KIIT POLYTECHNIC

LECTURE NOTES

ON

CRYPTOGRAPHY & NETWORK SECURITY

Compiled by

Swagatika Dalai

Lecturer, Department of Computer Science & Engineering,
KIIT Polytechnic, Bhubaneswar

CONTENTS

CHAPTER-1

POSSIBLE ATTACKS ON COMPUTERS

INTRODUCTION:

- Computer data often travels from one computer to another, leaving the safety of its protected physical surroundings.
- Once the data is out of hand, people with bad intention could modify or forge your data, either for enjoyment or for their own benefit.
- Cryptography can reformat and transform our data, making it safer on its trip between computers.
- The technology is based on the secret codes, modern mathematics that protects our data in powerful ways.
- **Computer Security** - generic name for the collection of tools designed to protect data and to prevent hackers.
- **Network Security** - measures to protect data during their transmission.
- **Internet Security -** measures to protect data during their transmission over a collection of interconnected networks.

NEED FOR SECURITY:

Computer security basically is the protection of computer systems and information from harm, theft, and unauthorized use. It is the process of preventing and detecting unauthorized use of your computer system. Cyber security is defined as protecting computer systems, which communicate over the computer networks.

Computer security is important because it keeps your information protected. It's also important for your computer's overall health; proper computer security helps prevent viruses and malware, which allows programs to run quicker and smoother.

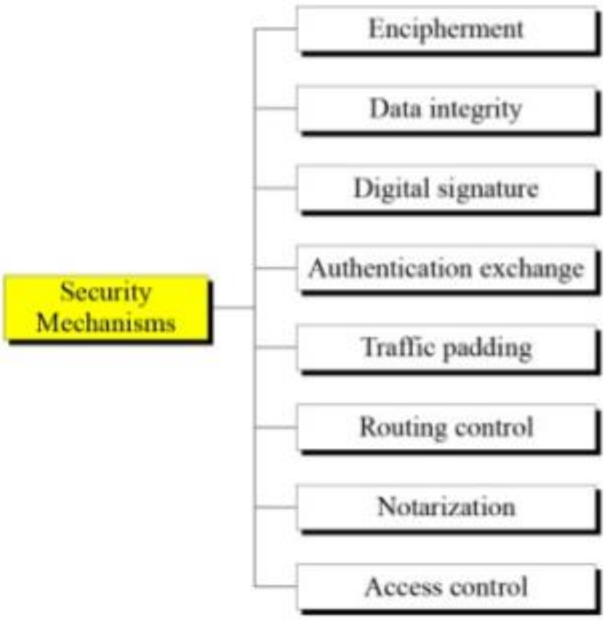
SECURITY ATTACKS, SERVICES AND MECHANISMS:

To assess the security needs of an organization effectively, the manager responsible for security needs some systematic way of defining the requirements for security and characterization of approaches to satisfy those requirements. One approach is to consider three aspects of information security:

- 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.

- Security mechanisms have been defined by ITU-T (X 800). They used to implement security services. Some of the security mechanisms defined by ITU-T (X 800) are shown in the figure.



Encipherment: This refers to the transformation of the message or data with the help of mathematical algorithms. The main aim of this mechanism is to provide confidentiality. The two techniques that are used for encipherment are cryptography and steganography.

Data integrity: This refers to the method of ensuring the integrity of data. For this, the sender computes a check value by applying some process over the data being sent, and then appends this value to the data. On receiving the data, the receiver again computes the check value by applying the same process over the received data. If the newly computed check value is same as the received one, then it means that the integrity of data is preserved.

Digital signature: This refers to the method of electronic signing of data by the sender and electronic verification of the signature by the receiver. It provides information about the author, date and time of the signature, so that the receiver can prove the sender's identity.

Authentication exchange: This refers to the exchange of some information between two communicating parties to prove their identity to each other.
Traffic padding: This refers to the insertion of extra bits into the stream of data traffic to prevent traffic analysis attempts by attackers.

Routing control: This refers to the selection of a physically secured route for data transfer. It also allows changing of route if there is any possibility of eavesdropping on a certain route.

Notarization: This refers to the selection of a trusted third party for ensuring secure communication between two communicating parties.

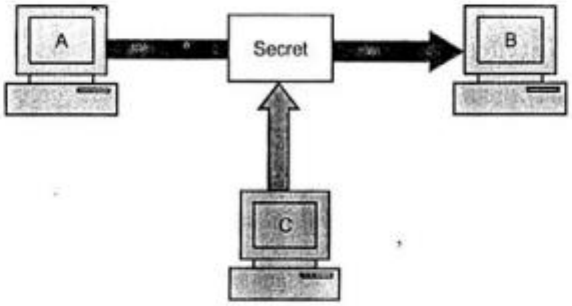
Access control: It refers to the methods used to ensure that a user has the right to access the data or resource.

PRINCIPLES OF SECURITY/ SECURITY SERVICES:

The classification of security services are as follows:

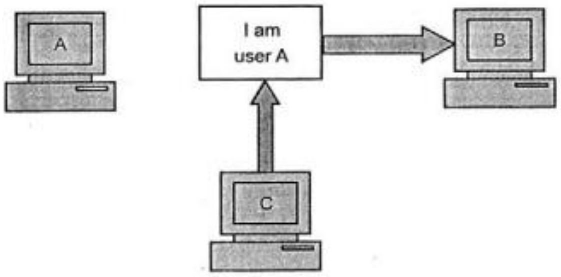
Confidentiality:

- The principle of confidentiality specifies that only the sender and the intended recipient(s) should be able to access the contents of a message.
- Confidentiality gets compromised if an unauthorized person is able to access a message.
- Unauthorized party could be a person, a program or a computer.
- Example: Suppose a confidential email message sent by user A to user B, which is accessed by user C without the permission or knowledge of A and B. This type of attack is called interception.
- **Interception** causes loss of message confidentiality.



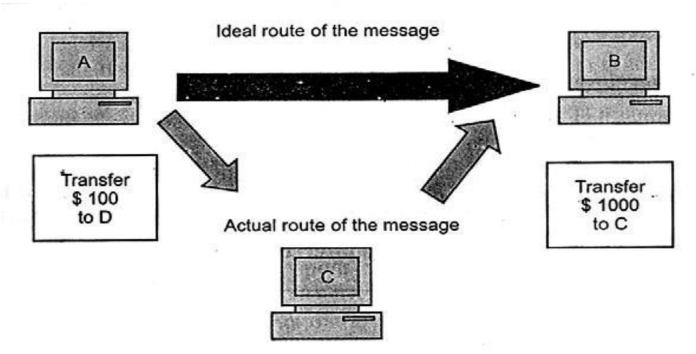
Authentication

- Authentication mechanism helps to establish **proof of identities**.
- The authentication process ensures that the origin of a electronic message or document is correctly identified. This concept is shown in figure.
- **Fabrication** is possible in absence of proper authentication mechanisms.



Integrity

- When the contents of a message are changed after the sender sends it, but before it reaches the intended recipient, we say that the integrity of the message is lost. It is shown in figure.
- For example, consider that user A sends message to user B. User C tampers with a message originally sent by user A, which is actually meant for user B. User C change its contents and send the changed message to user B. User B has no way of knowing that the contents of the message changed after user A had sent it. User A also does not know about this change. This type of attack is called modification.
- **Modification** causes of loss of message integrity.



Non repudiation

Requires that neither the sender nor the receiver of a message be able to deny the transmission.

Access control:

Access control determines and controls who can access what. It regulates which user has access to the resource, under what circumstances.

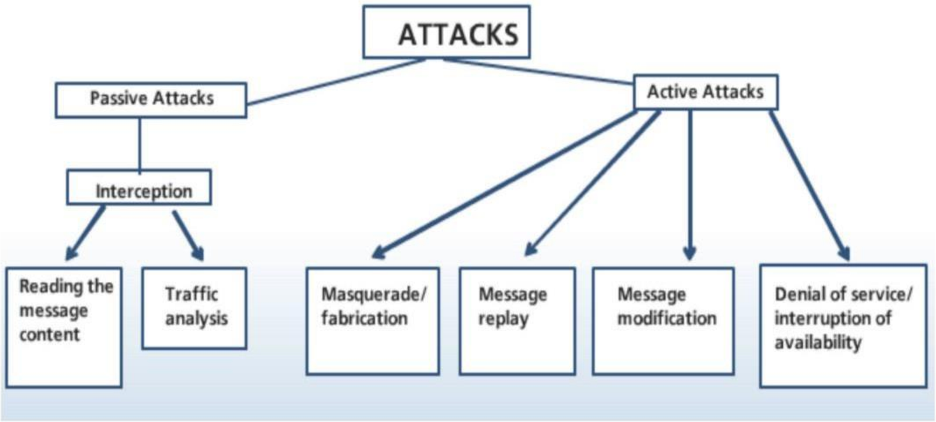
Availability:

- The principle of availability is that resources should be available to authorized parties at all times.
- For example, due to the intentional actions of an unauthorized user C, an authorized user A may not be able to contact a server B. This would defeat the principle of availability. Such an attack is called interruption.
- Interruption causes loss of availability.

TYPES OF SECURITY ATTACK:

There are two types of attacks.

1. Active attacks
2. Passive attacks

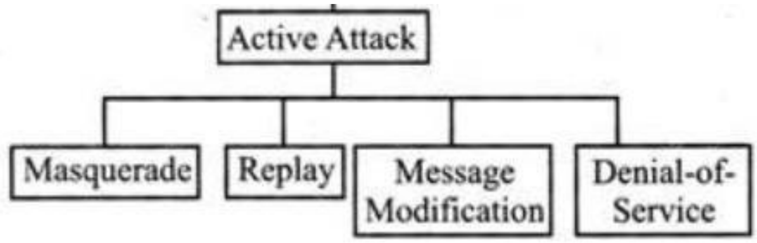


Active attacks

An active attack is an attempt to alter system resources or affect their operation.

I.e., these attacks involve in some modification to the original message in some manner or the creation of a false stream.

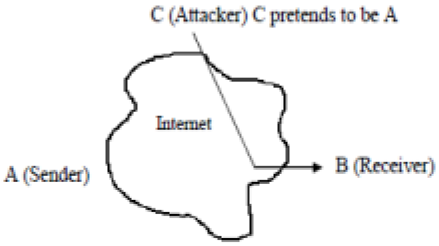
These attacks can be classified in to four categories:



Masquerade:

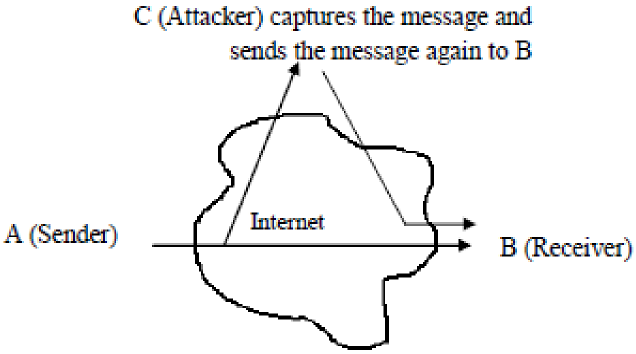
One entity pretends to be a different entity.

It is generally done by using stolen IDs and passwords or through bypassing authentication mechanism.



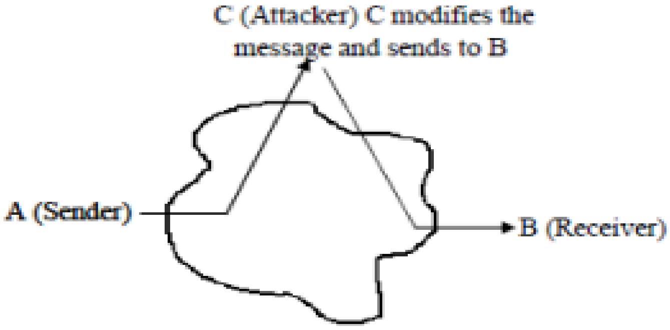
Replay:

This attack involves capturing a copy of the message sent by the original sender and retransmitting it later to bring an unauthorized result.


C (Attacker) captures the message and sends the message again to B
Internet
A (Sender)
B (Receiver)

Modification of messages:

- Some portion of message is altered or the messages are delayed or recorded, to produce an unauthorized effect.
- For example, a message meaning "Allow John Smith to read confidential file accounts" is modified to mean "Allow Fred Brown to read confidential file accounts."



Denial of service:

- A denial-of-service (DoS) is a form of cyberattack that prevents legitimate users from accessing a computer or network.
- In a DoS attack, rapid and continuous online requests are sent to a target server in order to overload the server’s bandwidth.
- Prevents the normal use or management of communication facilities.
- Another form of service denial is the disruption of an entire network, either by disabling the network or overloading it with messages so as to degrade performance.

Passive Attacks:

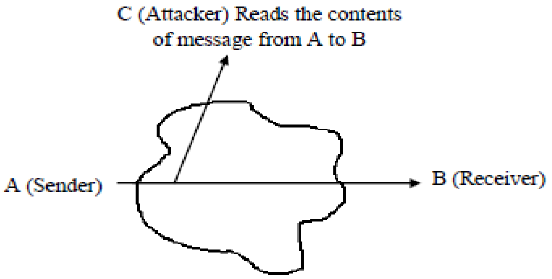
- Passive attacks are those where the attacker indulges in eavesdropping or monitoring of data transmission.
- Passive attacks do not involve any modifications to the contents of an original message.

There are two types of passive attacks.

1. Release of message contents and
2. Traffic analysis.

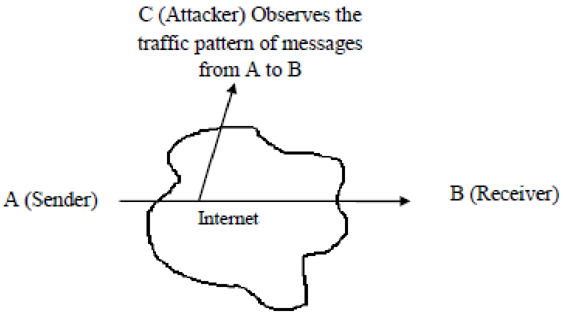
Release of message contents:

- The release of message contents is a type of attack that analyzes and read the message delivered between senders to receiver.
- A telephone conversation, an electronic mail message, or a transferred file may contain sensitive or confidential information.
- We would like to prevent an opponent from getting the contents of these transmissions.



Traffic analysis.

- The attacker simply listens to the network communication to perform traffic analysis to determine the location of key nodes, the routing structure, and even application behavior patterns.
- In this type of attack, an intruder observes the frequency and length of msg. being exchanged between communicating nodes.
- Attacker can then use this information for guessing the nature of communication that was taking place.


C (Attacker) Observes the traffic pattern of messages from A to B
A (Sender)
Internet
B (Receiver)

Passive attacks are very difficult to detect because they do not involve any alteration of the data. Typically, the messages are sent and received in normal fashion. Neither the sender nor receiver is aware that a third party has read the messages or observed the traffic pattern. However, message encryption is a simple solution to prevent passive attacks. Thus, the emphasis in dealing with passive attacks is on prevention rather than detection.

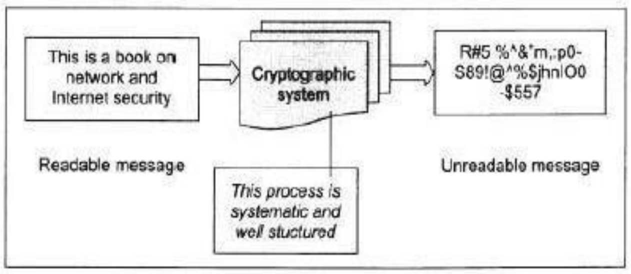
CHAPTER-2

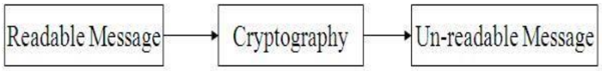
CRYPTOGRAPHY CONCEPTS

CRYPTOGRAPHY TECHNIQUES

From the beginning any era, human being has two natural needs:
To communicate and share information and
To communicate selectively.
These two needs gave rise to the art of coding the messages in such a way that only the intended people could have access to the information. Unauthorized people could not extract any information.
The word "cryptography‟ is the combination of two Greek words, "Krypto" meaning hidden or secret and "graphene" meaning writing.

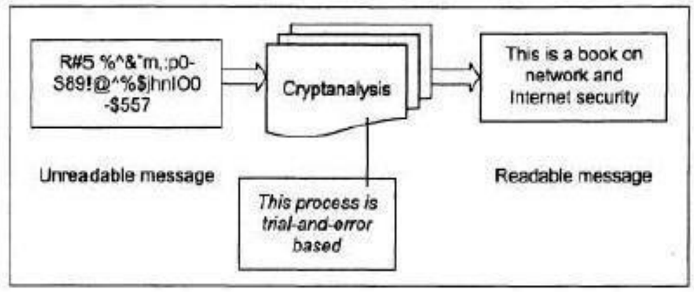
Cryptography: It is the art of achieving security by encoding messages to make them non-readable format.
It is a method of protecting information and communications through the use of codes, so that only those for whom the information is intended can read and process it.


This is a book on network and Internet security
Cryptographic system
R#5 %^&*m,:p0-S89!@^%$jhnlO0-$557
Readable message
Unreadable message
This process is systematic and well stuctured

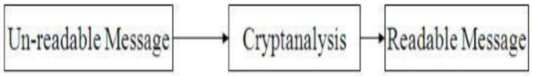


Cryptanalysis:

- It is the technique of decoding messages from a non-readable format back to a readable format.
- It is done without knowing how they were initially converted from readable format to non-readable format. Also called code breaking.


R#5 %^&*m,:p0-S89!@^%$jhnlO0-$557
Cryptanalysis
This is a book on network and Internet security
Unreadable message
Readable message
This process is trial-and-error based

Cryptanalysis



Cryptology: Cryptology is a combination of Cryptography and Cryptanalysis.

Plain Text: Clear text, or plain text, signifies a message that can be understood by the sender, the recipient, and also by anyone else who gets access to that message.

Cipher text:-When a plain text message is codifies using any suitable scheme, the resulting message is called as cipher text.

There are two types of techniques used to covert plain text to cipher text.

- **Substitution Techniques**
- **Transposition Techniques**

Substitution-cipher technique:

In the substitution-cipher technique, the each characters of a plain-text message are replaced byother characters, numbers or symbols.

