CRYPTOGRAPHY AND NETWORK SECURITY

6TH SEM COMPUTER SCIENCE AND ENGINEERING

CHAPTER-1

CRYPTOGRAPHY

Cryptography is a method of protecting information and communications through the use of codes, so that only those for whom the information is intended can read and process it. The prefix "crypt-" means "hidden" or "vault" -- and the suffix "-graphy" stands for "writing."

In computer science, cryptography refers to secure information and communication techniques derived from mathematical concepts and a set of rule-based calculations called algorithms, to transform messages in ways that are hard to decipher.

NETWORK SECURITY

Network security is protection of the access to files and directories in a computer network against hacking, misuse and unauthorized changes to the system. An example of network security is an anti virus system.

PRINCIPLES OF SECURITY

Data Confidentiality, Data Integrity, Authentication and Non-repudiation are core principles of modern-day cryptography.

1. **Confidentiality** refers to certain rules and guidelines usually executed under confidentiality agreements which ensure that the information is restricted to certain people or places.
2. **Data integrity** refers to maintaining and making sure that the data stays accurate and consistent over its entire life cycle.
3. **Authentication** is the process of making sure that the piece of data being claimed by the user belongs to it.
4. **Non-repudiation** refers to ability to make sure that a person or a party associated with a contract or a communication cannot deny the authenticity of their signature over their document or the sending of a message.

OSI SECURITY ARCHITECTURE

The Open System Interconnect (OSI) security architecture was designated by the ITU-T (International Telecommunication Union - Telecommunication). The ITU-T decided that their standard "X.800" would be the ISO security architecture.

This standardized architecture defines security requirements and specifies means by which these requirements might be satisfied.

The OSI architecture focuses on

i. Security attacks
ii. Security mechanism
iii. Security service

Security attack – Any action that compromises the security of information owned by an organization.

Security mechanism – A mechanism that is designed to detect, prevent or recover from a security attack.

Security service – A service that enhances the security of the data processing systems and the information transfers of an organization. The services are intended to counter security attacks and they make use of one or more security mechanisms to provide the service.

THREAT

A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm. That is, a threat is a possible danger that might exploit a vulnerability.

ATTACK

An assault on system security that derives from an intelligent threat; that is, an intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to evade security services and violate the security policy of a system.

SECURITY ATTACK

An attack is an information security threat that involves an attempt to obtain, alter, destroy or remove implant or reveal information without authorized access or permission.

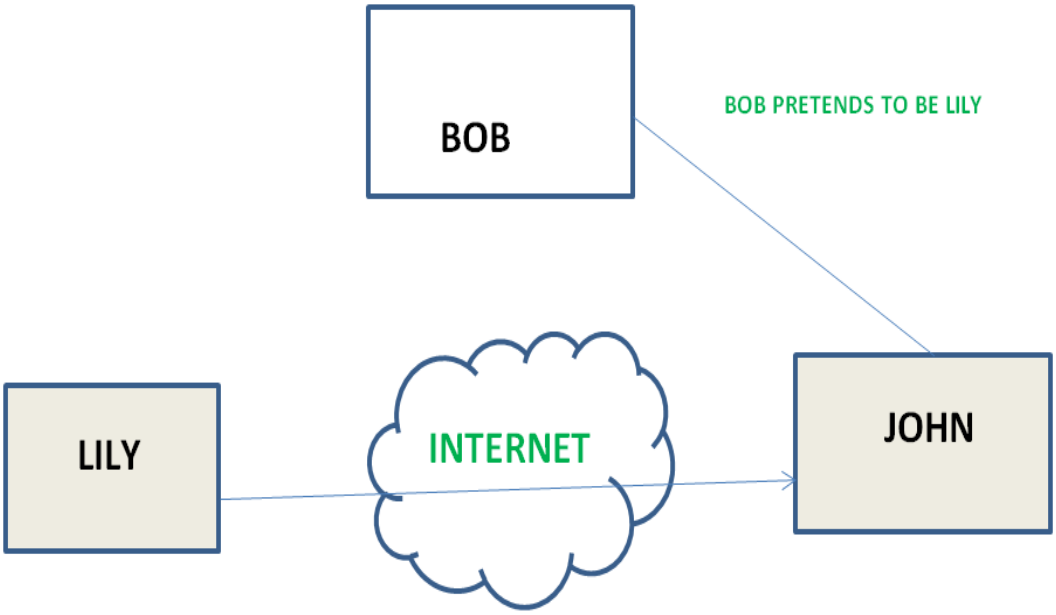
Security attacks are of two types

I. Active attack
II. Passive attack

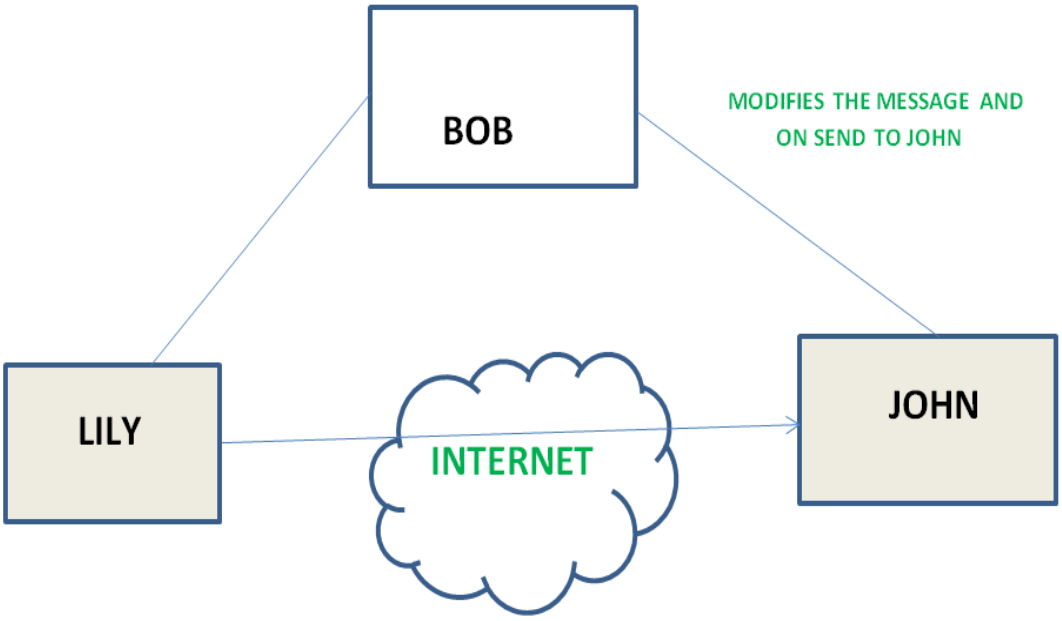
Active attacks:

An Active attack attempts to alter system resources or effect their operations. Active attack involves some modification of the data stream or creation of false statement. Types of active attacks are as following:

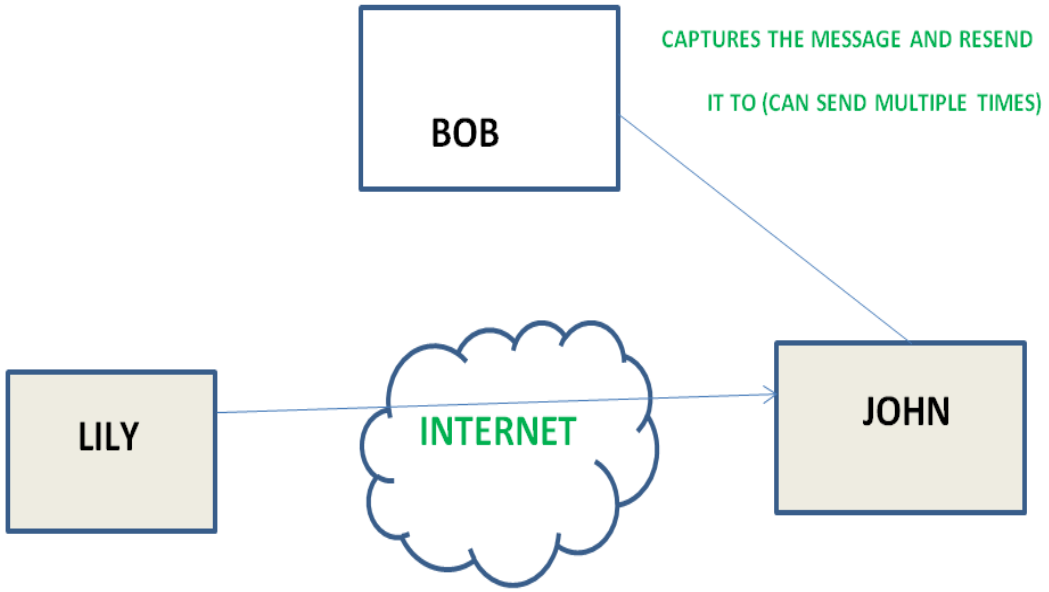
1. **Masquerade:** Masquerade attack takes place when one entity pretends to be different entity. A Masquerade attack involves one of the other form of active attacks.



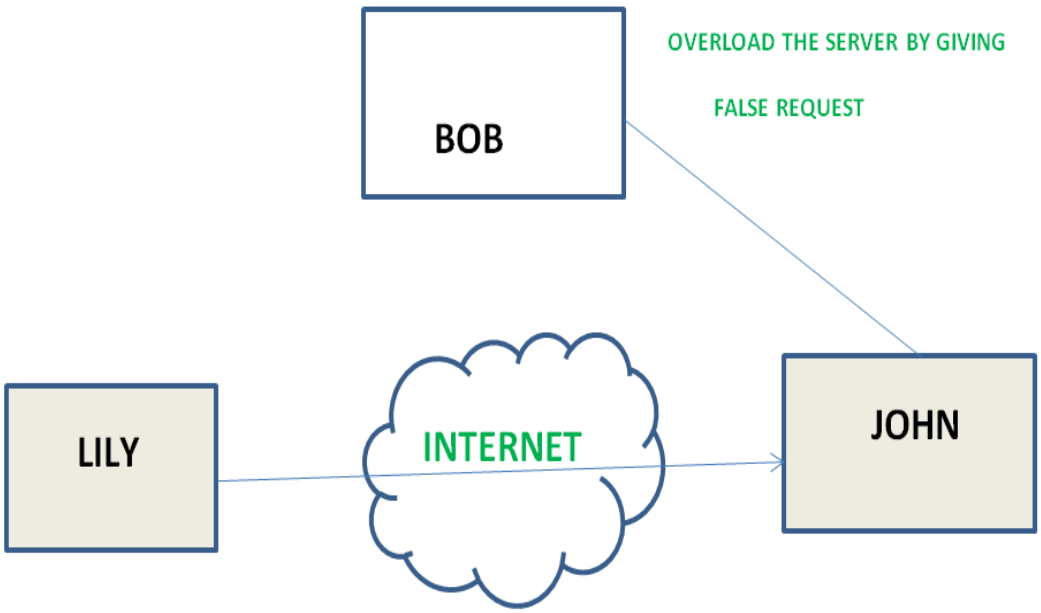
2. Modification of messages : It means that some portion of a message is altered or that message is delayed or reordered to produce an unauthorised effect. For example, a message meaning "Allow JOHN to read confidential file X" is modified as "Allow Smith to read confidential file X".



