# UNIT - I

## 1. 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 amusement 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 essentials of secret codes, augmented by modern mathematics that protects our data in powerful ways.

- **Computer Security** - generic name for the collection of tools designed to protect data and to thwarthackers
- **Network Security** - measures to protect data during theirtransmission
- **Internet Security** - measures to protect data during their transmission over a collection of interconnectednetworks.

### 1.1 WHY WE NEED INFORMATION SECURITY?

Because there are threats

**Threats**

A threat is an object, person, or other entity that represents a constant danger to an asset.

The 2007 CSI survey

- 494 computer security practitioners
- 46% suffered security incidents
- 29% reported to law enforcement
- Average annual loss $350,424
- 1/5 suffered _targeted attack‘
- The source of the greatest financial losses?
- Most prevalent security problem

- Insider abuse of network access
- Email

**Threat Categories**

- Acts of human error or failure
- Compromises to intellectual property
- Deliberate acts of espionage or trespass
- Deliberate acts of information extortion
- Deliberate acts of sabotage or vandalism
- Deliberate acts of theft
- Deliberate software attack
- Forces of nature
- Deviations in quality of service
- Technical hardware failures or errors
- Technical software failures or errors
- Technological obsolesce

## **Security Approaches**:

Here are some common security approaches in Cryptography and Network Security

Cryptography Security Approaches:

. Symmetric-key cryptography: Using the same key for encryption and decryption (e.g., AES).

Asymmetric-key cryptography: Using a pair of keys: public for encryption and private for decryption (e.g., RSA).

Hash-based cryptography: Using one-way hash functions for data integrity and authenticity (e.g., SHA-256).

Digital signatures: Using asymmetric cryptography to authenticate and ensure non-repudiation.

Homomorphic encryption: Enabling computations on encrypted data without decrypting it first.

## **Principles of Security:**

Defense in depth: Layering multiple security mechanisms to protect against various threats.

2. Least privilege: Granting only necessary access rights and permissions.

3. Segregation of duties: Dividing responsibilities to prevent single points of failure.

4. Secure communication protocols: Using protocols like TLS, IPsec, and SSH to protect data in transit.

5. Regular updates and patching: Keeping software and systems up-to-date to prevent exploitation of known vulnerabilities.

6. Monitoring and incident response: Detecting and responding to security incidents.

7. User education and awareness: Educating users about security best practices and threats.

NOTE:

1. TLS: Transport Layer Security, 2. IPsec: Internet Protocol Security, 3. SSH: Secure Shell

**Types Of Security Attacks:**

Here are some common types of security attacks in Cryptography and Network Security:

Cryptography Attacks:

1. Brute-force attacks: Trying all possible keys or combinations to decrypt data.

2. Side-channel attacks: Exploiting implementation flaws or environmental factors (e.g., timing, power consumption).

3. Differential cryptanalysis: Analyzing differences in ciphertext to deduce encryption keys.

4. Linear cryptanalysis: Using linear approximations to attack block ciphers.

5. Man-in-the-middle (MITM) attacks: Intercepting and altering encrypted communications.

6. Replay attacks: Reusing encrypted messages to gain unauthorized access.

7. Key exhaustion attacks: Forcing a system to generate new keys, potentially leading to weak keys.

8. Quantum computer attacks: Using quantum computers to break certain encryption algorithms.

## 1.2 ASPECTS OF SECURITY

- consider 3 aspects of information security:
- **Security Attack**
- **Security Mechanism**
- **Security Service**

## 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 securityattack.

**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.

## 1.3 SECURITY SERVICES

The classification of security services are as follows:

**Confidentiality:**Ensures that the information in a computer system and transmitted information are accessible only for reading by authorizedparties.

E.g. Printing, displaying and other forms of disclosure.

**Authentication:** Ensures that the origin of a message or electronic document is correctly identified, with an assurance that the identity is not false.

**Integrity:** Ensures that only authorized parties are able to modify computer system assets and transmitted information. Modification includes writing, changing status, deleting, creating anddelaying or replaying of transmittedmessages.