There are several techniques. They are:

- ➢ Caesar Cipher
- ➢ Modified version of Caesar Cipher
- ➢ Monoalphabetic Cipher
- ➢ Polyalphabetic Cipher
- ➢ Homophonic Substitution Cipher
- ➢ Polygram Substitution Cipher
- ➢ Playfair Cipher
- ➢ Hill Cipher

Caesar Cipher

- ➢ Proposed by Julius Caesar.
- ➢ Mechanism to make a plaintext message into ciphertext message.
- ➢ It replacing each letter of the alphabet with the letter standing 3 places further downthe alphabet.
- ➢ Example: Replace each A with D, B with E, etc.

ABCDEFGHIJKLMNOPQRSTUVYZ
DEFGHIJKLMNOPQRSTUVWXYZC

PT: KIIT
CT: NLLW

Modified version of Caesar Cipher

The Caesar cipher is very simple and very easy to break. To make it complicated the modified version of Caesar cipher comes into play.

Let us assume that the cipher-text alphabets corresponding to the original plain-text alphabets may not necessarily be three places down the order, but instead, can be *any* places down the order.

As we know, the English language contains 26 alphabets. Thus, an alphabet A can be replaced by any *other* alphabet in the English alphabet set, (i.e. B through Z). Of course, it does not make sense to replace an alphabet by itself (i.e. replacing A with A).

Thus, for each alphabet, we have 25 possibilities of replacement. Hence, to break a messagein the modified version of Caesar cipher, our earlier algorithm would not work.

Mono-alphabetic Cipher

- A *monoalphabetic cipher* is a substitution cipher where a symbol in the plaintext has a one-to-one relationship with a symbol in the ciphertext.
- It means that a symbol in the plaintext is always replaced with the same symbol in theciphertext, irrespective of its position in the plaintext.
- It uses random substitution.
- This means that in a given plain-text message, each A can be replaced by any other alphabet(B through Z), each B can also be replaced by any other random alphabet (A or C throughZ), and so on. The crucial difference being, there is no relation between the replacement ofB and replacement of A. That is, if we have decided to replace each A with D, we need notnecessarily replace each B with E—we can replace each B with any other character!

Polyalphabetic Substitution Cipher

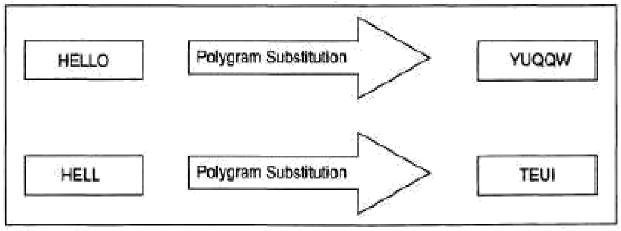
- Leon Battista invented the polyalphabetic substitution cipher in 1568.
- This cipher uses multiple one-character keys. Each of the keys encrypts one plain-text character. The first key encrypts the first plain-text character; the second key encrypts the second plain-text character, and so on.
- After all the keys are used, they are recycled. Thus, if we have 30 one-letter keys, every 30th character in the plain text would be replaced with the same key.

Homophonic Substitution Cipher

- This substitution cipher is very similar to mono-alphabetic cipher.
- However, the difference between the two techniques is in homophonic substitution cipher, one plain-text alphabet can map to more than one cipher-text alphabet.
- For instance, A can be replaced by <D, H, P, R>; B can be replaced by <E, I, Q, S> etc.

Polygram Substitution Cipher

- Polygram substitution cipher technique replaces one block of plain text with another block of cipher text—it does not work on a character-by-character basis.
- For instance, HELLO could be replaced by YUQQW, but HELL could be replaced by a totally different cipher text block TEUI,as shown in Fig.
- This is true in spite of the first four characters of the two blocks of text (HELL) being the same. This shows that in the polygram substitution cipher, the replacement of plain text happens block by block, rather than character by character.



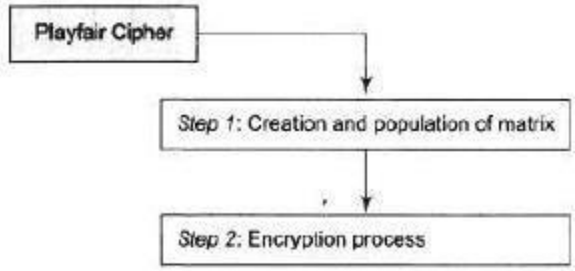
Polygram substitution

Playfair Cipher:

- ➢ The Playfair cipher scheme was invented in 1854 by Charles Wheatstone but was named after Lord Playfair who promoted the use of the cipher. In playfair cipher unlike traditional cipher we encrypt a pair of alphabets(digraphs) instead of a single alphabet.
- ➢ It was used for tactical purposes by British forces in the Second Boer War and in World War I and for the same purpose by the Australians during World War II. This was because Playfair is reasonably fast to use and requires no special equipment.

The Playfair encryption scheme uses two main processes.

> Creation and population of matrix
> Encryption process


Playfair Cipher
Step 1: Creation and population of matrix
Step 2: Encryption process

Step 1: Creation and Population of Matrix

- The Playfair cipher makes use of a 5 x 5 matrix (table), which is used to store a *keyword* or *phrase* that becomes the *key* for encryption and decryption.
- The way this is entered into the 5 x 5 matrix is based on some simple rules:

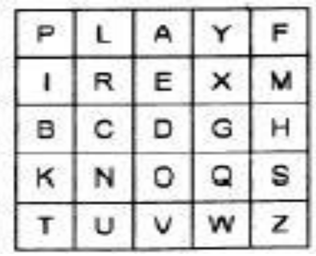
1. Enter the keyword in the matrix row-wise: left-to-right, and then top-to-bottom.
2. Drop duplicate letters.
3. Fill the remaining spaces in the matrix with the rest of the English alphabets (A-Z) that werenot a part of our keyword. While doing so, combine I and J in the same cell of the table.

In other words, if I or J is a part of the keyword, disregard both I and J while filling the remainingslots.

EXAMPLE OF ENCRYPTION AND DECRYPTION IN PLAYFAIR:

For example, suppose that our **keyword=PLAYFAIR EXAMPL**

Then, the 5 x 5 matrix containing our keyword will look as shownLet us say, our **Plaintext= “MY NAME IS ATUL”**



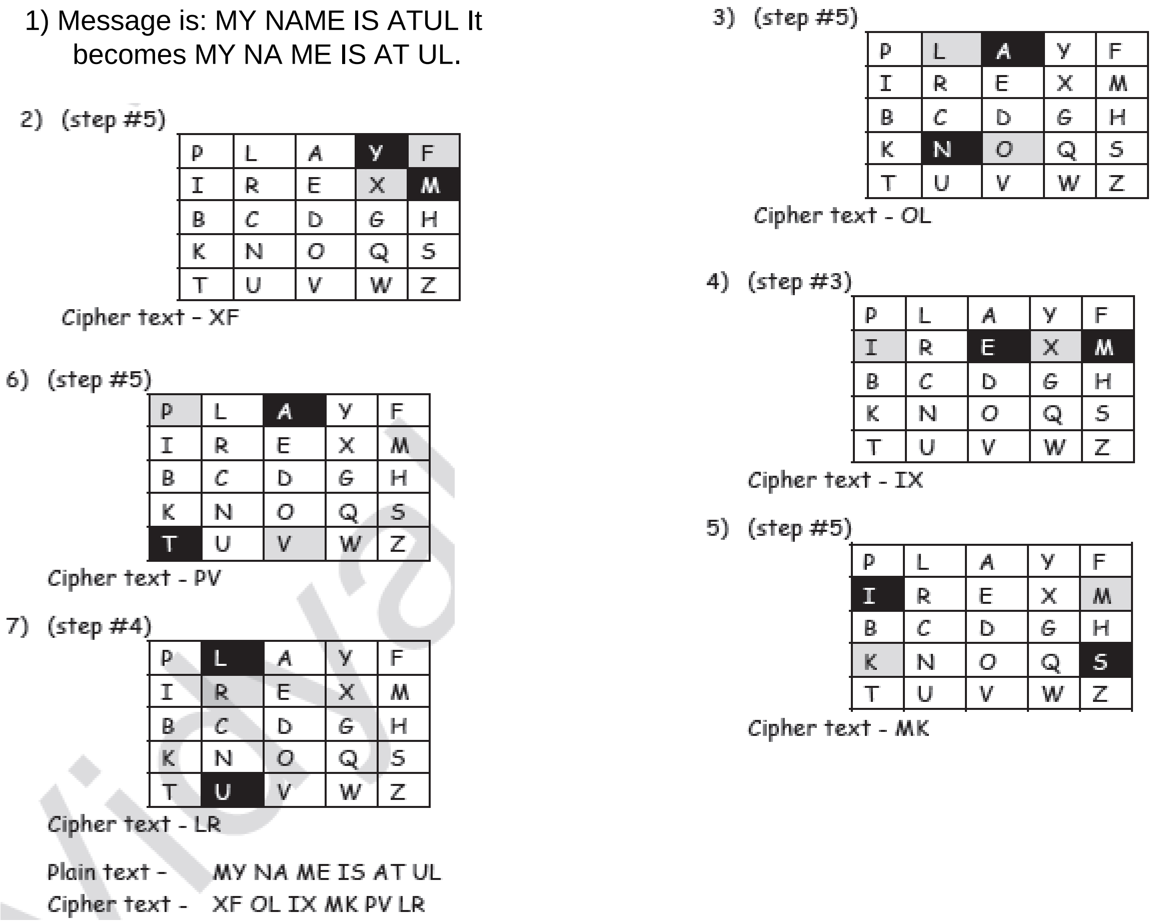
P	L	A	Y	F
I	R	E	X	M
B	C	D	G	H
K	N	O	Q	S
T	U	V	W	Z

Encryption process – it consists of following steps:

1. Before initiating the encryption, break the plain text in pair of 2letters.
   For ex. if our message is MY NAME IS ATUL, it becomes MY NA ME IS AT UL.
2. If both the alphabets are same or 1 letter is remaining, add X after the first alphabet.
3. After the initial process, take the pairs for encryption.
4. If the alphabets of the pair appear in same row of the matrix, then substitute them with their immediate right letter. If the alphabets of the plain text is itself the rightmost, then wrap itup with the left letter of the row it happens.

5. If the alphabets of the pair appear in same column of the matrix, then substitute them withtheir immediate below alphabets. If the letter of the plain text is itself below, then wrap it up with the top letter of the column it happens.
6. If the alphabets of the pair are not in same row or column then define a rectangle with theoriginal pair and substitute them with other corners of the rectangle.

Example



1) Message is: MY NAME IS ATUL It becomes MY NA ME IS AT UL.

2) (step #5)

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

Cipher text - XF

3) (step #5)

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

Cipher text - OL

4) (step #3)

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

Cipher text - IX

5) (step #5)

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

Cipher text - MK

6) (step #5)

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

Cipher text - PV

7) (step #4)

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

Cipher text - LR

Plain text - MY NA ME IS AT UL
Cipher text - XF OL IX MK PV LR

Hill Cipher

The **Hill cipher** works on multiple letters at the same time.

Lester Hill invented this in 1929. The Hill cipher uses the matrix theory of mathematics.

Working:

- Treat each letter with a number like A=0, B=1, C=2…… Z=25.
- Let us say, our original message is “TAJ”
- As per the rule, T=19 A=0 J=9
- Convert it into matrix form as:

$$\begin{bmatrix} 19 \\ 0 \\ 9 \end{bmatrix}$$

Now ***multiply the plain text matrix with any number as keys***. The multiplying matrix should beof *n* x *n* where n is the number of rows of original matrix

$$\begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix} \times \begin{bmatrix} 19 \\ 0 \\ 9 \end{bmatrix} = \begin{bmatrix} 123 \\ 337 \\ 515 \end{bmatrix}$$

Now compute ***mod 26*** on resultant matrix i.e. take the remainder after dividing by 26.

$$\begin{bmatrix} 123 \\ 337 \\ 515 \end{bmatrix} \bmod 26 = \begin{bmatrix} 19 \\ 25 \\ 21 \end{bmatrix}$$

Now translating numbers into alphabets, we get:
19=T 25= Z 21=V
Therefore our cipher text is ***TZV***

To decrypt hill cipher, follow the steps:
1.) Take cipher text matrix and multiply it by inverse of original
key matrix2.) Again perform mod by 26.
Thus we get our original text.

Transposition techniques:

Transposition technique is an encryption method which is achieved by performing **permutation over the plain text**.

Rail-Fence Technique

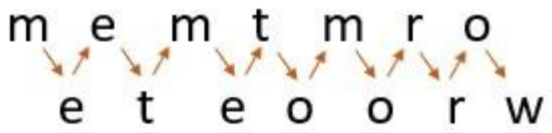
This technique is a type of Transposition technique which involves writing the plain text as a sequence of diagonals and then reading row-by-row to produce cipher text.

It uses a simple algorithm,

1. Writing down the plaintext message into a sequence of diagonals.
2. Read the plain text in step-1 as a sequence of rows.

Example:

Plain Text: meet me Tomorrow
Now, we will write this plain text sequence wise in a diagonal form as you can see below:



Cipher Text: m e m t m r o e t e o o r w

Simple Columnar Transposition Technique:

A. Basic Technique

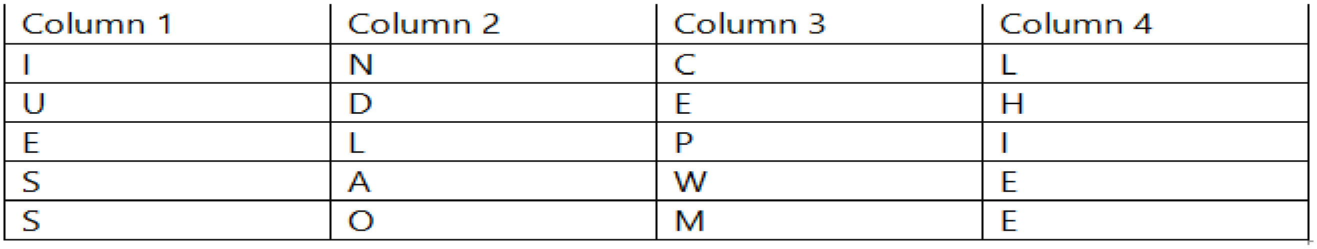
It is a slight variation to the Rail-fence technique, let’s see its algorithm:

1. In a rectangle of pre-defined size, write the plain-text message row by row.
2. Read the plain message in random order in a column-wise fashion. It can be any order such as 2, 1, 3 etc.
3. Thus Cipher-text is obtained.

Let’s see an example:

Original message: **"INCLUDEHELP IS AWESOME".**

Now we apply the above algorithm and create the rectangle of 4 columns (we decide to make a rectangle with four column it can be any number.)



Column 1	Column 2	Column 3	Column 4
I	N	C	L
U	D	E	H
E	L	P	I
S	A	W	E
S	O	M	E

Now let’s decide on an order for the column as 4, 1, 3 and 2 and now we will read the text in column-wise.

Cipher-text: **LHIEEIUESSCEPWMNDLAO**

B. Columnar Technique with multiple rounds

In this method, we again change the chipper text we received from a Basic technique that is in round 1 and again follows the same procedure for the cipher-text from round 1.

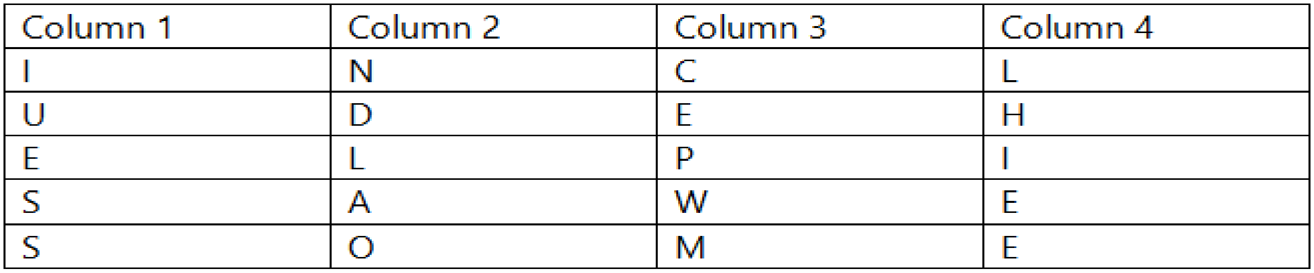
Algorithm:

1. In a rectangle of pre-defined size, write the plain-text message row by row.
2. Read the plain message in random order in a column-wise fashion. It can be any order such as 2, 1, 3 etc.
3. Thus, Cipher-text of round 1 is obtained.
4. Repeat from step 1 to 3.

Example:

Original message: **"INCLUDEHELP IS AWESOME"**.

Now we apply the above algorithm and create the rectangle of 4 column (we decide to make a rectangle with four column it can be any number.)



Column 1	Column 2	Column 3	Column 4
I	N	C	L
U	D	E	H
E	L	P	I
S	A	W	E
S	O	M	E

Now let’s decide on an order for the column as 4, 1, 3 and 2 and now we will read the text in column-wise.

Cipher-text of round 1: **LHIEEIUESSCEPWMNDLAO**

Round 2:

Column 1	Column 2	Column 3	Column 4
L	H	I	E
E	I	U	E
S	S	C	E
P	W	M	N
D	L	A	O

Now, we decide to go with a previous order that is 4,1,3,2.

Cipher-text: **EEENLESPICUMHISW**

These multi-round columnar techniques are harder to crack as compared to methods seen earlier.

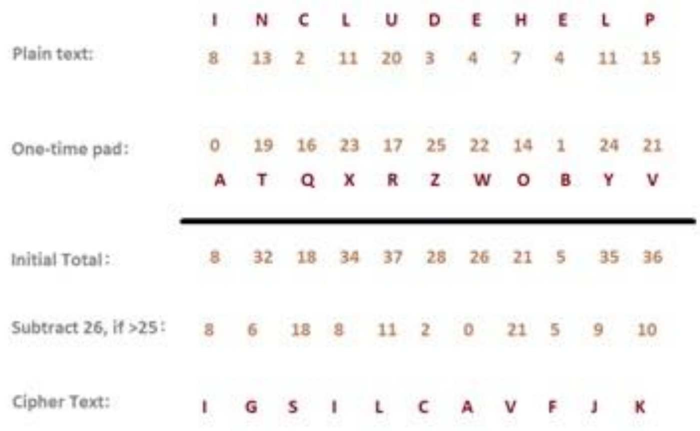
Vernam Cipher (one time pad):

The Vernam Cipher has a specific subset one-time pad, which uses input ciphertext as a random set of non-repeating character. The thing to notice here is that, once an input cipher text gets used it will never be used again hence one-time pad and length of cipher-text is the size that of message text.