3. **Replay:** It involves the passive capture of a message and its subsequent the transmission to produce an authorized effect.



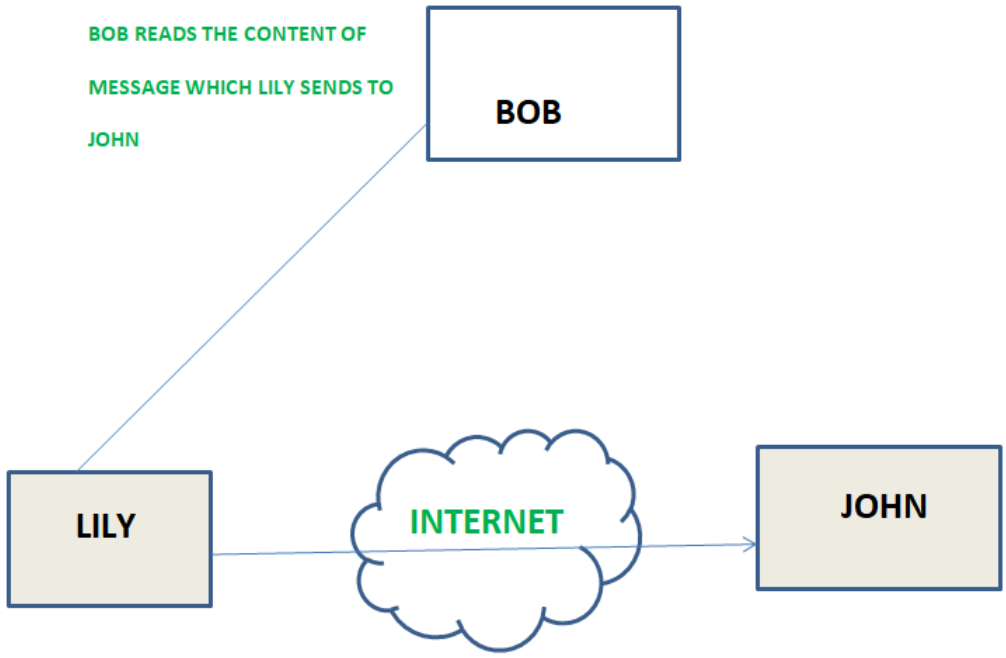
5 .Denial of Service : It prevents normal use of communication facilities. This attack may have a specific target. For example, an entity may suppress all messages directed to a particular destination. Another form of service denial is the disruption of an entire network wither by disabling the network or by overloading it by messages so as to degrade performance.



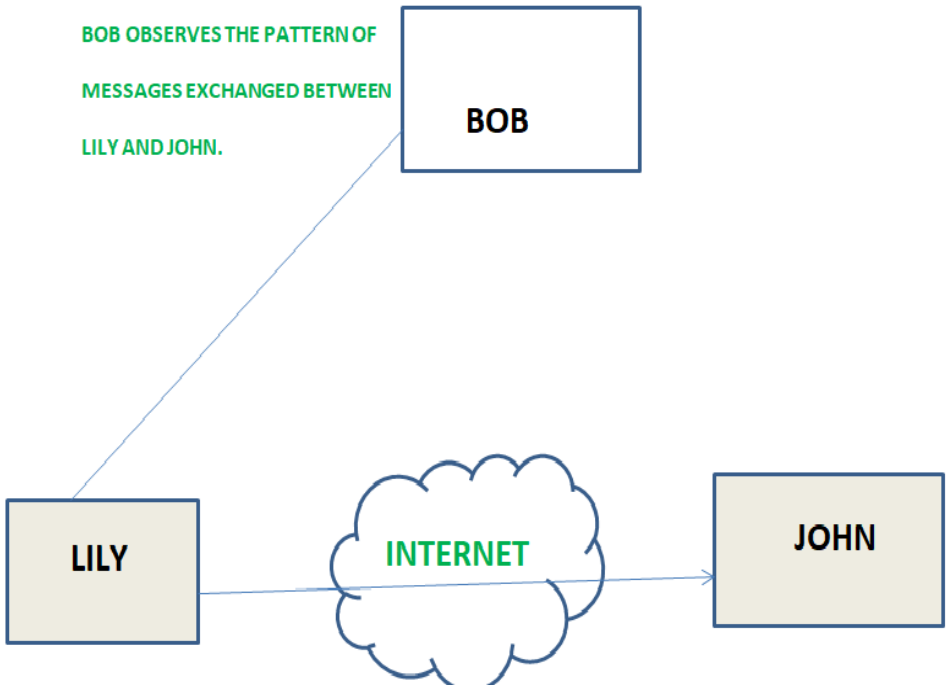
Passive attack

A Passive attack attempts to learn or make use of information from the system but does not affect system resources. Passive Attacks are in the nature of eavesdropping on or monitoring of transmission. The goal of the opponent is to obtain information is being transmitted. Types of Passive attacks are as following:

1. **The release of message content:** Telephonic conversation, an electronic mail message or a transferred file may contain sensitive or confidential information. We would like to prevent an opponent from learning the contents of these transmissions.



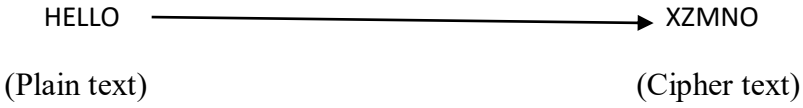
2. Traffic analysis:. Suppose that we had a way of masking (encryption) of information, so that the attacker even if captured the message could not extract any information from the message.
The opponent could determine the location and identity of communicating host and could observe the frequency and length of messages being exchanged. This information might be useful in guessing the nature of the communication that was taking place.


BOB OBSERVES THE PATTERN OF
MESSAGES EXCHANGED BETWEEN
LILY AND JOHN.
BOB
LILY
INTERNET
JOHN

CHAPTER-2

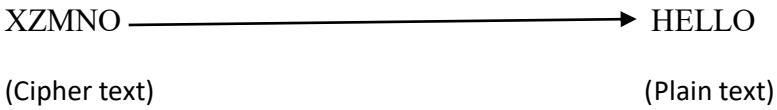
ENCRYPTION

It is the process of encoding of message so that it's meaning such that the meaning is not understandable by 3rd party.



DECRYPTION

It is the reverse process of transforming and encrypting message back in to it's normal or original position.



PLAIN TEXT

The original message is known as plain text.

CIPHER TEXT

Encrypted message is known as cipher text.

SYMMETRIC CRYPTOGRAPHY/SYMMETRIC ENCRYPTION

Symmetric key cryptography is any cryptographic algorithm that is based on a shared key that is used to encrypt or decrypt text/cipher text.

Symmetric encryption is generally more efficient than asymmetric encryption and therefore preferred when large amounts of data need to be exchanged.

Establishing the shared key is difficult using only symmetric encryption algorithms, so in many cases, an asymmetric encryption is used to establish the shared key between two parties.

Examples for symmetric key cryptography include AES, DES, and 3DES. Key exchange protocols used to establish a shared encryption key include Diffie-Hellman (DH), elliptic curve (EC) and RSA.

ASYMMETRIC CRYPTOGRAPHY/ ASYMMETRIC ENCRYPTION

Asymmetrical encryption is also known as public key cryptography, which is a relatively new method, compared to symmetric encryption. Asymmetric encryption uses two keys to encrypt a plain text. Secret keys are exchanged over the Internet or a large network. It ensures that malicious persons do not misuse the keys. It is important to note that anyone with a secret key can decrypt the message and this is why asymmetrical encryption uses two related keys to boosting security. A public key is made freely available to anyone who might want to send you a message. The second private key is kept a secret so that you can only know.

A message that is encrypted using a public key can only be decrypted using a private key, while also, a message encrypted using a private key can be decrypted using a public key. Security of the public key is not required because it is publicly available and can be passed over the internet. Asymmetric key has a far better power in ensuring the security of information transmitted during communication.

Asymmetric encryption is mostly used in day-to-day communication channels, especially over the Internet. Popular asymmetric key encryption algorithm includes EIGamal, RAS,DSA, PKCS.

SUBSTITUTION TECHNIQUES

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

Caesar cipher (or) shift cipher

The earliest known use of a substitution cipher and the simplest was by Julius Caesar. The Caesar cipher involves replacing each letter of the alphabet with the letter standing 3 places further down the alphabet.

e.g., plain text : pay more money

Cipher text: SDB PRUH PRQHB

Note that the alphabet is wrapped around, so that letter following „z“ is „a“.

For each plaintext letter p, substitute the cipher text letter c such that

$C = E(p) = (p+3) \bmod 26$

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

$C = E(p) = (p+k) \bmod 26$

Where k takes on a value in the range 1 to 25. The decryption algorithm is simply

$P = D(C) = (C-k) \bmod 26$

Playfair cipher

The best known multiple letter encryption cipher is the playfair, which treats diagrams in the plaintext as single units and translates these units into cipher text diagrams. The playfair-

-algorithm is based on the use of 5x5 matrix of letters constructed using a keyword. Let the keyword be „monarchy". The matrix is constructed by filling in the letters of the keyword (minus duplicates) from left to right and from top to bottom, and then filling in the remainder of the matrix with the remaining letters in alphabetical order.

The letter „i" and „j" count as one letter. Plaintext is encrypted two letters at a time
According to the following rules:

Repeating plaintext letters that would fall in the same pair are separated with a
Filler letter such as „x".

Plaintext letters that fall in the same row of the matrix are each replaced by the letter to the right, with the first element of the row following the last.

Plaintext letters that fall in the same column are replaced by the letter beneath, with the top element of the column following the last.

Otherwise, each plaintext letter is replaced by the letter that lies in its own row
And the column occupied by the other plaintext letter.

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

Plaintext = meet me at the school house

Splitting two letters as a unit => me et me at th es ch o x ol ho us ex
Corresponding cipher text => CL KL CL RS PD IL HY AV MP HF XL IU

Strength of playfair cipher

Playfair cipher is a great advance over simple mono alphabetic ciphers.

Since there are 26 letters, 26x26 = 676 diagrams are possible, so identification of individual diagram is more difficult.

Polyalphabetic ciphers

Another way to improve on the simple monoalphabetic technique is to use different monoalphabetic substitutions as one proceeds through the plaintext message. The general name for this approach is polyalphabetic cipher. All the techniques have the following features in common.

A set of related monoalphabetic substitution rules are used

A key determines which particular rule is chosen for a given transformation.