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

**Access control**: Requires that access to information resources may be controlled by or the target system.

**Availability**: Requires that computer system assets be available to authorized parties when needed.

## 1.4 SECURITY MECHANISMS

One of the most specific security mechanisms in use is cryptographic techniques. Encryption or encryption-like transformations of information are the most common means of providing security. Some of the mechanisms are

**Encipherment**

**DigitalSignature**

**AccessControl**

According to X.800, the security mechanisms are divided into those implemented in a specific protocol

layer and those that are not specific to any particular protocol layer or security service. X.800 also differentiates reversible & irreversible encipherment mechanisms. A reversible encipherment mechanism is simply an encryption algorithm that allows data to be encrypted and subsequently decrypted, whereas irreversible encipherment include hash algorithms and message authentication codesused in digital signature and message authentication applications.Incorporated into the appropriate protocol layer in order to provide some of the OSI security services,

**Encipherment:**

It refers to the process of applying mathematical algorithms forconverting data into a form that is not intelligible. This depends on algorithm used encryption keys.

**Digital Signature:** The appended data or a cryptographic transformation applied to anydata unit allowing to prove the source and integrity of the data unit and protect against forgery.

**Access Control:** A variety of techniques used for enforcing access permissions to thesystem resources

**Data Integrity:** A variety of mechanisms used to assure the integrity of a data unit orstream of data units.

**Authentication Exchange:** A mechanism intended to ensure the identity of an entity by means of information exchange.

**Traffic Padding:** The insertion of bits into gaps in a data stream to frustrate traffic analysis attempts.

**Routing Control:** Enables selection of particular physically secure routes for certain data and allows routing changes once a breach of security is suspected.

**Notarization:** The use of a trusted third party to assure certain properties of a data exchange

**Pervasive Security Mechanisms**

These are not specific to any particular OSI security service or protocol layer.

**Trusted Functionality:** That which is perceived to b correct with respect to some criteria **Security Level:** The marking bound to a resource (which may be a data unit) that names or designates the security attributes of that resource.

**Event Detection:** It is the process of detecting all the events related to network security. **Security Audit Trail:** Data collected and potentially used to facilitate a security audit, which is an independent review and examination of system records and activities. **Security Recovery:** It deals with requests from mechanisms, such as event handling and management functions, and takes recovery actions.

## 1.5 SECURITYATTACKS

There are four general categories of attack which are listed below.

### Interruption

An asset of the system is destroyed or becomes unavailable or unusable. This is an attack on availability e.g., destruction of piece of hardware, cutting of a communication line or

Disabling of file management system.

### Interception

An unauthorized party gains access to an asset. This is an attack on confidentiality.

Unauthorized party could be a person, a program or a

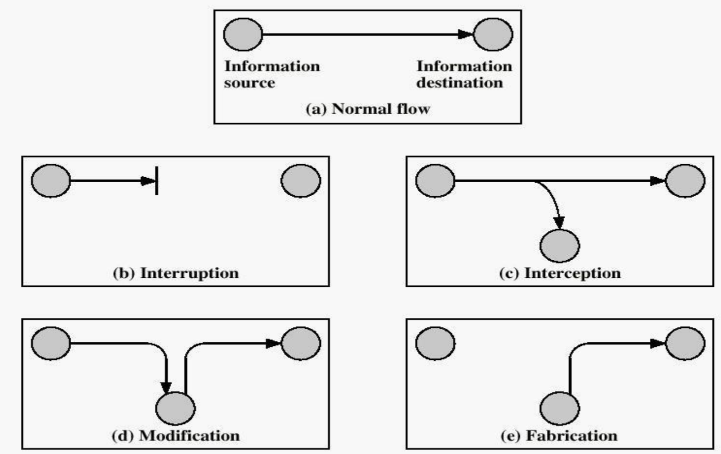
Computer .e.g., wire tapping to capture data in the network, illicit copying of files

### Modification

An unauthorized party not only gains access to but tampers with an asset. This is an attack on integrity. e.g., changing values in data file, altering a program, modifying the contents of messages being transmitted in a network.

### Fabrication

An unauthorized party inserts counterfeit objects into the system. This is an attack on authenticity. e.g., insertion of spurious message in a network or addition of records to a file.