Algorithm:

1. Plain text character will be represented by the numbers as A=0, B=1, C=2,... Z=25.
2. Add each corresponding number of a plain text message to the input cipher text alphabet numbers.
3. If the sum is greater than or equal to 26, subtract 26 from it.
4. Translate each number back to corresponding letters and we got our cipher text.

Example: Our message is **"INCLUDEHELP**" and input cipher text is "ATQXRZWOBYV"



	I	N	C	L	U	D	E	H	E	L	P
Plain text:	8	13	2	11	20	3	4	7	4	11	15
One-time pad:	0	19	16	23	17	25	22	14	1	24	21
	A	T	Q	X	R	Z	W	O	B	Y	V
Initial Total:	8	32	18	34	37	28	26	21	5	35	36
Subtract 26, if >25:	8	6	18	8	11	2	0	21	5	9	10
Cipher Text:	I	G	S	I	L	C	A	V	F	J	K

Example of Vernam Cipher

One time pad should be discarded after every single use and this technique is proved highly secure and suitable for small messages but illogical if used for long messages.

Encryption and Decryption:-

Encryption:-The process of encoding plain text messages into cipher text messages is called as encryption.

Decryption:-The reverse process of transforming cipher text messages back to plain text messages is called as decryption.

Symmetric and Asymmetric Key Cryptography:

Symmetric key Cryptography:-

Symmetric key cryptography (or symmetric encryption) is a type of encryption scheme in which the same key is used both to encrypt and decrypt messages.

Asymmetric key Cryptography:-

Asymmetric encryption uses the public key for the encryption, and a private key is used for decryption.

Or

Asymmetric cryptography, also known as public-key cryptography, is a process that uses a pair of related keys -- one public key and one private key .

CHAPTER-3

SYMMETRIC AND ASYMMETRIC KEY ALGORITHMS

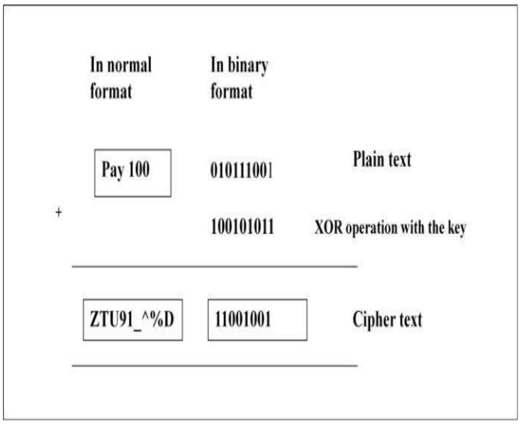
Algorithm Types and modes:

Algorithm types:

- It defines what size of plain text should be encrypted in each step of algorithm.
- It is of two types:
  - Stream Ciphers
  - Block Ciphers

Stream Ciphers

- Bit-by-bit encryption/decryption.
- In this scheme, the plaintext is processed one bit at a time i.e. one bit of plaintext is taken, and a series of operations is performed on it to generate one bit of cipher text.
- Technically, stream ciphers are block ciphers with a block size of one bit.
- Example: Suppose the original message (plain text) is Pay 100 in ASCII (i.e. text format).
- When we convert these ASCII characters to their binary values, let us assume that it translates to 01011100. Let us also Assume that we apply the XOR logic as the encryption algorithm.
- As a result of applying one bit of key for every respective bit of the original message, suppose thecipher text is generated as 11001001 in binary (ZTU91 A% in text).



Input 1	Input 2	Outputs
0	0	0
0	1	1
1	0	1
1	1	0

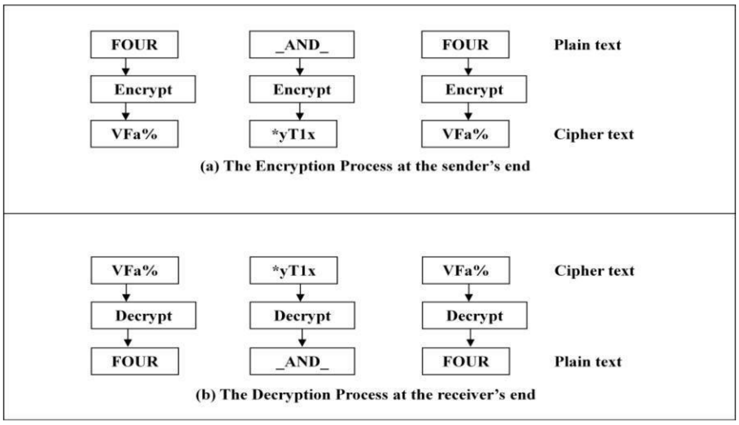
Block Cipher

- Block-by-block encryption / decryption.
- In this scheme, the plain binary text is processed in blocks (groups) of bits at a time; i.e. a block of plaintext bits is selected, a series of operations is performed on this block to generate a block of cipher text bits.
- The number of bits in a block is fixed. For example, the schemes DES and AES have block sizes of 64 and 128, respectively.

The basic scheme of a block cipher is given as follows:

Block Cipher Example:

Suppose we have a plain text "FOUR_AND _FOUR" that needs to be encrypted. By using this technique FOUR could be encrypted first followed by _AND_ and FOUR.

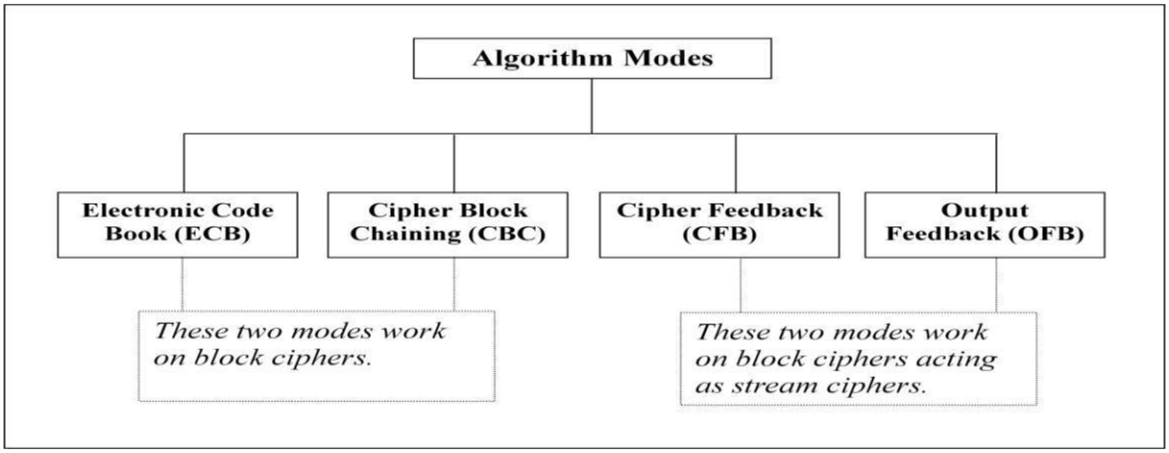


(a) The Encryption Process at the sender's end

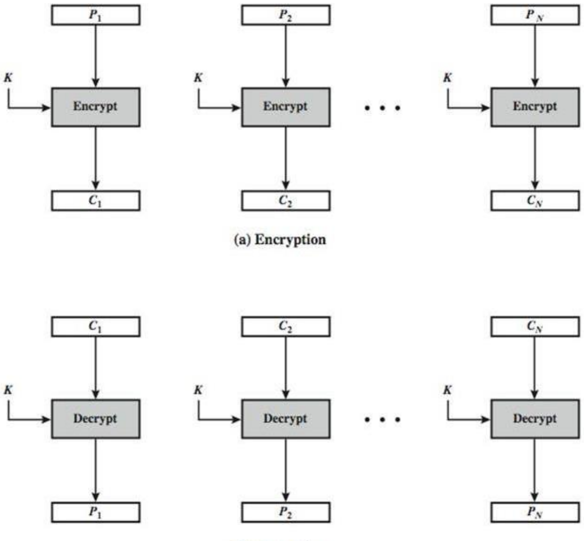
(b) The Decryption Process at the receiver's end

Algorithm Modes:

- It is a combination of series of basic algorithm steps on block cipher and some sort of feedbackfrom the previous steps.
- It is divided into four modes:


Algorithm Modes
Electronic Code Book (ECB)
Cipher Block Chaining (CBC)
Cipher Feedback (CFB)
Output Feedback (OFB)
These two modes work on block ciphers.
These two modes work on block ciphers acting as stream ciphers.

Electronic Code book (ECB) Mode:



(a) Encryption

(b) Decryption

- ECB is a simplest and straightforward method of converting a block of plaintext into cipher text.
- Here, plain-text message is divided into blocks of 64 bits each.
- Each such block is then encrypted independently of the other blocks.
- For all blocks in a message, the same key is used for encryption.
- This **encryption process** is shown figur
- At the receiver's end, the incoming data is divided into 64-bit blocks.
- By using the same key as was used for encryption, each block is decrypted to produce the corresponding plain-text block.
- This **decryption process** is shown figure.

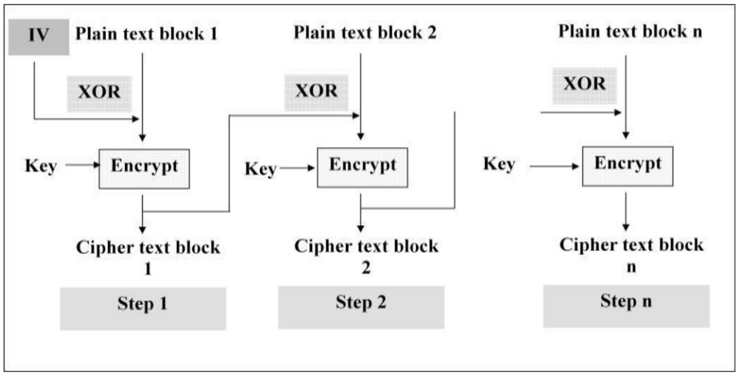
Cipher Block Chaining (CBC) Mode:

In CBC mode, a feedback mechanism is used. Chaining adds a feedback mechanism to a block cipher.

In Cipher Block Chaining (CBC), the results of the encryption of the previous block are fed back into the encryption of the current block.

That is, each block is used to modify the encryption of the next block.

Thus, each block of cipher text is dependent on the corresponding current input plain-text block, as well as all the previous plain-text blocks.



Operation:

The steps are as follows:

- Load the n-bit Initialization Vector (IV). IV is a random generated block of text in a register.
- XOR the n-bit plain text block with data value in IV register.
- Encrypt the result of XOR operation with the key K. Result is it produce the cipher text block.
- Feed cipher text block into the IVregister and continue the operation till all plaintext blocks are processed.

Cipher Feedback (CFB) Mode:

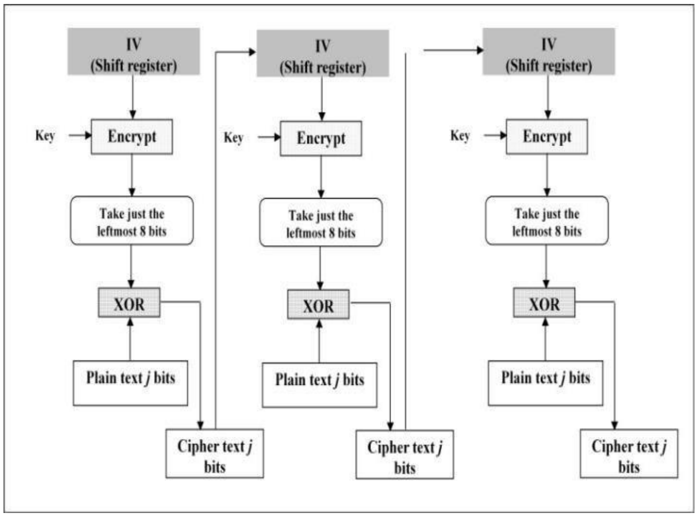
- Not all applications can work with blocks of data. Security is also required in applications that are character-oriented.
- For instance, an operator can be typing keystrokes at a terminal, which needs to be immediately transmitted across the communications link in a secure manner, i.e., by using encryption.
- In such situations, stream cipher must be used. The Cipher Feedback (CFB) mode is useful in such cases.
- In this mode, data is encrypted in units that are smaller (e.g., they could be of size 8 bits, i.e. the size of a character typed by an operator) than a defined block size (which is usually 64 bits).

Steps of operation are:

- Assuming that we are dealing with j bits at a time (as we have seen usually, but not always, j = 8).
- we shall study CFB in a step-by-step fashion.
- Step 1 Like CBC, a 64-bit Initialization Vector (IV) is used in the case of CFB mode. The IV is kept in a shift register. It is encrypted in the first step to produce a corresponding 64 bit cipher text.
- Step 2 Now, the leftmost (i.e. the most significant) j bits of the encrypted IV are XORed with the first j bits of the plain text.
- Step 3 Now, the bits of IV (i.e. the contents of the shift register containing IV) are shifted left by j positions. Thus, the rightmost j positions of the shift register now contain unpredictable data. These rightmost j positions are now filled with C.
- Step 4 Now, steps 1 through 3 continue until all the plain-text units are encrypted.

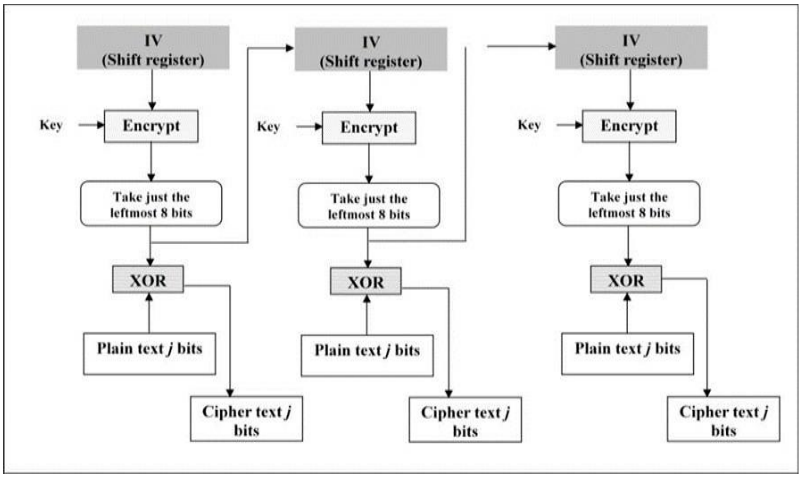
That is, the following steps are repeated:

- IV is encrypted.
- The leftmost j bits resulting from this encryption process are XORed with the next j bits of the plain text.
- The resulting cipher-text portion (i.e., the next j bits of cipher text) is sent to the receiver.
- The shift register containing the IV is left-shifted by j bits.
- The j bits of the cipher text are inserted from right into the shift register containing the IV.



Output Feedback (OFB) Mode:

- The OFB mode is similar to CFB, but the only difference is that in CFB, the cipher text is fed into the next stage of encryption process.
- But in case of OFB the output of IV encryption process is fed into the next stage of encryption process.
- In this mode, if there are errors in individual bits, they remain errors in individual bits and do not corrupt the whole message.
- That is, bit errors do not get propagated.



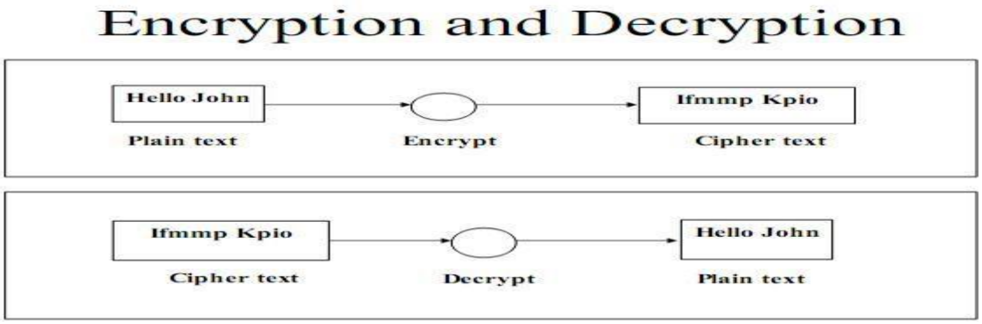
Encryption & Decryption:

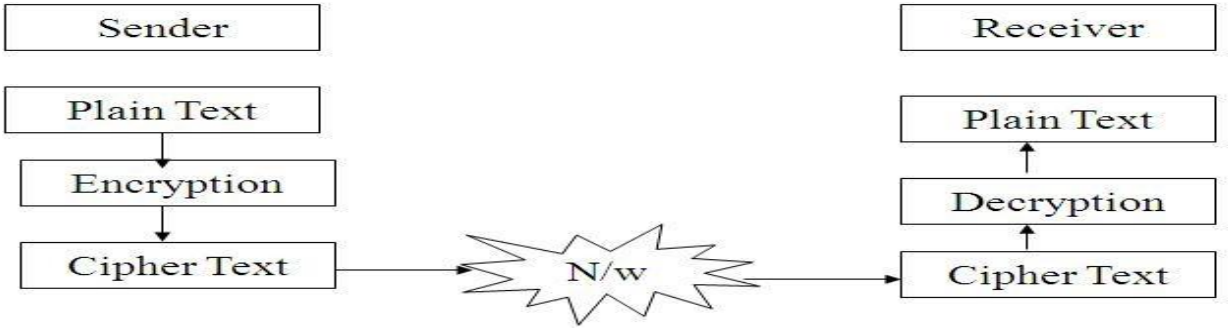
Encryption or Encoding or Encode:

- The process of converting or transforming plain text or original text into cipher text is called asencoding.
- This new form of the message is totally different from the initial message.
- It occurs at the sender's side.
- The sender uses an encryption algorithm and a key to transform the original message into an encryptedmessage i.e., **cipher text**.
- Encryption is also called **enciphering or encipherment**.