Vigenere cipher

In this scheme, the set of related monoalphabetic substitution rules consisting of

26 caesar ciphers with shifts of 0 through 25. Each cipher is denoted by a key letter. e.g., Caesar cipher with a shift of 3 is denoted by the key value 'd‟ (since a=0, b=1, c=2 and so on). To aid in understanding the scheme, a matrix known as vigenere tableau is Constructed

Each of the 26 ciphers is laid out horizontally, with the key letter for each cipher to its left. A normal alphabet for the plaintext runs across the top. The process of

	PLAIN TEXT															
KEY LETTERS		A	b	c	d	e	f	g	h	i	j	k	…	x	y	z
	a	A	B	C	D	E	F	G	H	I	J	K	…	X	Y	Z
	b	B	C	D	E	F	G	H	I	J	K	L	…	Y	Z	A
	c	C	D	E	F	G	H	I	J	K	L	M	…	Z	A	B
	d	D	E	F	G	H	I	J	K	L	M	N	…	A	B	C
	e	E	F	G	H	I	J	K	L	M	N	O	…	B	C	D
	f	F	G	H	I	J	K	L	M	N	O	P	…	C	D	E
	g	G	H	I	J	K	L	M	N	O	P	Q	…	D	E	F
	:	:	:	:	:	:	:	:	:	:	:	:	…	:	:	:
	x	X	Y	Z	A	B	C	D	E	F	G	H	…			W
	y	Y	Z	A	B	C	D	E	F	G	H	I	…			X
	z	Z	A	B	C	D	E	F	G	H	I	J	…			Y

Encryption is simple: Given a key letter X and a plaintext letter y, the cipher text is at the intersection of the row labeled x and the column labeled y; in this case, the ciphertext is V.

To encrypt a message, a key is needed that is as long as the message. Usually, the key is a repeating keyword.

e.g., key = d e c e p t i v e d e c e p t i v e d e c e p t i v e PT = w e a r e d i s c o v e r e d s a v e y o u r s e l f CT = ZICVTWQNGRZGVTWAVZHCQYGLMGJ

Decryption is equally simple. The key letter again identifies the row. The position of the cipher text letter in that row determines the column, and the plaintext letter is at the top of that column.

Strength of Vigener substitution:

- There are multiple cipher text letters for each plaintext letter.
- Letter frequency information is obscured.

One Time Pad Cipher

It is an unbreakable cryptosystem. It represents the message as a sequence of 0s and 1s. this can be accomplished by writing all numbers in binary, for example, or by using ASCII. The key is a random sequence of 0"s and 1"s of same length as the message. Once a key is used, it is discarded and never used again. The system can be expressed as Follows:

$C_i = P_i \oplus K_i$ C_i - i^{th} binary digit of cipher text P_i - i^{th} binary digit of plaintext K_i - i^{th} binary digit of key

Exclusive OR operation

Thus the cipher text is generated by performing the bitwise XOR of the plaintext and the key. Decryption uses the same key. Because of the properties of XOR, decryption simply involves the same bitwise operation:

$P_i = C_i \oplus K_i$

e.g., plaintext = 0 0 1 0 1 0 0 1

Key = 1 0 1 0 1 1 0 0

---------- ciphertext = 1 0 0 0 0 1 0 1

Advantage:

Encryption method is completely unbreakable for a ciphertext only attack.

Disadvantages

It requires a very long key which is expensive to produce and expensive to transmit.

Once a key is used, it is dangerous to reuse it for a second message; any knowledge on the first message would give knowledge of the second.

TRANSPOSITION TECHNIQUES

All the techniques examined so far involve the substitution of a cipher text symbol for a plaintext symbol. A very different kind of mapping is achieved by performing some sort of permutation on the plaintext letters. This technique is referred to as a transposition cipher.

Rail fence

is simplest of such cipher, in which the plaintext is written down as a sequence of diagonals and then read off as a sequence of rows.

Plaintext = meet at the school house

To encipher this message with a rail fence of depth 2, we write the message as follows:

m e a t e c o l o s
e t t h s h o h u e

The encrypted message is

MEATECOLOSETTHSHOHUE

Row Transposition Ciphers-

A more complex scheme is to write the message in a rectangle, row by row, and read the message off, column by column, but permute the order of the columns. The order of columns then becomes the key of the algorithm.

e.g., plaintext = meet at the school house

Key = 4	3	1	2	5	6	7
PT = m	e	e	T	a	t	t

h e s c h o o

l h o u s e

CT=ESOTCEHMHLAHSTOE

A pure transposition cipher is easily recognized because it has the same letter frequencies as the original plaintext. The transposition cipher can be made significantly more secure by performing more than one stage of transposition. The result is more complex permutation that is not easily reconstructed.

CHAPTER-3

Symmetric key algorithms are sometimes referred to as secret key algorithms. This is because these types of algorithms generally use one key that is kept secret by the systems engaged in the encryption and decryption processes. This single key is used for both encryption and decryption.

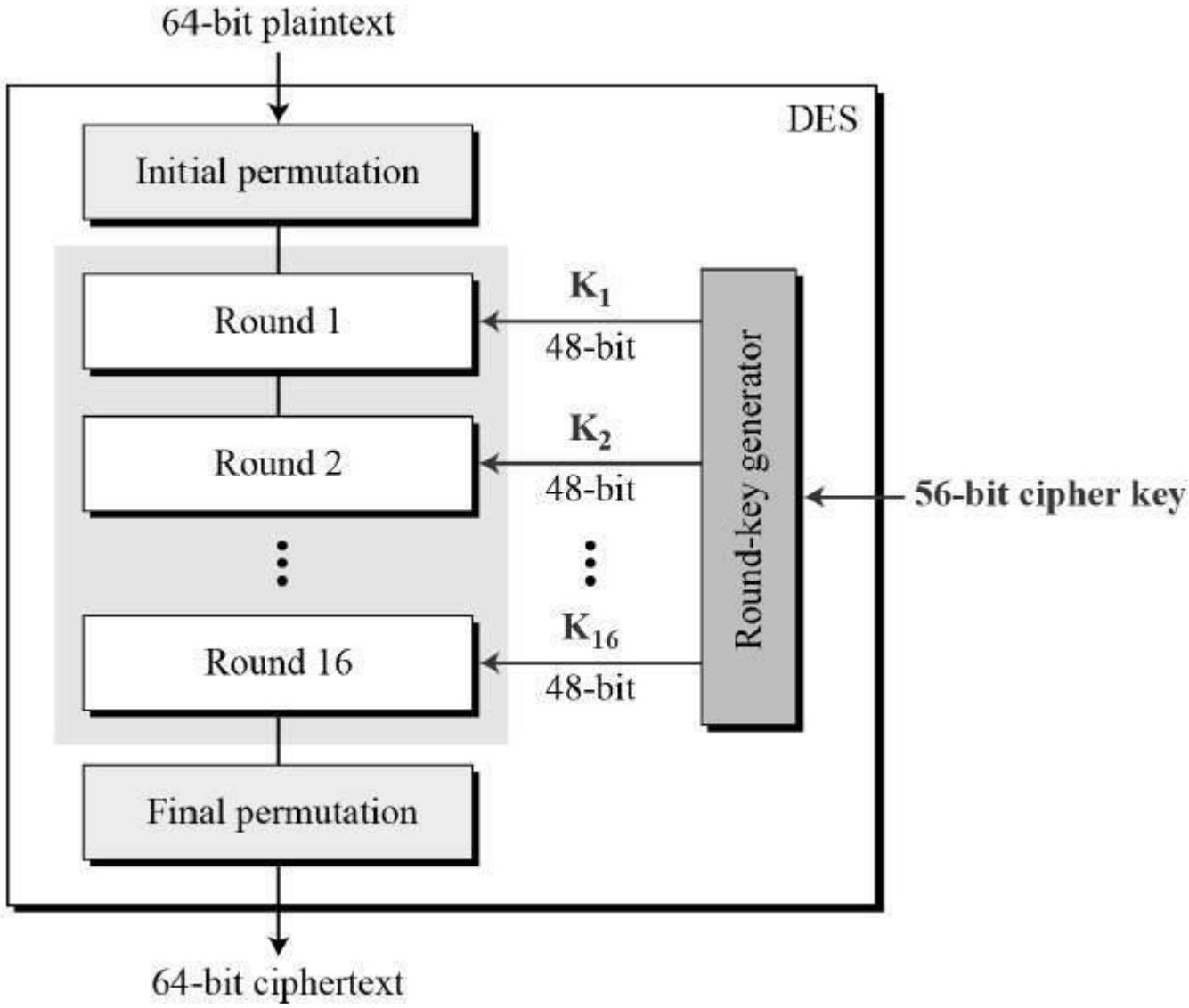
Symmetric key algorithms tend to be very secure. In general, they are considered more secure than asymmetric key algorithms. There are some symmetric key algorithms that are considered virtually unbreakable. Symmetric key algorithms are also very fast. This is why they are often used in situations where there is a lot of data that needs to be encrypted.

There are hundreds of different symmetric key algorithms available. Each has its own strengths and weaknesses. Some of the more common examples are DES, 3DES, AES, IDEA, RC4, and RC5.

DATA ENCRYPTION STANDARD

The Data Encryption Standard (DES) is a symmetric-key block cipher published by the National Institute of Standards and Technology (NIST).

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 of the 64 bits of the key are not used by the encryption algorithm (function as check bits only). General Structure of DES is depicted in the following illustration −



Since DES is based on the Feistel Cipher, all that is required to specify DES is −

