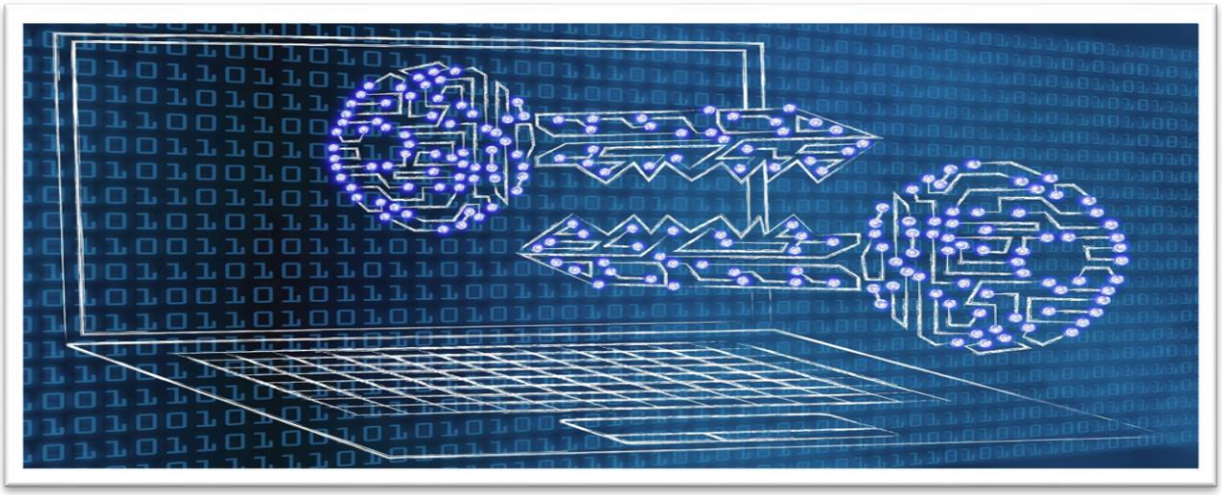
BHADRAK ENGINEERING SCHOOL & TECHNOLOGY
(BEST), ASURALI, BHADRAK

CRYPTOGRAPHY & NETWORK SECURITY (TH-01)

(As per the 2020-21 syllabus of the SCTE&VT, Bhubaneswar, Odisha)



SIX Semester

COMPUTER SCIENCE & ENGG.

Prepared By: Er. B.Moharana

Cryptography & Network Security
Contents

Chapter -01.
Possible attacks on computers

1.1 The need for security

- The network needs security against attackers and hackers.
- Network Security includes two basic securities. The first is the security of data information i.e. to protect the information from unauthorized access and loss. And the second is computer security i.e. to protect data and to thwart hackers.
- Here network security not only means security in a single network rather in any network or network of networks.
- Now our need for network security has broken into two needs. One is the need of information security and other is the need of computer security.

Information security

- On the internet or any network of an organization, thousands of important information is exchanged daily. This information can be misused by attackers. The information security is needed for the following given reasons.

1. To protect the secret information users on the net only. No other person should see or access it.

2. To protect the information from unwanted editing, accidentally or intentionally by unauthorized users.

3. To protect the information from loss and make it to be delivered to its destination properly.

4. To manage the acknowledgement of messages received by any node in order to protect from denial by the sender in specific situations. For example, a customer orders to purchase a few shares of XYZ to the broader market and denies the order after two days as the rates go down.

5. To restrict a user to send some message to another user with the name of a third one. For example a user X for his own interest makes a message containing some favourable instructions and sends it to user Y in such a manner that Y accepts the message as coming from Z, the manager of the organization.

6. To protect the message from unwanted delay in the transmission lines/route in order to deliver it to the required destination in time, in case of urgency. 7. To protect the data from wandering the data packets or information packets in the network for infinitely long time and thus increasing congestion in the line in case the destination machine fails to capture it because of some internal faults.

Computer security

- Computer security means to protect your computer system from unwanted damages caused due to the network.
- One of the major reasons for such damages are the viruses and spywares that can wipe off all the information from your hard disk or sometimes they may be destructive and may cause hardware problems too.
- Certainly the network must be protected from such damage.
- The people who intentionally put such software on the network are called Hackers.
- As the network computers are part of it, so the computer security from Hackers is also a part of network security.
- The needs of computer security from Hackers are as follows:-

> It should be protected from replicating and capturing viruses from infected files.

> It needs proper protection from worms and bombs.

> There is a need for protection from Trojan Horses as they are dangerous enough for your computer.

1.2 Security approach

Trusted System

➢ A trusted system is a computer system that can be trusted to a specified extent to enforce a specified security policy.
➢ Trusted Systems often use the term reference monitor.
➢ It is mainly responsible for all decisions related to access controls.
➢ Naturally following are the expectations from the reference monitor.
A. It should be temper proof.
B. It should always be invoked.
C. It should be small enough so that it can be independently tested.

Security Models An organization can take several approaches to implement its security model. Let us summarize these approaches.

• **No security** In this simplest case, the approach could be a decision to implement no security at all.

• **Security through obscurity** In this model, a system is secure simply because nobody knows about its existence and contents. This approach cannot work for too long, as there are many ways an attacker can come to know about it.

• **Host security** In this scheme, the security for each host is enforced individually. This is a very safe approach, but the trouble is that it cannot scale well. The complexity and diversity of modern sites/ organizations makes the task even harder.

• **Network security** Host security is tough to achieve as organizations grow and become more diverse. In this technique, the focus is to control network access to various hosts and their services, rather than individual host security. This is a very efficient and scalable model.

Security Management Practices

Good security management practices always talk of a security policy being in place. Putting a security policy in place is actually quite tough. A good security policy and its proper implementation go a long way in ensuring adequate security management practices. A good security policy generally takes care of four key aspects, as follows:

• Affordability Cost and effort in security implementation.
• Functionality Mechanism of providing security.
• Cultural issues Whether the policy gels well with people's expectations, working style and beliefs.
• Legality Whether the policy meets the legal requirements.

Once a security policy is in place, the following points should be ensured.
(a) Explanation of the policy to all concerned.
(b) Outline everybody's responsibilities.

(c) Use simple language in all communications.
(d) Establishment of accountability.
(e) Provision for exceptions and periodic reviews.

1.3 Principles of security

The Principles of Security can be classified as follows:

1. Confidentiality:

   The principle of confidentiality specifies that only the sender and receiver will be able to access the contents of a message shared between them. Confidentiality compromises if an unauthorized person is able to access a message. For example, let us consider sender A wants to share some confidential information with receiver B and the information gets intercepted by the attacker C. Now the confidential information is in the hands of an intruder C.

2. Authentication:

   Authentication is the mechanism to identify the user or system or the entity. It ensures the identity of the person trying to access the information. The authentication is mostly secured by using username and password. The authorized person whose identity is pre registered can prove his/her identity and can access the sensitive information.

3. Integrity:

   Integrity gives the assurance that the information received is exact and accurate. If the content of the message is changed after the sender sends it but before reaching the intended receiver, then it is said that the integrity of the message is lost.

4. Non-Repudiation:

Non-repudiation is a mechanism that prevents the denial of the message content sent through a network. In some cases the sender sends the message and later denies it. But the non-repudiation does not allow the sender to refuse the receiver.

5. Access control:

The principle of access control is determined by role management and rule management. Role management determines who should access the data while rule management determines up to what extent one can access the data. The information displayed is dependent on the person who is accessing it.

6. Availability:

The principle of availability states that the resources will be available to authorize parties at all times. Information will not be useful if it is not available to be accessed. Systems should have sufficient availability of information to satisfy the user request.

1.4 Types of attacks

➢ A network attack is an attempt to gain unauthorized access to an organization's network, with the objective of stealing data or performing other malicious activity.

➢ Active Attackers not only gain unauthorized access but also modify data, either deleting, encrypting or otherwise harming it.

➢ Attacks are of 2 types.

- ❖ Passive attacks
- ❖ Active attacks

Passive attacks

● Passive attacks do not involve any modifications to the contents of an original

message.

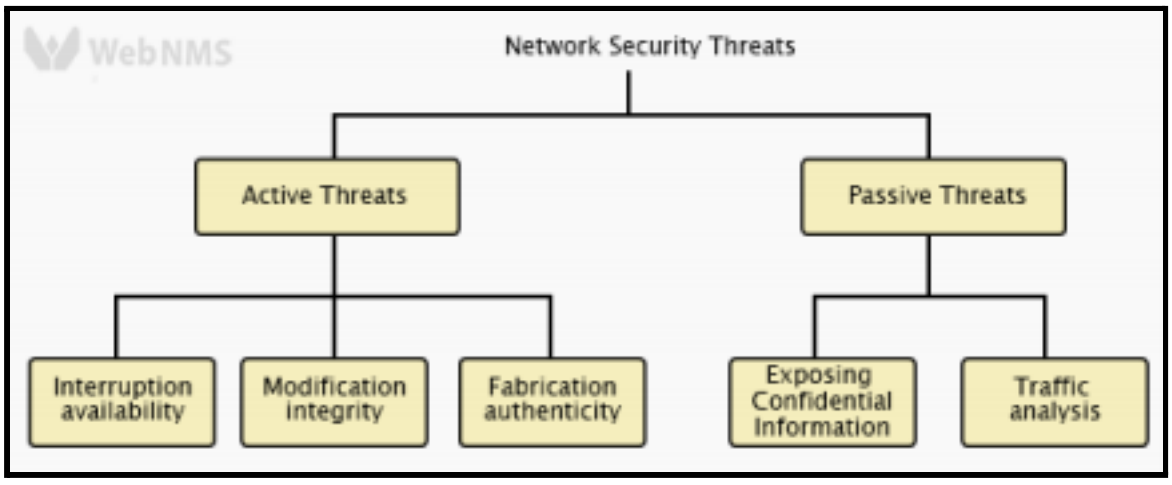
- It is 2 types
  - A. Release of message contents
  - B. Traffic Analysis.