Decryption or Decoding or Decode:

- The process of converting cipher text into plain text is called as decoding.
- It occurs at the receiver's end.
- The receiver uses decryption algorithms and a key to transform the cipher text back to original plaintext message.
- The decryption is also called deciphering or decipherment.
- Decryption is the reverse process of encryption.





An Overview of Symmetric Key Cryptography

Symmetric key cryptography (or symmetric encryption) is a type of encryption scheme in which the same key is used both to encrypt and decrypt messages. Such a method of encoding information has been largely used in the past decades to facilitate secret communication between governments and militaries.

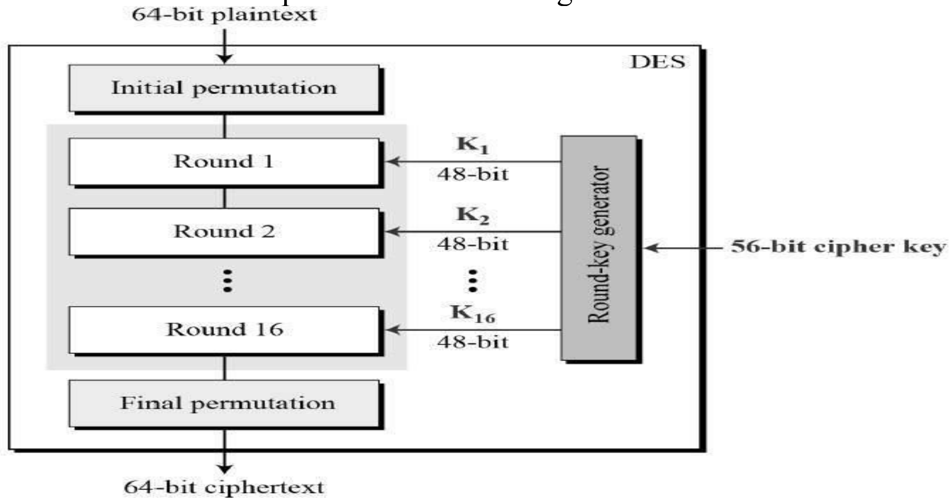
Data Encryption Standard:

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.

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

How DES Works?

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 −

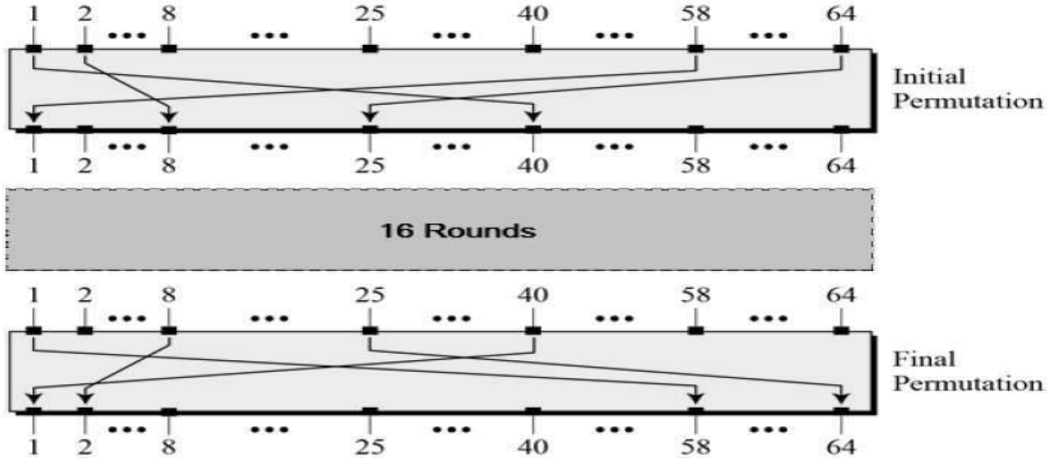
Round function

Key schedule

Any additional processing − Initial and final permutation

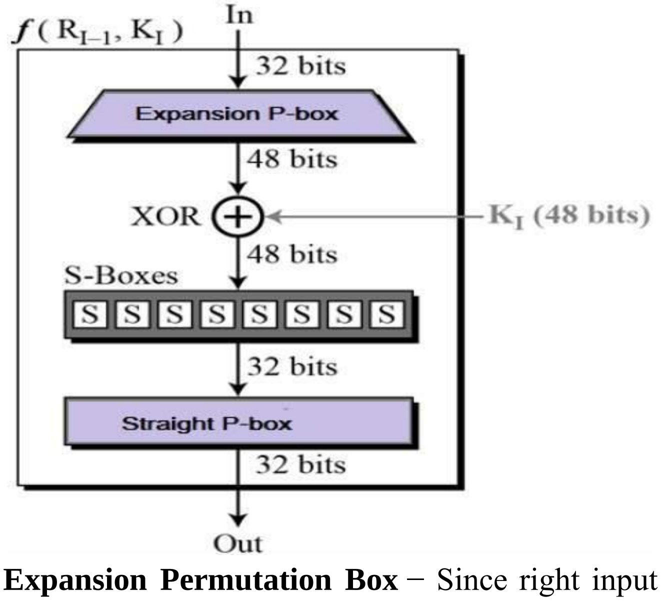
Initial and Final Permutation

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 −

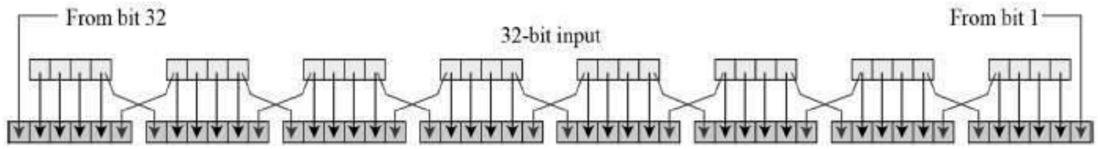


Round Function

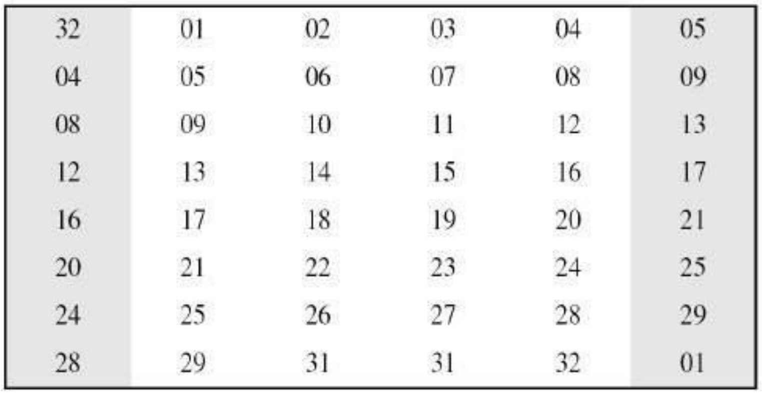
The heart of this cipher is the DES function, *f*. The DES function applies a 48-bit key to the rightmost 32 bits to produce a 32-bit output.



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 −



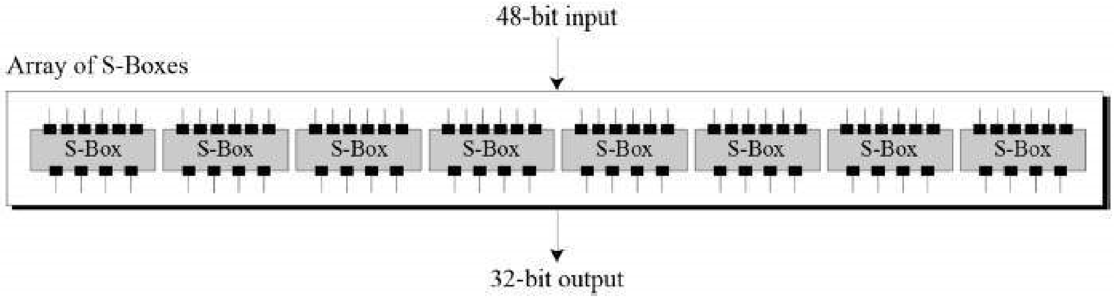
The graphically depicted permutation logic is generally described as table in DES specification illustrated as shown −



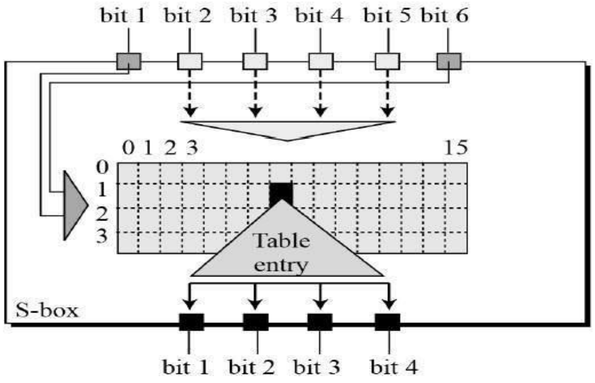
32	01	02	03	04	05
04	05	06	07	08	09
08	09	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	31	31	32	01

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 −

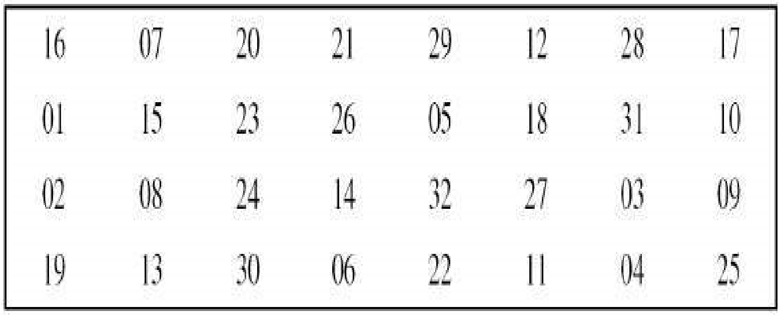


The S-box rule is illustrated below −



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

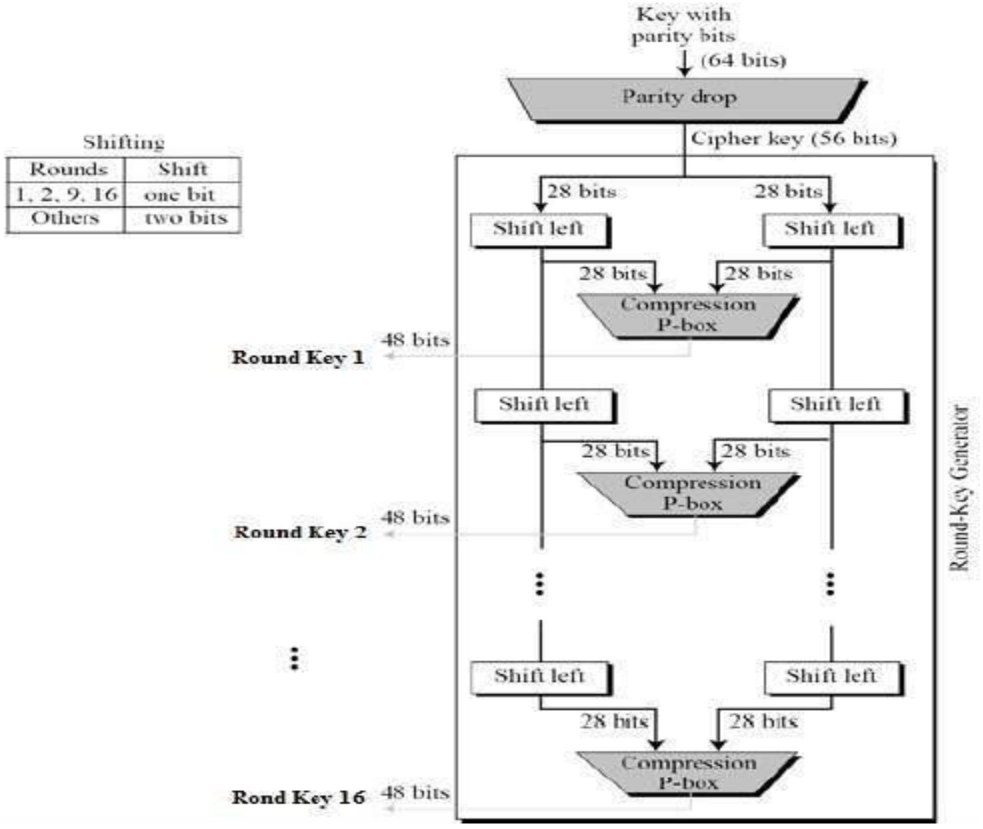
Straight Permutation − The 32 bit output of S-boxes is then subjected to the straight permutation with rule shown in the following illustration:



16	07	20	21	29	12	28	17
01	15	23	26	05	18	31	10
02	08	24	14	32	27	03	09
19	13	30	06	22	11	04	25

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 drops, shifting, and Compression P-box is given in the DES description.

DES Analysis

The DES satisfies both the desired properties of block cipher. These two properties make cipher very strong.

Avalanche effect − A small change in plaintext results in the very great change in the ciphertext.

Completeness − Each bit of cipher text depends on many bits of plaintext.

During the last few years, cryptanalysis has found some weaknesses in DES when key selected are weak keys. These keys shall be avoided.

DES has proved to be a very well designed block cipher. There have been no significant cryptanalytic attacks on DES other than exhaustive key search.

Asymmetric-key Enclpherment:

The asymmetric-key encipherment also called public-key encipherment or public-key cryptography, was introduced by Diffie and Hellman in 1976 to overcome the problem found in symmetric key cryptography.

It uses two different keys for encryption and decryption.

These two keys are referred to as the public key (used for encryption) and the private key (used for decryption).

Each authorized user has a pair of public and private keys. The public key of each user is known to everyone, whereas the private key is known to its owner only.

A **public-key encryption** scheme has six ingredients as shown in figure.

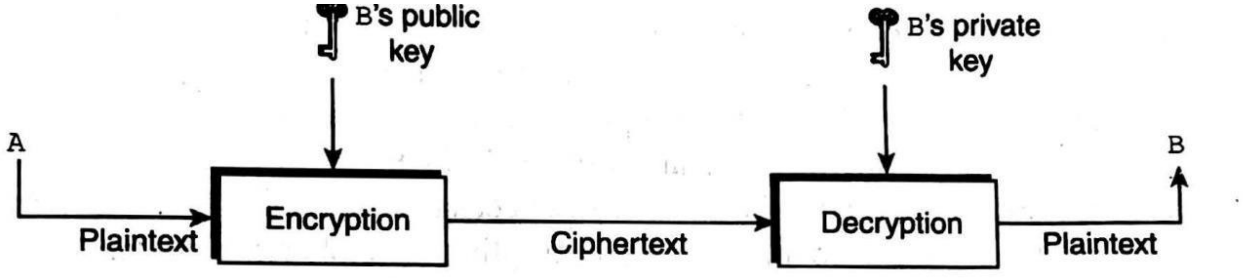


Figure 2.2 Message exchange using public key

- **Plaintext:** This is the readable message or data that is fed into the algorithm as input.
- **Encryption algorithm:** The encryption algorithm performs various transformations on the plaintext.This encrypts plain text using public key of receiver.
- **Public and Private keys:** This is a pair of keys used for encryption; the other is used for decryption.In figure, encryption is done using public key and decryption using private key.
- **Cipher-text:** This is the coded message produced as output. It depends on the plaintext and the key.
- **Decryption algorithm:** This algorithm accepts the cipher text and the matching key and produces the original plaintext. In figure, decryption algorithm uses private key.
- Now, suppose that a user ·A wants to transfer some information to· user B securely. The user A encrypts the data by using the public key of B and sends the

encrypted message to B.

- On receiving the encrypted message, B decrypts it by using his/ her private key. Since decryption process requires a private key of user B, which is only known to B, the information is transferred securely. The above figure states the whole process.
- RSA is a well-known example of asymmetric-key algorithm.
- The main advantage of public-key cryptography is that the sender and the receiver need not have to share the secret key. All communication involves only public keys.
- Thus, the private key is never transmitted or shared. Anyone can send a confidential message using a public key, but the message can only be decrypted with a private key, which is kept by the intended recipient.

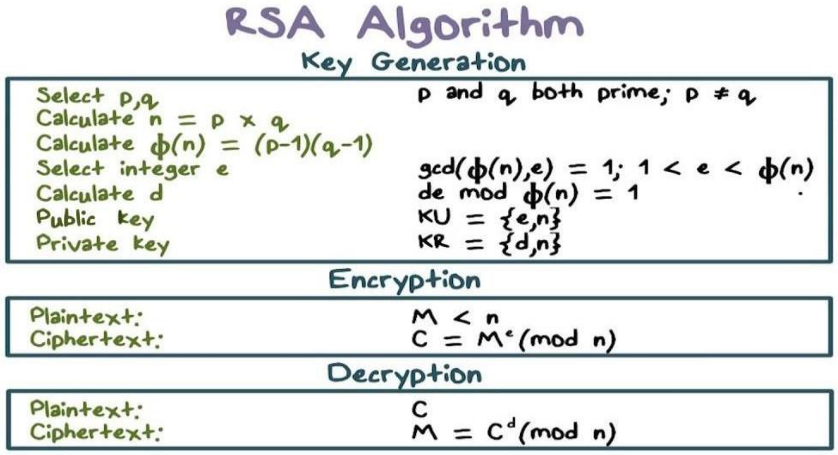
Differentiate between symmetric-key and asymmetric-key cryptography:

Symmetric-key	Asymmetric-key
1. It uses a single key for both encryption and decryption of data.	1. It uses .two different keys-public key for encryption and private key for decryption.
2. Both the communicating parties share the same algorithm and the key.	2. Both the communicating parties should have at least one of the matched pair of keys.
3.The processes of encryption and decryption are very fast.	3. The encryption and decryption processes are slower as compared to symmetric-key cryptography.
4. Key distribution is a big problem.	4. Key distribution is not a problem.
5.The size of encrypted text is usually same or less than the original text.	5. The size of encrypted text is usually more than the size of the original text.
6.It can only be used for confidentiality, that is, only for encryption and decryption of data.	6. It can be used for confidentiality of data as well as for integrity and non-repudiation checks (i.e.for digital signatures).

THE RSA ALGORITHM:

This algorithm proposed by Ron Rivest, Adi Shamir, Len Adleman (RSA) in 1978 at MIT. It is based onasymmetric key cryptography.

