MODULE 1

INTRODUCTION TO CRYPTOGRAPHY , OSI SECURITY ARCHITECTURE

OSI SECURITY ARCHITECTURE

1. SECURITY SERVICES

Any action intended to safeguard the integrity and usefulness of your data and network is known as network security. In other words, Network security is defined as the activity created to protect the integrity of your network and data. Network security is the practice of protecting a computer network from unauthorized access, misuse, or attacks.

The Principles of Security can be classified as follows:

- **Confidentiality**
- **Authentication**
- **Access Control**
- **Non-Repudiation**
- **Integrity**

Confidentiality:

- The degree of confidentiality determines the secrecy of the information.
- The principle specifies that only the sender and receiver will be able to access the information shared between them.
- Confidentiality compromises if an unauthorized person is able to access a message.

For eg, 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.

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 preregistered can prove his/her identity and can access the sensitive information.

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.

  System Integrity: System Integrity assures that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.

  Data Integrity: Data Integrity assures that information (both stored and in transmitted packets) and programs are changed only in a specified and authorized manner.

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.

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.

Availability:

- The principle of availability states that the resources will be available to authorize party at all times.
- Systems should have sufficient availability of information to satisfy the user request.

2. SECURITY ATTACKS

ATTACKS

● Types of attacks:

- ● **Passive attacks** : does not involve any modification to the contents of an original message
- ● **Active attacks** : the contents of the original message are modified in some ways.

ACTIVE ATTACKS:

- Active attacks are a type of cybersecurity attack in which an attacker attempts to alter, destroy, or disrupt the normal operation of a system or network.
- Active attacks involve the attacker taking direct action against the target system or network, and can be more dangerous than passive attacks, which involve simply monitoring or eavesdropping on a system or network.
- **Types of active attacks** are as follows:
  - Modification of messages
  - Repudiation
  - Replay
  - Masquerade
  - Denial of Service

Masquerade –

- Masquerade is a type of cybersecurity attack in which an attacker pretends to be someone else in order to gain access to systems or data. This can involve impersonating a legitimate user or system to trick other users or systems into providing sensitive information or granting access to restricted areas.
- Several types of masquerade attacks, including:
  - **Username and password masquerade**
  - **IP address masquerade**
  - **Website masquerade**
  - **Email masquerade**

Modification of messages-

- Simply means that some portion of a legitimate message is altered, or that messages are delayed or reordered, 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."

Repudiation –

- Repudiation attacks are a type of cybersecurity attack in which an attacker attempts to deny or repudiate actions that they have taken, such as making a transaction or sending a message.
- These attacks can be a serious problem because they can make it difficult to track down the source of the attack or determine who is responsible for a particular action.

Replay –

- It involves the passive capture of a message and its subsequent transmission to produce an authorized effect.
- In this attack, the basic aim of the attacker is to save a copy of the data originally present on that particular network and later on use this data for personal uses.
- Once the data is corrupted or leaked it is insecure and unsafe for the users.

Denial of Service –

- Denial of Service (DoS) is a type of cybersecurity attack that is designed to make a system or network unavailable to its intended users by overwhelming it with traffic or requests.
- In a DoS attack, an attacker floods a target system or network with traffic or requests in order to consume its resources, such as bandwidth, CPU cycles, or memory, and prevent legitimate users from accessing it.

PASSIVE ATTACKS:

- A Passive attack attempts to learn or make use of information from the system but does not affect system resources.
- Passive Attacks are in the nature of eavesdropping on or monitoring transmission. The goal of the opponent is to obtain information that is being transmitted.
- Passive attacks involve an attacker passively monitoring or collecting data without altering or destroying it.
- Examples of passive attacks include eavesdropping, where an attacker listens in on network traffic to collect sensitive information, and sniffing, where an attacker captures and analyzes data packets to steal sensitive information.

Types of Passive attacks are as follows:

- The release of message content
- Traffic analysis

The release of message content –

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

Traffic analysis –

- In this attack the eavesdropper analyses the traffic, determine the location, identifying communicating hosts etc. All incoming and outgoing traffic of network is analyzed but not altered.

