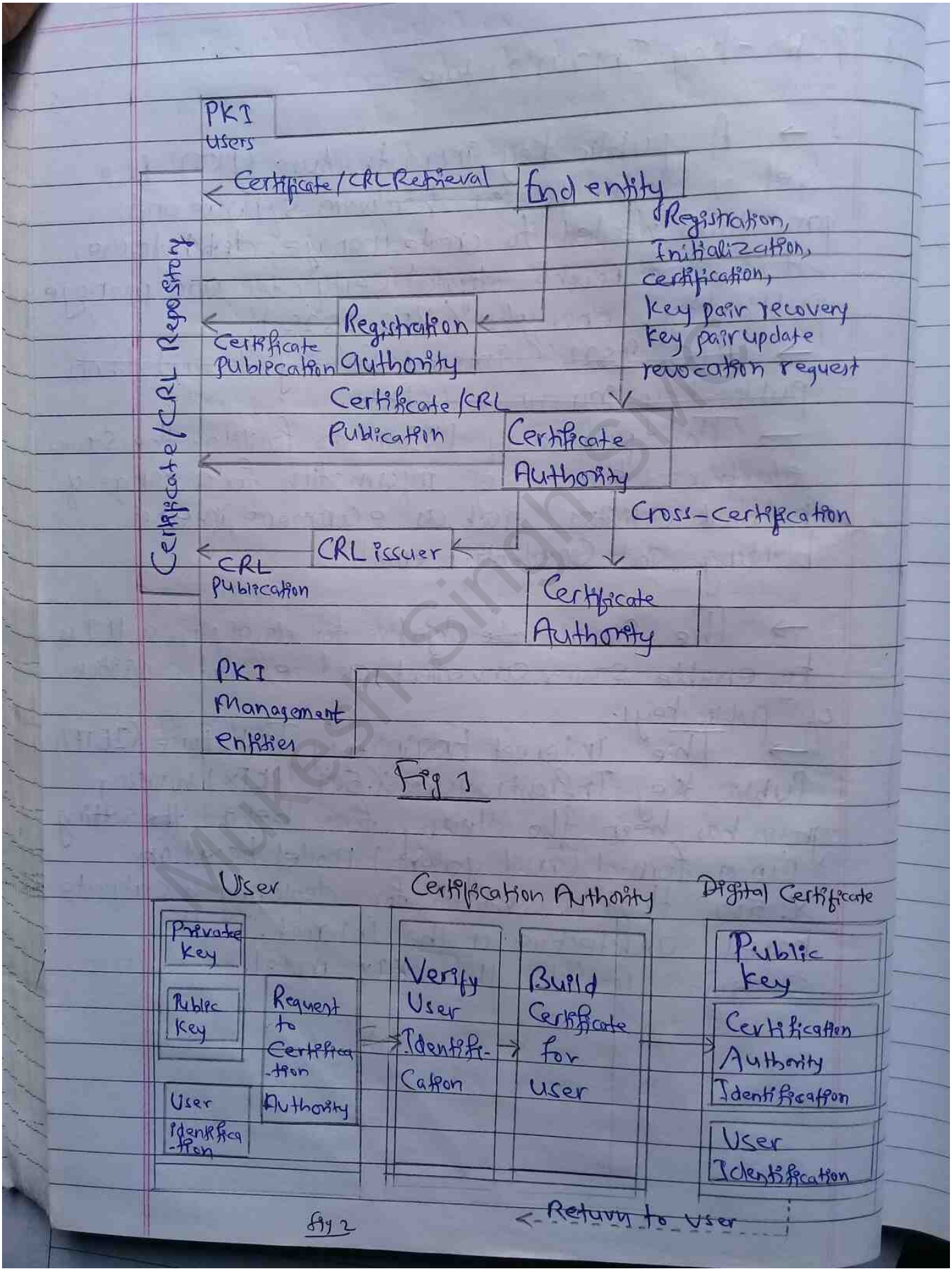


Fig 1

fig 2

Figure 1 shows the relationship among the key elements of the PKIX model. These elements are:

i) End entity → A generic term used to denote end users, devices (e.g. servers, routers) or any other entity that can be identified in the field of a public key certificate. End entities typically consume and/or support PKI-related services.

ii) Certification Authority (CA) → The issuer of certificates and (usually) certificate revocation lists (CRLs). It may also support a variety of administrative functions, although these are often delegated to one or more Registration Authorities.

iii) Registration Authority (RA) → An optional component that can assume a number of administrative functions from the CA. The RA is often associated with the end entity registration process but can assist in a number of other areas as well.

iv) CRL issuer → An optional component that a CA can delegate to publish CRLs.

v) Repository → A generic term used to denote any method for storing certificates and CRLs so that they can be retrieved by end entities.

Digital Certificates

In order to bind public keys (with their associated user (owner of the private key), PKIs use digital certificates.

Digital ~~signature~~ certificates are the credentials that facilitates the verification of identities between users in a transaction. Much as a passport certifies one's identity as a citizen of a country, the digital certificate establishes the identity of users within the ecosystem. Because digital ~~signatures~~ certificates are used to identify the user to whom encrypted data is sent, or to verify the identity of the signer of information, protecting the authenticity and integrity of the certificate is imperative to maintain the trustworthiness of the system.