(a) Normal flow

(b) Interruption

(c) Interception

(d) Modification

(e) Fabrication

Figure 1.1 Security Threats

## CRYPTOGRAPHIC ATTACKS

## PASSIVE ATTACKS

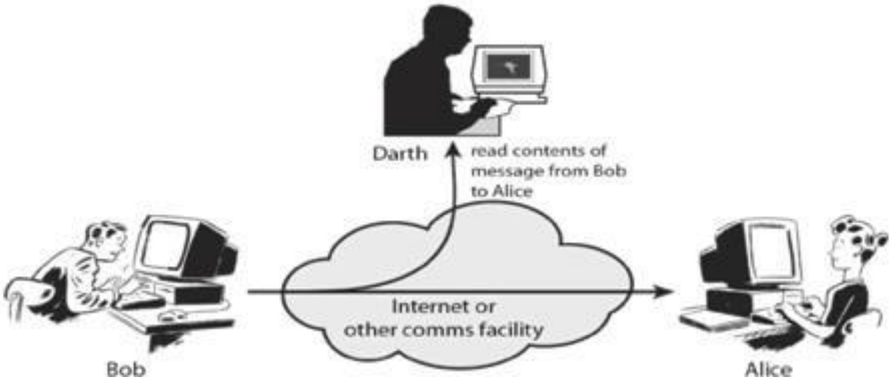
Passive attacks are in the nature of eavesdropping on, or monitoring of, transmissions. The goal of the opponent is to obtain information that is being transmitted. Passive attacks are of two types:

**Release of message contents:** A telephone conversation, an e-mail message and a transferred file may

contain sensitive or confidential information. We would like to prevent the opponent from learning the contents of these transmissions.

**Traffic analysis**: If we had encryption protection in place, an opponent might still be able to observe the pattern of the message. The opponent could determine the location and identity of communication hosts and could observe the frequency and length of messages being exchanged. This information might be useful in guessing the nature of communication that was taking place.

Passive attacks are very difficult to detect because they do not involve any alteration of data. However, it is feasible to prevent the success of these attacks.


Darth
read contents of message from Bob to Alice
Internet or other comms facility
Bob
Alice

## ACTIVE ATTACKS

These attacks involve some modification of the data stream or the creation of a false stream. These attacks can be classified in to four categories:

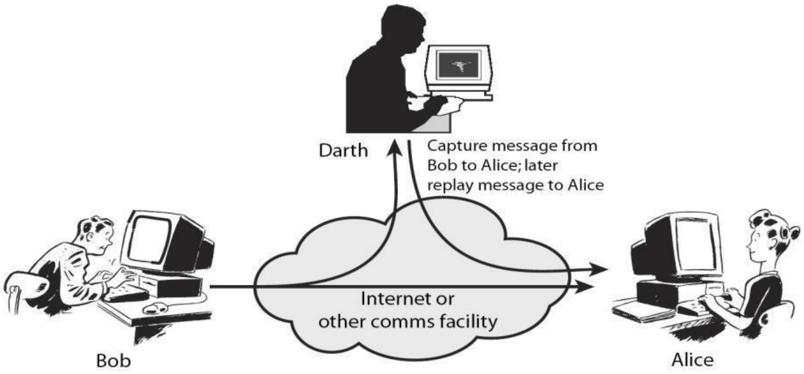
**Masquerade** – One entity pretends to be a different entity.

**Replay** – involves passive capture of a data unit and its subsequent transmission to produce an unauthorized effect.

**Modification of messages** – Some portion of message is altered or the messages are delayed or recorded, to produce an unauthorized effect.

**Denial of service** – Prevents or inhibits 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.

It is quite difficult to prevent active attacks absolutely, because to do so would require physical protection of all communication facilities and paths at all times. Instead, the goal is to detect them and to recover from any disruption or delays caused by them.


Darth
Capture message from Bob to Alice; later replay message to Alice
Internet or other comms facility
Bob
Alice

## 1.6 BASIC CONCEPTS

**Cryptography** The art or science encompassing the principles and methods of transforming an intelligible message into one that is unintelligible, and then retransforming that message back to its original form

**Plaintext** The original intelligible message

**Cipher text** The transformed message

**Cipher** An algorithm for transforming an intelligible message into one that is unintelligible by transposition and/or substitution methods

**Key** Some critical information used by the cipher, known only to the sender& receiver

**Encryption** The process of converting plaintext to cipher text using a cipher and a key

**Decryption** The process of converting cipher text back into plaintext using a cipher and a key

**Cryptanalysis** The study of principles and methods of transforming an unintelligible message back into an intelligible message *without* knowledge of the key. Also called **codebreaking**

**Cryptology** Both cryptography and cryptanalysis

**Code** An algorithm for transforming an intelligible message into an unintelligible one using a code-book

## 1.7 CRYPTOGRAPHY

Cryptographic systems are generally classified along 3 independent dimensions:

**Type of operations used for transforming plain text to cipher text**

All the encryption algorithms are based on two general principles: **substitution**, in which each element in the plaintext is mapped into another element, and **transposition**, in which elements in the plaintext arerearranged.