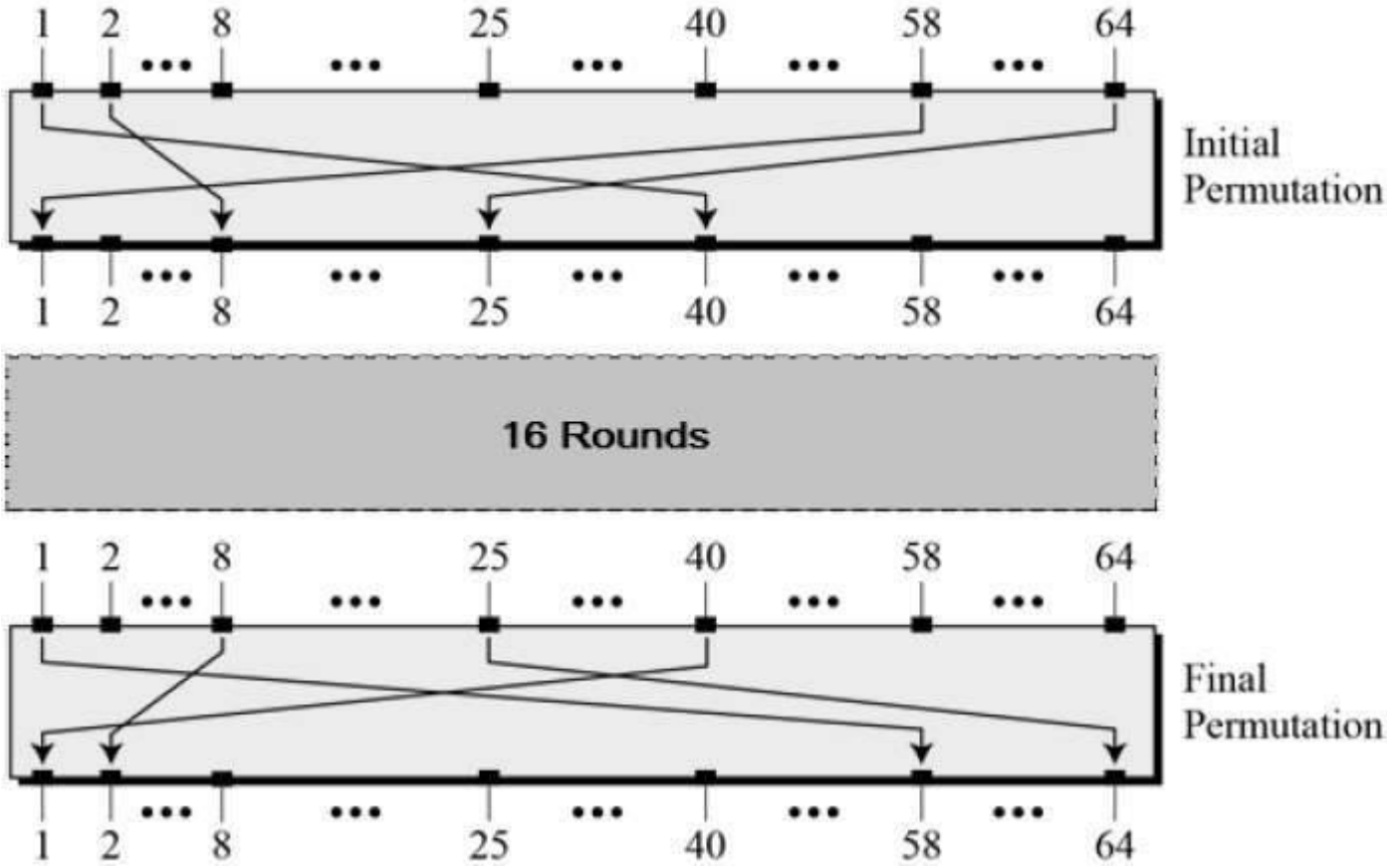
Round function

Key schedule

Any additional processing − Initial and final permutation

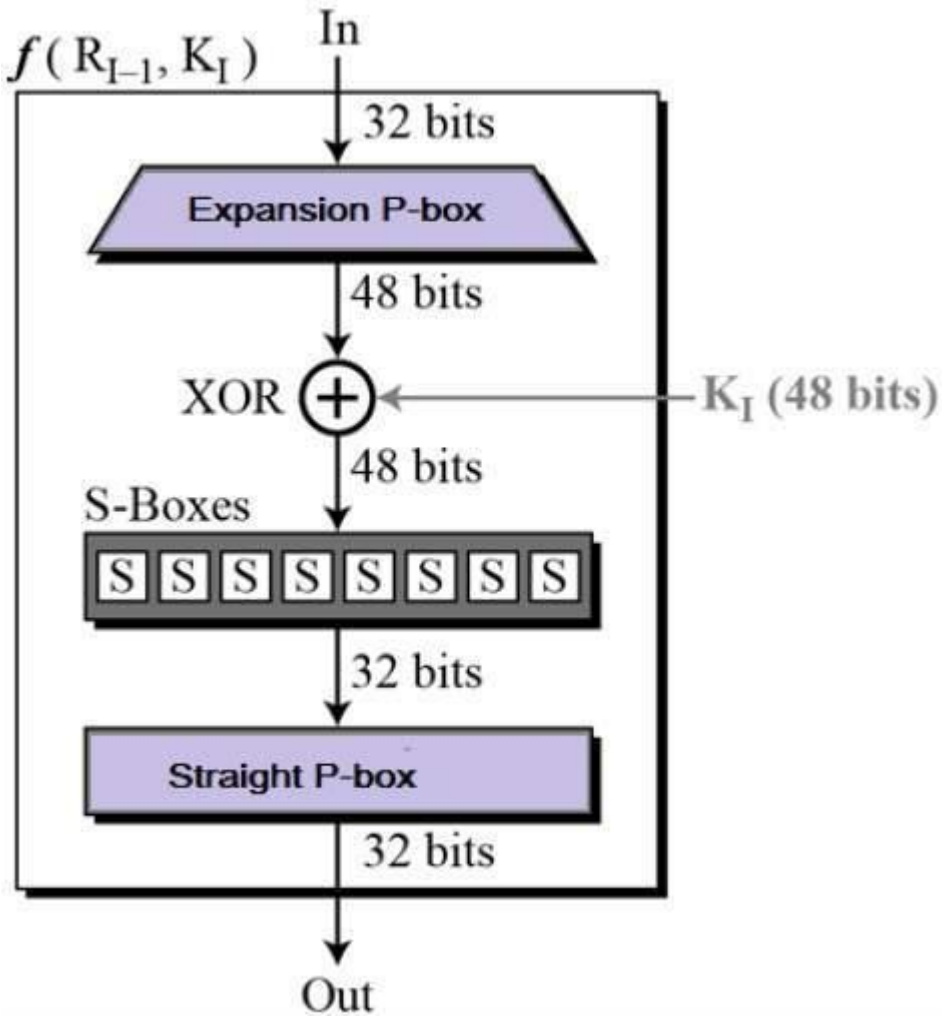
Initial and Final Permutation

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

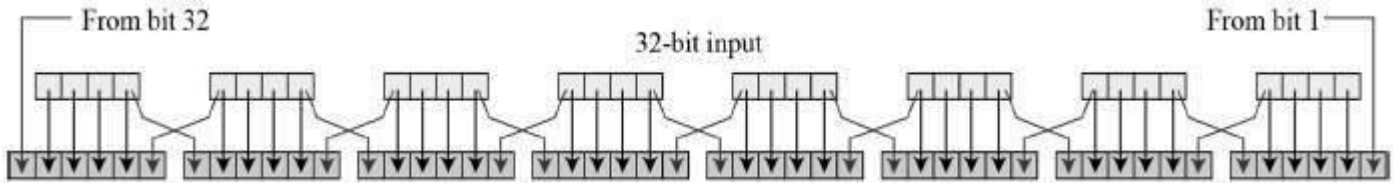


Round Function

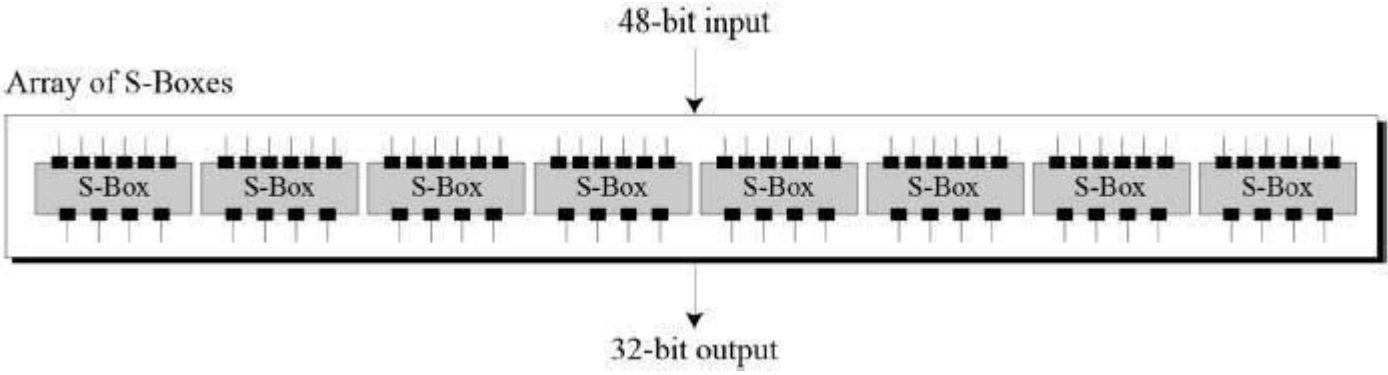
The heart of this cipher is the DES function, f. The DES function applies a 48-bit key to the rightmost 32 bits to produce a 32-bit output.



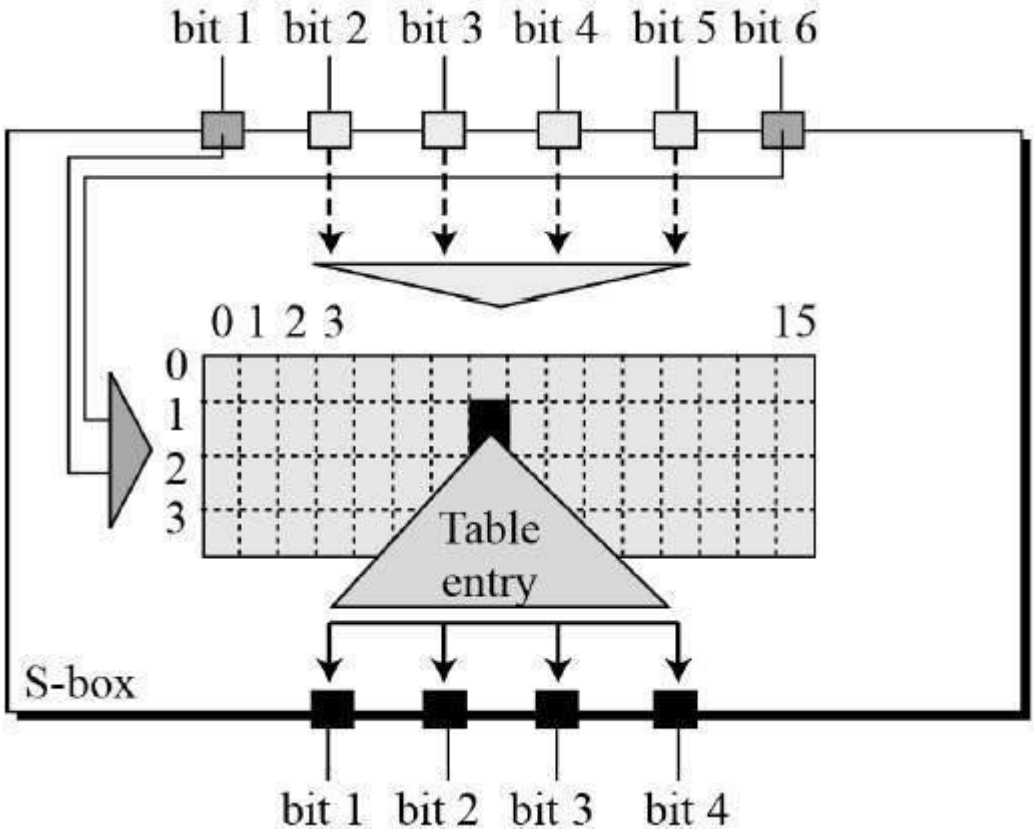
Expansion Permutation Box − Since right input is 32-bit and round key is a 48-bit, we first need to expand right input to 48 bits. Permutation logic is graphically depicted in the following illustration −



- **XOR (Whitener).** − After the expansion permutation, DES does XOR operation on the expanded right section and the round key. The round key is used only in this operation.
- **Substitution Boxes.** − The S-boxes carry out the real mixing (confusion). DES uses 8 S-boxes, each with a 6-bit input and a 4-bit output. Refer the following illustration −