3. SECURITY MECHANISMS

- A security mechanism is a method or technology that protects data and systems from unauthorized access, attacks, and other threats.
- Security measures provide data integrity, confidentiality, and availability, thereby protecting sensitive information and maintaining trust in digital transactions

Types of Security Mechanism

- **Encipherment :** This security mechanism deals with hiding and covering of data which helps data to become confidential. It is achieved by applying mathematical calculations or algorithms which reconstruct information into not readable form.

- **Access Control :** This mechanism is used to stop unattended access to data which you are sending. It can be achieved by various techniques such as applying passwords, using firewall, or just by adding PIN to data.

- **Notarization :** This security mechanism involves use of trusted third party in communication. It acts as mediator between sender and receiver so that if any chance of conflict is reduced. This mediator keeps record of requests made by sender to receiver for later denied.

- **Data Integrity :** This security mechanism is used by appending value to data to which is created by data itself. It is similar to sending packet of information known to both sending and receiving parties and checked before and after data is received. When this packet or data which is appended is checked and is the same while sending and receiving data integrity is maintained.

- **Digital Signature :** This security mechanism is achieved by adding digital data that is not visible to eyes. It is form of electronic signature which is added by sender which is checked by receiver electronically. This mechanism is used to preserve data which is not more confidential but sender's identity is to be notified.

Difference Between Cryptography and Cryptanalysis

Cryptography and Cryptanalysis overlap in the area of ensuring data protection.

Cryptography sets up a secure communication and information protection process through the process of encryption, whereas cryptanalysis tests the strength of cryptographic algorithms and brings forward the vulnerabilities that the system might have.

Cryptography Terminologies

- **Plaintext :** The medium, the non-encrypted source data, and the clear message.
- **Ciphertext :** The ciphertext is the form of incomprehensible plaintext. Only the encryption key can open the cipher and let the message be read.
- **Encryption :** The process of applying cryptographic algorithms and keys to convert the plaintext into ciphertext.
- **Decryption :** The process that is equivalent to encryption does decryption by way of converting ciphertext to plaintext with the aid of decryption keys.

Cryptanalysis Terminologies

- **Brute Force Attack :** A cryptanalysis technique whereby you keep on trying all the keys until you find the correct one.
- **Frequency Analysis :** A method involves untangling encrypted messages by studying the frequency of the letters or symbols in the ciphertext.
- **Cryptanalysis :** The activity of solving coded messages in cryptographic systems by disclosing the initial messages or the keys of decryption.
- **Vulnerability :** Cryptanalysts can make use of cryptographic algorithm's weaknesses as well as imperfections in their implementations.

Cryptography	**Cryptanalysis**
Ensures secure communication through encryption	Involves breaking cryptographic systems
Protects data confidentiality and integrity	Reveals plaintext or decryption keys
Converts plaintext to ciphertext	Analyzes and deciphers ciphertext
Maintain data security and privacy	Identify weaknesses and vulnerabilities
Prevents unauthorized access to plaintext	Focuses on deciphering ciphertext to access plaintext
Crucial for securing sensitive information	Essential for evaluating cryptographic system

CLASSICAL ENCRYPTION TECHNIQUES

The two basic building blocks of all encryption techniques are **substitution and transposition**

SUBSTITUTION TECHNIQUES

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

1.CAESAR CIPHER (OR) SHIFT CIPHER

- The simplest technique.
- The Caesar cipher involves replacing each letter of the alphabet with the letter standing three places further down the alphabet

For each plaintext letter P

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

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

The decryption algorithm is simply $P = D(C)$

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

For example,

PT :	MEET	ME	AFTER	THE	TOGA	PARTY
CT :	PHHW	PH	DIWHU	WKH	WRJD	SDUWB

The alphabet is wrapped around, so that the letter following Z is A. We can define the transformation by listing all possibilities,as follows:

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

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

If it is known that a given ciphertext is a Caesar cipher, then a brute-force cryptanalysis is easily performed

Three important characteristics of this problem enabled us to use a bruteforce cryptanalysis:

1. The encryption and decryption algorithms are known.

2. There are only 25 keys to try.

3. The language of the plaintext is known and easily recognizable.

2. MONOALPHABETIC CIPHERS

A monoalphabetic cipher is any cipher in which the letters of the plain text are mapped to cipher text letters based on a single alphabetic key.