**The number of keys used**

If the sender and receiver uses same key then it is said to be **symmetric key (or) single key (or) conventional encryption**.

If the sender and receiver use different keys then it is said to be **public key encryption**.

**The way in which the plain text is processed**

A **block cipher** processes the input and block of elements at a time, producing output block for each input block.A**stream cipher** processes the input elements continuously, producing output element one at a time, as it goes along.

**CRYPTANALYSIS**

The process of attempting to discover X or K or both is known as cryptanalysis. The strategy used by the cryptanalysis depends on the nature of the encryption scheme and the information available to the cryptanalyst.

**There are various types of cryptanalytic attacks**based on the amountof information known to thecryptanalyst.

**Cipher text only** – A copy of cipher text alone is known to the cryptanalyst.

**Known plaintext** – The cryptanalyst has a copy of the cipher text and the corresponding plaintext.

**Chosen plaintext** – The cryptanalysts gains temporary access to the encryption machine. They cannot open it to find the key, however; they can encrypt a large number of suitably chosen plaintexts and try to use the resulting cipher texts to deduce the key.

**Chosen cipher text** – The cryptanalyst obtains temporary access to the decryption machine, uses it to decrypt several string of symbols, and tries to use the results to deduce the key

## SYMMETRIC AND PUBLIC KEY ALGORITHMS

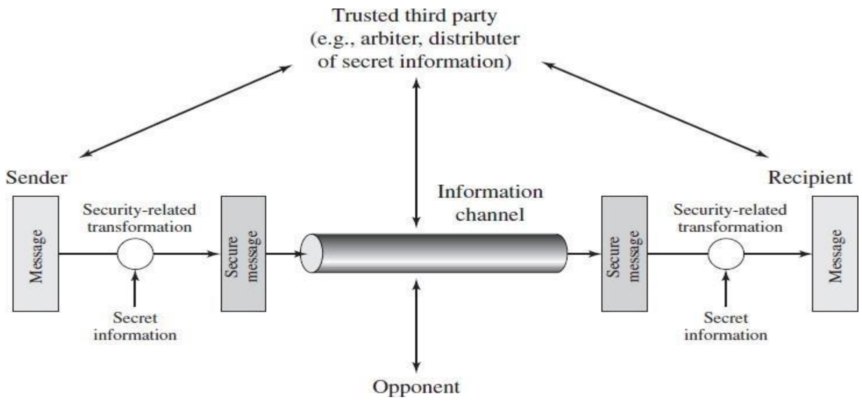
Encryption/Decryption methods fall into two categories.

Symmetric key Public key

In symmetric key algorithms, the encryption and decryption keys are known both to sender and receiver. The encryption key is shared and the decryption key is easily calculated from it. In many cases, the encryption and decryption keys are thesame.

In public key cryptography, encryption key is made public, but it is computationally infeasible to find the decryption key without the information known to the receiver.

## 1.8 A MODEL FOR NETWORK SECURITY



A message is to be transferred from one party to another across some sort of internet. The two parties, who are the principals in this transaction, must cooperate for the exchange to take place. A logical information channel is established by defining a route through the internet from source to destination and by the cooperative use of communication protocols (e.g., TCP/IP) by the twoprincipals.

**Using this model requires us to:**

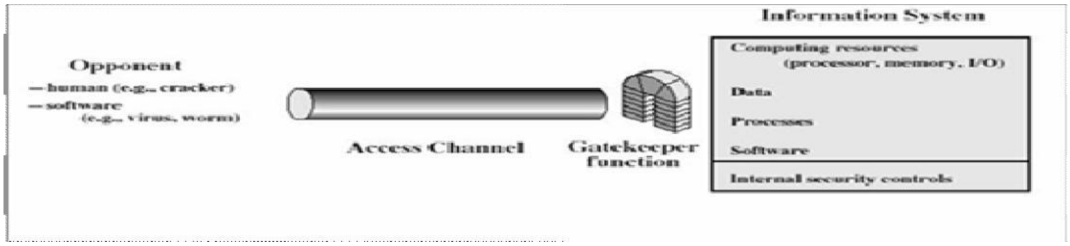
– design a suitable algorithm for the securitytransformation