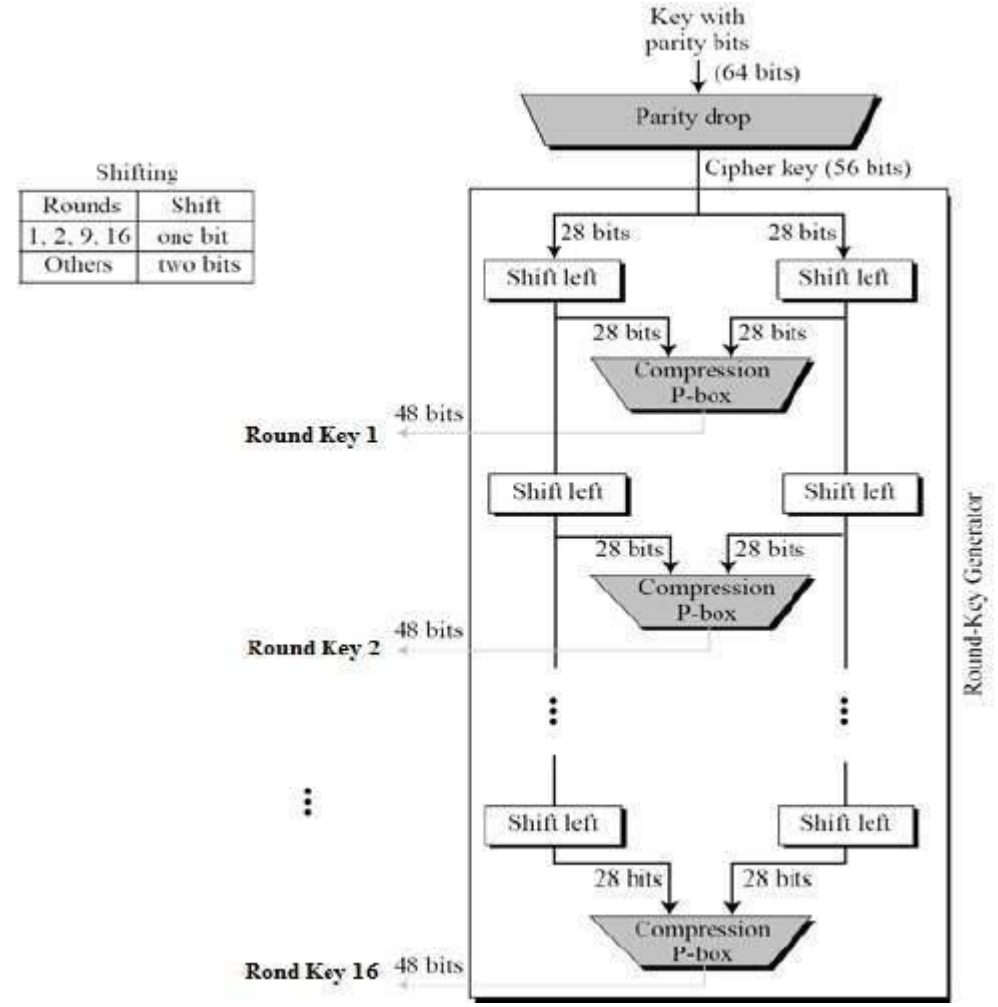
- The S-box rule is illustrated below −



- There are a total of eight S-box tables. The output of all eight s-boxes is then combined in to 32 bit section.

Key Generation

The round-key generator creates sixteen 48-bit keys out of a 56-bit cipher key. The process of key generation is depicted in the following illustration −



The logic for Parity drop , shifting, and Compression P-box is given in the DES description.

Triple DES

- DES variant
- standardised in ANSI X9.17 & ISO 8732 and in PEM for key management
- proposed for general EFT standard by ANSI X9
- backwards compatible with many DES schemes
- uses 2 or 3 keys

  C = DES_(K1) Bbc{(DES^(-1)_(K2)Bbc{(DES_(K1)(P)))
- no known practical attacks

ASYMMETRIC KEY ALGORITHM

Asymmetric key algorithms aren't as widely used as their symmetric counterparts.

RSA ALGORITHM

RSA (Rivest–Shamir–Adleman) is an algorithm used by modern computers to encrypt and decrypt messages. It is an asymmetric cryptographic algorithm. Asymmetric means that there are two different keys. This is also called public key cryptography, because one of the keys can be given to anyone. The other key must be kept private. The algorithm is based on the fact that finding the factors of a large composite number is difficult: when the factors are prime numbers, the problem is called prime factorization. It is also a key pair (public and private key) generator.

RSA involves a public key and private key. The public key can be known to everyone- it is used to encrypt messages. Messages encrypted using the public key can only be decrypted with the private key. The keys for the RSA algorithm are generated the following way:

1. Choose two different large random prime numbers p and q
2. Calculate n=pq

   Where n is the modulus for the public key and the private keys

3. Calculate the totient : $\Phi(n)=(p-1)(q-1)$

4. Choose an integer e such that $1 < e < \Phi(n)$ and e is co-prime to $\Phi(n)$ **i.e.: $\Phi(n)$** and e share no factors other than 1; gcd(e, $\Phi(n)$) = 1.

   - e is released as the public key exponent

5. Compute d to satisfy the congruence relation $de \equiv 1 \mod \Phi(n)$ **i.e.: $de = 1+x\Phi(n)$** for some integer x.

   - d is kept as the private key exponent

ENCRYPTING MESSAGE

Alice gives her public key (n& e) to Bob and keeps her private key secret. Bob wants to send message **M** to Alice.

First he turns **M** into a number m smaller than n by using an agreed-upon reversible protocol known as a padding scheme. He then computes the ciphertext c corresponding to:

$C = m^e \mod n$

This can be done quickly using the method of exponentiation by squaring. Bob then sends c to Alice.

DECRYPTING MESSAGE

Alice can recover m from c by using her private key d in the following procedure:

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

Given m, she can recover the original distinct prime numbers, applying the Chinese remainder theorem to these two congruences yields

$$m^{ed} \equiv m \bmod pq$$

Thus,

$$c^d \equiv m \bmod n$$

DIGITAL SIGNATURE

A digital signature is a mathematical technique used to validate the authenticity and integrity of a message, software or digital document.

Key Generation Algorithms : Digital signature are electronic signatures, which assures that the message was sent by a particular sender. While performing digital transactions authenticity and integrity should be assured, otherwise the data can be altered or someone can also act as if he was the sender and expect a reply.

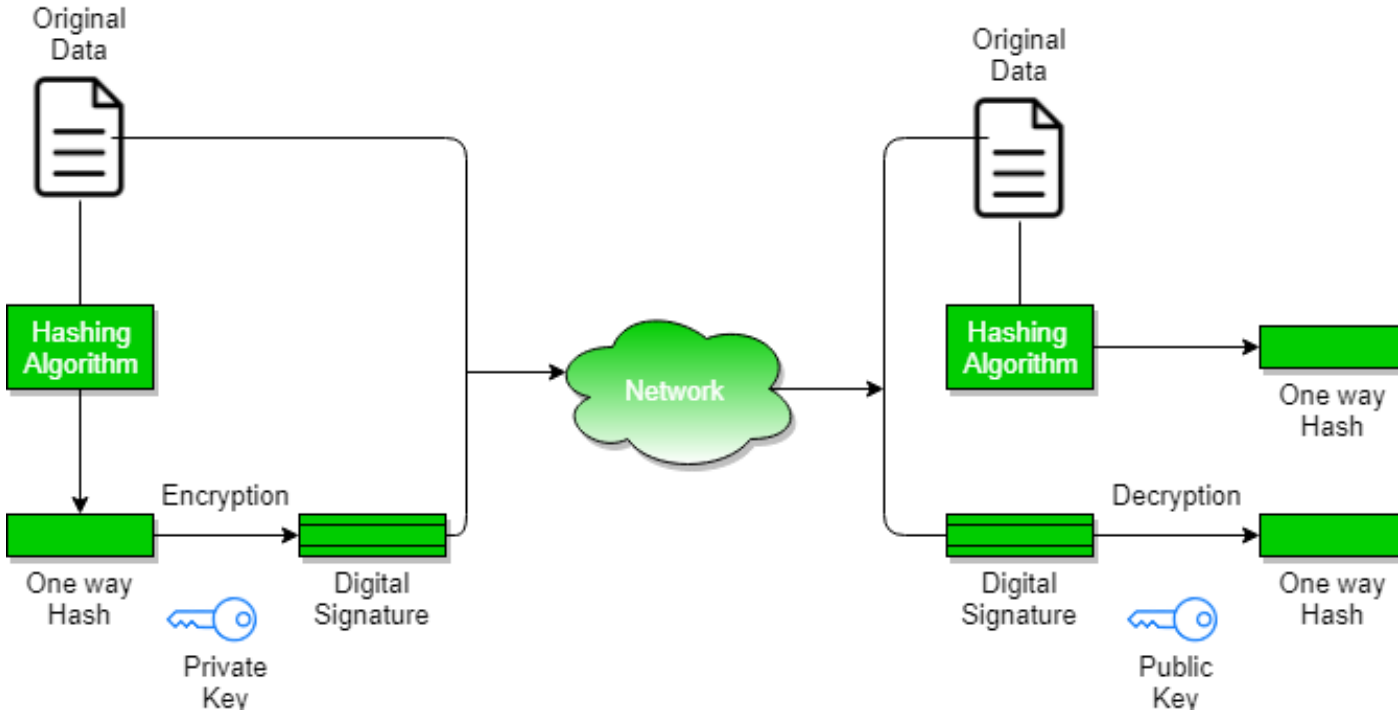
Signing Algorithms: To create a digital signature, signing algorithms like email programs create a one-way hash of the electronic data which is to be signed. The signing algorithm then encrypts the hash value using the private key (signature key). This encrypted hash along with other information like the hashing algorithm is the digital signature. This digital signature is appended with the data and sent to the verifier. The reason for encrypting the hash instead of the entire message or document is that a hash function converts any arbitrary input into a much shorter fixed length value. This saves time as now instead of signing a long message a shorter hash value has to be signed and moreover hashing is much faster than signing.

Signature Verification Algorithms : Verifier receives Digital Signature along with the data. It then uses Verification algorithm to process on the digital signature and the public key (verification key) and generates some value. It also applies the same hash function on the received data and generates a hash value. Then the hash value and the output of the verification algorithm are compared. If they both are equal, then the digital signature is valid else it is invalid.

The steps followed in creating digital signature are :

1. Message digest is computed by applying hash function on the message and then message digest is encrypted using private key of sender to form the digital signature. (digital signature = encryption (private key of sender, message digest) and message digest = message digest algorithm(message)).
2. Digital signature is then transmitted with the message.(message + digital signature is transmitted)
3. Receiver decrypts the digital signature using the public key of sender.(This assures authenticity,as only sender has his private key so only sender can encrypt using his private key which can thus be decrypted by sender's public key).
4. The receiver now has the message digest.
5. The receiver can compute the message digest from the message (actual message is sent with the digital signature).
6. The message digest computed by receiver and the message digest (got by decryption on digital signature) need to be same for ensuring integrity.

Message digest is computed using one-way hash function, i.e. a hash function in which computation of hash value of a message is easy but computation of the message from hash value of the message is very difficult.