1. Choose two large prime numbers *P* and Q.
2. Calculate $N = P \times Q$.
3. Select the public key (i.e. the encryption key) *E* such that it is not a factor of (P - 1) and (Q - 1).
4. Select the private key (i.e., the decryption key) *D* such that the following equation is true:(D x E) mod (P - 1) x (Q - 1) = 1
5. For encryption, calculate the cipher text *CT* from the plain text *PT* as follows: $CT = PT^E \bmod N$.
6. Send CT as the cipher text to the receiver.
7. For decryption, calculate the plain text *PT* from the cipher text *CT* as follows: $PT = CT^D \bmod N$



RSA Algorithm

Key Generation

Select p,q	p and q both prime; $p \neq q$
Calculate $n = p \times q$	
Calculate $\phi(n) = (p-1)(q-1)$	
Select integer e	$\gcd(\phi(n),e) = 1;\ 1 < e < \phi(n)$
Calculate d	$de \bmod \phi(n) = 1$
Public key	$KU = \{e,n\}$
Private key	$KR = \{d,n\}$

Encryption

Plaintext:	$M < n$
Ciphertext:	$C = M^e \pmod n$

Decryption

Plaintext:	C
Ciphertext:	$M = C^d \pmod n$

Examples of RSA

Let us take an example of this process to understand the concepts.

1. Choose two large prime numbers P and Q. Let P = 7, Q = 17.
2. Calculate N = P x Q.
   We have N = 7 x 17= 119.
3. Select the public key (i.e., the encryption key) E such that it is not a factor of (P - 1) X (Q - 1).Let us find (7 - 1) x (17 - 1) = 6 x 16 = 96.
   The factors of 96 are 2, 2, 2, 2, 2 and 3 (because 96 = 2 x 2 x 2 x 2 x 2 X 3).Thus, we have to choose E such that it is not the factors of E is 2 and 3.
   Let us choose E as 5 (it could have been any other number that does not its factors as 2 and 3).
4. Select the private key (i.e., the decryption key) D such that the following equation is true:(D x E) mod (P - 1) x (Q -1) = 1.
   Let us substitute the values of E, P and Q in the equation.We have: (D x 5) mod (7 - 1) x (17 - 1) = 1
   That is: (D x 5) mod (6) x (16) = 1
   That is: (D x 5) mod (96) = 1
   After some calculations, let us take D = 77. Then the following is true: (77 x 5) mod (96) = 385 mod96 = 1.
5. For encryption, calculate the cipher text CT from the plain text PT as follows:CT= PT^E mod N.

   Let us assume that we want to encrypt plaintext=10. Then we have:
   CT = 10^5 *mod 119 = 100000 mod 119 = 40.*

6. Send CT as the cipher-text to the receiver. Send 40 as the cipher text to the receiver.
7. For decryption, calculate the plaintext PT from the cipher-text CT as follows: PT = CTD mod N.
   That is: PT = 4077 mod 119 = 10.
   This was the original plaintext of step 5

Digital signature:

- It is an authentication mechanism that allows the sender to attach an electronic code with the message. This electronic code acts as the signature of the sender and hence, is named digital signature.
- It is done to ensure its authenticity and integrity.
- Digital signature uses the public-key cryptography technique. The sender uses his or her private keyand a signing algorithm to create a digital signature and the signed document can be made public. The receiver, uses the public key of the sender and a verifying algorithm to verify the digitalsignature.
- A normal message authentication scheme protects the two communicating parties against attacks from a third party (intruder). However, a secure digital signature scheme protects the two parties against each other also.
- Suppose A wants to send a signed message (message with A's digital signature) to B through a network. For this, A encrypts the message using his or her private key, which results in a signed message. The signed message is then sent through the network to B.
- Now, B attempts to decrypt the received message using A's public key in order to verify that the received message has really come from A.
- If the message gets decrypted, B can believe that the message is from A. However, if the message or the digital signature has been modified during transmission, it cannot be decrypted using A's public key. From this, B can conclude that either the message transmission has tampered with, or that the message has not been generated by A.

Message integrity:

- Digital signatures also provide message integrity.
- If a message has a digital signature, then any change in the message after the signature is attached will invalidate the signature.
- That is, it is not possible to get the same signature if the message is changed. Moreover, there is no efficient way to modify a message and its signature such that a new message with a valid signature is produced.

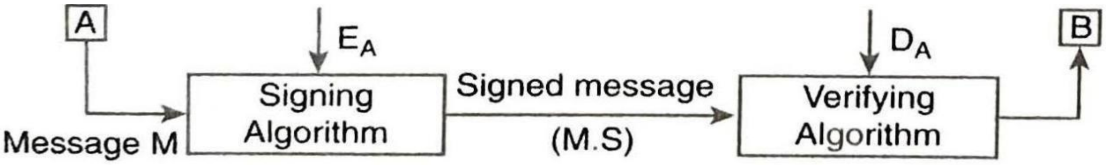
Non-repudiation:

- Digital signatures also ensure non-repudiation.
- For example, if A has sent a signed message to B, then in future A cannot deny about the sending ofthe message. B can keep a copy of the message along with A's signature.
- In case A denies, B can use A’s public key to generate the original message. If the newly createdmessage is the same as that initially sent by A, it is proved that the message has been sent by A only.

- In the same way, B can never create a forged message bearing A's digital signature, because only Acan create his or her digital signatures with the help of that private key.

Message confidentiality:

- Digital signatures do not provide message confidentiality, because anyone knowing the sender's public key can decrypt the message.



Digital signature process:

The digital signature process is shown in Figure. Suppose user A wants to send a signed message to B through a network. To achieve this communication, these steps are followed:

- A uses his private key (EA), applied to a signing algorithm, to sign the message (M).
- The message (M) along with A's digital signature (S) is sent to B.
- On receiving the message (M) and the signature (S), B uses A's public key (DA), applied to the verifying algorithm, to verify the authenticity of the message. If the message is authentic, B accepts the message, otherwise it is rejected.

CHAPTER-4

DIGITAL CERTIFICATE & PUBLIC KEY INFRASTRUCTURE

Digital Certificate:

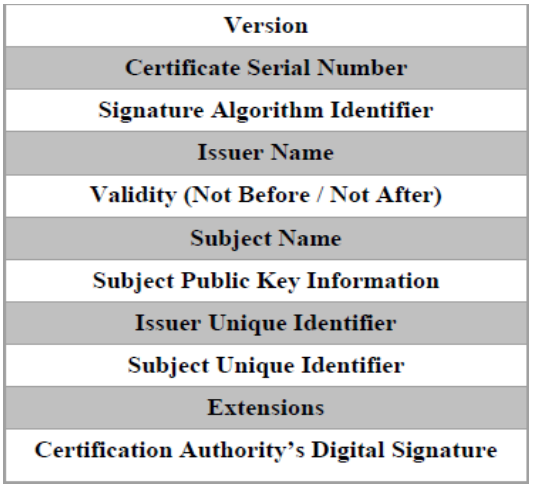
- A digital certificate is simply a small computer file. For example, my digital certificate would actually be a computer file with a file name such as name .cer.
- The digital certificate is actually quite similar to a passport. As we know every passport has a unique passport number, similarly every digital certificate has a unique serial number. Also gives information of the issuer's name, serial number, public key, validity period, etc.
- Digital Certificate is issued by **a trusted agency called as CA (Certification Authority).**
- Another third party called as RA (Registration Authority) acts as a intermediate entity between CA and end user.
- Satisfies the principle of Authentication, non-repudiation.

Certification Authority (CA)

- CA has to be someone, who everybody trusts. Consequently, the governments in variouscountries decide who can and who cannot be a CA.
- Usually, a CA is a reputed organization, such as a post office, financial institution, software company, etc. Two of the world's most famous CAs are VeriSign and Entrust. Safescrypt Limited is the first Indian CA.
- Thus, a CA has the authority to issue digital certificates to individuals and organizations, who want to use those certificates in asymmetric-key cryptographic applications.

Technical Details of a Digital Certificate:

A standard called X.509 defines the structure of a digital certificate. The International Telecommunication Union (ITU) designs this standard. At that time, it was a part of another standard called X.500. The current version of the standard is Version 3, called X.509V3**.**



Version
Certificate Serial Number
Signature Algorithm Identifier
Issuer Name
Validity (Not Before / Not After)
Subject Name
Subject Public Key Information
Issuer Unique Identifier
Subject Unique Identifier
Extensions
Certification Authority's Digital Signature

Contents of Digital Certificate:

Version: Version of X.509 protocol. Version can be 1,2 or 3
Certificate Serial No.: Contains unique integer which is generated by CA
Signature Algorithm Identifier: Identifies the algorithm used by CA to sign the certificate.
Issuer Name: Identifies the Distinguished Name that created & signed the certificate Validity: (not before/not after) Contains two date-timevalues. This value generally specifies the date & time up to seconds or milliseconds.
Subject name: Distinguished Name of the end user (user or organization)
Subject Public key info.: This field can never be blank. Contains public key & algorithm related.
Issuer Unique Identifier: Helps identify a CA uniquely if two or more CAs have used the same Issuer Name over time.
Subject Unique Identifier: Helps identify a subject uniquely if two or more subjects have used the same Subject Name over time.

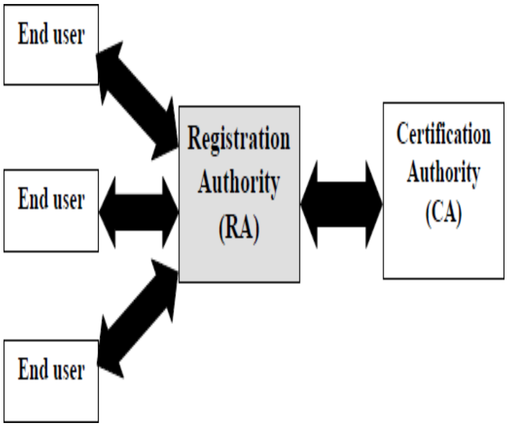
Digital-Certificate Creation:

1. ***Parties Involved***

- end user (may be a single user or organization),
- issuer (CA),
- third party is also (optionally) called a Registration Authority (RA), involved in the certificate creation and management.

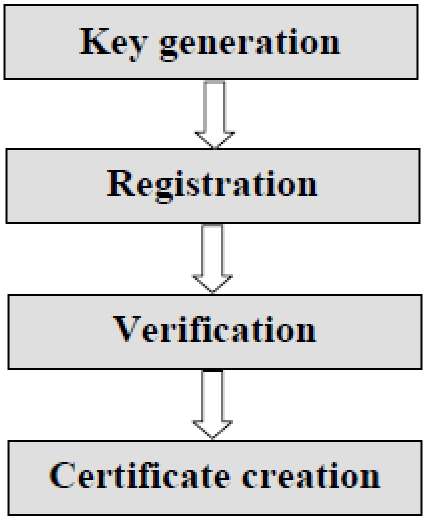
The RA commonly provides the following services

- Accepting and verifying registrationinformation about new users.
- Generating keys on behalf of the end users.
- Accepting and authorizing requests for keybackups and recovery.
- Accepting and authorizing the requests forcertificate revocation.
- RA is mainly set up for facilitating the interaction between the end users and the CA
- The RA cannot issue digital certificates.
- The CA must handle this. Additionally, after a certificate is issued, the CA is responsible for all the certificate management aspects, such as tracking its status, issuing revocation notices if the certificate needs to be invalidated for some reason, etc.



2. Certificate Creation Steps

Step 1: Key Generation:



- The action begins with the subject (i.e. the user/organization) who wants to obtain a certificate.
- There are two different approaches for this purpose:
- Firstly, the subject can create a private key and public key pair using some software.
  - The subject must keep the private key which is generated, keep it secret. The subject then sends the public key along with other information to the RA.
- Secondly, the RA can generate a key pair on-behalf the subject.
  - This can happen in cases where either the user is not aware of the technicalitiesinvolved in the generation of a key pair.
  - The RA sends the private key which is generated, to the subject. The RA keepsthe public key.

Step 2: Registration:

- This step is required only if the user generates the key pair in the first step. If the RA generates the key pair on the user's behalf, this step will also be a part of the first step itself.
- Assuming that the **user has generated the key pair**, the user now sends the public key and the associated registration information (e.g. subject name, as it is desired to appear in the digital certificate) and all the required evidence about himself/herself to the RA.
- For this, the software provides a wizard in which the user enters all the data then submits it. This data then travels over the network/Internet to the RA. This format for the certificate requests has been is called **Certificate Signing Request (CSR).** This is one of the **Public Key Cryptography Standards (PKCS),**

- Note that the user must not send the private key to the RA—the user must keep it securely.

Step 3: Verification:

After the registration process is complete, the RA has to verify the user's credentials. This verification is in two respects, as follows.

1. Firstly, the RA needs to verify the user's credentials which are provided by the user.
    - If the user were actually an **organization** then the RA would perhaps like to check the business records, historical documents and credibility proofs.
    - If it is an **individual** user then simpler checks are in call, such as verifying the postal address, email id, phone number, passport or driving-license details can be sufficient.
2. Secondly, check is to ensure that the user who is requesting for the certificate, whether he/she possesses the private key or not corresponding to the public key that is sent to the RA.

This is very important, because there must be a record that the user possesses the private key corresponding to the given public key. Otherwise, this can create legal problems. This check is called the **Proof Of Possession (POP)** of the private key.

How can the RA perform this check? There are many approaches to this, the chief ones being as follows.

- The RA can demand that the user must digitally sign his/her Certificate Signing Request (CSR) using his/her private key. If the RA can verify the signature (i.e. de-sign the CSR) correctly using the public key of the user, the RA can believe that the user indeed possesses the private key.
- Alternatively, the RA can create a random number challenge; encrypt it with the user's public key and send the encrypted challenge to the user. If the user can successfully decrypt the challenge using his/her private key, the RA can assume that the user possesses the right private key.
- Thirdly, the RA can actually generate a dummy certificate for the user, encrypt it using the user's public key and send it to the user. The user can decrypt it only if he/she can decrypt the encrypted certificate, and obtain the plain-text certificate.

Step 4: Certificate Creation:

- Assuming that all the steps so far have been successfully done, and then RA passes on allthe details of the user to the CA.
- The CA does its own verification (if required) and creates a digital certificate for the user.
- The creation of certificate as per the X.509 standard.
- The CA sends the certificate to the user, and also retains a copy of the certificate for itsown record.
- The CA's copy of the certificate is maintained in a **certificate directory.** This is a centralstorage location maintained by the CA.

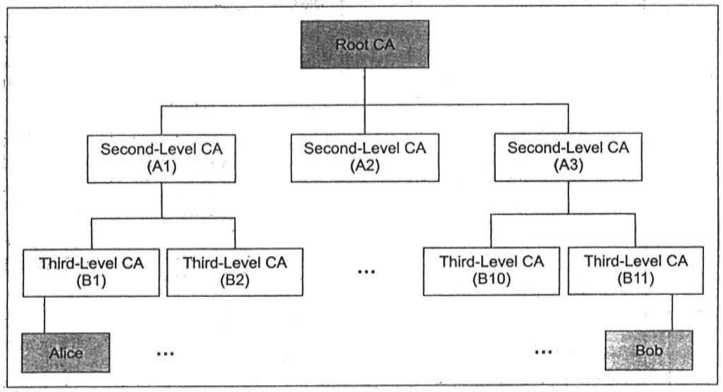
Certificate Hierarchies and Self-signed Digital Certificates:

Certificate hierarchy relieves the root CA from having to manage all the possible digital certificates.

As a substitute, the root CA can hand over this job to the second-level CAs. This hand over can happen region-wise. E.g. one second level CA could be responsible for the Western region, another for the Eastern region, a third one for the Northern region, and a fourth one for the Southern region, etc.). Each of these second-level CAs could appoint third-level CAs state-wise within that region. Each third-level CA could hand over its responsibilities to a fourth-level CA city-wise, and so on.
The root CA signs its own certificate. This certificate of the root CA is called **self-signed certificate.**

Cross-Certification

- It is quite possible that user A and user B live in different countries.
- This would mean that their root CAs may be different. Because generally each countryappoints its own root CA. In fact, one country can have multiple root CAs as well.
- For instance, the root CAs in the US are VeriSign, Thawte, and the US Postal Service. In such cases, there is no *single* root CA, which can be trusted by all the concerned parties.
- In our example, why should user A—a Japanese national, trust user B's root CA—a US-based organization?
- Cross-certification allows CAs and end users from different PKI domains to interact called cross certification**.**



Certificate Revocation:

Reasons for revocation:

- If the private key corresponding to the public key is stolen.
- The CA realizes that it had made mistake while issuing the certificate.
- The certificate holder leaves a job and the certificate was issued specifically while thePerson was employed in that job.
- It checks: Online revocation status, Off-line revocation status

Private Key Management:

To protect the private key by means:-

- Password protection
- Tokens
- Biometrics
- Smart Cards
- Apart from these, the private key used for digital signing must be destroyed. In contrast,the Private key used for encryption/decryption must be archived.
  - In case of certificate expiration, the user needs to update its key.
  - The CA should maintain history of certificates & keys to prevent any legalproblems.

The PKIX (Public Key Infrastructure X.509) model:

(a) Registration:
In this process the end-entity (subject/user) registers to a CA. Usually this is via an RA.

(b) Initialization:
Process to verify that the end-entity is talking to the right CA.

(c) Certification:
In this step, the CA creates a digital certificate for the end-entity and returns it to the end-entity and keeps a copy for its own records.

(d) Key-Pair Recovery:
Keys used for encryption of some old documents may be required to be recovering datafor decrypting. Key archival and recovery services can be provided by a CA.

(e) Key Generation:
PKIX specifies that the end-entity should be able to generate private-and public-keypairs, or the CA/RA should be able to do this for the end-entity.

(f) Key Update:
This allows issuing new key pair from old one by the automatic renewal of digitalcertificates. But there is a provision for issuing digital certificate manually.

(g) Cross-certification:
In this, each end-entity that are certified by different CAs can cross-verify each other.

(h) Revocation:
PKIX provides support for the checking of the certificate status in two modes: online oroffline.

PKIX Architectural Model:

- **X.509 v3 Certificate & v2 Certificate Revocation List profiles**:
  Lists the use of various options while describing extensions of a digital certificate.
- **Operational Protocol**:
  Defines the underlying protocols that provide the transport mechanism.
- **Management Protocol**:
  Enables exchange of information between the various PKI entities and specifies thestructure & details of PKI messages.