A. Release of message contents

For a release of message content, a telephonic conversation, an E-mail message or a transferred file may contain confidential data. A passive attack monitors the contents of the transmitted data. When the messages are exchanged neither the sender nor the receiver is aware that a third party may capture the messages.

B. Traffic Analysis.

An attacker can analyze network traffic patterns to infer a packet's content, even though it is encrypted.



Active attacks

- ➢ The active attacks are based on modification of the original message or creation of a false message.
- ➢ These attacks can't be prevented easily. However they can be detected with some effort and attempts can be made to recover from them.
- ➢ These attacks can be in the form of Fabrication, modification and interruption.

Fabrication(Masquerade)

Masquerade is caused when an unauthorised entity pretends to be another entity.

Modification

Modification is again divided into 2 types.

1. **Replay attacks-**
   - ➢ A user captures a sequence of events or some data units and resends them.
   - ➢ Suppose user A wants to transfer some amount to user C's bank account . Both A & C have accounts with bank B. User A might send an electronic message to bank B, requesting for funds transfer. User C could capture this message and send a second copy of the same to bank B . Bank B would have no idea that this is an unauthorised message and would treat it as a second and different, funds transfer request from user A. Therefore user C would get the benefit for fund transfer twice: once authorised and once through replay attack.
2. **Alteration of messages**-
   - ➢ It involves some changes to the original message.
   - ➢ For instance suppose user A transfers Rs.1000 to D's account . User C might capture this and change it to transfer Rs.10,000 to his own account.

Interruption(Denial of services)

Denial of service attacks make an attempt to prevent legitimate users from accessing some services, which they are eligible for.

Short Questions with answers

Q1. What do you mean by Trusted System?

➢ A Trusted System is a computer based system that can be trusted to a specified extent to enforce a specified security policy.

➢ It was initially used in the military. These Days it is used in the Banking and Financial sector.

Q2. **Name various types of attacks on Computer system.**

- Basically Attack is of 2 types.
  - ❖ Passive Attack
    - ➢ Release of message contents
    - ➢ Traffic Analysis
  - ❖ Active Attacks
    - ➢ Interruption
    - ➢ Modification
    - ➢ Fabrication

Long Questions

Q1. What are the different principles of security explain with example?

Q2. Explain the different types of attacks that may occur in the field of computer networking.

Chapter-02.
Cryptography Concepts

2.1 Plain text & Cipher text

- **Plain Text :**
  - ➢ The Original message before being transformed is known as plain text.
  - ➢ The plain text is generated at the sender site.

  Ex - Hello

- **Cipher text:**
  - ➢ The message after transformation is known as cipher text.
  - ➢ Ciphertext is transmitted from the sender to the receiver over a network.

  Ex- ifmmp

2.2 Substitution techniques

Substitution techniques

➢ In the substitution cipher technique the characters of a plain text message are replaced by other characters, numbers or symbols.

The substitution technique is classified into two types.

1. Monoalphabetic Cipher
2. Polyalphabetic Cipher

1.Monoalphabetic Cipher

- ➢ Monoalphabetic cipher is a substitution cipher, where the cipher alphabet for each plain text alphabet is fixed, for the entire encryption.
- ➢ In simple words, if the alphabet ‘p’ in the plain text is replaced by the cipher alphabet ‘d’. Then in the entire plain text wherever the alphabet ‘p’ is used, it will be replaced by the alphabet ‘d’ to form the ciphertext.
- ➢ Caesar cipher is an example of monoalphabetic cipher.

Caesar Cipher

- ➢ This is the simplest substitution cipher by Julius Caesar. In this substitution technique, to encrypt the plain text, each alphabet of the plain text is replaced by the alphabet three places after it and to decrypt the ciphertext each alphabet of cipher text is replaced by the alphabet three places before it.

Let us take a simple example:

Plain Text: meet me tomorrow

Cipher Text: phhw ph wrpruurz

Look at the example above, we have replaced ‘m’ with ‘p’ which occurs three places after, ‘m’. Similarly, ‘e’ is replaced with ‘h’ which occurs in three places after ‘e’.

Note: If we have to replace the letter ‘z’ then the next three alphabets counted after ‘z’ will be ‘a’ ‘b’ ‘c’. So, z will be replaced by c.

2.Polyalphabetic Cipher

- ➢ Polyalphabetic cipher is far more secure than a monoalphabetic cipher. A monoalphabetic cipher maps a plain text symbol or alphabet to a ciphertext symbol and uses the same ciphertext symbol wherever that plain text occurs in the message.
- ➢ But a polyalphabetic cipher, each time replaces the plain text with the different ciphertext.

➢ Examples of polyalphabetic ciphers are:

A. Playfair Cipher
B. Hill Cipher
C. One-Time Pad

A. Playfair Cipher

➢ A Playfair cipher is a substitution cipher which involves a 5X5 matrix. ➢ The Playfair cipher is a written code or symmetric encryption technique that was the first substitution cipher used for the encryption of data.

➢ Introduced in 1854, it involved the use of keys that arrange alphabetical letters in geometric patterns in order to encode messages.

➢ The Playfair cipher is also known as the Playfair square.

B. Hill Cipher

➢ Hill cipher is a polyalphabetic cipher introduced by Lester Hill in 1929. The Hill cipher is a polygraphic substitution cipher built on concepts from Linear Algebra. ➢ The Hill cipher makes use of modulo arithmetic, matrix multiplication, and matrix inverses; hence, it is a more mathematical cipher than others.

➢ Polygraphic substitution is a uniform substitution where a block of letters is substituted by a word, character, number, etc.

C. One-Time Pad

➢ The one-time pad cipher suggests that the **key length** should be **as long as the plain text** to prevent the repetition of key. Along with that, the **key** should be **used** only **once** to encrypt and decrypt the single message after that the key should be discarded.

➢ One Time pad suggests a new key for each new message and of the same length as a new message.

So, this is all about the substitution cipher techniques.

2.3 Transposition techniques
Transposition technique

- Transposition Cipher is a cryptographic algorithm where the order of alphabets in the plaintext is rearranged to form a cipher text.
- There are 2 types of transposition techniques.
    1. Rail Fence Technique
    2. Simple Columnar Transposition Technique .

1. Rail Fence Technique

A **Rail Fence** technique involves writing plain text as Sequence of diagonals and then reading it row by row to produce ciphertext.

Example

Plain text- BEST

B	S	
	E	T

Cipher text- BSET

2.Simple Columnar Transposition Technique

Simple columnar transposition technique simply arranges the plain text as a sequence of rows of a rectangle that are read in columns randomly.

Example

Plain text- meet me after the viva.

Key order- 2 4 5 1 3 6

1	2	3	4	5	6
m	e	e	t	m	e
a	f	t	e	r	t
h	e	v	i	v	a

efeteimrvmahetveta

2.4 Encryption & Decryption

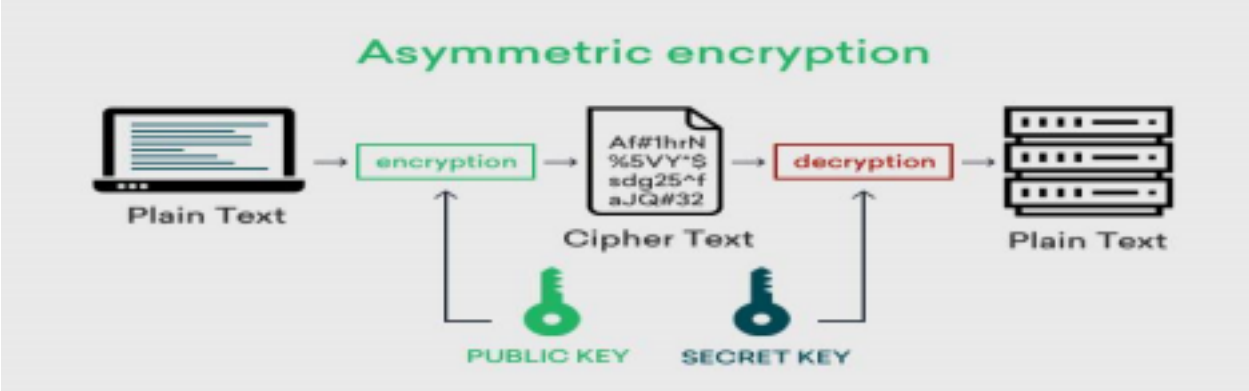
- ➢ The process of encoding plain text messages into cipher text messages is called **Encryption**.
- ➢ The reverse process of converting ciphertext messages back to plain text messages is called **Decryption**.