PKIX Management Functions:

PKIX identifies a number of management functions that potentially need to be supported by management protocols. These are indicated in and include the following:

i) Registration → This is the process whereby a user first makes itself known to a CA (directly or through RA), prior to that CA issuing a certificate or certificates for that user. Registration begins the process of enrolling in a PKI. Registration usually involves some offline or online procedure for mutual

authentication. Typically, the end entity is issued one or more shared secret keys used for subsequent authentication.

ii) Initialization → Before a client system can operate securely, it is necessary to install key materials that have the appropriate relationship with keys stored elsewhere in the infrastructure. For example, the ~~client~~ client needs to be securely initialized with the public key and other assured information of the trusted CA(s), to be used in validating certificate paths.

iii) Certification → This is the process in which a CA issues a certificate for a user's public key and returns that certificate to the user's client system and/or posts that certificate in a repository.

iv) Key pair recovery → Key pairs can be used to support digital signature creation and verification, encryption and decryption, or both. Key pair recovery allows end entities to restore their encryption / decryption key pair from an authorized key backup facility.

v) Key pair update → All key pairs need to be updated regularly and new certificates issued. Update is required when the certificate lifetime expires and as a result of certificate revocation.

vi) Revocation request → An authorized person advises a CA of an abnormal situation requiring certificate revocation. Reasons for revocation include private key compromise, change in affiliation, and name change.

vii) Cross Certification → Two CAs exchange information used in establishing a cross-certificate. A cross-certificate is a certificate issued by one CA to another CA that contains a CA signature key used for issuing certificates.

PKIX Management Protocols

The PKIX working group has defined two alternative management protocols between PKIX entities that support the management functions listed in the preceding subsection.

1) RFC 2510 defines the certificate management protocols (CMP). Within CMP, each of the management function is explicitly identified by specific protocol exchange. CMP is designed to be a flexible protocol able to accomodate a variety of technical, operational and business models.

2) RFC 2797 defines certificate management messages (CMS) over (CMC), where CMS refers to RFC 2630, cryptographic message syntax. CMC is built on earlier work and is intended to leverage existing implementations. Although

Page No.
Date

All of the PKIX functions are supported, the function do not all map into specific protocol exchanges.

4.2 Transport Layer Security: SSL, HTTPS, Secure Shell (SSH)

Transport Layer Security (TLS) is a cryptographic protocol that provides end-to-end communications security over networks and is widely used for internet communications and online transactions.

Transport Layer Security (TLS) are designed to provide security at the transport layer.

TLS ensures that no third party may eavesdrops or tempers with any message.

TSL was proposed by the Internet Security Task force (IETF), an international standards organization, and the first version of the protocol was published in 1999. The most recent version is TLS 1.3, which was published in 2018.

There are different types of transport layer security which are explained below.

1. SSL (Secure Socket Layer)

SSL is designed to make use of TCP to provide a reliable end to end secure service.

SSL is not a single protocol but rather two layers of protocols, as illustrated in the figure.

The SSL record protocol provides basic security services to various higher layer protocols.

Three high layer protocols are defined as part of SSL ① The Handshake protocol, ② The Change Cipher Spec Protocol and

③ The Alert Protocol.

These specific SSL protocols are used in the management of SSL exchanges and are examined later in this section.

Two important SSL concepts are SSL session and SSL connection, which are defined in the specification as follows:

i) Connection → It is a transport that provides the suitable types of services. For SSL, such connections are peer-to-peer relationships. Every connection is associated with one session.

ii) Session → It is an association between a client and a server. Sessions are created by the Handshake Protocols. ~~Session~~

Architecture of SSL:

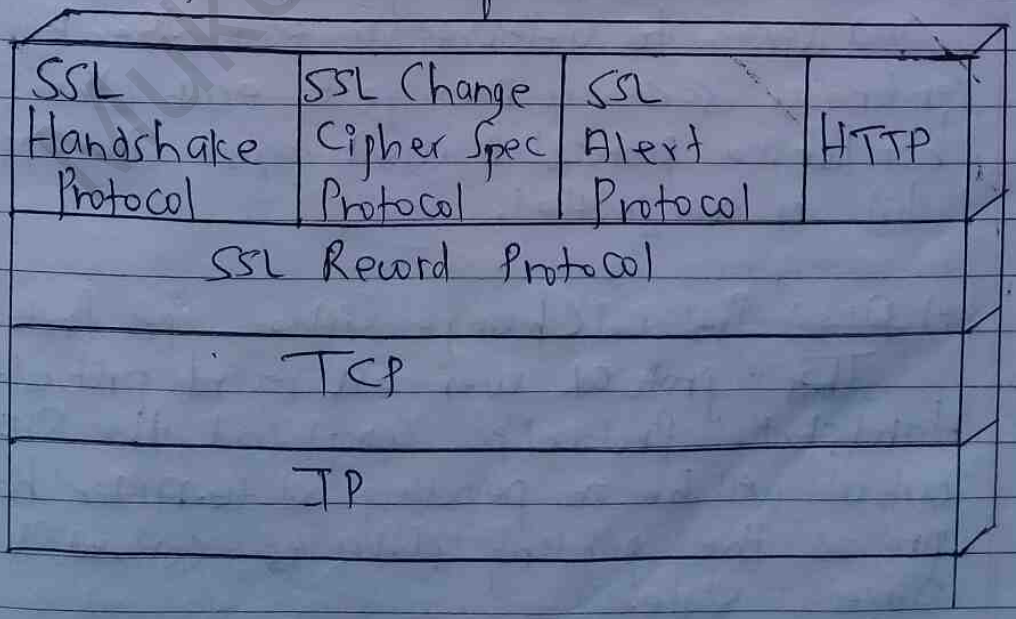


fig: SSL Protocol Stack

i) SSL Record Protocol →
SSL record protocol provide two services to SSL connection.
→ Confidentiality
→ Message Integrity
In SSL record protocol application data is divided into fragments. The fragement is compressed and then encrypted MAC generated by algorithms like SHA and MD5 is appended. After that the encryption of data is done and in last SSL header is appended to the data.
The SSL record protocol is responsible for ensuring data security through encryption and data integrity.