CHAPTER-4

DIGITAL CERTIFICATES

Digital certificate is issued by a trusted third party which proves sender's identity to the receiver and receiver's identity to the sender.
A digital certificate is a certificate issued by a Certificate Authority (CA) to verify the identity of the certificate holder. The CA issues an encrypted digital certificate containing the applicant's public key and a variety of other identification information. Digital certificate is used to attach public key with a particular individual or an entity.
Digital certificate contains:-

1. Name of certificate holder.
2. Serial number which is used to uniquely identify a certificate, the individual or the entity identified by the certificate
3. Expiration dates.
4. Copy of certificate holder's public key.(used for decrypting messages and digital signatures)
5. Digital Signature of the certificate issuing authority.

Digital certificate is also sent with the digital signature and the message.

PRIVATE KEY MANAGEMENT

Key management refers to management of cryptographic keys in a cryptosystem. This includes dealing with the generation, exchange, storage, use, crypto-shredding (destruction) and replacement of keys. It includes cryptographic protocol design, key servers, user procedures, and other relevant protocols.

Key management concerns keys at the user level, either between users or systems. This is in contrast to key scheduling, which typically refers to the internal handling of keys within the operation of a cipher.

Successful key management is critical to the security of a cryptosystem. It is the more challenging side of cryptography in a sense that it involves aspects of social engineering such as system policy, user training, organizational and departmental interactions, and coordination between all of these elements, in contrast to pure mathematical practices that can be automated.

PKIX MODEL

RFC 2822 (*Internet Security Glossary*) defines public-key infrastructure (PKI) as the set of hardware, software, people, policies, and procedures needed to create, manage, store, distribute, and revoke digital certificates based on asymmetric cryptography. The principal 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. These elements are

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 subject field of a public key certificate. End entities typically consume and/or support PKI-related services.

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.

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.

CRL issuer: An optional component that a CA can delegate to publish CRLs.

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

PKIX MANAGEMENT FUNTIONS

PKIX identifies a number of management functions that potentially need to be supported by management protocols. These are:

Registration: This is the process whereby a user first makes itself known to a CA (directly or through an 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.

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 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.

Certification: This is the process in which a CA issues a certificate for a user's public key, returns that certificate to the user's client system, and/or posts that certificate in a reposition.

Key pair recovery: Key pairs can be used to support digital signature creation and verification, encryption and decryption, or both. When a key pair is used for encryption/decryption, it is important to provide a mechanism to recover the necessary decryption keys when normal access to the keying material is no longer possible, otherwise it will not be possible to recover the encrypted data. Loss of access to the decryption key can result from forgotten passwords/PINs, corrupted disk drives, damage to hardware tokens, and so on. Key pair recovery allows end entities to restore their encryption/decryption key pair from an authorized key backup facility (typically, the CA that issued the end entity's certificate.

Key pair update: All key pairs need to be updated regularly (i.e., replaced with a new key pair) and new certificates issued. Update is required when the certificate lifetime expires and as a result of certificate revocation.

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.

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.

PUBLIC KEY CRYPTOGRAPHY STANDARDS

PKCS are a group of non-vendor dependent standards that are aimed to foster better secure communications through the use of extensive cryptography.

PKCS did not become industry standards initially because RSA retained control over them, but many of the standards were adapted by other working groups.

The standards were developed by RSA with the cooperation of industry partners which included Apple, Microsoft, Lotus, Sun, DEC and MIT.

CHAPTER-5

Network security is one of the essential branches of cyber security, and protocols play a vital role in securing the network. Because of its top-notch needs and the internet continues to evolve at a fast pace, the computer network grows faster, and along with comes the cybercrime in networks. So, it is essential to know the protocols that govern the data flow in a network.

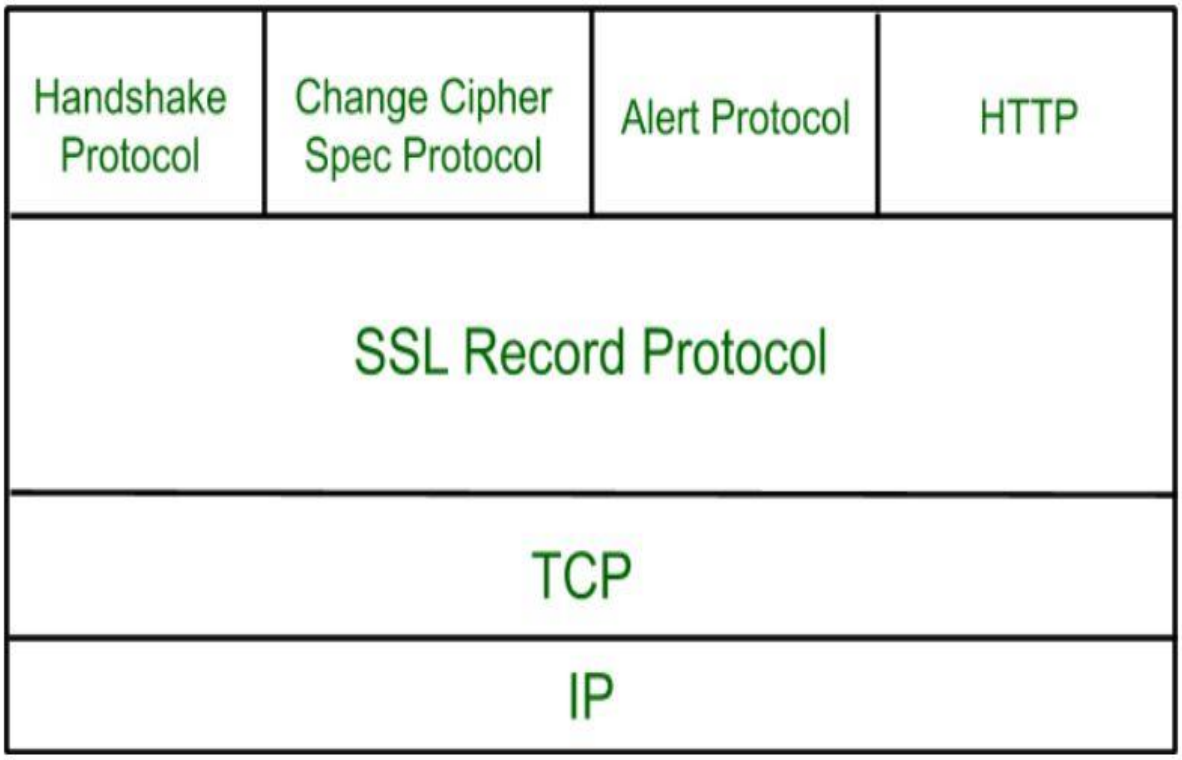
SECURE SOCKET LAYER (SSL)

SSL provide security to the data that is transferred between web browser and server. SSL encrypt the link between a web server and a browser which ensures that all data passed between them remain private and free from attack.

Secure Socket Layer Protocols:

- SSL record protocol
- Handshake protocol
- Change-cipher spec protocol
- Alert protocol

SSL Protocol Stack:



SSL Record Protocol: SSL Record provides two services to SSL connection.

- Confidentiality
- Message Integrity

In SSL Record Protocol application data is divided into fragments. The fragment is compressed and then encrypted MAC (Message Authentication Code) generated by algorithms like SHA (Secure Hash Protocol) and MD5 (Message Digest) is appended. After that encryption of the data is done and in last SSL header is appended to the data.

Handshake Protocol: Handshake Protocol is used to establish sessions. This protocol allow client and server to authenticate each other by sending a series of messages to each other. Handshake protocol uses four phases to complete its cycle.

- **Phase-1:** In Phase-1 both Client and Server send hello-packets to each other. In this IP session, cipher suite and protocol version are exchanged for security purpose.
- **Phase-2:** Server send his certificate and Server-key-exchange. Server end the phase-2 by sending Server-hello-end packet.
- **Phase-3:** In this phase Client reply to the server by sending his certificate and Client-exchange-key.

- **Phase-4:** In Phase-4 Change-cipher suite occurred and after this Handshake Protocol ends.

Change-cipher 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.

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

Level is further classified into two parts:

- **Warning:**
  This Alert have no impact on the connection between sender and receiver.
- **Fatal Error:**
  This Alert breaks the connection between sender and receiver.

Silent Features of Secure Socket Layer:

- Advantage of this approach is that the service can be tailored to the specific needs of the given application.
- Secure Socket Layer was originated by Netscape.

- SSL is designed to make use of TCP to provide reliable end-to-end secure service.
- This is two-layered protocol.

TRANSPORT LAYER SECURITY

Transport Layer Securities (TLS) are designed to provide security at the transport layer. TLS was derived from a security protocol called Secure Service Layer (SSL). TLS ensures that no third party may eavesdrops or tamper with any message.

There are several benefits of TLS:

- **Encryption:**
  TLS/SSL can help to secure transmitted data using encryption.
- **Interoperability:**
  TLS/SSL works with most web browsers, including Microsoft Internet Explorer and on most operating systems and web servers.
- **Algorithm flexibility:**
  TLS/SSL provides operations for authentication mechanism, encryption algorithms and hashing algorithm that are used during the secure session.
- **Ease of Deployment:**
  Many applications TLS/SSL temporarily on a windows server 2003 operating systems.
- **Ease of Use:**
  Because we implement TLS/SSL beneath the application layer, most of its operations are completely invisible to client.

Working of TLS:
The client connect to server (using TCP), the client will be something. The client sends number of specification:

1. Version of SSL/TLS.
2. which cipher suites, compression method it wants to use.

The server checks what the highest SSL/TLS version is that is supported by them both, picks a cipher suite from one of the clients option (if it supports one) and optionally picks a compression method. After this the basic setup is done, the server provides its certificate. This certificate must be trusted either by the client itself or a party that the client trusts. Having verified the certificate and being certain this server really is who he claims to be (and not a man in the middle), a key is exchanged. This can be a public key, “PreMasterSecret” or simply nothing depending upon cipher suite.

Both the server and client can now compute the key for symmetric encryption. The handshake is finished and the two hosts can communicate securely. To close a connection by finishing. TCP connection both sides will know the connection was improperly terminated. The connection cannot be compromised by this through, merely interrupted.

SECURE HYPERTEXT TRANSFER PROTOCOL

S-HTTP (Secure HTTP) is an extension to the Hypertext Transfer Protocol (HTTP) that allows the secure exchange of files on the World Wide Web. Each S-HTTP file is either encrypted, contains a digital certificate, or both. For a given document, S-HTTP is an alternative to another well-known security protocol, Secure Sockets Layer (SSL). A major difference is that S-HTTP allows the client to send a certificate to authenticate the user whereas, using SSL, only the server can be authenticated. S-HTTP is more likely to be used in situations where the server represents a bank and requires authentication from the user that is more secure than a user id and password.

S-HTTP does not use any single encryption system, but it does support the Rivest-Shamir-Adleman public key infrastructure encryption system. SSL works at a program layer slightly higher than the Transmission Control Protocol (TCP) level. S-HTTP works at the even higher level of the HTTP application. Both security protocols can be used by a browser user, but only one can be used with a given document. Terisa Systems includes both SSL and S-HTTP in their Internet security tool kits.

TIME STAMP PROTOCOL

The **Time-Stamp Protocol**, or **TSP** is a cryptographic protocol for certifying timestamps using X.509 certificates and public key infrastructure. The timestamp is the signer's assertion that a piece of electronic data existed at or before a particular time.