2.5 Symmetric & Asymmetric key cryptography

Symmetric key Cryptography

- ➢ Symmetric cryptography relies on one shared key that both parties know and can use to encrypt or decrypt data.
- ➢ Establishing the shared key is difficult using only symmetric encryption algorithms, so in many cases, an asymmetric encryption is used to establish the shared key between two parties.
- ➢ It requires (nx(n-1))/2 number of keys to connect 'n' devices .
- ➢ Examples for symmetric key cryptography include AES, DES etc.

Asymmetric key Cryptography



- ➢ 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.
- ➢ The public key of the receiver is used to encrypt and the private key of receiver is used to decrypt a message and protect it from unauthorized access or use.
- ➢ It requires 2n number of different keys to connect ‘n’ devices.
- ➢ Examples- RSA Algorithm, Diffie Hellman key exchange method.

Difference between Symmetric and Asymmetric key Cryptography

S.N.	Symmetric key Cryptography	Asymmetric key Cryptography
1	Single key required for both Encryption & Decryption.	2 Keys are required . one for encryption, one for decryption
2	nx(n-1)/2 no. of keys needed to connect n systems.	2n no.of keys needed.
3	Key distribution is difficult	Each system has 2 keys.it is easy.
4	Faster	Slower
5	Less secure	More Secure
5	Ex- AES,DES	EX- RSA, Diffie hellman key exchange method

Short Questions with answer

Q1. Distinguish between encryption & Decryption.

- ➢ The process of encoding plain text messages into cipher text messages is called **Encryption**.
- ➢ The reverse process of converting ciphertext messages back to plain text messages is called **Decryption**.

Q2.**Define Cryptography.**

- ➢ Cryptography is the art and science of achieving security by encoding messages to make them secure and immune to attacks.
- ➢ It is of 2 types
  - 1) Symmetric key Cryptography
  - 2) Asymmetric key Cryptography

Q3.Define Substitution technique.

In the substitution cipher technique the characters of a plain text message are replaced by other characters, numbers or symbols.

The substitution technique is classified into two types.

3. Monoalphabetic Cipher
4. Polyalphabetic Cipher

Long Questions

Q1.. Describe symmetric and asymmetric key cryptography.

Q2.. Explain various types of Transposition techniques used in cryptography.

Q3.Explain various types of substitution techniques used in cryptography.

CHAPTER-03
Symmetric & Asymmetric key algorithms

3.1 Symmetric key algorithm types

- The algorithm type defines what size of plain text should be encrypted in each step of the algorithm.
- The Symmetric key algorithms are of 2 types.

1. Stream Cipher
2. Block Cipher

Stream Cipher

Stream cipher technique involves the encryption of one plain text byte at a time.

The decryption also happens one byte at a time.

Encryption :

For Encryption,

- Plain Text and Keystream produces Cipher Text (Same keystream will be used for decryption.).
- The Plaintext will undergo XOR operation with keystream bit-by-bit and produces the Cipher Text.

Example –

Plain Text : 100

Keystream : 110

Cipher Text : 010

Decryption :

For Decryption,

- Cipher Text and Keystream gives the original Plain Text (Same keystream will be used for encryption.).
- The Ciphertext will undergo XOR operation with keystream bit-by-bit and produces the actual Plain Text.

Example –

Cipher Text : 010

Keystream : 110

Plain Text : 100

Decryption is just the reverse process of Encryption i.e. performing XOR with Cipher Text.

Block Cipher

- ➢ Block cipher technique involves encryption of one block of text at a time.
- ➢ Decryption also takes one block of encrypted text at a time.

Example-

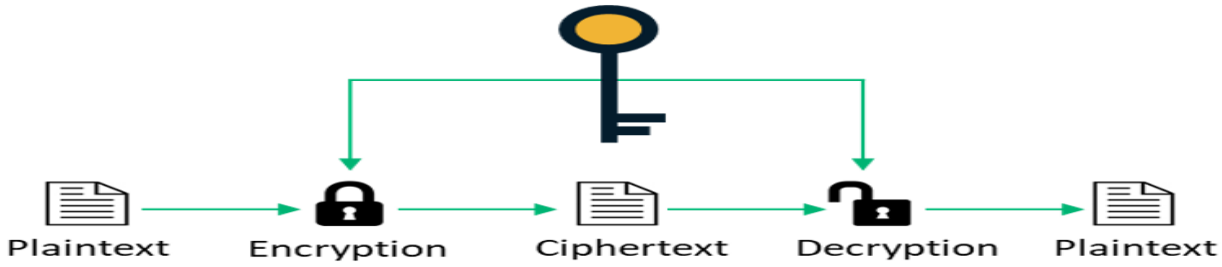
Encryption

- ➢ Suppose we have a plain text *FOUR_AND_FOUR* that needs to be encrypted . Using a block cipher , FOUR could be encrypted first, followed by _AND_ and finally FOUR.
- ➢ Thus one block of characters gets encrypted at a time.

Decryption

- ➢ During decryption , each block would be translated back to original form

3.2 Overview of Symmetric key cryptography



- ➢ Symmetric cryptography relies on one shared key that both parties know and can use to encrypt or decrypt data.
- ➢ Establishing the shared key is difficult using only symmetric encryption algorithms, so in many cases, an asymmetric encryption is used to establish the shared key between two parties.
- ➢ It requires (nx(n-1))/2 number of keys to connect 'n' devices .
- ➢ Examples for symmetric key cryptography include AES, DES etc.

3.3 Data encryption standards

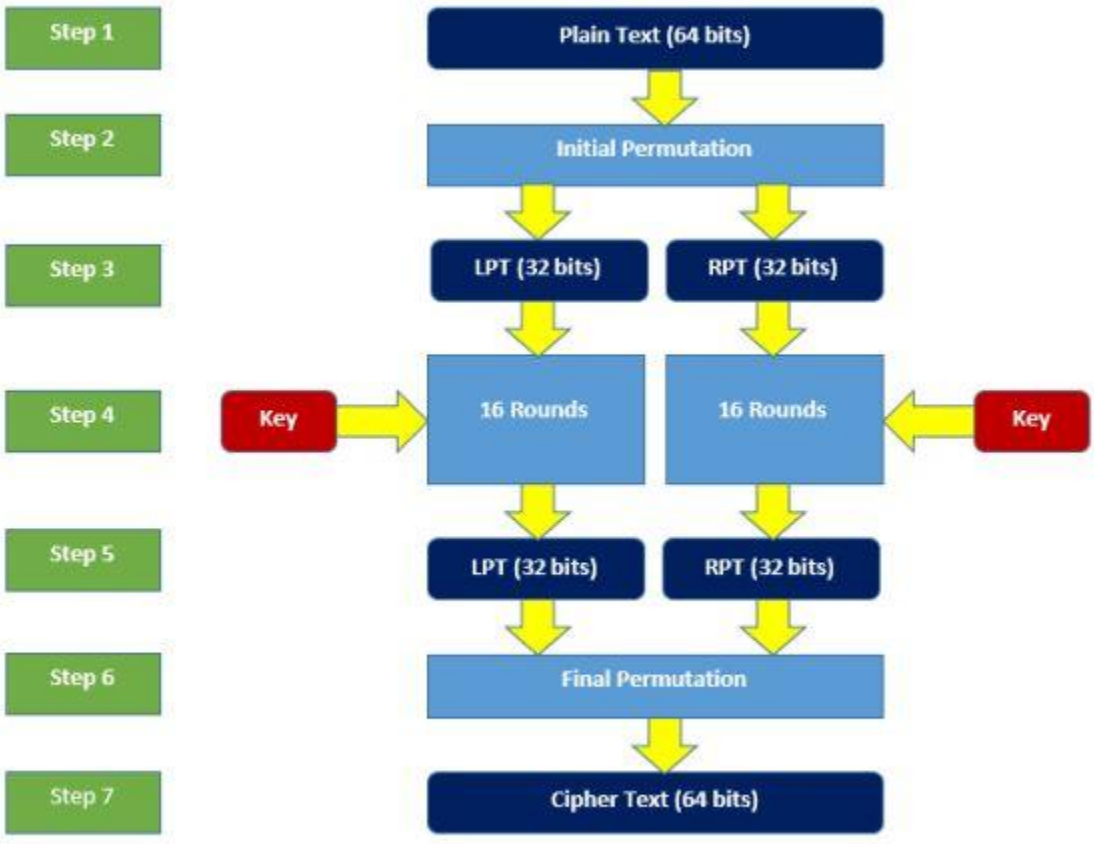
- ➢ The DES (Data Encryption Standard) algorithm is a symmetric-key block cipher created in the early 1970s by an IBM team and adopted by the National Institute of Standards and Technology (NIST).
- ➢ The algorithm takes the plain text in 64-bit blocks and converts them into ciphertext using 48-bit keys.
- ➢ Since it's a symmetric-key algorithm, it employs the same key in both encrypting and decrypting the data.
- ➢ DES uses 16 rounds of the Feistel structure, using a different key for each round.