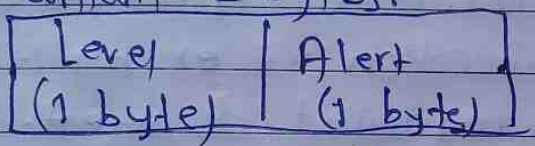
ii) Handshake Protocol →
The handshake protocol is used to establish sessions. This protocol allows client and server to authenticate each other by sending a series of message to each other. The handshake protocol is used before any application data is transmitted.

iii) ~~Alert Protocol~~ Change Cipher Spec Protocol
This protocol uses SSL record protocol. Unless Handshake Protocol is completed, the SSL record output will be in pending state. After handshake protocol the pending state is converted into current state.
Change cipher protocol consists of single message

which is 1 byte in length and can have only one value. This protocol purpose is to cause the pending state to be copied into current state.

iv) Alert Protocol

This protocol is used to convey SSL-related alerts to the peer entity. Each message in this protocol contain 2 bytes.



As with other applications that uses SSL, alert messages are compressed and encrypted, as specified by the current state.

The Hypertext Transfer Protocol (HTTP), which provides the transfer service for web client/server interaction, can operate on top of SSL.

2. HTTPs

HTTPs refers to the combination of HTTP and SSL to implement secure communication between a web browser and a web server. A normal HTTP connection uses the port 80. If HTTPS is specified, port 443 is used, which invokes SSL.

When HTTPs is used, the following elements of the communication are encrypted:

→ URL of the requested document.
→ Contents of the document.
→ Contents of web browser forms.
→ Cookies sent from browser to server and from server to browser.
→ Contents of HTTP header.

HTTP is documented in the RFC 2818, HTTP over TLS. There is no fundamental change in using HTTP over either SSL or TLS, and both implementations are referred to as HTTPs.

Processes in HTTPs:

i) Connection Initiation

For HTTPs, the agent acting as the HTTP client also acts as the TLS client. The client initiates a connection to the server on the appropriate port and then sends the TLS client Hello to begin the TLS handshake. When the TLS handshake is finished, the client may then initiate the first HTTP request.

ii) Connection Closure →

TLS provides a facility for secure connection closure. When a valid closure alert is received, an implementation can be assured that no further data will be received on that connection.

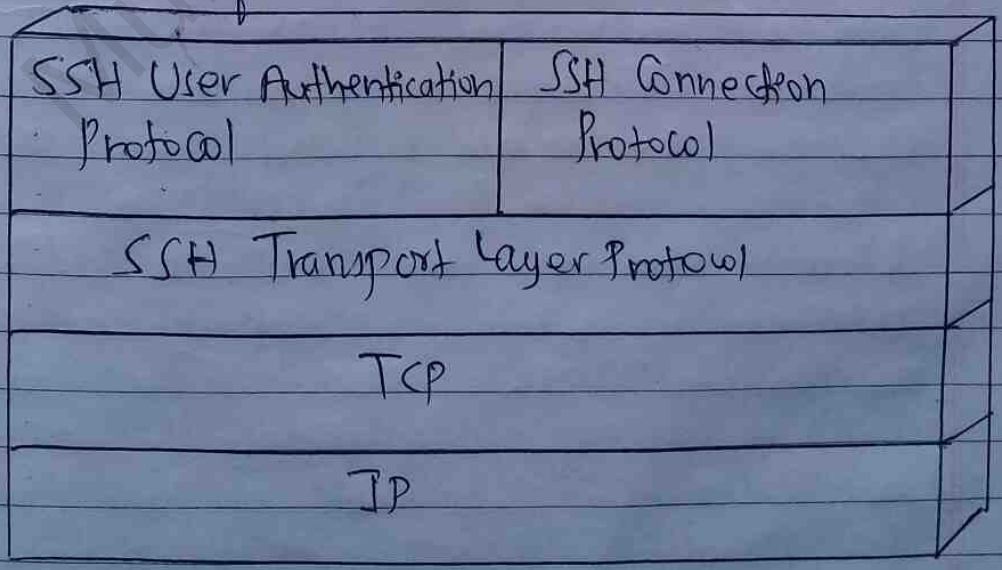
3. Secure Shell (SSH)

SSH is a network protocol that gives users, particularly system administrators, a secure way to access a computer over an unsecured network.

The initial version, SSH1 was focused on providing a secure remote login facility to remove/replace TELNET and other remote logon schemes that provides no security.

A new version, SSH2, fixes a number of security flaws in the original scheme.

Architecture of SSH:



i) SSH Transport Layer Protocol
Provides server authentication, data confidentiality, and data integrity with forward secracy. The transport layer may optionally provide compression.

ii) User Authentication Protocol -
Authenticates the user to the server.

iii) Connection Protocol -
Multiplexes multiple logical communications channels over a single, underlying SSH connection.