Time stamping is an increasingly valuable complement to digital signing practices, enabling organizations to record when a digital item—such as a message, document, transaction or piece of software—was signed. For some applications, the timing of a digital signature is critical, as in the case of stock trades, lottery ticket issuance and some legal proceedings. Even when time is not intrinsic to the application, time stamping is helpful for record keeping and audit processes, because it provides a mechanism to prove whether the digital certificate was valid at the time it was used. The growing importance of digital signing solutions has created a corresponding demand for time stamping, so many software programs, such as Microsoft Office, support time stamping capabilities.

SECURE ELECTRONIC TRANSACTION

Secure Electronic Transaction or SET is a system which ensures security and integrity of electronic transactions done using credit cards in a scenario. SET is not some system that enables payment but it is a security protocol applied on those payments. It uses different encryption and hashing techniques to secure payments over internet done through credit cards. SET protocol was supported in development by major organizations like Visa, Mastercard, Microsoft which provided its Secure Transaction Technology (STT) and NetScape which provided technology of Secure Socket Layer (SSL).

SET protocol restricts revealing of credit card details to merchants thus keeping hackers and thieves at bay. SET protocol includes Certification Authorities for making use of standard Digital Certificates like X.509 Certificate.

Before discussing SET further, let's see a general scenario of electronic transaction, which includes client, payment gateway, client financial institution, merchant and merchant financial institution. **Requirements in SET :**
SET protocol has some requirements to meet, some of the important requirements are :

- It has to provide mutual authentication i.e., customer (or cardholder) authentication by confirming if the customer is intended user or not and merchant authentication.
- It has to keep the PI (Payment Information) and OI (Order Information) confidential by appropriate encryptions.
- It has to be resistive against message modifications i.e., no changes should be allowed in the content being transmitted.
- SET also needs to provide interoperability and make use of best security mechanisms.

Participants in SET :
In the general scenario of online transaction, SET includes similar participants:

1. **Cardholder –** customer
2. **Issuer –** customer financial institution
3. **Merchant**
4. **Acquirer –** Merchant financial
5. **Certificate authority –** Authority which follows certain standards and issues certificates(like X.509V3) to all other participants.

SET functionalities :

- **Provide Authentication**
  - **Merchant Authentication** – To prevent theft, SET allows customers to check previous relationships between merchant and financial institution. Standard X.509V3 certificates are used for this verification.
  - **Customer / Cardholder Authentication** – SET checks if use of credit card is done by an authorized user or not using X.509V3 certificates.
- **Provide Message Confidentiality** : Confidentiality refers to preventing unintended people from reading the message being transferred. SET implements confidentiality by using encryption techniques. Traditionally DES is used for encryption purpose.
- **Provide Message Integrity** : SET doesn't allow message modification with the help of signatures. Messages are protected against unauthorized modification using RSA digital signatures with SHA-1 and some using HMAC with SHA-1,

CHAPTER-6

AUTHENTICATION

Authentication is the process of determining whether someone or something is, in fact, who or what it declares itself to be. Authentication technology provides access control for systems by checking to see if a user's credentials match the credentials in a database of authorized users or in a data authentication server.

Users are usually identified with a user ID, and authentication is accomplished when the user provides a credential, for example a password, that matches with that user ID. Most users are most familiar with using a password, which, as a piece of information that should be known only to the user, is called a knowledge authentication factor.

PASSWORD

- Passwords are the most common method of authentication.
- Consists of a string of characters to gain access to resources.
- Usually, passwords are human memorable that considered as a vulnerability in security.
- Passwords are derived from a small domain.

Passwords creation rule have been enforced to increase the quality of passwords like:

- Letters and numeric.
- Non-alphanumeric characteristics.
- Passphrases
- Symbols
- Increased password length

WELLKNOWN PASSWORDS ATTACKS

- Guessing attacks
  - Brute force attacks
  - Dictionary attacks
    - ✓ Online dictionary attacks
    - ✓ Offline dictionary attacks
- Resetting attacks
- Replay attacks
- Syllabus attacks
- Social engineering and shoulder surfing

AUTHENTICATION TOKENS

Authentication tokens/security tokens are tools that allow to prove one's identity electronically. They are usually used as additional means of authentication, typically together with passwords.

The tokens may be either physical devices or pure software applications, operating on computers or mobile devices. Depending on their implementation, security tokens may be referred to as authentication tokens, cryptographic tokens, hardware or software tokens, USB tokens, or key fobs.

Tokens may use different means for generating authentication codes.

Static password tokens

The tokens with a static password are the simplest type of security tokens. The secret code is stored inside the token and it is released when the user asks for it.

It is quite obvious that such tokens do not provide good security.

Time-synchronized tokens

The time-synchronized tokens generate a password based on the current time. They must contain a timer which is synchronized with another timer, operating on the authentication server side. The passwords generated by time-synchronized tokens change constantly at a set time interval, for example every minute.

The time-synchronized tokens may, over time, become unsynchronized. In such a case, the passwords generated by them cannot be used to access the protected service, until a resynchronization is performed.

Asynchronous tokens

The passwords generated by asynchronous tokens change every time they are generated. The algorithms may be based on hash functions that generate series of one-time codes based on a shared secret symmetric key.

Each created password must be unpredictable to guess, even if all the previously generated passwords are known.

Tokens with public and private keys

If the token contains a private key, the server may use the corresponding public key to authenticate it, without the need of transmitting the private key outside the token environment.

Usually the server sends the data encrypted with the public key. After decrypting the message, the token sends it back to the server, allowing it to confirm the token identity. In such a case, a direct communication between the token and the server must be established.

BIOMETRIC AUTHENTICATION

Biometric authentication is a user identity verification process that involves biological input, or the scanning or analysis of some part of the body.

Biometric authentication methods are used to protect many different kinds of systems - from logical systems facilitated through hardware access points to physical systems protected by physical barriers, such as secure facilities and protected research sites.

They fall roughly into two categories: physical identifiers and behavioral identifiers. Physical identifiers are, for the most part, immutable and device independent:

- **Fingerprints:** Fingerprint scanners have become ubiquitous in recent years due to their widespread deployment on smartphones. Any device that can be touched, such as a phone screen, computer mouse or touchpad, or a door panel, has the potential to become an easy and convenient fingerprint scanner. According to Spiceworks, fingerprint scanning is the most common type of biometric authentication in the enterprise, used by 57 percent of companies.

- **Photo and video:** If a device is equipped with a camera, it can easily be used for authentication. Facial recognition and retinal scans are two common approaches.

- **Physiological recognition:** Facial recognition is the second most common type of authentication, according to Spiceworks, in place at 14 percent of companies. Other image-based authentication methods include hand geometry recognition, used by 5 percent of companies, iris or retinal scanning, palm vein recognition, and ear recognition.

- **Voice:** Voice-based digital assistants and telephone-based service portals are already using voice recognition to identify users and authenticate customers. According to Spiceworks, 2 percent of companies use voice recognition for authentication within the enterprise.

- **Signature:** Digital signature scanners are already in widespread use at retail checkouts and in banks and are a good choice for situations where users and customers are already expecting to have to sign their names.

- **DNA:** Today, DNA scans are used primarily in law enforcement to identify suspects -- and in the movies. In practice, DNA sequencing has been too slow for widespread use. This is starting to change.

CHAPTER-7

INTRODUCTION TO TCP/IP

TCP/IP is widely used throughout the world to provide network communications. TCP/IP communications are composed of four layers that work together. When a user wants to transfer data across networks, the data is passed from the highest layer through intermediate layers to the lowest layer, with each layer adding information.

Security controls exist for network communications at each layer of the TCP/IP model. Data is passed from the highest to the lowest layer, with each layer adding more information. Because of this, a security control at a higher layer cannot provide protection for lower layers, because the lower layers perform functions of which the higher layers are not aware. Security controls that are available at each layer include:

- **Application Layer.** Separate controls must be established for each application. For example, if an application needs to protect sensitive data sent across networks, the application may need to be modified to provide this protection. While this provides a very high degree of control and flexibility over the application's security, it may require a large resource investment to add and configure controls properly for each application. Designing a cryptographically sound application protocol is very difficult, and implementing it properly is even more challenging, so creating new application layer security controls is likely to create vulnerabilities. Also, some applications, particularly off-the-shelf software, may not be capable of providing such protection. While application layer controls can protect application data, they cannot protect TCP/IP information such as IP addresses because this information exists at a lower layer. Whenever possible, application layer controls for protecting network communications should be standards-based solutions that have been in use for some time. One example is Secure Multipurpose Internet Mail Extensions (S/MIME), which is commonly used to encrypt email messages.
- **Transport Layer.** Controls at this layer can be used to protect the data in a single communication session between two hosts. Because IP information is added at the network layer, transport layer controls cannot protect it. The most common use for transport layer protocols is securing HTTP traffic; the Transport Layer Security (TLS) protocol is usually used for this. The use of TLS typically requires each application to support TLS; however, unlike application layer controls, which typically involve extensive customization of the application, transport layer controls such as TLS are much less intrusive because they do not need to understand the application's functions or characteristics. Although using TLS may require modifying some applications, TLS is a well-tested protocol that has several implementations that have been added to many applications, so it is a relatively low-risk option compared to adding

protection at the application layer. Traditionally TLS has been used to protect HTTP-based communications and can be used with SSL portal VPNs.

- **Network Layer.** Controls at this layer can be applied to all applications; thus, they are not application-specific. For example, all network communications between two hosts or networks can be protected at this layer without modifying any applications on the clients or the servers. In some environments, network layer controls such as Internet Protocol Security (IPsec) provide a much better solution than transport or application layer controls because of the difficulties in adding controls to individual applications. Network layer controls also provide a way for network administrators to enforce certain security policies. Another advantage of network layer controls is that since IP information (e.g., IP addresses) is added at this layer, the controls can protect both the data within the packets and the IP information for each packet. However, network layer controls provide less control and flexibility for protecting specific applications than transport and application layer controls. SSL tunnel VPNs provide the ability to secure both TCP and UDP communications including client/server and other network traffic, and therefore act as network layer VPNs.
- **Data Link Layer.** Data link layer controls are applied to all communications on a specific physical link, such as a dedicated circuit between two buildings or a dial-up modem connection to an Internet Service Provider (ISP). Data link layer controls for dedicated circuits are most often provided by specialized hardware devices known as *data link encryptors*; data link layer controls for other types of connections, such as dial-up modem communications, are usually provided through software. Because the data link layer is below the network layer, controls at this layer can protect both data and IP information. Compared to controls at the other layers, data link layer controls are relatively simple, which makes them easier to implement; also, they support other network layer protocols besides IP. Because data link layer controls are specific to a particular physical link, they cannot protect connections with multiple links, such as establishing a VPN over the Internet. An Internet-based connection is typically composed of several physical links chained together; protecting such a connection with data link layer controls would require deploying a separate control to each link, which is not feasible. Data link layer protocols have been used for many years primarily to provide additional protection for specific physical links that should not be trusted.