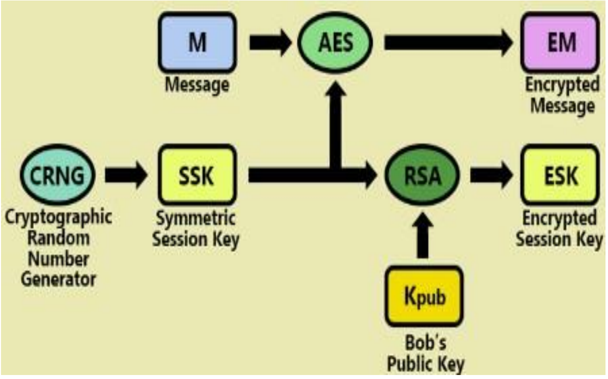
- **Policy outlines**:
  Defines policies for the creation of Certificate Policies & Certificate Practice Statements.
- **Timestamp & Data Certification Services**:
  Both are the trusted third parties that provide services to guarantee the existence ofcertificate & DCS verifies the correctness of data that it receives.

PKCS (Public Key Cryptography Standards)

Standard	**Description**
PKCS#1:	RSA Encryption Standard. Defines rules for calculating digital certificate.
PKCS#2:	RSA Encryption Standard for Message Digest.
PKCS#3:	Diffie-Hellman Key Agreement Standard.
PKCS#4:	NA. Merged with PKCS#1
PKCS#5:	Password Based Encryption(PBE). Defines method to encrypt symmetric key.
PKCS#6:	Extended Certificate Syntax Standard. Defines syntax for extending the basicattribute of an X.509 digital certificate.
PKCS#7:	Cryptographic Message Syntax Standard.
PKCS#8:	Private Key Information Standard.
PKCS#9:	Selected Attribute Types. Defines selected attribute for use in PKCS#6 extendedcertificates.
PKCS#10:	Certificate Request Syntax Standard
PKCS#11:	Cryptographic Token Interface Standard.
PKCS#12:	Personal Information Exchange Syntax Standard.
PKCS#13	Elliptic Curve Cryptography Standard.
PKCS#14	Pseudo –Random Number Generation Standard.
PKCS#15	Cryptographic Token Information Syntax standard.

Digital Envelop:

- A digital envelope is a secure electronic data container that is used to protect a message through encryption and data authentication.
- A Digital Envelope is created by symmetric key algorithm (e.g. AES) and the symmetric key.
- The symmetric key is then encrypted with an asymmetric key algorithm (e.g. RSA) and the recipient's public key.



CHAPTER-5

INTERNET SECURITY PROTOCOL

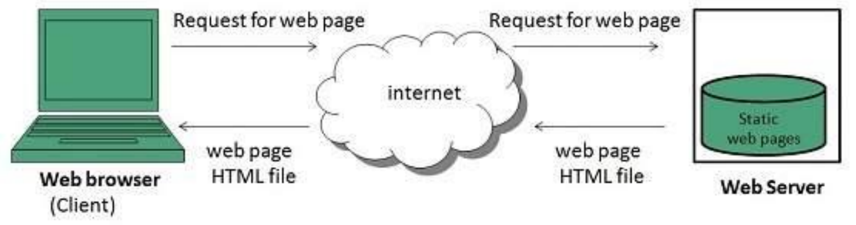
Basic concept

In computing, Internet Protocol Security (IPSec) is a secure network protocol suite that authenticates and encrypts the packets of data to provide secure encrypted communication between two computers over an Internet Protocol network. It is used in virtual private networks (VPNs).

Static Web page

Static web pages are also known as flat or stationary web page. They are loaded on the client's browser as exactly they are stored on the web server. Such web pages contain only static information. User can only read the information but can't do any modification or interact with the information.

Static web pages are created using only HTML. Static web pages are only used when the information is no more required to be modified.



Dynamic Web page

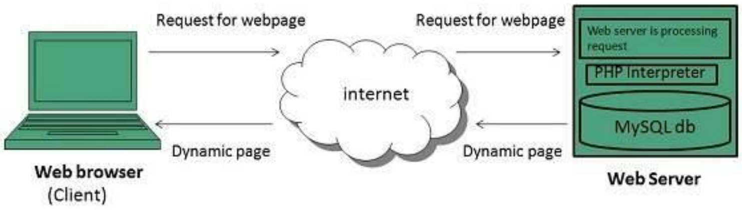
Dynamic web page shows different information at different point of time. It is possible to change a portion of a web page without loading the entire web page. It has been made possible using **Ajax** technology.

Server-side dynamic web page

It is created by using server-side scripting. There are server-side scripting parameters that determine how to assemble a new web page which also includes setting up of more client-side processing.

Client-side dynamic web page

It is processed using client side scripting such as JavaScript. And then passed in to **Document Object Model (DOM).**



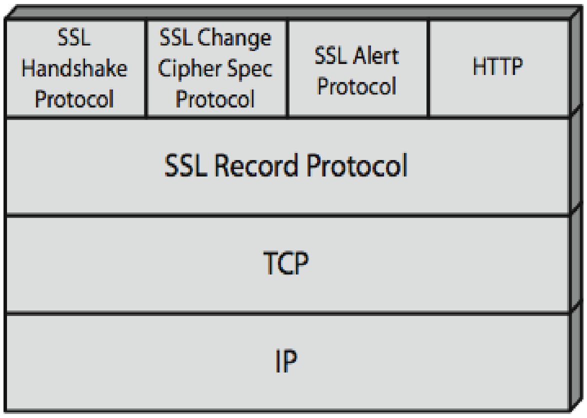
A **static web page** (sometimes called a **flat page** or a **stationary page**) is a web page that is delivered to the user's web browser exactly as stored,[1] in contrast to dynamic web pages which are generated by a web application.

Consequently, a static web page displays the same information for all users, from all contexts, subject to modern capabilities of a web server to negotiate content-type or language of the document where such versions are available and the server is configured to do so.

Secure Socket Layer

- ➢ World's most widely used security mechanism on the Internet.
- ➢ Secures communication between a client and a server.
- ➢ Located between the Application and Transport Layers of TCP/IP protocol suite.

SSL Architecture:



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.

The SSL Record Protocol provides basic security services to various higher-layer protocols.

The HTTP which provides the transfer service for Web client/server interaction, can operate on top of SSL.

SSL consists of three higher-layer protocols:

- Handshake Protocol
- the Change CipherSpec Protocol
- Alert Protocol.

SSL consists of one lower-layer protocols:

SSL Record Protocol

SSL Record Protocol Operation:

The SSL Record Protocol provides two services for SSL connection:
Confidentiality: The original data and the MAC are encrypted using secret key cryptography to provide confidentiality.
Message Integrity: The Hash function is applied on compressed data to compute a MAC. This provides integrity.
Fragmentation: each upper layer message is fragmented into block of 214 bytes (16384bytes) or less.
Compression: must be lossless and may not increase the content length by more than 1024 bytes.
Message Authentication Code: it is compute a code over the compressed data. For this purpose a shared secret key is used.
Next, the compressed message plus the MAC are encrypted using symmetric encryption.

Handshake Protocol:

This protocol allows the server and client to authenticate each other.

Used to negotiate an encryption and MAC algorithm and cryptographic keys to be used to encrypt data in an SSL record.

In this protocol several msg. are exchanged between client and server.

All of these messages have a fixed format with three fields.

Change CipherSpec protocol:

The cryptographic secret (encrypted data) is generated, once the handshake protocol is over.

It is used to signal that cryptographic secret is ready to use.

This protocol consists of a single message, which consists of a single byte with the value 1.

The sole purpose of this message is to cause the pending state to be copied to into the current state.

Alert Protocol:

The alert protocol is Used to signal errors or any abnormal condition.

Each message in this protocol consists of two bytes.

The first byte takes the value warning(1) or fatal(2) to convey the severity of the Message.

In case of fatal error, the connection is immediately terminated.

SECURE HYPER TEXT TRANSFER PROTOCOL (SHTTP)

- The Secure Hyper Text Transfer Protocol (SHTTP) is a set of security mechanisms defined for protecting the Internet traffic.
- This includes the data-entry forms and Internet-based transactions.
- The services offered by SHTTP are quite similar to those of SSL. However, SSL has become highly successful—SHTTP has not.

- SHTTP works at the application layer, and so it is tightly coupled with HTTP, unlike SSL.
- SHTTP supports both authentication and encryption of HTTP traffic between the client and the server.
- The key difference between SSL and SHTTP is that SHTTP works at the level of individual messages.
- It can encrypt and sign individual messages. On the other hand, SSL does not differentiate between different messages.
- It aims at making the connection between a client and the server, regardless of the messages that they are exchanging.
- Not as popular as SSL
- Almost obsolete.

SET (Secure Electronic Transaction):

- SET is an open encryption and security specification designed to protect credit cardtransactions on the internet.
- It is developed by VISA and MasterCard for securing credit card transactions overinsecure networks, specifically, the internet.
- SET was not itself a payment system. It provides a set of security protocols and formatsthat enable users to do credit card payment on an open network in secure fashion.
- Merchant does not get to know the credit card details of the cardholder.
- It requires software set up on both client and server.

SET specification:

- Uses public key cryptography and digital certificates for validating both consumers andmerchants.
- It provides the four security requirements – confidentiality, data integrity, user andmerchant authentication, and consumer non-repudiation.

Architecture OR participants of SET:

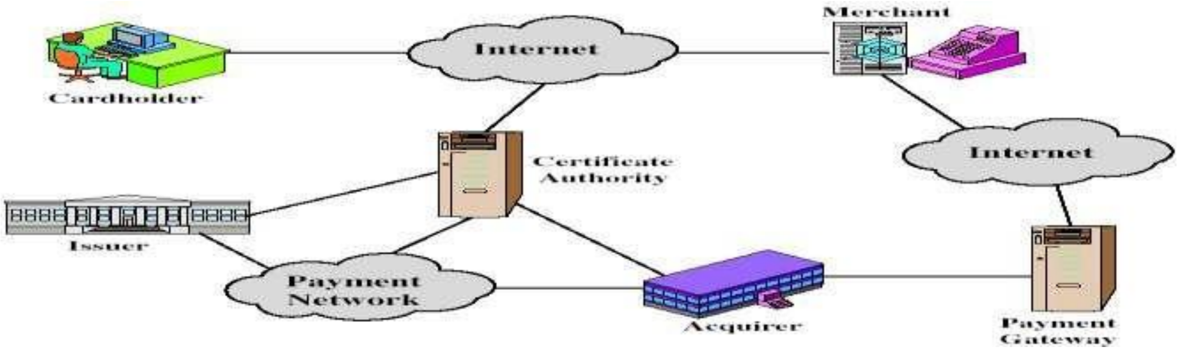
The SET protocol coordinates the activities of:

1. Card Holder (Consumer) – he is the buyer who is the registered holder of the credit card.
2. Card Issuer(Consumer’s Bank) – bank that issues the credit card to card holder.
3. Merchant – refers to the seller who is connected to an acquirer.
4. Acquirer (Merchant’s Bank) – bank that serves as an agent to link a merchant to multipleissuers(customer’s banks).
5. Payment Gateway – this is connected to acquirer. It is situated between the SET systemand the financial network of the credit card system for processing the credit card payment.
6. Certification Authority (CA) – Issues digital signatures to concerned parties.

Working/ Process of SET

Before using SET, both the cardholder and the merchant must register with the CA. After theregistration process, the working of SET involves many steps, which are as follows:

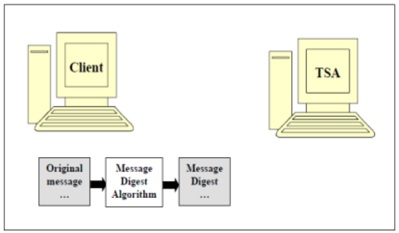
l. The customer browses the merchant's website to evaluate the products offered by the merchant. He or she then selects the products to be purchased and adds them to the shopping cart.
2. The customer then uses a single message to communicate with the merchant and payment gateway. The message has two parts, namely, *purchase order*, which is used by the merchant, and *card information*, which is used by the merchant's bank (acquirer).
3. The card information is then forwarded to the acquirer authorization.
5. If the purchase is authorized, the issuer sends the authorization to the acquirer.
6. A copy of the authorization is also forwarded to the merchant.
7. The merchant completes the order and informs the customer about it.
8. Merchant captures the transaction from its bank.
9. Finally, the credit card invoice is printed by the issuer and provided to the customer.



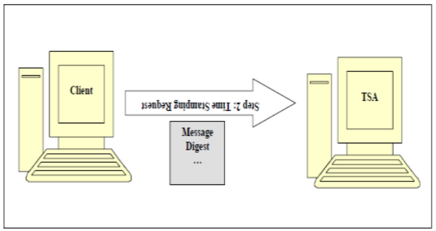
Time Stamping Protocol (TSP)

- ➢ It is a Digital version of a notary service.
- ➢ It proves that a document existed at a specific date and time.
- ➢ Time Stamping Authority (TSA) is used.

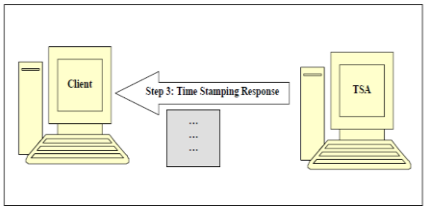
Time Stamping Protocol – Step



Time Stamping Protocol – Step 2



Time Stamping Protocol – Step 3



CHAPTER-6

USER AUTHENTICATION

Authentication Basics:

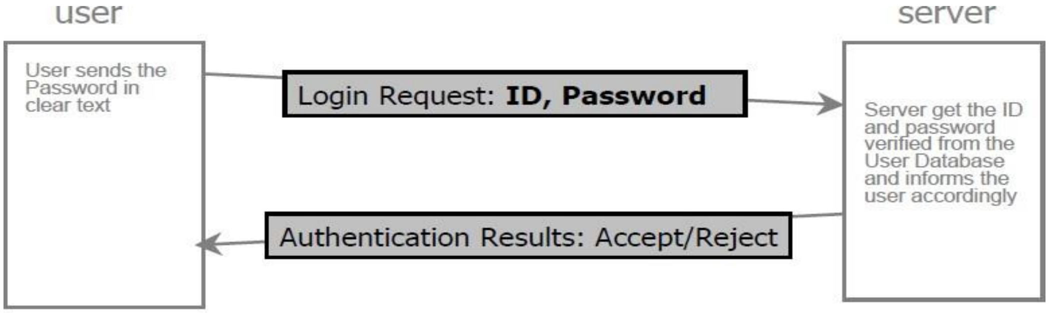
Authentication

- Proof of identity or we can say that "who is Who".
- It is the process of giving someone identity so that he or she can access that particular application or data.
- For e.g.: giving identity-card to a student of an institute.
- Authentication is the first step in any cryptographic solution
  - –Because unless we know who is communicating, there is no point in encryption what is beingcommunicated.
- Authentication is any process by which a system verifies the identity of a user who wishes to access it.
- Establish trust before communication takes place.

Passwords:

- A password is a string of alphabets, numbers and special characters, which is supposed to be known only to theentity (usually person) that is being authenticated.
- Password Based Authentication
  - –Clear Text Passwords is the Simplest Password based Authentication Mechanism.
- How it works?
  - –Prompt for user ID and Password
  - –User enters user ID and Password
  - –User ID and Password Validation i.e user-id and password are validated.
  - –Authentication Result: Inform user accordingly.

Password Based Authentication:


user
server
User sends the Password in clear text
Login Request: ID, Password
Server get the ID and password verified from the User Database and informs the user accordingly
Authentication Results: Accept/Reject

User Authentication using Clear Text Password

Problems with Clear Text/plain-text Passwords:

i)Database contains Passwords in clear text

•It is advised that password should not be stored in clear text in databases.

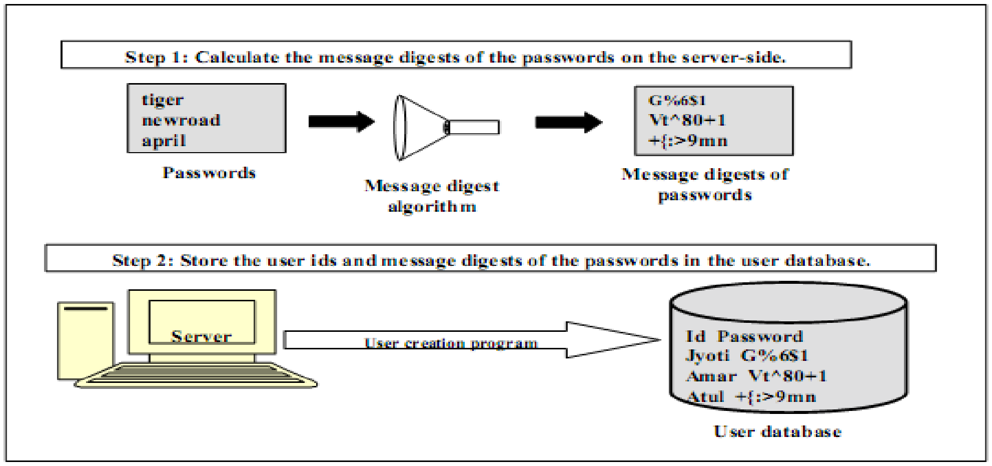
•The passwords should be stored in encrypted form in database.

ii)**Password travel in clear text/ plain-text from user's computer to the server**

•If the attacker breaks into the communication link, he can easily obtain the clear textpassword.