4.3 Wireless Security : WEP, ~~WPA~~ WPA, WPA 2

Wireless security is the prevention of unauthorized access or damage to computer or data using wireless networks, which include Wi-fi networks.

It aims to ensure that your data remains only accessible to users you authorize.

There are four wireless security protocols currently available:

1) Wired Equivalent Privacy (WEP)
2) Wi-fi Protected Access (WPA)
3) Wi-fi Protected Access 2 (WPA 2)
4) Wi-fi Protected Access 3 (WPA 3)

1. Wired Equivalent Privacy (WEP)

WEP is the first security protocol ever put in practice. Designed in 1997, it has become obsolete but is still used in modern times with older devices.

WEP is an old IEEE 802.11 standard.

WEP uses a data encryption scheme that is based on a combination of user and system generated key values. However, it is widely known that WEP is the least secured network type as hackers have developed the tactics of reverse engineering and cracking the encryption system.

At the beginning, maximum 64-bit encryption was allowed in US. So, WEP was using 64-bit encryption. After the restrictions, 128-bit and 256-bit WEP has developed.

2. Wi-Fi Protected Access (WPA)

WPA was developed in 2003 by Wi-Fi Alliance. Because of the vulnerabilities of WEP, a new protocol must be developed. WPA offers features such as the Temporal key Integration Protocol (TKIP) which was a dynamic 128-bit key that was harder to break into than WEP's static unchanging key.

It also introduced the message integrity check, which scanned for any altered packets sent by hackers, the TKIP and the Pre-shared key (PSK), among others for encryption.

3. Wi-Fi Protected Access 2 (WPA 2)

WPA 2 was developed in 2004. It was advanced version of WPA. Vulnerable parts of WPA becomes stronger with WPA 2.

WPA 2 offered new encryption and authentication and mechanisms to provide more secured networks. These mechanisms were AES (Advanced Encryption Standard) and CCMP (Counter Cipher Mode with Block Chaining Message Authentication Code Protocol). These mechanisms were used instead of previous mechanisms, TKIP.

Page No.
Date

4. Wi-Fi Protected Access 3 (WPA 3)

The last developed security standard for wireless is WPA 3. WPA 3 offers improved authentication and encryption. It will be used more with 802.11 ax standard. WPA 3 will be mandatory with Wi-Fi 6.

With wi-fi 6, better security will be needed and there will be more wireless devices. So, with these requirements, security will become more important and WPA 3 will be used with Wi-Fi 6.

4.4 E-mail Security : PGP, S/MIME

Email Security is a term for describing different procedures and techniques for protecting email accounts, content and communication against unauthorized access, loss or compromise. Email is often used to spread malware, spam and phishing attacks.

Email Security protocols are ~~used~~ designed to secure your communications as they pass between webmail services over the internet.

We will take a look at each of the commonly used security protocols, and explain what each of them does to keep your emails safe.

1. PGP (Pretty Good Privacy)

→ PGP stands for Pretty Good Privacy which is invented by Phil Zimmermann, in 1991.

→ PGP was designed to provide all four aspects of security i.e. privacy, integrity, authentication and non-repudiation in the sending of email.

→ PGP is an open source and freely available software package for email security.

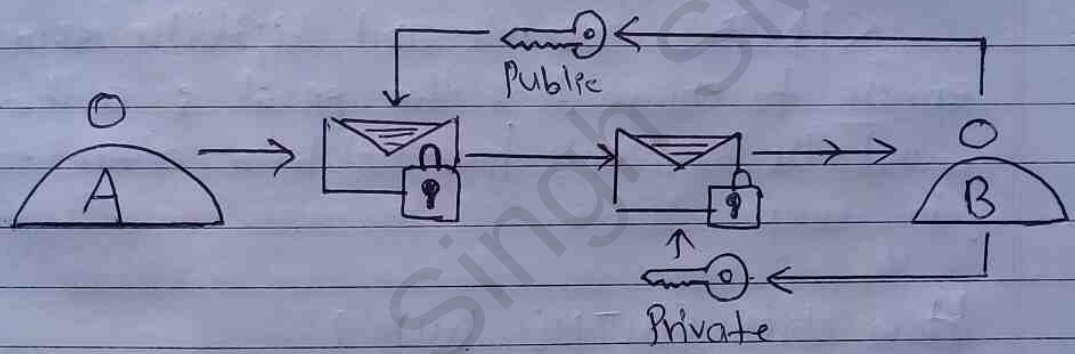
→ PGP provides authentication through the use of Digital Signature.

→ It provides confidentiality through the use of symmetric block encryption.

→ It provides compression by using the ZIP algorithm, and EMAIL compatibility using the Radix-64 encoding scheme.

→ PGP is an encryption protocol used for sending highly secure end-to-end encrypted (E2EE) emails.
→ PGP is used for signing, encrypting and decrypting texts, e-mails, files, directories and whole disk partitions and to increase the security of email-communication.

How PGP Encryption Works:



→ User A wants to sent user B a private email.
→ User B generates a public and private key.
→ User B keeps the private key and sends back the public key.
→ User A encrypts their message using the public key.
→ User A sends the private encrypted message.
→ User B decrypts the message with the private key.

Q. S/MIME

Secure/Multipurpose Internet Mail Extensions) is a widely accepted method/protocol for sending digitally signed and encrypted messages.