DES Algorithm Steps

- ➢ To put it in simple terms, DES takes 64-bit plain text and turns it into a 64-bit ciphertext. And since we're talking about asymmetric algorithms, the same key is used when it's time to decrypt the text.

The algorithm process breaks down into the following steps:

1) The process begins with the 64-bit plain text block getting handed over to an initial permutation (IP) function.
2) The initial permutation (IP) is then performed on the plain text.
3) Next, the initial permutation (IP) creates two halves of the permuted block, referred to as Left Plain Text (LPT) and Right Plain Text (RPT).
4) Each LPT and RPT goes through 16 rounds of the encryption process.
5) Finally, the LPT and RPT are rejoined, and a Final Permutation (FP) is performed on the newly combined block.
6) The result of this process produces the desired 64-bit ciphertext.



Broad Level Steps in DES

The encryption process step (step 4, above) is further broken down into five stages:

1. Key transformation
2. Expansion permutation
3. S-Box permutation
4. P-Box permutation
5. XOR and swap

For decryption, we use the same algorithm, and we reverse the order of the 16 round keys.

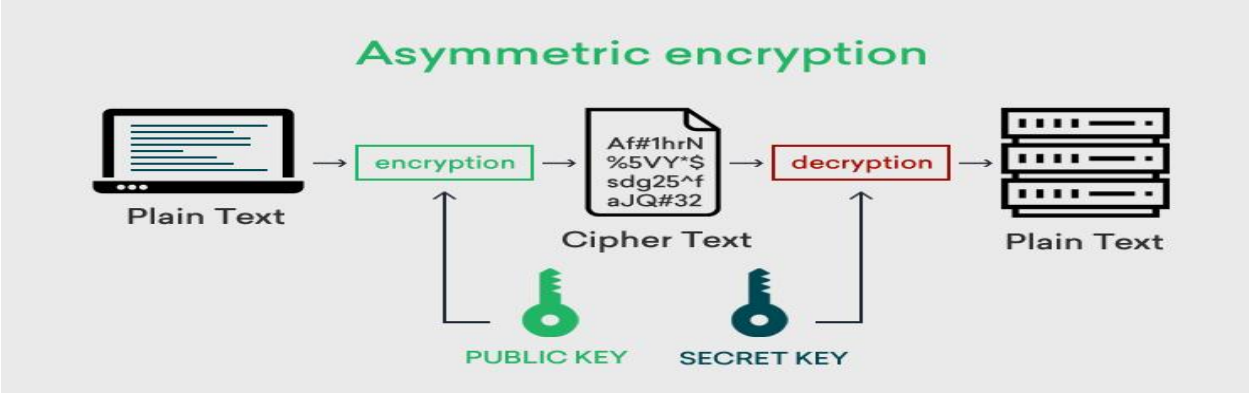
Next, to better understand what is DES, let us learn the various modes of operation for DES.

DES Modes of Operation

Data encryption experts using DES have five different modes of operation to choose from.

1. Electronic Codebook (ECB). Each 64-bit block is encrypted and decrypted independently.
2. Cipher Block Chaining (CBC). Each 64-bit block depends on the previous one and uses an Initialization Vector (IV)
3. Cipher Feedback (CFB). The preceding ciphertext becomes the input for the encryption algorithm, producing pseudorandom output, which in turn is XORed with plaintext, building the next ciphertext unit
4. Output Feedback (OFB). Much like CFB, except that the encryption algorithm input is the output from the preceding DES.
5. Counter (CTR). Each plaintext block is XORed with an encrypted counter. The counter is then incremented for each subsequent block

3.4 Over view of Asymmetric key cryptography



- ➢ 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.
- ➢ The public key of the receiver is used to encrypt and the private key of receiver is used to decrypt a message and protect it from unauthorized access or use.
- ➢ It requires 2n number of different keys to connect ‘n’ devices.
- ➢ Examples- RSA Algorithm, Diffie Hellman key exchange method.

3.5 The RSA algorithm

Step-1. Choose two large prime numbers P and Q.

Step-2. Calculate N = P x Q

Calculate Ø(N)=(P-1)x(Q-1)

.

Step-3. Select the public key (i.e. the encryption key) E such that

- 1 < E < Ø(n)
- gcd (E, Ø(n)) = 1

Step-4. Select the private key (j.e. the decryption key) D such that the following equation is true: (D x E) mod Ø(N) = 1

D=(1+K .Ø(N))/E

Step-5. For encryption, calculate the ciphertext CT from the plain text PT as follows:

$CT = PT^E \bmod N$

Step-6. Send CT as the cipher text to the receiver.

Step-7. For decryption, calculate the plain text PT from the ciphertext CT as follows:

$PT = CT^D \bmod N$

3.6 Symmetric & Asymmetric key cryptography

Symmetric Key Encryption	Asymmetric Key Encryption
It only requires a single key for both encryption and decryption.	It requires two key one to encrypt and the other one to decrypt.
The size of cipher text is same or smaller than the original plain text.	The size of cipher text is same or larger than the original plain text.
The encryption process is very fast.	The encryption process is slow.
It is used when a large amount of data is required to transfer.	It is used to transfer small amount of data.

It only provides confidentiality.	**It provides confidentiality, authenticity and non-repudiation.**
Examples: 3DES, AES, DES and RC4	**Examples: Diffie-Hellman, ECC, El Gamal, DSA and RSA**
In symmetric key encryption, resource utilization is low as compared to asymmetric key encryption.	**In asymmetric key encryption, resource utilization is high.**

3.7 Digital signature

- A digital signature is a mathematical technique used to validate the authenticity and integrity of a message, software or digital document.
- **Digitally signed** messages may be anything representable as a bitstring: **examples** include **electronic** mail, contracts, or a message sent via some other cryptographic protocol.

Short Questions with answer

Q1. Define Digital signature

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

- **Digitally signed** messages may be anything representable as a bitstring: **examples** include **electronic** mail, contracts, or a message sent via some other cryptographic protocol.

Q2. What is Block Cipher?

- Block cipher technique involves encryption of one block of text at a time.
- Decryption also takes one block of encrypted text at a time.

Long Questions

Q1.Explain various symmetric key algorithm types used in the field of cryptography and Network security.

Q2. What do you mean by DES ? Explain how DES works.

Q3. Differentiate Symmetric key & Asymmetric key cryptography.

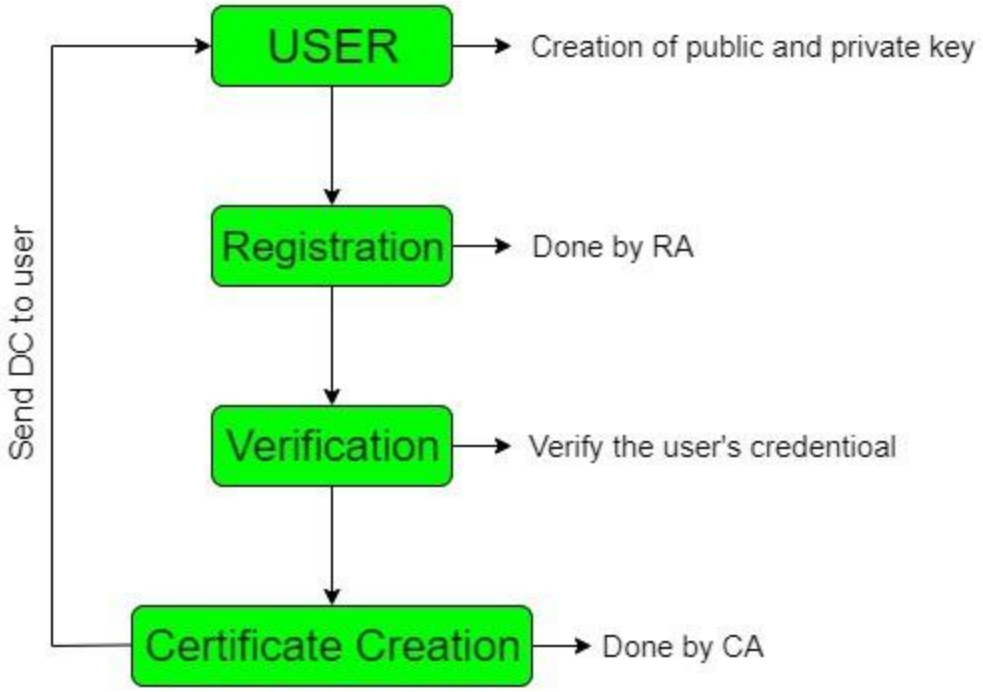
CHAPTER-04
Digital certificate & Public key infrastructure

4.1 Digital certificates

- ➢ Digital certificates are electronic credentials that are used to assert the online identities of individuals, computers, and other entities on a network.
- ➢ Digital certificates function similarly to identification of cards such as passports and driving licenses.
- ➢ Most commonly they contain a public key and the identity of the owner.
- ➢ They are issued by certification authorities (CAs) that must validate the identity of the certificate-holder both before the certificate is issued and when the certificate is used.
- ➢ Common uses include business scenarios requiring authentication, encryption, and digital signing.