Message Digests of the Passwords

Message Digests of Passwords


Step 1: Calculate the message digests of the passwords on the server-side.
tiger
newroad
april
Passwords
Message digest algorithm
G%6$1
Vt^80+1
+{:>9mn
Message digests of passwords
Step 2: Store the user ids and message digests of the passwords in the user database.
Server
User creation program
Id Password
Jyoti G%6$1
Amar Vt^80+1
Atul +{:>9mn
User database

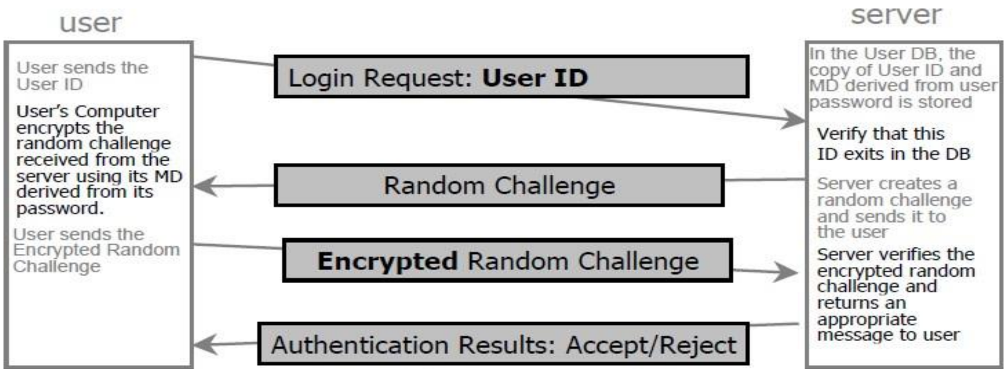
•Adding Randomness

To improve the security and to detect a replay attack we need to add a bit of randomness to the earlier schemes.

Steps

1. Storing Message Digests as derived passwords in the user database.
2. User sends a login request
3. Server creates a random Challenge
4. User Signs the Random Challenge with the Message Digest of the Password
5. Server Verifies the Encrypted Random Challenge from the user

Server returns an appropriate message back to the user


user
server
User sends the User ID
User's Computer encrypts the random challenge received from the server using its MD derived from its password.
User sends the Encrypted Random Challenge
Login Request: User ID
Random Challenge
Encrypted Random Challenge
Authentication Results: Accept/Reject
In the User DB, the copy of User ID and MD derived from user password is stored
Verify that this ID exits in the DB
Server creates a random challenge and sends it to the user
Server verifies the encrypted random challenge and returns an appropriate message to user

Authentication Tokens:

•It is an extremely useful alternative to a password
•These small devices are usually of the size of a small key chain.
•Usually an authentication Token has the following features
–Processor
–LCD for displaying outputs
–Battery
–Optionally a small keypad for entering information
–Optionally a real-time clock

Each Authentication Token is pre-programmed with a unique number called as a random seed or just**seed.**

Step Involved in Authentication Token:

1. Creation of a Token

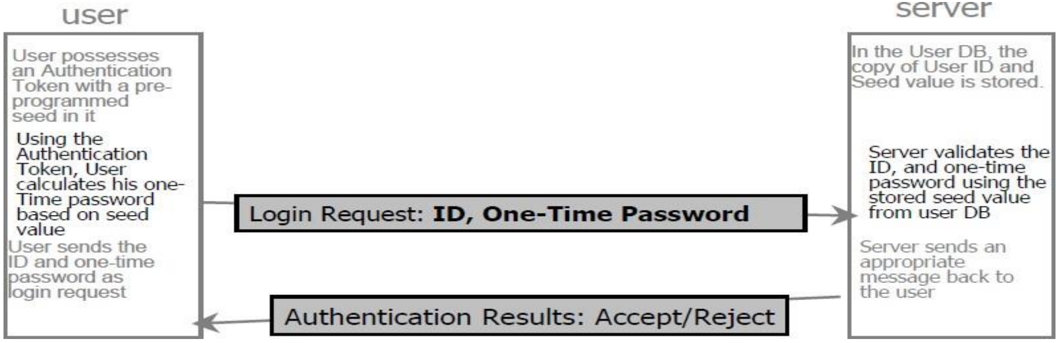
–Created by the Authentication servers that are designed to use with authentication tokens.
–A unique value i.e. a seed is automatically placed or pre-programmed inside each token by the server.
–Server also keeps a copy of the seed against the user ID in the user database.
–Seed can be conceptually considered as a user password.
–Difference is that the user password is known to the user, seed value remains unknown to the user.

2. Use of the Token

–An Authentication Token automatically generates pseudorandom numbers called **one- time passwords**.
–One-time passwords are generated randomly by authentication tokens using seed value.
–When a user wants to be authenticated by any server, the user will get a screen to enter user ID and the latest one-time password.
–The users enter its ID and gets is latest one-time password from the authentication token.
–The user ID and password travels to the server as a part of the login request
–Server verifies using some mechanism that this one-time password is created using the valid seed value.

3: Server Returns an Appropriate Message back to the User

Finally, the server sends an appropriate message back to the user, depending on whether the previous operations yielded success or failure.


user
User possesses an Authentication Token with a pre-programmed seed in it
Using the Authentication Token, User calculates his one-Time password based on seed value
User sends the ID and one-time password as login request
server
In the User DB, the copy of User ID and Seed value is stored.
Server validates the ID, and one-time password using the stored seed value from user DB
Server sends an appropriate message back to the user
Login Request: **ID, One-Time Password**
Authentication Results: Accept/Reject

Authentication Token Types:

1. Challenge/Response Tokens
2. Time-based Tokens

1. Challenge/Response Tokens:

Step 1: User Sends a Login Request.

In this technique, the user sends the login request only with his/her user id (and not the one-timepassword).

Step 2: Server Creates a Random Challenge

If the user id is valid, the server now creates a random challenge (a random number, generated using a pseudo-random number generation technique), and sends it back to the user.

Step 3: User Signs the Random Challenge with the Message Digest of the Password

This request is then sent to the server as the login request.

Step 4: Server Verifies the Encrypted Random Challenge Received from the User

The server receives the random challenge, which was encrypted with the seed by the user's authentication token. In order to verify that the random challenge, the server must perform an identical operation.

Step 5: Server Returns an Appropriate Message Back to the User

Finally, the server sends an appropriate message back to the user, depending on whether the operation is success or failure.

2. Time-based Tokens:

Step 1: **Password Generation and Login Request:**

The seed value and the system time of token, together perform cryptographic algorithm to generate a password automatically.

Step 2: **Server-side Verification:**

The server receives the password. It also performs an independent cryptographic function on the user's seed value and the current system time to generate its version of the password. If the two values match, it considers the user as a valid one.

Step 3: **Server Returns an Appropriate Message Back to the User:**

Finally, the server sends an appropriate message back to the user, depending on whether the operation is success or failure.

Certificate Based Authentication:

This is based on the Digital Certificates of the user.

•In PKI, the digital certificates are used for secure digital transactions.

•This can be re-used for user authentication as well.

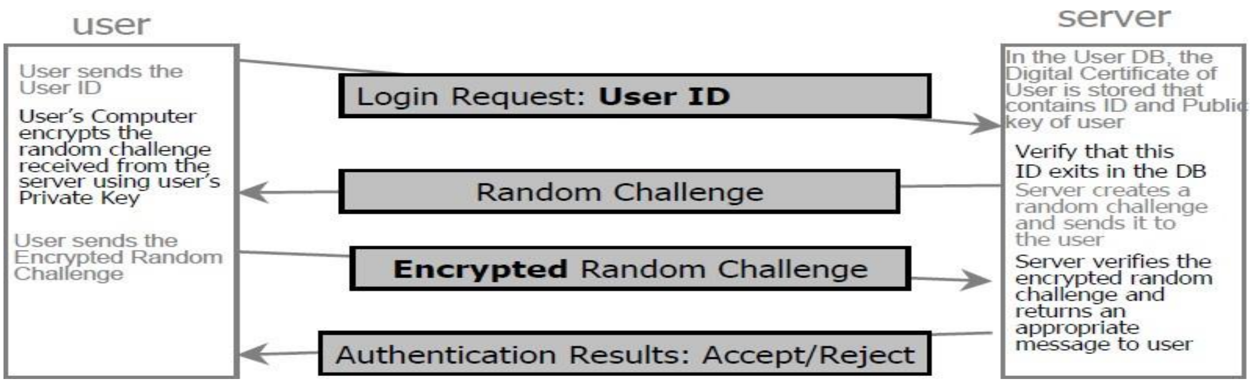
•This is a stronger mechanism as compared to password based authentication

How does Certificate Based Authentication works?

1. Creation, Storage and Distribution of Digital Certificates.

–Certificates are created by CA (Certificate Authority), sent to user as well as a copy to the server.

2. Login Request
–User sends its ID only.
3. Server Creates a Random Challenge
–User ID validity is checked.
–Sends random challenge in plain text to user.
4. User Signs the Random Challenge
–User signs the random challenge received from Server by using its Private Key
–User's private key is stored in a file in user computer
–To access its private key file, user has to give a correct password
–User sends the signed random challenge to the server
5. Server returns an appropriate message back to the user


user
server
User sends the User ID
User's Computer encrypts the random challenge received from the server using user's Private Key
User sends the Encrypted Random Challenge
Login Request: User ID
Random Challenge
Encrypted Random Challenge
Authentication Results: Accept/Reject
In the User DB, the Digital Certificate of User is stored that contains ID and Public key of user
Verify that this ID exits in the DB
Server creates a random challenge and sends it to the user
Server verifies the encrypted random challenge and returns an appropriate message to user

Smart Cards:

- A smart card is a security token that has an embedded chip.
- Smart cards are typically the same size as a driver's license and can be made out of metal orplastic.
- They connect to a reader either by direct physical contact (also known as chip and dip) orthrough a short-range wireless connectivity standard such as Near Field Communication (NFC).
- It is Portable.
- Used to perform cryptographic mechanisms

Use of Smart Cards:

- The use of Smart Cards is related to Certificate Based Authentication
- This is because the smart cards allows the generation of public-private key pairs within the card
- They also support the storage of digital certificates within the card.
- The private key always remain in the smart card in a secure fashion
- The public key and the certificate is exposed outside
- Also the smart cards are capable of performing cryptographic functions such as encryption, decryption,message digest creation and signing within the card
- T
  hus during the certificate based authentication, the signing of random challenge sent by the server can be performed inside the card

Problems and issues in Smart Cards:

- Lack of standardization and inter-operability between smart cards vendors
- Smart card reader are not yet a part of a desktop computer like hard disk drive or floppy drives
- Non-availability of smart card reader driver software
- Non-availability of smart card aware cryptographic service software
- cost of smart cards and card reader is high.

Biometric Authentication:

Definition:
Biometrics refers to the automatic identification of a person based on his or her physiological orbehavioral characteristics.

- A biometric device works on the basis of some human characteristics, such as fingerprints,voice orthe pattern of lines in the iris of your eye
- The user database contains a sample of user's biometric characteristics
- During the authentication, the user is required to provide another sample of the users' biometriccharacteristic.
- This is matched with the one in the database, and if the two samples are same, the user is considered tobe a valid one.
- The samples produced during every authentication process can vary slightly. (e.g. cuts on the finger)
- An approximate match can be acceptable.

Any Biometric Authentication System defines two configurable parameters:

False Accept Ratio (FAR):

•It is a measurement of the chance that a user who should be rejected is actually accepted byasystem as good enough.

–**False Reject Ratio (FRR):**

•It is a measurement of the chance that a user who should be accepted as valid is actuallyrejected by a system as not good enough

•Thus FAR and FRR are exactly opposite to each other.

Biometric characteristics:

1) Physiological
2) Behavioral

Physical biometrics:

- Fingerprint
- Facial recognition/face location
- Hand geometry
- Iris scan
- Retina scan

Fingerprint recognition

- A live acquisition of a person's fingerprint.
- Dots (very small ridges),
- Space between two temporarily divergent ridges),
- Spurs (a notch protruding from a ridge),

- Bridges (small ridges joining two longer adjacent ridges), crossovers (two ridges that cross eachother).

Facial Recognition
1. Capture image
2. Find face in image
3. Extract features (store template)
4. Compare templates
5. Declare matches

Hand Geometry

Hand or finger geometry is an automated measurement of many dimensions of the hand and fingers.

Iris recognition

Iris scanning measures the iris pattern in the colored part of the eye.

Retina recognition

Images back of the eye and compares blood vessels with existing data.

<u>Behavioral biometrics</u>

- Speaker/ voice recognition.
- Signature/ handwriting.
- Keystroke/ patterning.

Speaker / Voice Recognition

- Voice or speaker recognition uses vocal characteristics to identify individuals using a pass-phrase.
- A telephone or microphone can serve as a sensor.

Signature Verification

- An automated method of measuring an individual’s signature.
- This technology examines speed, direction, and pressure of writing; the time that the stylus is inand out of contact with the “paper’’.

Keystroke dynamics

- It is an automated method of examining an individual’s keystrokes on a keyboard.
- This technology examines such dynamics as speed and pressure, the total time taken to typeparticular words, and the time elapsed between hitting certain keys.

APPLICATIONS:

- Prevent unauthorized access to ATMs, Cellular phones Desktop PCs.
- Criminal identification.
- In automobiles biometrics can replace keys with keyless entry devices.
- Airport security.

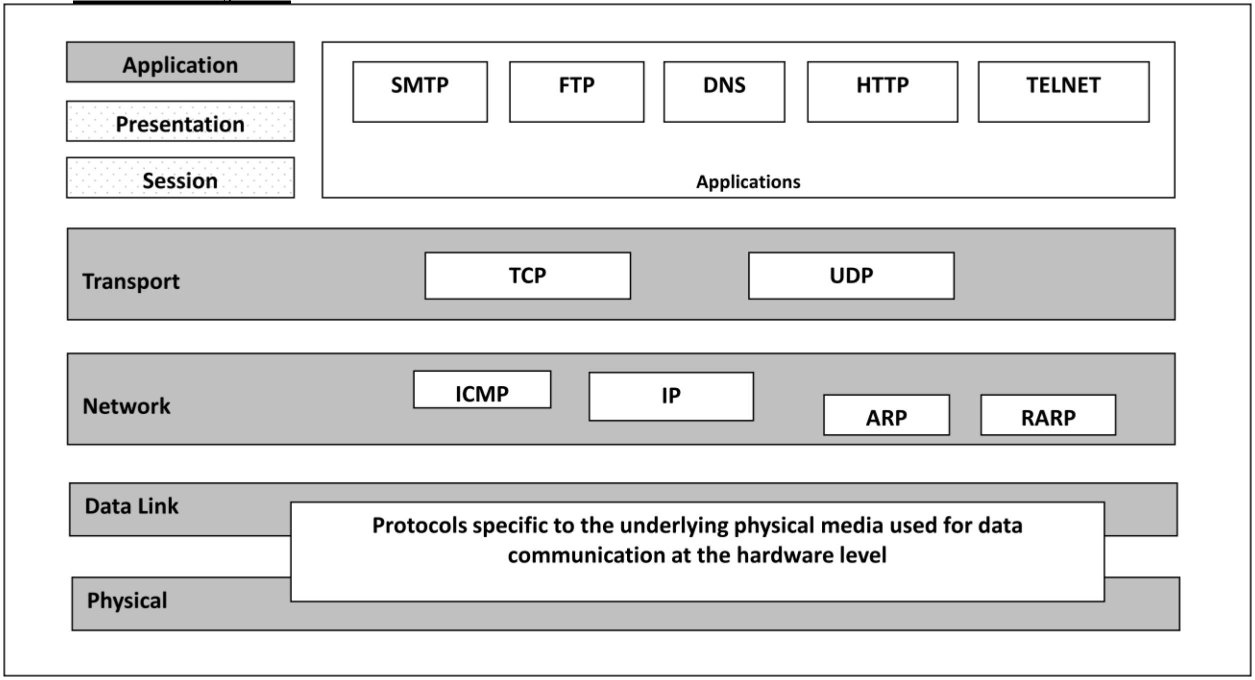
CHAPTER-7

NETWORK SECURITY AND VPN

TCP/IP Protocol Suite:

- The TCP/IP protocol suite was developed prior to the OSI model. Therefore, the layers in the TCP/IP protocol suite do not exactly match those in the OSI model.
- **TCP/IP protocol suite is made of five layers: Application Layer, Transport Layer,Internet Layer, Network Access Layer**
- *TCP/IP* is a hierarchical protocol made up of interactive modules, each of which provides a specific functionality; however, the modules are not necessarily interdependent.
- At the transport layer, *TCP/IP* defines three protocols: **Transmission Control Protocol (TCP), User Datagram Protocol (UDP), and Stream Control Transmission Protocol (SCTP).**
- At the Internet layer, the main protocol defined by TCP/IP is the **Internet Protocol (IP);**there are also some other protocols that support data movement in this layer.

TCP/IP Layers:



TCP segment format:

A packet in TCP is called a **segment.** The segment consists of a header of 20 to 60 bytes, followedby data from the application program. The header is 20 bytes if there are no options and up to 60 bytes if it contains options.

Source port address:

This is a 16-bit field that defines the port number of the application program in the host that is sending the segment. This serves the same purpose as the source port address in the UDP.

Destination port address:

This is a 16-bit field that defines the port number of the application program in the host that is receiving the segment. This serves the same purpose as the destination port address in the UDP.

Sequence number:

This 32-bit field defines the number assigned to the first byte of data contained in this segment. As TCP is a stream transport protocol. To ensure connectivity, each byte to be transmitted is numbered. The sequence number tells the destination which byte in this sequence is the first byte in the segment. During connection establishment each party uses a random number generator to create an **initial sequence number** (ISN), which is usually different in each direction.

Acknowledgment number:

This 32-bit field defines the byte number that the receiver of the segment is expecting to receive from the other party. If the receiver of the segment has successfully received byte number *x* from the other party, it Returns *x*+1 as the acknowledgment number.

Header length:

This 4-bit field indicates the number of 4-byte words in the TCP header. The length of the header canbe between 20 and 60 bytes. Therefore, the value of this field is always between 5 (5 *4=20) and 15 (15*4=60).

Reserved: This is a 6-bit field reserved for future use.