S/MIME allows you to encrypt emails and digitally sign them.

It was originally developed by RSA security.

S/MIME encrypts and digitally signs emails to ensure that the email is authenticated and its contents have not been altered in any way.

How does S/MIME work?

S/MIME works based on asymmetric encryption. This means that there is a set of keys involved to encrypt and decrypt an email.

An S/MIME certificate is installed on the email clients of both the recipient and the sender. When an email is sent, the sender encrypts the email using the recipients public key and the recipient decrypts the email using the private key. S/MIME also attaches a digital signature to an email. This ensures that the sender is authorized to send emails from a certain domain.

4.5 IP Security

→ The IP Security is an Integrated Internet Engineering Task Force (IETF) standard suite of protocols between two communication points across the IP networks that provides data authentication, integrity and confidentiality. It also defines the encrypted, decrypted and authenticated packets.
→ The protocol needed for secure key exchange and key management are defined in it.
→ It is used in VPNs.
→ IP Security refers to security mechanisms implemented at the IP (Internet Protocol) Layer to ensure integrity, authentication and confidentiality of data during transmission in the open internet environment.

Components of IP Security:

1. Encapsulating Security Payload (ESP)
   It provides data integrity, encryption, authentication and anti replay. It also provides authentication for payload.

2. Authentication Header (AH)
   It also provide data integrity, authenticaton and ~~replay~~ anti replay and it does not provide encryption. The anti replay protection protects against ~~the~~ unauthorized transmission of packets. It does not provide data's confidentiality.

IP HDR	AH	TCP	DATA

3. Internet Key Exchange (IKE)

It is a network security protocol designed to dynamically exchange encryption keys and find a way over Security Association (SA). between two devices.

IKE provides menage content protection and ~~the~~ also an open frame for implementing standard algorithms such as SHA and MD5.

IP HDR	TCP	DATA

Original Packet

IP HDR	ESP HDR	TCP	DATA	ESP Trailer	ESP Authentication

← Encryption →

← Authentication →

Working Mechanism of IP Security:

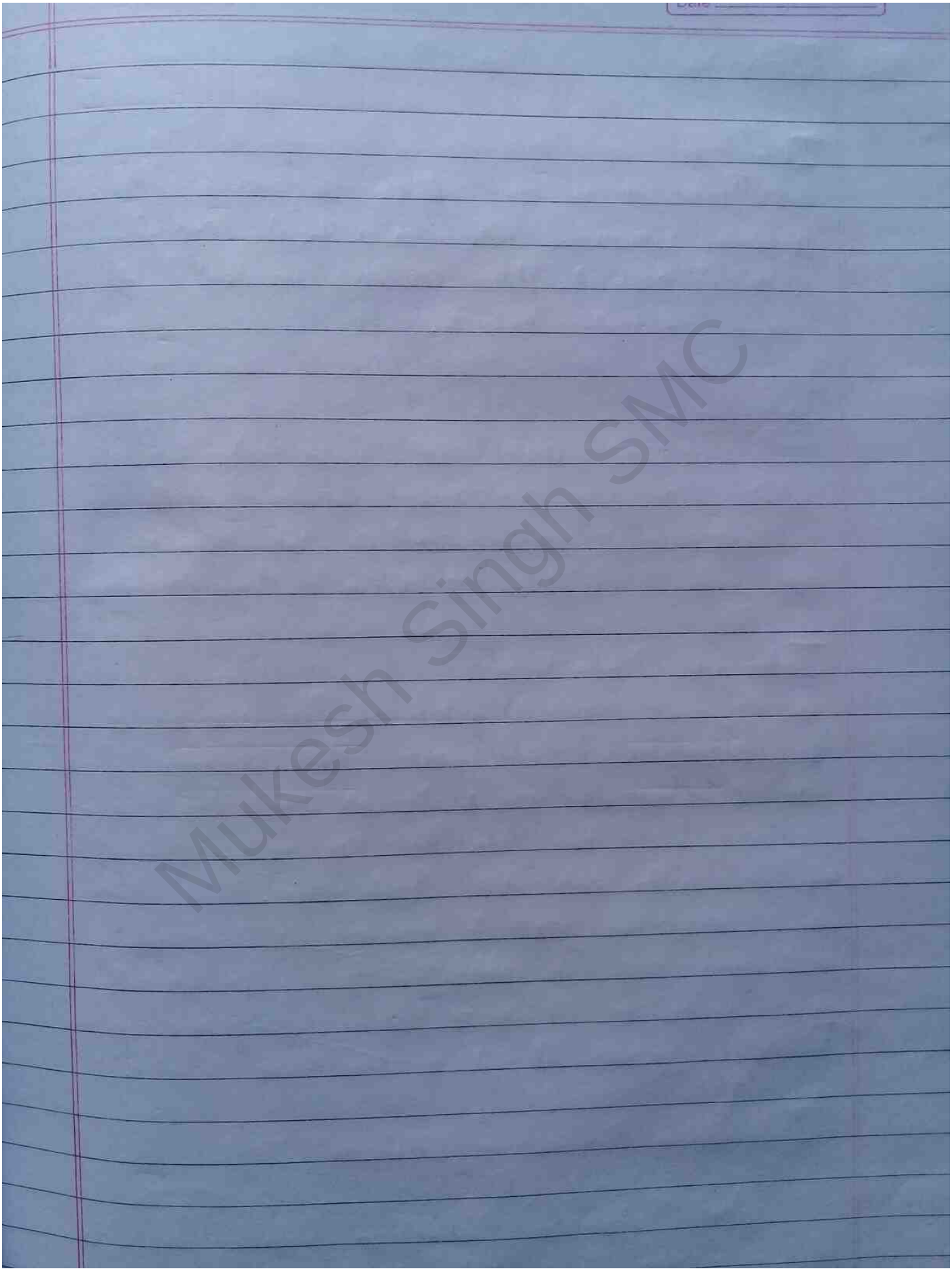
1) The host checks if the packet should be transmitted using IPSec or not. The incoming packets are also checked by the host that they are encrypted properly or not.