Steps for Digital Certificate Creation:

- **Step-1:** Key generation is done by either user or registration authority. The public key which is generated is sent to the registration authority and the private key is kept secret by the user.
- **Step-2:** In the next step the registration authority registers the user.
- **Step-3:** Next step is verification which is done by the registration authority in which the user's credentials are being verified by the registration authority. It also checks that the user who sends the public key has a corresponding private key or not.
- **Step-4:** In this step the details are sent to the certificate authority by the registration authority who creates the digital certificate and gives it to users and also keeps a copy to itself.



4.2 Private key management

Protecting private keys

- A user must hold the private key secretly. It must not be possible for another user to access someone's private key.

The mechanisms for protecting private keys are as follows.

Password Protection

This is the simplest and most common mechanism to protect a private key.The private is stored on the hard disk of the user's computer as a disk file. This file can be accessed only with the help of a password or PIN.

PCMCIA CARDS

The personal computer memory card International Association (PCMCIA) cards are cheap cards. Private Key is stored on such a card which reduces the chances of being stolen.

Tokens

A token stores the private key in an encrypted format. To decrypt and access it, the user must provide a one time password**(OTP).**

Biometrics

The private key is associated with unique characteristics of an individual finger print, retina scan or voice recognition.

Smart cards

In a smart card the private key of the user is stored in a tamper proof card . This card performs cryptographic functions which keeps the private key secured.

Multiple key pair

- ➢ The PKI recommends that in serious business applications users should possess multiple digital certificates which also means multiple key pairs.
- ➢ The need for this is that one certificate could be strictly used for signing and another for encryption.
- ➢ This ensures that the loss of one of the private keys does not affect the complete operations of the user.

key update

- ➢ Good security practices demand that the key pair should be updated periodically.
- ➢ This is because of over time the keys become susceptible to cryptanalysis attacks.

Key Archival

- ➢ The CA must plan for and maintain the history of the certificates and keys of its users.
- ➢ The key archival is a very significant aspect of any PKI solution.

4.3 PKIX Model

- The X.509 standard defines the digital certificate structure, format and fields.
- It also specifies the procedure for distributing the public keys.
- In order to extend such standards and make them universal, the Internet Engineering Task Force (IETF) formed the Public Key Infrastructure X.509 (PKIX) working group.
- This extends the basic philosophy of the X.509 standard and species how the digital certificates can be deployed in the world of the Internet.
- Additionally, other PKI models have been defined for use by applications in various domains. For example, the ANSI ASC X9F standards are used by financial institutions.

PKIX Services

PKIX identifies the primary goals of PKI infrastructure in the form of the following broad label services.

- **Registration:** It is a process where end-entity registers itself to a CA. Usually, the registration is done via the RA.
- **Initialization:** This deals with basic problems such as the methodology of verifying that the end entity is talking to the right CA.
- **Certification:** It is a process where CA creates a digital certificate for end-entity and returns it to the end entity. CA also maintains a copy of the certificate for its records. If required, CA also copied it in public directories.
- **Key pair recovery:** Keys which are used for encrypting documents may be required to be recovered later for decrypting the same old documents. Key archival and recovery services can be provided by CA or by an independent key recovery system.
- **Key generation:** PKIX model specifies that the end entity should be able to generate the public key and private key pairs or CA should be able to do this for the end entity.
- **Key update:** It is a process where the expired key of the digital certificate is automatically renewed and replaced with a new key pair. However, there is a provision for manual digital certificate renewal requests and responses.

- **Cross certification:** It is a process where end entities that are re-certified by different CA, can cross verify each other. It helps in establishing trust models.
- **Revocation:** PKIX model provides support for checking certificate status in two modes, online using OCSP and offline using CRL.

4.4 Public key cryptography standards(PKCS)

- The PKCS model was initially developed by RSA Laboratories with help from representatives of the government, industry and academia.
- The main purpose of PKCS is to standardize Public Key Infrastructure (PKI).
- The standardization is in many respects, such as formatting, algorithms and APIs.
- This would help organizations to develop and implement inter-operable PKI solutions, rather than everyone choosing their own standard.

Standard	Purpose	Details
PKCS#1	RSA Encryption Standard	Defines the basic formatting rules for RSA public key functions, more specifically the digital signature. It defines how digital signatures should be calculated, including the structure of the data to be signed as well as the format of the signature. The standard also defines the syntax for RSA private and public keys.
PKCS#2	RSA Encryption Standard	This standard outlined the message digest calculation.
PKCS#3	Diffie-Hellman Key	Defines a mechanism to implement Diffie-Hellman Key Agreement Standard Agreement protocol.

PKCS#4	NA	Merged with PKCS#1.
PKCS#5	Password Based Encryption (PBE)	Describes a method for encrypting an octet string with a symmetric key. The symmetric key is derived from a password.
PKCS#6	Extended Certificate Syntax	Defines syntax for extending the basic attributes of an X.509 digital certificate.
PKCS#7	Cryptographic Message	Specifies a format/syntax for data that is the result of a cryptographic operation. Examples of this are digital signatures and digital envelopes.

Short Questions with Answer

Q1. What are the Roles of CA in digital certificate.

- ➢ The role of the Certificate Authority (CA) is to guarantee that the individual granted the unique certificate is, in fact, who he or she claims to be.
- ➢ Certificate Authority (CA) Verifies the identity of the entity who requests a digital certificate before issuing it.
- ➢ Certificate Authority (CA) issues digital certificates.
- ➢ Certificate Authority (CA) maintains Certificate Revocation List (CRL).

Q2. What is a Digital envelope ?

- ➢ A digital envelope is a secure electronic data container that is used to protect a message through encryption and data authentication.
- ➢ An example of a digital envelope is Pretty Good Privacy (PGP).

Long Questions

Q1.Explain Digital Certificate. What are certificate creations procedures?

2. Explain private key management.

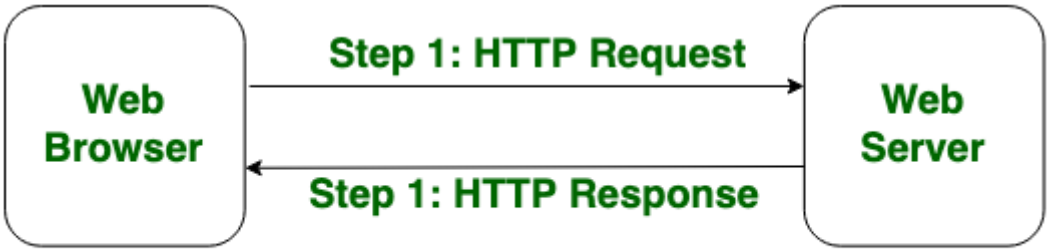
3. Explain the PKIX services.

CHAPTER-05
Internet security protocols

5.1 Basic concept

Static Web pages:

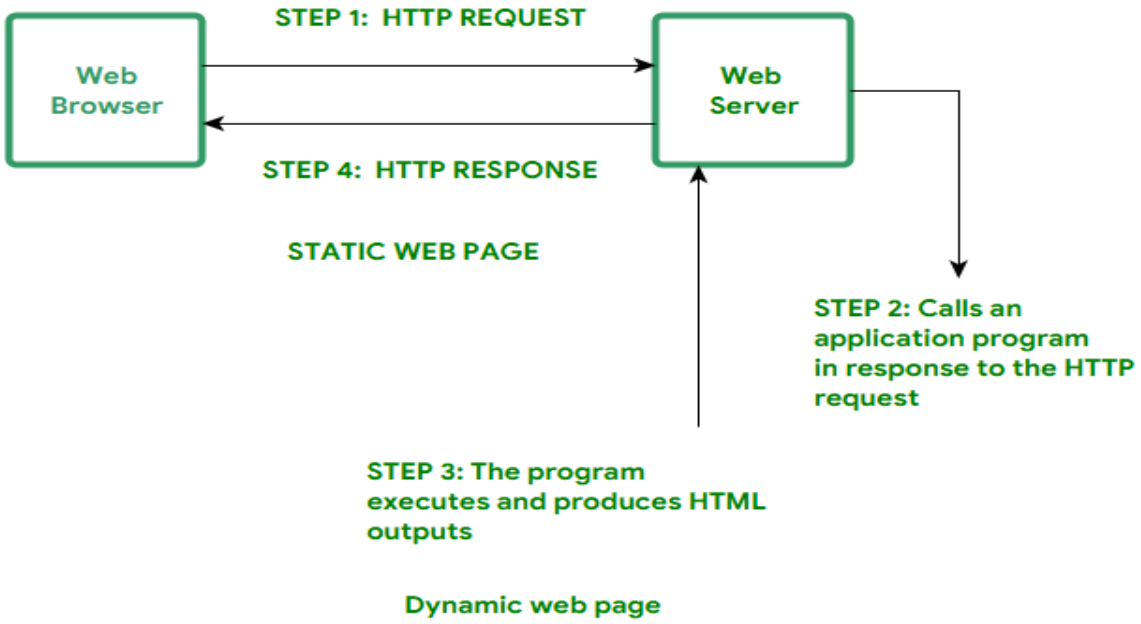
Static Web pages are very simple. It is written in languages such as HTML, JavaScript, CSS, etc. For static web pages when a server receives a request for a web page, then the server sends the response to the client without doing any additional process. And these web pages are seen through a web browser. In static web pages, Pages will remain the same until someone changes it manually.