Control:

This field defines 6 different control bits or flags . One or more of these bits can be set at a time. These bits enable flow control, connection establishment and termination, connection abortion, and the mode of Flags from left to right:

Window size:

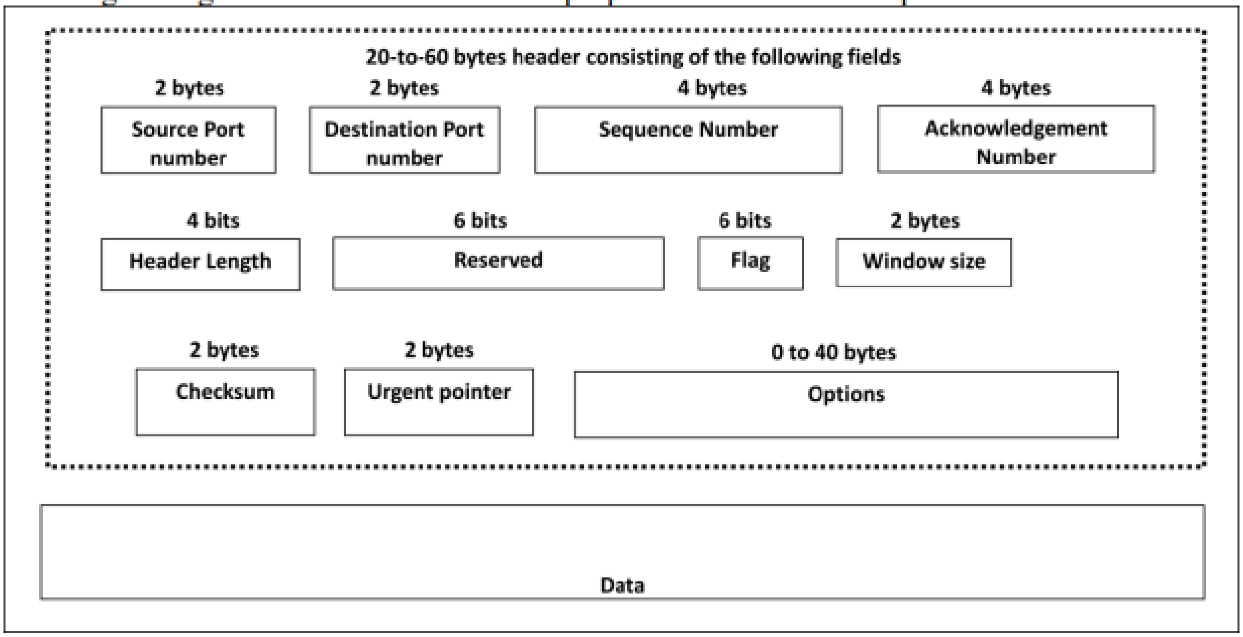
This field defines the window size of the sending TCP in bytes. Note that the length of this field is 16bits, which means that the maximum size of the window is 65,535 bytes.

Checksum:

The 16-bit checksum field is used for error-checking of the header and data.

Urgent pointer:

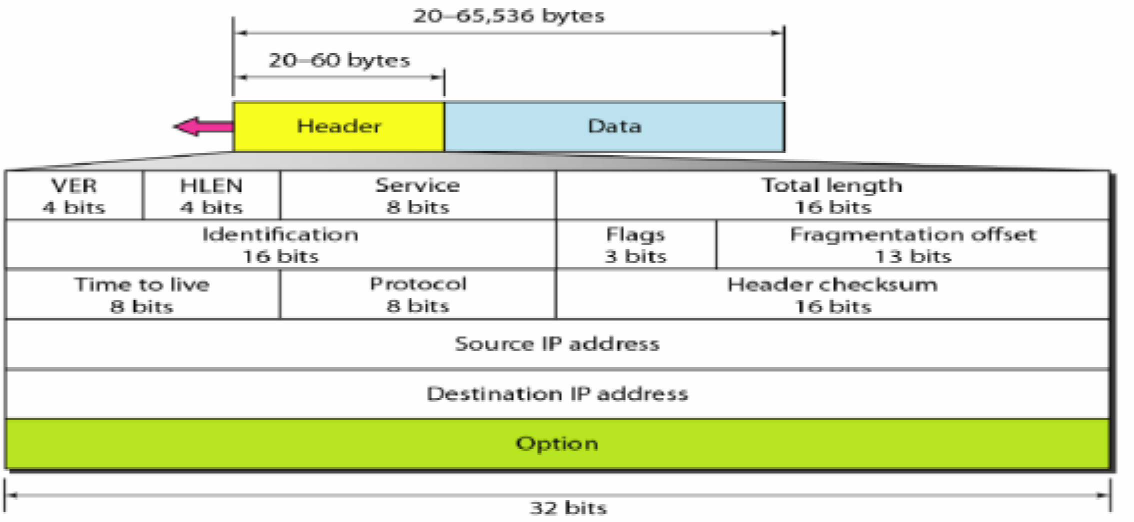
if the URG flag is set, then this 16-bit field is an offset from the sequence number indicating the lasturgent data byte.



IP DATAGRAM FORMAT:

- Packets in the network (internet) layer are called *datagram*.
- A datagram is a variable-length packet consisting of two parts: header and data.
- The header is 20 to 60 bytes in length and contains information essential to routing anddelivery.

IP header format:



Version (VER):

This 4-bit field defines the version of the IP protocol. Currently the version is 4(IPv4).

Header length (HLEN):

This 4-bit field defines the total length of the datagram header in 4-byte words. This field is needed because the length of the header is variable (between 20 and 60 bytes). When there are no options, the header length is 20 bytes, When the option field is at its maximum size(i.e. 60)

Service type (TOS):

It defines how the datagram should be handled. Part of the field was used to define the precedence of the datagram; the rest defined the type of service (low delay, high throughput, and so on).

Total length:

It defines the total length of the datagram including the header in bytes. It is a 16-bit number so maximum IP size is 216 bytes.

Identification:

This 16-bit field identifies a datagram originating from the source host. The combination of theidentification and source IP address must uniquely define a datagram as it leaves the source host.

Flags:

This is a three-bit field. The first bit is reserved (not used). The second bit is called the do not fragment bit. If its value is 1, the machine must not fragment the datagram. If its value is 0, the datagram can be fragmented if necessary. The third bit is called the more fragment bit. If its value is 1, it means the datagram is not the last fragment; there are more fragments after this one. If its value is 0, it means this is the last or only fragment.

Fragmentation offset:

This 13-bit field shows the relative position of this fragment with respect to the whole datagram.

Time to live:

A datagram has a limited lifetime in its travel through an internet. This field was originally designed to hold a timestamp, which was decremented by each visited router. The datagram was discarded when the value became zero.

Protocol:

This 8-bit field defines the higher-level protocol that uses the services of the IP layer. An IP datagram can encapsulate data from several higher level protocols such as TCP, UDP, ICMP, and IGMP. This field specifies the final destination protocol to which the IP datagram should be delivered.

Header Checksum:

This fields represents a value that is calculated using an algorithm covering all the fields in header. This field is used to check the integrity of an IP datagram.

Source address:

This 32-bit field defines the IP address of the source. This field must remain unchanged during the time the IP datagram travels from the source host to the destination host.

Destination address:

This 32-bit field defines the IP address of the destination. This field must remain unchanged during the time the IP datagram travels from the source host to the destination host.

Firewall:

Firewalls can be used to protect a local system or network of systems (Internal Network) fromOut-side networks (Internet) from security threats.

- Special type of router.
- Frequently used to prevent unauthorized internet users from accessing private networksconnected to the internet, especially intranets.
- Controls transmission between internal and external networks. i.e. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria.
- It is essentially a barrier between two networks that evaluates all incoming or outgoing traffic to determine whether or not it should be permitted to pass to the other network. i.e. decides what to allow/disallow.
- Can be implemented in both hardware and software, or a combination of both.
- At broad level, there are two kind of attacks:
    - Most corporations have large amounts of valuable and confidential data in their networks. Leaking of this critical information to competitors can be a great setback.
    - Apart from the danger of the insider information leaking out, there is a great danger of the outside elements (such as viruses and worms) entering a corporate network to create disaster.

Firewall characteristics/ Design Goals of Firewalls:

A firewall is defined as collection of components placed between two networks that collectively haveFollowing characteristics:

All traffic from inside to outside, and vice versa, must pass through the firewall.

This is achieved by physically blocking all access to the local network except via thefirewall.Only authorized traffic, as defined by the local security policy, will be allowed to pass.

Limitations of Firewalls:

The firewall itself must be strong enough, so as to render attacks on it useless.

- Firewalls cannot stop users from accessing malicious websites, making it vulnerable to internal threats or attacks.
- Firewalls cannot protect against the transfer of virus-infected files or software.
- Firewalls cannot prevent misuse of passwords.
- Firewalls cannot protect if security rules are misconfigured.
- Firewalls cannot protect against non-technical security risks, such as social engineering.
- Firewalls cannot stop or prevent attackers with modems from dialing in to or out of the internal network.
- Firewalls cannot secure the system which is already infected.

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

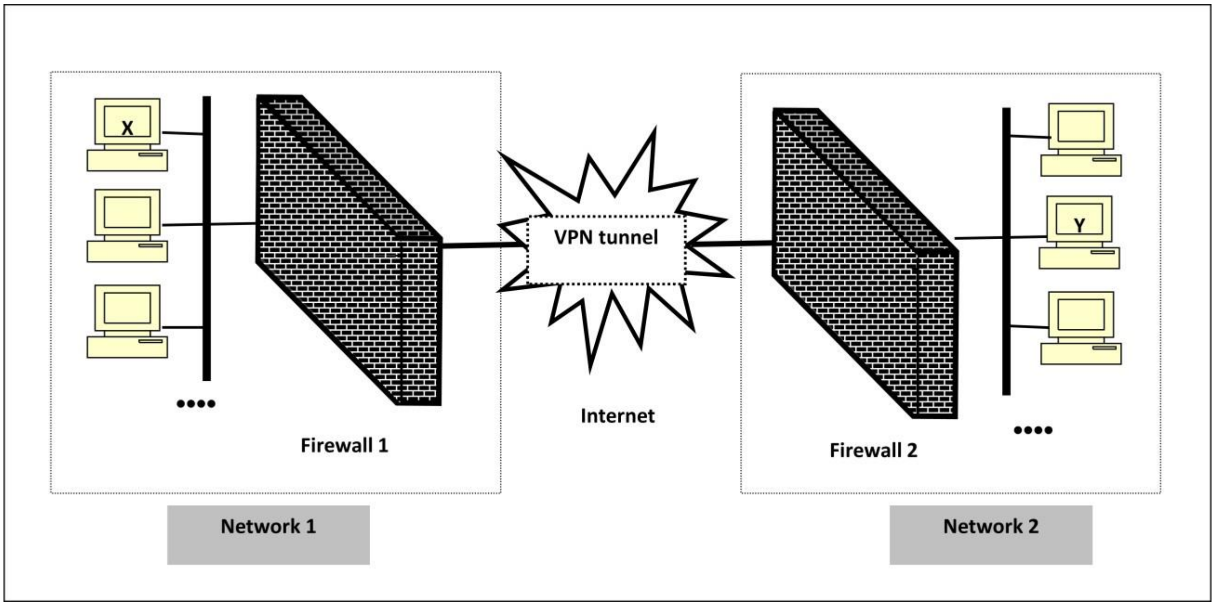
Firewalls are generally of two types: *Host-based* and *Network-based.*

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.

Virtual Private Network (VPN):

- A VPN is thus a mechanism to simulate a private network over a public network, such as theInternet.
- The term *virtual* signifies that it depends on the use of virtual connections.
- These connections are temporary and do not have any Physica1 presence. They are made upof packets.
- Uses the Internet as if it is a private network.
- Far less expensive than a leased line.
- Uses IPSec protocol.

VPN Architecture:

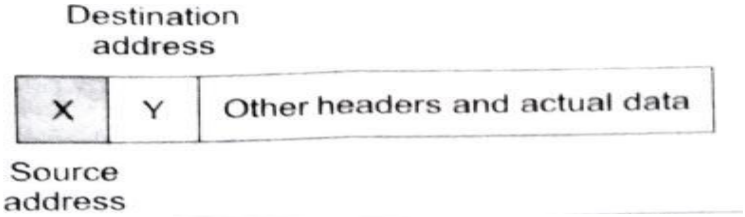


We have shown two networks, *Network* I and *Network* 2. Network l connects to the Internet via a firewall named Firewall I. Similarly, *Network* 2 connects to the Internet with its own firewall 2.

The two firewalls are *virtually* connected to each other via the Internet. We have shown this with the help of a *VPN tunnel* between the two firewalls.

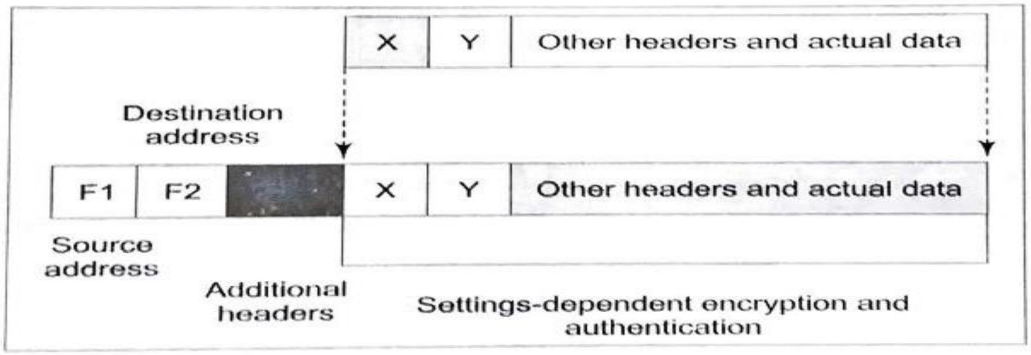
Let us understand how the VPN protects the traffic passing between any two hosts on the two different networks. For this, let us assume that host *X* on *Network* 1 wants to send a data packet to host Y on *Network* 2. This transmission would work as follows.

1.Host X creates the packet, inserts its own IP address as the source address and the IP address of host Y as the destination address. This is shown in figure. It sends the packet using the appropriate mechanism.



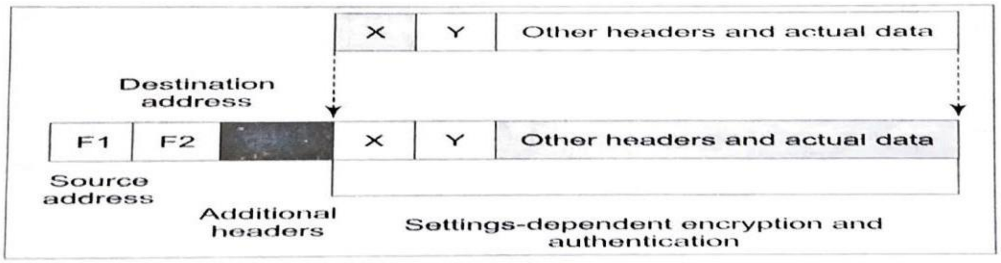
Original packet

2. The packet reaches firewall 1. As we know, firewall 1 now adds new headers to the packet. In these new headers, it changes the source IP address or the packet from that of host X to its own address (i.e. the IP address of Firewall 1, say F1). It also changes the destination IP address of the packet from that of host Y to the IP address of Firewall 2. say F2). This is shown in Fig. It also performs the packet encryption and authentication, depending on the settings and sends the modified packet over the Internet.


X
Y
Other headers and actual data
Destination address
F1
F2
X
Y
Other headers and actual data
Source address
Additional headers
Settings-dependent encryption and authentication

Firewall 1 changes the packet contents

3. The packet reaches firewall1 2 over the internet, via one more routers, as usual, Firewall 2 discards the outer header and performs the outer header and performs appropriates decryption and other cryptographic functions as necessary. This yields the original packets, as was created by host X in step 1. This is shown in fig. It then takes a look the plain text contents of the packets and realizes that the packet is meant for host Y. Therefore, it delivers the packet to host Y.


X
Y
Other headers and actual data
Destination address
F1
F2
X
Y
Other headers and actual data
Source address
Additional headers
Settings-dependent encryption and authentication

Firewall 1 changes the packet contents

IP Security (IPSec) Protocols:

- Before IPSec was initiated, the IP packets were prone to security failure.
- The technology that brings secure communications to the internet protocol layer or networklayer is called IP Security, commonly abbreviated IPSec.
- IPSec is a set of services and protocols that provide a complete security solution for an IPnetwork.
- It is a collection of protocols designed by the Internet Engineering Task Force (IETF) toprovide security in the internet layer.
- It can be used in protecting data flows between a pair of host(host-to-host), between a pair of security gateways(network-to-network), or between a security and a host(network-to-host).

Applications of IP security: (Important)

- IPSec provides the capability to secure communications across a LAN, across private and public WANs, and across the Internet. Examples of its use include:

Secure remote access over the Internet:

- An end user whose system is equipped with IP security protocols can make a local call to an Internet Service Provider (ISP) and gain secure access to a company network. This reduces travelling cost and time wastage of employees and telecommuters.

Secure branch office connectivity over the Internet:

- A company can build a secure virtual private network over the Internet or over a public WAN. This enables connecting all the branches of company. That will save the costs of creating a private network and network management overhead.

Establishing extranet and intranet connectivity with partners:

- IPSec can be used to secure communication with other organizations, ensuring authentication and confidentiality and providing a key exchange mechanism.

Enhancing electronic commerce security:

- Even though some Web and electronic commerce applications have built-in security protocols, the use of IPSec enhances that security.

<u>Benefits of IP security: (Important)</u>

- IPSec can be transparent to end users.
  - There is no need to train users on security mechanisms.
  - No need to issue or cancel keys to and from the users.
- When IPSec is implemented in a firewall or router, it provides strong security that can beapplied to all traffic crossing the perimeter.
  - Traffic within a company or workgroup does not have to use IPSec, thus it minimizethe overhead of security-related processing.
- IPSec in a firewall is resistant to bypass if all traffic from the outside must use IP and thefirewall is the only means of entrance from the Internet into the organization.
- Since IPSec is implemented at network layer, there is no need to make any changes at theupper layers such as transport layer (TCP, UDP) and application layer.
- IPSec can provide security for individual users if needed. Individuals can set up a securevirtual sub-network within an organization for sensitive applications.

IP security services: (Important)

- IPSec provides security services at the IP layer.
- Two protocols are used to provide security:
  - An authentication protocol designated by the header of the protocol, AuthenticationHeader (AH).
  - And a combined encryption/ authentication protocol designated by the format of thepacket for that protocol, Encapsulating Security Payload (ESP).

- Lists the following services:

  1. Access control
  2. Connectionless integrity
  3. Data origin authentication
  4. Rejection of replayed packets (a form of partial sequence integrity)
  5. Confidentiality (encryption)

References:

1. Cryptography & Network security by A. Kahate
2. Cryptography & Network Security Principals and Practices by W.Stallings
3. Cryptography & Information security by Pachghare
4. https://en.wikipedia.org
5. https://nptel.ac.in
6. https://www.geeksforgeeks.org/