2) Then the IKE Phase 1 starts in which the two hosts authenticate themselves to each other to start a secure channel. It has two modes: The Main Mode and the Aggressive Mode.

3) Now the IKE phase 2 is conducted over the secure channel in which the two hosts negotiate the type of cryptographic algorithms to use on the session and aggreeing on secret key material to be used with those algorithms.

4) Then the data is exchanged across the newly created IPSec encrypted tunnel. There packets are encrypted and decrypted by the hosts using IPSec SAs.

5) When the communication between the hosts is completed or the session times out, then the IPSec tunnel is terminated by discarding the keys by both the hosts.


Mukesh Singh SMC

Unit-5

System Security

Page No.
Date

System Security is defined as the various methodologies that helps in keeping confidential information safe. It protects information from theft, corruption, and other types of damages. All the system resources that contains sensitive information are accessed by the system security.

Further, different approaches like the use of firewall, data encryption and biometrics are used to protect the information.

The system must therefore include a certain amount of ~~data~~ protection for such data, and must in turn control access to those parts of the system that administer this protection.

A system is said to be secure if its resources are used and accessed as intended under all the circumstances, but no system can guarantee absolute security from several of the various malicious threats and unauthorized access.

5.1. Intruders

Intrusion

Intrusion is an act of accessing data and using computer resources without privileges (special rights), thus causing incidental damage and security breach.

Intruders

A legitimate (legal) user who accesses data, programs or resources for which such access is not authorized or who is authorized for such access but misuses his/her privileges.

Intrusion Detection

Intrusion detection is the process of monitoring and analyzing the events occuring in a computer or network and to identify security breaches, i.e. the process of detecting events with intrusive behaviour.

Security breach means a successful attempt by an attacker to gain unauthorized access to an organization's computer system which involves theft of sensitive data.

Intrusion Detection System (IDS)

An Intrusion Detection System is a tool or software that works with your network to keep it secure when somebody is trying to break into your system.

It monitors a network or systems for malicious activity or policy violations.

Types of Intrusion Detection System

Intrusion Detection Systems are broadly classified into two main categories:

1. Network Intrusion Detection System (NIDS)
2. Host Intrusion Detection System (HIDS)

1. Network Intrusion Detection System (NIDS)
→ Monitors the entire network for suspicious traffic by analyzing protocol authority.

→ Network-based intrusion detection system software analyzes a large amount of network traffic which means they sometimes have low specificity.
This means sometimes they miss an attack or might not detect something happening in encrypted traffic.

2. Host Intrusion Detection System (HIDS)
→ Host based IDS takes care of single system. HIDS runs on individual hosts or devices on the network.

→ It takes a snapshot of existing files and matches it to the previous snapshot.

→ If the critical system files were modified or deleted, an alert is sent to the administrator to investigate.

Methods of Intrusion Detection System

There are two main methods of detecting intrusion:

1. Signature-based IDS
2. Anomaly-base IDS

1. Signature-Based IDS

→ Signature-based IDS detects the attacks on the bases of the specific patterns such as number or bytes or number of 1's or 0's in the network traffic.

→ The detected pattern in the IDS are known as signatures.

→ It also detects on the bases of the already known malicious intrusion sequence that is already used by the malware.

→ Signature-based IDS can easily detect the attacks whose pattern (signature) already exists in system but it is quite difficult to detect the new malware attacks as their pattern (signature) is not known.

2. Anomaly-based IDS

→ Anomaly-based IDS was introduced to detect the unknown malware attacks as new malware are developed rapidly.

→ In anomaly-based IDS there is use of machine learning to create a ~~useful~~ trustful activity model and anything coming is compared with that model and it is declared suspicious if it is not found in model.

→ Machine-learning based method has a better generalized property in compared to signature-based IDS as these models can be trained according to the applications and hardware configurations.

~~5.2~~ ~~Firewalls~~

5.2 Malicious Software

The word "malicious software" is the word "malware" and the meaning remains the same.

Malicious software (malware) is any software that intentionally designed to cause damage to a computer, server, client or computer network.

It is a software that gets into the system without user consent with an intention to steal private and confidential data of the user that includes bank details and password. They also generates annoying pop up ads and make changes in the system settings.

Malicious software attacks a computer or network in the form of viruses, worm, trojans, spyware, adware or rootkit.

They get into the system through various means
→ Along with free downloads.
→ Clicking on suspicious links.
→ Opening mails from malicious source.
→ Visiting malicious websites.
→ Not installing an updated version of antivirus in the system.

Page No.
Date

Types of Malicious software:

Malicious software comes in many forms but the most common types are:

1. Computer Virus (or Virus)

A computer virus is a malicious software which self-replicates and attaches itself to other files/programs. It is capable of executing secretly when the host program/file is activated. The purpose of creating computer virus is to infect vulnerable systems, gain admin control and steal user sensitive data.