  Because they can provide protection for many applications at once without modifying them, network layer security controls have been used frequently for securing communications, particularly over shared networks such as the Internet. Network layer security controls provide a single solution for protecting data from all applications, as well as protecting IP information. Nevertheless, in many cases, controls at another layer are better suited to providing protection than network layer controls.

FIREWALL

A firewall is a network security device, either hardware or software-based, which monitors all incoming and outgoing traffic and based on a defined set of security rules it accepts, rejects or drops that specific traffic.

Accept : allow the traffic
Reject : block the traffic but reply with an "unreachable error"
Drop : block the traffic with no reply

A firewall establishes a barrier between secured internal networks and outside untrusted network, such as the Internet.

HOW FIREWALL WORKS

Firewall match the network traffic against the rule set defined in its table. Once the rule is matched, associate action is applied to the network traffic. For example, Rules are defined as any employee from HR department cannot access the data from code server and at the same time another rule is defined like system administrator can access the data from both HR and technical department. Rules can be defined on the firewall based on the necessity and security policies of the organization.
From the perspective of a server, network traffic can be either outgoing or incoming. Firewall maintains a distinct set of rules for both the cases. Mostly the outgoing traffic, originated from the server itself, allowed to pass. Still, setting a rule on outgoing traffic is always better in order to achieve more security and prevent unwanted communication.
Incoming traffic is treated differently. Most traffic which reaches on the firewall is one of these three major Transport Layer protocols- TCP, UDP or ICMP. All these types have a source address and destination address. Also, TCP and UDP have port numbers. ICMP uses *type code* instead of port number which identifies purpose of that packet.

TYPES OF FIREWALL

Firewalls are generally of two types: *Host-based* and *Network-based.*

1. **Host- based Firewalls :** Host-based firewall is installed on each network node which controls each incoming and outgoing packet. It is a software application or suite of applications, comes as a part of the operating system. Host-based firewalls are needed because network firewalls cannot provide protection inside a trusted network. Host firewall protects each host from attacks and unauthorized access.
2. **Network-based Firewalls :** Network firewall function on network level. In other words, these firewalls filter all incoming and outgoing traffic across the network. It protects the internal network by filtering the traffic using rules defined on the firewall. A Network firewall might have two or more network interface cards (NICs). A network-based firewall is usually a dedicated system with proprietary software installed.

IP security

The **IP security (IPSec)** is an Internet Engineering Task Force (IETF) standard suite of protocols between 2 communication points across the IP network that provide data authentication, integrity, and confidentiality. It also defines the encrypted, decrypted and authenticated packets. The protocols needed for secure key exchange and key management are defined in it.

Uses of IP Security –
IPsec can be used to do the following things:

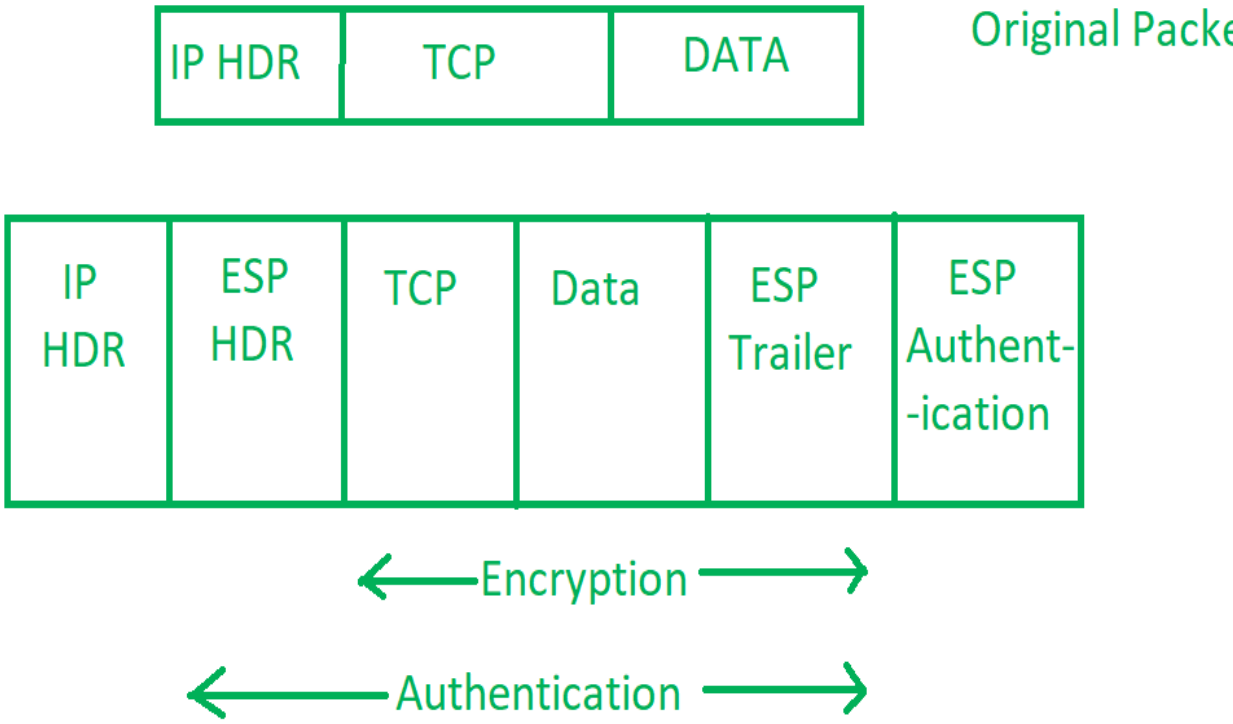
- To encrypt application layer data.
- To provide security for routers sending routing data across the public internet.
- To provide authentication without encryption, like to authenticate that the data originates from a known sender.
- To protect network data by setting up circuits using IPsec tunneling in which all data is being sent between the two endpoints is encrypted, as with a Virtual Private Network (VPN) connection.

Components of IP Security –
It has the following components:

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 provides data integrity, authentication and anti replay and it does not provide encryption. The anti replay protection, protects against unauthorized transmission of packets. It does not protect data's confidentiality.

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 2 devices. The Security Association (SA) establishes shared security attributes between 2 network entities to support secure communication. The Key Management Protocol (ISAKMP) and Internet Security Association which provides a framework for authentication and key exchange. ISAKMP tells how the set up of the Security Associations (SAs) and how direct connections between two hosts that are using IPsec.

Internet Key Exchange (IKE) provides message content protection and also an open frame for implementing standard algorithms such as SHA and MD5. The algorithm's IP sec users produces a unique identifier for each packet. This identifier then allows a device to determine whether a packet has been correct or not. Packets which are not authorized are discarded and not given to receiver.



Working of IP Security –

1. The host checks if the packet should be transmitted using IPsec or not. These packet traffic triggers the security policy for themselves. This is done when the system sending the packet apply an appropriate encryption. 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 2 hosts(using IPsec) authenticate themselves to each other to start a secure channel. It has 2 modes. The **Main mode** which provides the greater security and the **Aggressive mode** which enables the host to establish an IPsec circuit more quickly.
3. The channel created in the last step is then used to securely negotiate the way the IP circuit will encrypt data across the IP circuit.
4. 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 agreeing on secret keying material to be used with those algorithms.
5. Then the data is exchanged across the newly created IPsec encrypted tunnel. These packets are encrypted and decrypted by the hosts using IPsec SAs.

6. 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.

VIRTUAL PRIVATE NETWORK

VPN stands for virtual private network. A virtual private network (VPN) is a technology that creates a safe and encrypted connection over a less secure network, such as the internet. Virtual Private network is a way to extend a private network using a public network such as internet. The name only suggests that it is Virtual "private network" i.e. user can be the part of local network sitting at a remote location. It makes use of tunneling protocols to establish a secure connection.

Virtual Private Network (VPN) is basically of 2 types:

1. **Remote Access VPN:**
   Remote Access VPN permits a user to connect to a private network and access all its services and resources remotely. The connection between the user and the private network occurs through the Internet and the connection is secure and private. Remote Access VPN is useful for home users and business users both.

   An employee of a company, while he/she is out of station, uses a VPN to connect to his/her company's private network and remotely access files and resources on the private network. Private users or home users of VPN, primarily use VPN services to bypass regional restrictions on the Internet and access blocked websites. Users aware of Internet security also use VPN services to enhance their Internet security and privacy.

2. **Site to Site VPN:**
   A Site-to-Site VPN is also called as Router-to-Router VPN and is commonly used in the large companies. Companies or organizations, with branch offices in different locations, use Site-to-site VPN to connect the network of one office location to the network at another office location.

   - **Intranet based VPN:** When several offices of the same company are connected using Site-to-Site VPN type, it is called as Intranet based VPN.
   - **Extranet based VPN:** When companies use Site-to-site VPN type to connect to the office of another company, it is called as Extranet based VPN.

   Basically, Site-to-site VPN create a imaginary bridge between the networks at geographically distant offices and connect them through the Internet and

sustain a secure and private communication between the networks. In Site-to-site VPN one router acts as a VPN Client and another router as a VPN Server as it is based on Router-to-Router communication. When the authentication is validated between the two routers only then the communication starts.

Types of Virtual Private Network (VPN) Protocols:

1. **Internet Protocol Security (IPSec):**
   Internet Protocol Security, known as IPSec, is used to secure Internet communication across an IP network. IPSec secures Internet Protocol communication by verifying the session and encrypts each data packet during the connection.

   IPSec runs in 2 modes:

   - (i) Transport mode
   - (ii) Tunneling mode

   The work of transport mode is to encrypt the message in the data packet and the tunneling mode encrypts the whole data packet. IPSec can also be used with other security protocols to improve the security system.

2. **Layer 2 Tunneling Protocol (L2TP):**
   L2TP or Layer 2 Tunneling Protocol is a tunneling protocol that is often combined with another VPN security protocol like IPSec to establish a highly secure VPN connection. L2TP generates a tunnel between two L2TP connection points and IPSec protocol encrypts the data and maintains secure communication between the tunnel.

3. **Point–to–Point Tunneling Protocol (PPTP):**
   PPTP or Point-to-Point Tunneling Protocol generates a tunnel and confines the data packet. Point-to-Point Protocol (PPP) is used to encrypt the data between the connection. PPTP is one of the most widely used VPN protocol and has been in use since the early release of Windows. PPTP is also used on Mac and Linux apart from Windows.

4. **SSL and TLS:**
   SSL (Secure Sockets Layer) and TLS (Transport Layer Security) generate a VPN connection where the web browser acts as the client and user access is prohibited to specific applications instead of entire network. Online shopping websites commonly uses SSL and TLS protocol. It is easy to switch to SSL by web browsers and with almost no action required from the user as web browsers come integrated with SSL and TLS. SSL connections have “https” in the initial of the URL instead of “http”.

5. **OpenVPN:**
   OpenVPN is an open source VPN that is commonly used for creating Point-to-Point and Site-to-Site connections. It uses a traditional security protocol based on SSL and TLS protocol.
6. **Secure Shell (SSH):**
   Secure Shell or SSH generates the VPN tunnel through which the data transfer occurs and also ensures that the tunnel is encrypted. SSH connections are generated by a SSH client and data is transferred from a local port on to the remote server through the encrypted tunnel