Static Web Page

Dynamic Web Pages:

Dynamic Web Pages are written in languages such as CGI, AJAX, ASP, ASP.NET, etc. In dynamic web pages, the Content of pages is different for different visitors. It takes more time to load than the static web page. Dynamic web pages are used where the information is changed frequently, for example, stock prices, weather information, etc.



Active Web pages

- An active web page is a page where the *browser* performs the logic instead of the server.
- So for example when you've got a page where you're showing share prices, then you want it to update e.g. every 5 seconds.
- A solution would be to use AJAX with JavaScript.
- In contrast to PHP, your browser is able to execute JavaScript, so it is happening without reloading the page.
- So with an active page, everything is happening inside your browser without the need to reload the page every time you want new information.

5.2 Secure socket layer

- The secure socket layer protocol is an internet protocol for exchange of information between a web browser and a web server.

Working of SSL

SSL has 3 sub-protocols, namely

- Handshake protocol
- Record protocol
- Alert protocol

These three sub-protocols constitute the overall working of SSL.

The Handshake Protocol

➢ The handshake protocol of SSL is the first sub-protocol used by the client and the server to communicate using an SSL enabled connection.

➢ Similar to how Alice and Bob would first shake hands with each other with hello message before they start conversing.

Type	Length	Content

1byte 3byte 1 or more byte

(Format of the handshake protocol messages)

each handshake message has 3 fields as follows

- Type (1 byte) :This field indicates one of the ten possible message types.
- Length (3 bytes) :This fields Indicates the length of the message in bytes.
- Content(1 or more bytes) : This field contains the parameters associated with this message depending on the message type.

The handshake protocol is actually made up of four phases. These phases are:

1. Establish security capabilities
2. Server authentication and key exchange
3. Client authentication and key exchange
4. Finish

The record protocol

- ➢ The record Protocol in SSL comes into picture after a successful handshake is complete between the client and the server .

- ➢ That is after the client and the server authenticated each other and have decided what algorithms to use for secure information exchange , the system enters into the SSL record protocol
- ➢ This protocol provides two services to an SSL connection.
  - Confidentiality: This is achieved by using the secret key that is defined by the handshake protocol.
  - Integrity: the handshake protocol also defines the shared secret key that is used for assuring the message integrity.
- ➢ The SSL record protocol takes an application message as input, fragments it into smaller blocks, optionally compresses each block, adds MAC, encrypts it , adds a header and gives it to the transport layer where the TCP processes it. At the receiver's end the header of each block is removed, the block is then decrypted, verified, decompressed and reassembled into application messages.

The Alert protocol

- ➢ when either the client or the server detects an error the detecting party sends an alert message to the other party. If the error is fatal both the parties immediately close the SSL connection.

5.3 Transport layer security

- ➢ Transport Layer Security (TLS) is an IETF standardization initiative, whose goal is to come. an Internet standard version of SSL.
- ➢ Netscape wanted to standardize SSL, and hence handed the protocol over to IETF.
- ➢ There are subtle differences between SSL and TLS. However, the core idea and implementations are quite similar.
- ➢ TLS is defined in RFC 2246.

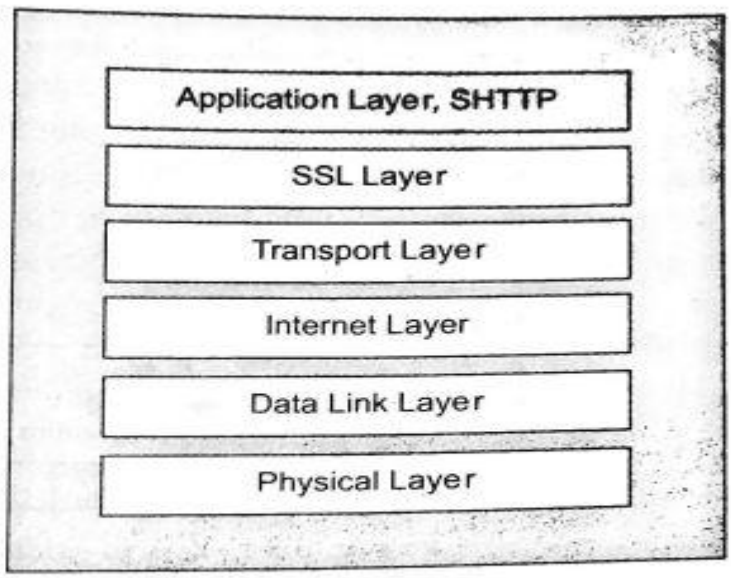
Difference between SSL and TLS

Property	*SSL*	*TLS*
Version	3.0	1.0
Cipher suite	Supports an algorithm called as Fortezza	Does not support Fortezza
Cryptography secret	Computed as explained earlier in the chapter	Uses a pseudorandom function to create master secret
Alert protocol	As explained earlier in the chapter	The *No certificate* alert message is deleted. The following are newly added: *Decryption failed*, *Record overflow*, *Unknown CA*, *Access denied*, *Decode error*, *Export restriction*, *Protocol version*, *Insufficient security*, *Internal error*.
Handshake protocol	As explained earlier in the chapter	Some details are changed
Record protocol	Uses MAC	Uses HMAC

5.4 Secure Hyper text transfer protocol(SHTTP)

- ➢ The Secure HyperText Transfer Protocol (SHTTP) is a set of security mechanisms protecting Internet traffic.
- ➢ This includes the data entry forms and Internet-based transacti that an HTTP request sent by using SSL is identified as HTTPS (e.g. HTTPs://www.yahoo.com), whereas this is SHTTP (e.g. sHTTP://www.yahoo.com).
- ➢ The services offered by SHTTP are quite similar to those of SSL.
- ➢ However, SSL has become highly successful.
- ➢ SHTTP works at the application layer, and is therefore tightly coupled with HTTP, unlike SSL (Which sits between application and the transport layers).
- ➢ 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.
- ➢ Instead, it aims at making the connection between a client and the server, regardless of the messages that they are exchanging. Also, SSL cannot perform digital signatures. SHTTP is very rarely used.



Positions of SHTTP and SSL in TCP/IP protocol suite

5.5 Time stamping protocol (TSP)

- ➢ The Time Stamping Protocol (TSP) provides proof that a certain piece of data existed at a particular time. This PKI service is provided by an authority called Time Stamping Authority (TSA).
- ➢ TSP is currently under the development of the PKIX working group.
- ➢ Digital signatures provided via the use of PKI can lead to disputes, if the signer of an important document (e.g. a funds transfer order) later wants to repudiate her digital signature.

- She can dishonestly claim later that her private key was compromised, and that it should be revoked.
- In such situations, it may be difficult to prove whether the document was signed before the signer reported the key compromise or not. Using the time stamping technique, we can ascertain whether an electronic document was created or signed at or before a particular date and time.
- This can have serious legal implications, now that digital signatures are almost as good as pen-and-paper signatures.
- The TSA acts like a trusted third-party notary in this scheme.
- The TSP is a simple request-response protocol, similar to HTTP.
- This works as described below, step-by-step.
- **Step1: Message digest calculation** Firstly, the entity (client) requiring a timestamp calculates a message digest of the original message, which needs a timestamp from the TSA. The client should use a Standard message digest algorithm, such as MD5 or SHA-1 for this purpose.
- **Step 2: Time stamping request**

Now, the client sends the message digest calculated in step 1 to the Time

Stamp Authority (TSA) for getting it time stamped. This is called as a Time

Stamping Request.

-
- **Step 3: Time stamping response**
- In response to the client's request, the TSA might decide to grant time stamp. If it decides to accept the request and process it, it signs the client's reques with the time stamp by the TSA private key. Regardless, it returns a Time Stamping Response back to the client.

5.6 Secure electronic transaction (SET)

Secure Electronic Transaction (SET)

- ➢ Secure electronic transaction (SET) Is an open encryption and security specification that is designed for protecting credit card transactions on the internet
- ➢ Secure electronic transaction was used to facilitate the secure transmission of consumer card information via electronic portals on the Internet.

SET process

1. The customer opens an account – The customer opens a credit card account (MasterCard or Visa) with a bank (issuer) that supports electronic payment mechanisms and the SET protocol.

2. The customer receives a certificate - After the customer's identity is verified (with the

details such as passport, business documents etc.), the customer receives a digital certificate from CA. The certificate also contains details such as the customer's public key and its expiration date.

3. The merchant receives a certificate – A merchant that wants to accept a certain brand of credit cards must possess a digital certificate.

4. The customer places an order – This is a typical shopping cart process wherein the customer browses the list of items available, searches for specific items, selects one or more of them and places the order.