Some file types are more susceptible to virus infections -.doc/.docx, .exe, .html, .xls/.xlsx, .zip etc.

The different types of computer viruses are Memory-Resident Virus, Program file virus, Bootsector Virus, Stealth virus, Macro virus and Email Virus.

2. Worms

A worm is a malicious software like a virus, that fills a computer system with self-replicating information, clogging the system so that its operations are slowed down or stopped.

Unlike viruses, a worm does not require a host program in order to run, self-replicate and propagate.

Different types of worms are Email worm, instant messaging worm, internet worm, Internet Relay Chat (IRC) worm, payloads etc.

3. Trojan Horse

Unlike a Computer virus or a worm, the trojan horse is a non-replicating program that appears legitimate (legal).

After gaining the trust, it secretly performs malicious and illicit activities when executed.

It usually pretends to, as a Computer games or application software.

Hackers can make use of trojan horse to steal a users password information, destroy data or programs on the hard desk.

It is hard to detect.

4. Spyware / Adware

Spyware and adware both are unwanted software.

Spyware is a type of malware designed to gain access and damage your Computer. Spyware secretly records information about a user such as habits, browsing history etc. and forward it to third parties.

Attackers then sell your data to advertisers, captures your bank account information or steal your personal identity.

Adware as the name suggest displays advertising banners while a program is running. It's usually installed in the background when downloading a program without your knowledge or permission. While harmless, adware can be annoying for the user.

~~5. Rootkits~~

5. Ransomware / Crypto-Malware

Ransomware is a type of malware designed to lock users out of their system or deny access to data until a ransom is paid.

Crypto-malware is a type of ransomware that encrypt user files and requires payment within a time frame and often through a digital currency like BitCoin.

6. Rootkits

A rootkit is a malicious program / software that alters the regular functionality of an OS on a computer in a stealthy manner. The altering helps the hacker to take full control of the system and the hacker acts as the system administrator on the victim's system. Almost all the rootkits are designed to hide their existence.

7. Logic Bomb

A logic bomb is a destructive program that performs an activity when a certain action has occured. These are hidden in programming code. Executes only when a specific condition is met, e.g. Jerusalem.

8. Script Virus

Commonly found Script Viruses are written using the Visual Basic Scripting Edition (VBS) and the JavaScript Programming Language.

5.3 Firewalls

A firewall is a network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules.

Firewalls have been a first line of defense in network security for over 25 years. They establish a barrier between a secured and controlled internal networks that can be trusted and untrusted outside networks, such as the internet.

A firewall can be hardware, software or both.

Characteristics / features of Firewalls

The main characteristics of firewall protection include the following:

1.) Different Protection levels based on the location of the computer

When your PC connect to a network, the firewall applies a security level in accordance with the type of network. If you want to change the security level assigned initially, you can do this at any time through the firewall settings.

2) Protection of Wireless Networks (Wi-Fi)

This blocks intrusion attempts launched through wireless networks (Wi-Fi). When an

intruder attempts to access, a pop-up warning is displayed that allows you to immediately block the attack.

3) Access to the network and the Internet

It specifies which program installed on your computer can access the network or the Internet.

4) Protection against intruders

It prevents hacker attacks that try to access your computer to carry out certain actions.

5) Blocks

The firewall can block the access of the programs that you specify should not be able to access the local network or the Internet. It also blocks access from other computers that try to connect to programs installed on your computer.

6) Definition of Rules

This defines rules that you can use to specify which connection you want to allow and the ports and zones through which the connection can be established.

Some

Some more important features of firewalls:

1) Network Threat Prevention
2) Application and Identity-based Control
3) Hybrid Cloud Support
4) Scalable performance
5) Network Traffic Management and Control
6) Access Validation
7) Record and Report on Events

Types of firewalls

Depending on their structure and functionality, there are different types of firewalls. The following is the list of some common types of firewalls:

1. Proxy Firewall (Application-level Gateways)
An early type of firewall device, a proxy firewall serves as the gateway from one network to another for a specific application. Proxy servers can provide additional functionality such as content caching and security by preventing direct connections from outside the network. However, this may also impact throughput capabilities and the applications they can support.

2. Packet-filtering firewalls
It acts like a management program that monitors network traffic and filters incoming

packets based on configured security rules. These firewalls are designed to block network traffic IP protocols, an IP address, and a port number if a data packet does not match the established rule set.

3. Stateful Multi-layer Inspection (SMLI) firewall

A stateful inspection firewall allows or blocks traffic based on state, port and protocol. It monitors all activity from the opening of a connection until it is closed. Filtering decisions are made based on both administrator-defined rules as well as context, which refers to using information from previous connections and packets belonging to the same connection.

4. Unified Threat Management (UTM) firewall

UTM firewalls are a special type of device that includes the features of a stateful inspection firewall with anti-virus and intrusion prevention support. Such firewalls are designed to provide simplicity and ease of use. These firewalls can also add many other services, such as cloud management.

5. Next Generation Firewall (NGFW)

NGFW is usually defined as a security device combining the features and functionalities of other firewalls. NGFW includes higher level of security than packet-filtering and stateful inspection firewalls. Unlike traditional firewalls, NGFW monitors the entire transaction of data, including packet headers, packet contents and sources.