3.POLYALPHABETIC CIPHER

- Polyalphabetic Cipher is a cipher where each letter in the plaintext can be encrypted to multiple possible letters in the ciphertext, depending on its position and a more complex algorithm.
- The **Vigenère cipher** is probably the best-known example of a polyalphabetic cipher

Difference Between Monoalphabetic Ciphers & Polyalphabetic Cipher

Monoalphabetic Cipher	**Polyalphabetic Cipher**
A monoalphabetic cipher is one where each symbol in plain text is mapped to a fixed symbol in cipher text.	Polyalphabetic cipher is any cipher based on substitution, using multiple substitution alphabets.
The relationship between a character in the plain text and the characters in the cipher text is one-to-one.	The relationship between a character in the plain text and the characters in the cipher text is one-to-many.
Each alphabetic character of plain text is mapped onto a unique alphabetic character of a cipher text.	Each alphabetic character of plain text can be mapped onto 'm' alphabetic characters of a cipher text
It is a simple substitution cipher.	It is multiple substitutions cipher.
Monoalphabetic ciphers are not that strong as compared to polyalphabetic cipher.	Polyalphabetic ciphers are much stronger.
Eg: Affine cipher.	Eg: Playfair,Vigenere, Hill Ciphers

4. PLAYFAIR CIPHER

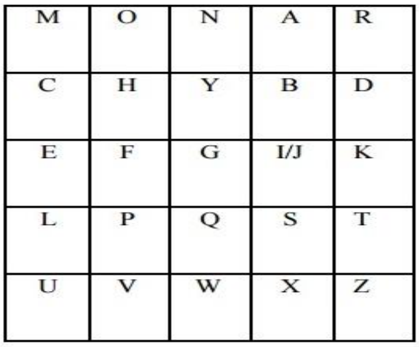
- **Multiple letter encryption cipher is the playfair**, which treats digrams in the plaintext as single units and translates these units into cipher text digrams.
- The playfair algorithm is based on the use of **5x5 matrix** of letters constructed using a keyword.
- The matrix is constructed by filling in the letters of the keyword (minus duplicates) from left to right and from top to bottom, and then filling in the remainder of the matrix with the remaining letters in alphabetical order.

The letter „i and „jcount as one letter.

Rules :

- Repeating plaintext letters that would fall in the same pair are separated with a filler letter such as „x
- Plaintext letters that fall in the **same row of the matrix are each replaced by the letter to the right**, with the first element of the row following the last.
- Plaintext letters that fall in the **same column are replaced by the letter beneath**, with the top element of the column following the last.
- **Otherwise, each plaintext letter is replaced by the letter that lies in its own row and the column occupied by the other plaintext letter**.

Let the keyword be, “MONARCHY”.



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

Plaintext = meet me at the school house

Splitting two letters as a unit => ME ET ME AT TH ES CH OX OL HO US EX

Corresponding cipher text => CL KL CL RS PD IL HY AV MP HF XL IU

5. VIGENERE CIPHER

In this scheme, the set of related monoalphabetic substitution rules consisting of 26 caesar ciphers with shifts of 0 through 25. Each cipher is denoted by a key letter.

e.g.,

Caesar cipher with a shift of 3 is denoted by the key value 'd‟ (since a=0, b=1, c=2 and so on). To aid in understanding the scheme, a matrix known as vigenere tableau is constructed.

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

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

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

Eg : **key = DECEPTIVEDECEPTIVEDECEPTIVE**

PT = WEAREDISCOVEREDSAVEYOURSELF

CT = ZICVTWQNGRZGVTWAVZHCQYGLMGJ

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

6. ONE TIME PAD CIPHER

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

$$C_i = P_i \oplus K_i$$

C_i - i^{th} binary digit of cipher text

P_i - i^{th} binary digit of plaintext

K_i - i^{th} binary digit of key

$\oplus$ – exclusive OR opearaiton

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

XOR Operation:

Same input -> ouput = 0

Different input -> output = 1

```
e.g.,   plaintext  = 0 0 1 0 1 0 0 1
        Key        = 1 0 1 0 1 1 0 0
                     ------------------
        ciphertext = 1 0 0 0 0 1 0 1
```

TRANSPOSITION TECHNIQUES

.A very different kind of mapping is achieved by performing some sort of permutation on the plaintext letters.This technique is referred to as a transposition cipher.