5. The merchant is verified – The merchant also sends its digital certificate to the customer. This assures the customer that he is dealing with a valid merchant.

6. The order and payment details are sent – The customer sends both the order and payment details to the merchant along with the customer's digital certificate. The order confirms the purchase transaction with reference to the items mentioned in the order form. The payment contains credit card details. However, the payment information is so encrypted that the merchant cannot read it.

7. The merchant requests payment authorization - The merchant forwards the payment details sent by the customer to the payment gateway via the acquirer (or to the acquirer if the acquirer also acts as the payment gateway) and requests the payment gateway to authorize the payment

8. The payment gateway authorizes the payment - Using the credit card information received from the merchant, the payment gateway verifies the details of the customer's credit card with help of the issuer, and either authorizes or rejects the payment.

9. The merchant confirms the order - Assuming that the payment gateway authorizes the

payment, the merchant sends a confirmation of the order to the customer.

10. The merchant provides goods or services – The merchant now ships the goods services as per the customer's order.

11. The merchant requests payment - The payment gateway receives a request from the merchant for making the payment.

Short Questions with answer

Q1. Define TSP.

- ➢ The Time Stamping Protocol (TSP) provides proof that a certain piece of data existed at a particular time.
- ➢ This PKI service is provided by an authority called Time Stamping Authority (TSA).

Q2. **What is SSL?**

The secure socket layer protocol is an internet protocol for exchange of information between a web browser and a web server.

Q3. Explain static web pages.

- Static Web pages are very simple. It is written in languages such as HTML, JavaScript, CSS, etc.
- For static web pages when a server receives a request for a web page, then the server sends the response to the client without doing any additional process And these web pages are seen through a web browser.
- In static web pages, Pages will remain the same until someone changes it manually.

Long Questions

Q1.What do you mean by secure electronic transaction?explain the set process.

Q2. Describe the position of SSL in TCP/IP Protocol Suite with diagram.

Q3. Explain SHTTP.

CHAPTER-06
User authentication

6.1 Authentication basics

- Authentication can be defined as determining an identity to the required level of assurance.
- Authentication is the first step in any cryptographic solution.
- We say this because unless we know who is communicating, there is no point in encrypting what is being communicated.
- As we know, the whole purpose of encryption is to secure communication between two or more parties. Unless we are sure that the parties are really what they claim to be, there is no point in encrypting the information flowing between them.
- Otherwise, there is a chance that an unauthorized user can access the information. In cryptographic terms, we can put this in other words: there is no use of encryption without authentication.
- We see authentication checks many times every day. We are required to wear and produce our cards at work, whenever demanded.
- To use our ATM card, we must make use of the card as the PIN. Many such examples can be given. The whole idea of authentication is based on secrets.
- Most likely, the entity being authenticated and the authenticator both share the same secret (e.g. the PIN in the ATM example).

6.2 Password

➢ Password is a string of alphabets, numbers and special characters which is known only to the entity who gets authentication.

Password Authentication Mechanism steps:

➢ The Client enters a Username and password.
➢ The Username and password are sent across the network to the Server.
➢ The server determines whether the User Name and password sent from the client matches the User Name and password stored in the server database. If it matches then the user gets authenticated.

6.3 Authentication Tokens

➢ An authentication token is an extremely useful alternative to a password.

➢ An authentication token is a small device that generates a new random value every time it is used. this random value becomes the basis for authentication.

➢ Small devices are typically of the size of small key chains, calculators or credit cards.

Usually an authentication token at the following features

- Processor
- LCD for displaying output
- Battery
- A small keypad for entering information(optionally)
- A real time clock(optionally)

Each authentication token that is each device is pre programmed with a unique number called as a random seed.

Step-1: Generation of token

➢ Whenever an authentication token is created the corresponding random seed is generated for the token by the authentication server.

➢ The seed is stored inside the token as well as its entry is made against the users record in the users database.

➢ Seed can be conceptually considered as a user password.

➢ Difference is that the user password is known to the user but the seed value is kept by the server and is unknown to the user.

(Random Seed storage in the database and authentication token)

Step-2: Use of token

➢ An authentication token automatically generates random numbers called as one time password or one time passcodes.

➢ One time passwords are generated randomly by an authentication token based on the seed value.

➢ They are one time because they are generated, used once and discarded forever.

➢ when a user wants to be authenticated the user will get a screen where
the user enters id and the latest one time password.
➢ For this the user enters the user id and OTP obtained from the authentication token.
➢ The user id and password travels to the server as a part of the login request.
➢ The server obtains the seed corresponding to the user ID from the user database and calls a program called a password validation program which establishes the relation between the seed and OTP.

Step-3: Server returns an appropriate message back to the user.
Finally the server sends an appropriate message to the user depending on whether the previous operation was success or failure.
Authentication token types
It is a two types
1. Challenge/response token
2. Time based token
1.Challenge/response token
The seed preprogrammed inside an authentication token is secret and unique. This fact is the base for challenge/response tokens. The Seed becomes the encryption key in this technique.
2.Time based token
This is the usage of time as variable input in place of the random challenges.

6.4 Certificate based authentication

- certificate-based authentication is based on the digital certificate of a user. FIPS-196 is a standard that specifies the operation of this mechanism.
- As we know, in PKI, the server and (optionally) the client are required to possess a digital certificate in order to perform digital transactions.
- The digital certificates can then be reused for user authentication as well.

- In fact, if we use SSL, the server must have a digital certificate, whereas the clients (users) may have digital certificates.
- This is because the client authentication is optional in SSL, but not the server authentication.
- Certificate-based authentication is a stronger authentication mechanism as compared to a password based authentication mechanism, because here the user is expected to have something (certificate) and not know something (password).
- At the time of login, the user is requested to send her certificate to the server over the network as a part of the login request.
- A copy of the certificate exists on the server, which can be used to verify that the certificate is indeed a valid one.

However, this is not all that simple. How do we deal with the following situations?

• Suppose user A has gone for a cup of tea. User B uses this opportunity to login from A's computer, using A's certificate and performs some high-value transaction, posing as A.

• Without A's knowledge. B copies A's certificate (which is nothing but a computer file on the disk) on a floppy disk, copies it back on to her own computer and starts logging in as A as and when she likes.

As we can see, the main concern here is the misuse of someone else's certificate. How do we do that? Well, to tackle such issues, in practice, certificate-based authentication is also made a 2-Factor process (have something and know something), as we shall see.

Step 1: Creation, storage and distribution of digital certificates The first step in certificate based authentication is actually a pre-requisite. Here, the digital certificates are created by the CA for each user and the certificates are sent to the respective users. Moreover, a copy of the certificate is stored by the server in its database (usually in a binary format), in order to verify the certificate during the user's certificate-based authentication.

Step 2: Login request During a login request, the user sends only her user id to the server.

Step 3: Server creates a random challenge Now, the server employs the technique that we have explained earlier. When the server receives the user's login request containing the user id alone, it first checks to see if the user id is a valid one (note that only the user id is checked). If it is not, it sends an appropriate error message back to the user. 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. The random challenge can travel as plain text from the server to the user's computer.

Step-4: User signs the random challenge with its private key.

Step-5: Server returns an appropriate message back to the user Finally, the server sends appropriate message back to the user, depending on whether the previous operations yielded suce failure.

6.5 Biometric authentication

- ➢ Biometric authentication refers to security processes that verify a user's identity through unique biological traits such as retinas, irises, voices, facial characteristics, and fingerprints.
- ➢ Biometric authentication is perhaps the ultimate at end in trying to prove who you are.

Process of Biometric Authentication

- ➢ An authentication process involving biometric fastly involves the creation of the users sample and its storage in the users database.
- ➢ During the actual authentication,a user is required to provide a sample of the same(e.g. retina scan or fingerprint) .
- ➢ Usually this is sent to the server in encrypted format.
- ➢ On the server, users current sample is decrypted and compared with the one stored in the database.
- ➢ If the two samples match then the user is considered as authenticated successfully. Otherwise the user is invalid.

Short Questions with answers

Q1. Define Password.

Password is a string of alphabets, numbers and special characters which is known only to the entity who gets authentication.

Q2. Define Biometric authentication.

- Biometric authentication refers to security processes that verify a user's identity through unique biological traits such as retinas, irises, voices, facial characteristics, and fingerprints.
- Biometric authentication is perhaps the ultimate end in trying to prove who you are.

Long Questions

Q1. Explain Authentication Token.

Q2. Describe Biometric Authentication.

Q3. Explain Authentication basics.