6. Threat-Focused NGFW

Threat-focused NGFW includes all the features of a traditional NGFW. Additionally, they also provide advanced threat detection and remediation. These types of firewalls are capable of reacting against attacks quickly.

7. Network Address Translation (NAT) Firewalls

NAT firewalls are primarily designed to access Internet traffic and block all unwanted connections. These type of firewalls usually hide the IP address of our devices, making it safe from attackers.

8. Cloud Firewalls

Whenever a firewall is designed using a cloud solution, it is known as a cloud firewall or FaaS (Firewall-as-a Service).

Cloud firewalls are typically maintained and run on the Internet by third-party vendors. This type of firewall is considered similar to a proxy firewall as they are used as proxy servers. The main advantage of Cloud firewall is scalability because they are easy to scale according to the organization's demand or traffic load.

Page No
Date

Unit-6

Network Management Security

Network Management Security or Network Security Management is a set of policies and routines procedure implemented by the networking system to shield their network from unauthorized access, denial of Computer Service, interruption in running, etc.

Network Security Management includes various rules and procedures, adopted by network administers to ensure the unauthorized users do not obtain access.

6.1 Basic Concept of SNMP

Simple Network Management Protocol, SNMP is an Internet standard protocol for collecting and organizing information about managed devices on IP network and for modifying that information to change device behaviour.

Devices that typically support SNMP include cable modems, routers, switches, servers, workstations, printers and more.

Components of SNMP:
There are 3 components of SNMP:

1. SNMP Manager ~~(Managed device)~~
It is a centralized GUI based system used to monitor the network. It is also known as Network Management Station (NMS).
It interfaces the bi-directional flow of information between the NMS node and the network elements.

2. SNMP Agent
It is the module of network management software installed on a network/managed device like host PC, server, router, switches, etc. An agent has a local knowledge of management information and translates that information to or from an SNMP-specific form.

3. Management Information Base (MIB)

MIB consists of information of resources that are to be managed. These informations are organized hierarchically. It consists of objects instances which are essentially variables.

The SNMP manager utilizes the database to ask the agent for information about the particular device or for NMS. Thus, the shared information among the agent and the manager is known as a Management Information Base (MIB).

There are 7 SNMP protocol data units (PDUs):

1. GetRequest → The GetRequest message is sent from a manager (client) to the agent (server) to retrieve the value of a variable.

2. SetRequest → The SetRequest message is sent from a manager to the agent to set a value in a variable.

3. GetNextRequest → The GetNextRequest message is sent from the manager to an agent to retrieve the value of a variable.

4. GetBulkRequest → An enhanced version of GetNextRequest. The GetBulkRequest message is sent from the manager to the agent to retrieve a large data at once.

~~5. Response →~~

5. GetResponse → The GetResponse message is sent from an agent to the manager in response to the GetRequest and GetNextRequest message. This menage contains the value of variable requested by the manager.

6. Trap → The Trap message is sent from an agent to the manager to report an event. For example, if the agent is rebooted then it informs the manager as well as sends the time of rebooting.

7. Inform Request → It is same as trap but adds an acknowledgement that trap doesn't provide. It is used to identify if the trap message has been received or by the manager or not.

Versions of SNMP

1. SNMPv1
2. SNMPv2
3. SNMPv3

Page No.
Date

16.2 SNMPv1

It is the initial version of SNMP.

It provides the least number of network management functions.

Its authentication is based on Community names, thus it also returns fewer error control codes that offer a very low-security level.

It uses Community strings for authentication and use UDP only.

Features of SNMPv1:

2. SNMPv2

It is the revised version of the SNMPv1 which is having improvisation in the area of security, network management and performance management. This setup a new PDP message "GetBulkRequest" which is used to extract large data from the agent in a single request. The SNMPv2 which is called a community based simple network management version 2, is compatible with the security model of other versions.

Features of SNMPv2:

3) 6.3 SNMPv3

This version provides the additional feature of cryptographic security, which makes it more efficient than the prior versions. It also has the facility of remote network management and configuration for the network elements and is based on the user-based Security Module (USM) as well as on the View-based Access Control Model (VACM).

The SNMPv3 architecture introduces the USM for manage security and VACM for access control.

SNMPv3 Security model comes in 2 forms: authentication and encrypting.

Comparison between SNMP v1, SNMP v2 and SNMP v3

Content	SNMP v1	SNMP v2	SNMP v3
Standards	RFC-1155, 1157, 1212	RFC-1441, 1952 RFC-1909, 1910 RFC-1901, to 1908	RFC-1902 to 1908, 2271 to 2275
Version	SNMP v1 was the first version of SNMP.	SNMP v2 currently exists in at least three flavors, SNMP v2c, SNMP v2u, and SNMP v2.	SNMP v3 is the newest version of SNMP.
Security	No security from someone with access to the network.	SNMP v2 failed to improve on security.	Its primary feature is enhanced security.
Complexity	Performance and security limitations.	More powerful but more complex than SNMP v1.	SNMP v3 focuses on improving the security aspect
Message format	Five messages (GetRequest, GetNextRequest, SetRequest, Trap, Response)	Seven messages instead of five (inform-request, get-bulk-request)	Implements SNMP v1 and v2 specifications along with proposed new features.
Protocol	An open protocol, standard protocol, streamlined protocol.	Simple request/response protocol.	The "Engine ID" identifier in SNMP v3 uniquely identifies each SNMP identity.
Plaintext Community strings	Yes	Yes	No