- They are of two types: **Keyed and Keyless Transposition Cipher**.

KEYLESS TRANSPOSITION CIPHER:

- In this cipher technique, the message is converted to ciphertext by either of two permutation techniques:

a. Text is written into a table column-by-column and is then transmitted row-by-row.

b. Text is written into a table row-by-row and is then transmitted column-by-column

- The first method (a) is also popularly known as **Rail-fence cipher**

RAIL FENCE TECHNIQUE

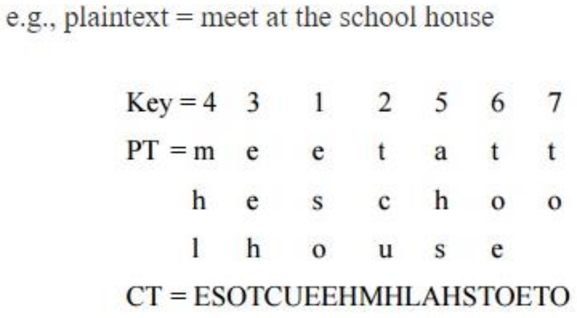
- **Rail fence** is simplest of such cipher, in which the plaintext is written down as a sequence of diagonals and then read off as a sequence of rows.
- For eg ,to encipher the message “ GOOD MORNING ” with a rail fence of depth 2,we write the following:

G		O		M		R		I		G
	O		D		O		N		N	

The encrypted message is : G O M R I G O D O N M

ROW TRANSPOSITION CIPHERS

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



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

Key = 4	3	1	2	5	6	7
PT = m	e	e	t	a	t	t
h	e	s	c	h	o	o
l	h	o	u	s	e	

CT = ESOTCUEEHMHLAHSTOETO

KEYED TRANSPOSITION CIPHER:

- In this approach, rather than permuting all the symbols together, we divide the entire plaintext into blocks of predetermined size and then permute each block independently.

Substitution TechniqueV/S Transposition Technique

Substitution Technique	Transposition Technique
It replaces the plaintext characters with other numbers, characters, and symbols.	It scrambles the character's position in the plaintext.
The character's identity is changed, while its position does not change	The character's identity is changed instead of its identity.
It utilizes the monoalphabetic, polyalphabetic substitution cipher, and Playfair cipher.	It utilizes the keyed and keyless transpositional ciphers.
Eg :Caesar Cipher	Eg: Rail Fence Cipher

STEGANOGRAPHY

Steganography is a method of hiding information by hiding the ***secret*** *message* within a *fake message*.

The steganography technique contains a cover carrier, stego key, secret message, and stego carrier.

Text, image, voice, and video are cover carriers for the secret information, and Stego carrier is produced by utilizing a cover carrier and an embedded message.

The Stego key may also be utilized as additional secret information, such as a password utilized by the receiver to extract the message.

There are various forms of steganography:

- Audio Steganography
- Image Steganography
- Video Steganography
- Text Steganography
- Network or Protocol Steganography

Steganography	Cryptography
It is less popular than cryptography.	It is more popular and commonly used than steganography.
It relies on the key.	It doesn't have any parameters.
Its main goal is to offer secure communication.	Its main goal is to provide data protection.
The structure of data is not frequently altered.	The structure of data is allowed to alter while encrypting
The attack's name in the steganography technique is steganalysis	The attack's name in cryptography is cryptanalysis
It offers only confidentiality and authentication.	It provides security principles, including integrity, secrecy, authentication, and non-repudiation.
Some of the techniques used in steganography are transformed domain embedding, spatial domain, and model-based.	It employs techniques such as stream, substitution, transpositional, and block ciphers.