CHAPTER-07.
Network Security & VPN

7.1 Brief introduction of TCP/IP

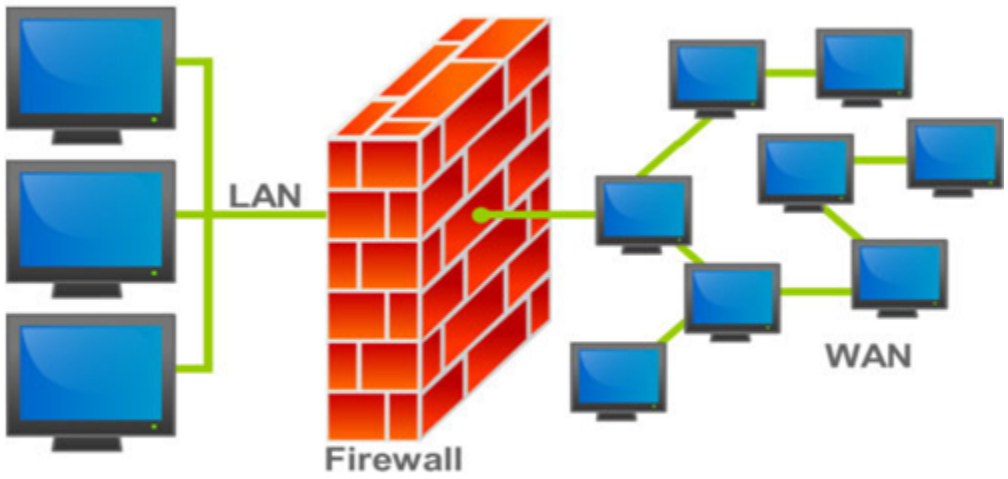
TCP/IP stands for Transmission Control Protocol/ Internet Protocol. It is a set of conventions or rules and methods that are used to interconnect network devices on the Internet.

TCP/IP Layers

- **Application Layer** : An application layer is the topmost layer within the TCP/IP model. When one application layer protocol needs to communicate with another application layer, it forwards its information to the transport layer.
- **Transport Layer** It is responsible for the reliability, flow control, and correction of data that is being sent over the network. There are two protocols used in this layer are User Datagram Protocol and Transmission control protocol.
- **Internet/Network Layer** It is the third layer of the TCP/IP Model and also known as the Network layer. The main responsibility of this layer is to send the packets from any network, and they arrive at the goal irrespective of the route they take.
- **Network Access Layer** It is the lowest layer of the TCP/IP Model. It is the combination of the Physical Layer and the Data link layer which present in the OSI Model. Its main responsibility is to the transmission of information over the same network between two devices.

7.2 Firewall

A firewall is a network security device that monitors incoming and outgoing network traffic and permits or blocks data packets based on a set of security rules.



Types of Firewalls

Packet Filters –

- ❏ It works in the network layer of the OSI Model. It applies a set of rules (based on the contents of IP and transport header fields) on each packet and based on the outcome, decides to either forward or discard the packet.
- ❏ For example, a rule could specify to block all incoming traffic from a certain IP address or disallow all traffic that uses UDP protocol. If there is no match with any predefined rules, it will take default action. The default action can be to ‘discard all packets’ or to ‘accept all packets’.

Application Gateways –

It is also known as Proxy server. It works as follows:

1. **Step-1:** User contacts the application gateway using a TCP/IP application such as HTTP.
2. **Step-2:** The application gateway asks about the remote host with which the user wants to establish a connection. It also asks for the user id and password that is required to access the services of the application gateway.
3. **Step-3:** After verifying the authenticity of the user, the application gateway accesses the remote host on behalf of the user to deliver the packets.

7.3 IP Security

- ➢ The IP security (IPSec) is an Internet Engineering Task Force (IETF) standard suite of protocols between 2 communication points across the IP network that provide data authentication, integrity, and confidentiality.
- ➢ It also defines the encrypted, decrypted and authenticated packets.

Uses of IP Security –

IPsec can be used to do the following things:

- To encrypt application layer data.
- To provide security for routers sending routing data across the public internet.
- To provide authentication without encryption, like to authenticate that the data originates from a known sender.

- To protect network data by setting up circuits using IPsec tunneling in which all data is being sent between the two endpoints is encrypted, as with a Virtual Private Network(VPN) connection.

Components of IP Security –

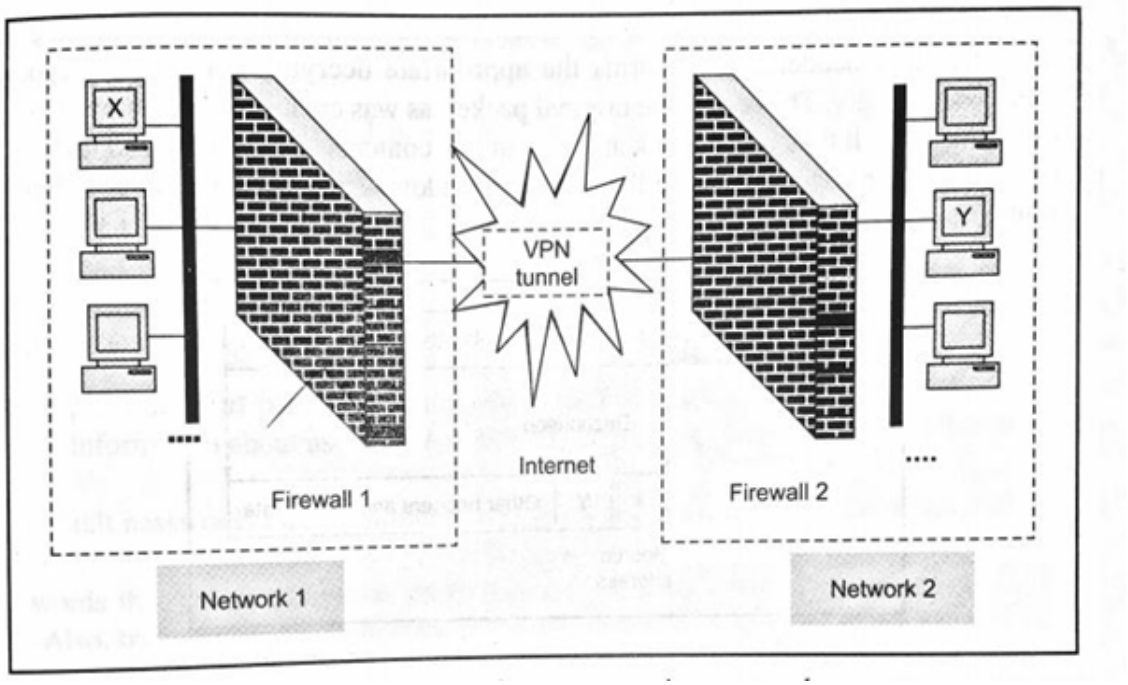
It has the following components:

1. **Encapsulating Security Payload (ESP) –**
   It provides data integrity, encryption, authentication and anti replay. It also provides authentication for payload.
2. **Authentication Header (AH) –**
   It also provides data integrity, authentication and anti replay and it does not provide encryption. The anti replay protection, protects against unauthorized transmission of packets. It does not protect data's confidentiality.

7.4 Virtual Private Network (VPN)

- ➢ A VPN is a mechanism of employing encryption, authentication and integrity protection so that we can use a public network (such as the Internet) as if it is a private network (such as a physical network created and controlled by you).
- ➢ VPN offers a high amount of security.
- ➢ A VPN can connect distant networks of an organization or it can be used to allow traveling users to remotely access a private network (e.g. the organization's intranet) securely over the Internet.
- ➢ A VPN is thus a mechanism to simulate a private network over a public network, such as the Internet.

➢ The term virtual signifies that it depends on the use of virtual connections. These connections are temporary and do not have any physical presence. They are made up of packets.



VPN Architecture

➢ The idea of a VPN is actually quite simple to understand. Suppose an organization has two networks, Network 1 and Network 2, which are physically apart from each other and we want to connect them using the VPN approach.

➢ In such a case, we set up two firewalls, Firewall 1 and Firewall 2.

➢ The encryption and decryption are performed by the firewalls. The architectural overview is shown in Fig.

.

➢ We have shown two networks, Network 1 and Network 2.

- ➢ Network 1 connects to the Internet via a firewall named Firewall 1. Similarly, Network 2 connects to the Internet with its own firewall. Firewall 2.
- ➢ The key point here is that 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.
- ➢ With this configuration in mind, 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 I 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.

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 of the packet from that of host X to its own IP address(i.e. the IP address of Firewall 1, say F1). It also changes the destination IP address address of the packet from that of host Y to the IP address of Firewall 2, say F2).

3. The Packet reaches firewall -2 to over the internet. The fire wall-2 discards the outer header and performs appropriate decryption and gets the original packet.

Short Questions with answers

Q1. Define Ip security.

- ➢ The IP security (IPSec) is an Internet Engineering Task Force (IETF) standard suite of protocols between 2 communication points across the IP network that provide data authentication, integrity, and confidentiality.
- ➢ It also defines the encrypted, decrypted and authenticated packets.

Q2. What is VPN?

- A VPN is a mechanism of employing encryption, authentication and integrity protection so that we can use a public network (such as the Internet) as if it is a private network (such as a physical network created and controlled by you).
- VPN offers a high amount of security.

Q3. Define TCP/IP

- TCP/IP stands for Transmission Control Protocol/ Internet Protocol.
- It is a set of conventions or rules and methods that are used to interconnect network devices on the Internet.

Long Questions

Q1. Explain VPN architecture.

Q2. What is a firewall? Explain different types of firewalls.

Q3.What is TCP/IP? Explain each layer in TCP/ IP suite