– generate the secret information (keys) used by thealgorithm

– develop methods to distribute and share the secretinformation

– specify a protocol enabling the principals to use the transformation and secret information for a securityservice

**MODEL FOR NETWORK ACCESS SECURITY**



**Using this model requires us to:**

– select appropriate gatekeeper functions to identifyusers

– implement security controls to ensure only authorized users access designated information orresources

- **Trusted computer systems can be used to implement thismodel**

### 1.9 CONVENTIONAL ENCRYPTION

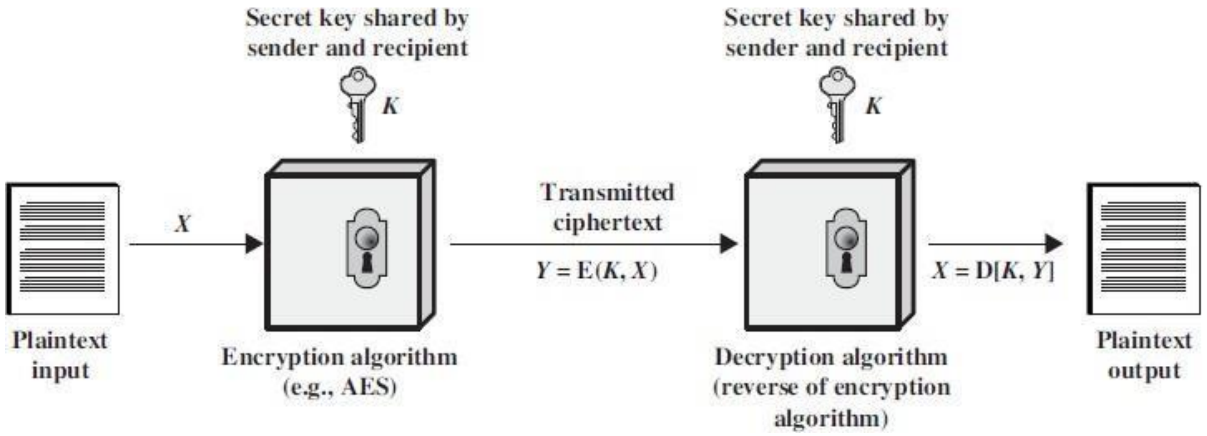
- Referred conventional / private-key /single-key
- Sender and recipient share a common key

All classical encryption algorithms are private-key was only type prior to invention of public- key in 1970‟**plaintext** - the originalmessage

Some basic terminologies used:

- **cipher text** - the codedmessage
- **Cipher** - algorithm for transforming plaintext to ciphertext
- **Key** - info used in cipher known only tosender/receiver
- **encipher (encrypt)** - converting plaintext to ciphertext
- **decipher (decrypt)** - recovering cipher text fromplaintext
- **Cryptography** - study of encryptionprinciples/methods
- **Cryptanalysis (code breaking)** - the study of principles/ methods of deciphering ciphertext

  *without*knowing key
- **Cryptology** - the field of both cryptography andcryptanalysis


Secret key shared by sender and recipient
K
Secret key shared by sender and recipient
K
X
Transmitted ciphertext
Y = E(K, X)
X = D[K, Y]
Plaintext input
Encryption algorithm (e.g., AES)
Decryption algorithm (reverse of encryption algorithm)
Plaintext output

Here the original message, referred to as plaintext, is converted into apparently random nonsense, referred to as cipher text. The encryption process consists of an algorithm and a key. The key is a value independent of the plaintext. Changing the key changes the output of the algorithm. Once the cipher text is produced, it may be transmitted.Uponreception,thecipher text can be transformed back to the original plaintext by using a decryption algorithm and the same key that was used for encryption. The security depends on several factors. First, the encryption algorithm must be powerful enough that it is impractical to decrypt a message on the basis of cipher text alone. Beyond that, the security depends on the secrecy of the key, not the secrecy of thealgorithm.

- **Two requirements for secure use of symmetricencryption:**

– A strong encryptionalgorithm
– A secret key known only to sender /receiver

$Y = \mathrm{E}K(X)$

$X = \mathrm{D}K(Y)$

- **assume encryption algorithm isknown**
- **implies a secure channel to distributekey**

A source produces a message in plaintext, X = [X1, X2… XM] where M are the number of letters in the message. A key of the form K = [K1, K2… KJ] is generated. If thekey is generated at the source, then it must be provided to the destination by means of some secure channel.

With the message X and the encryption key K as input, the encryption algorithm forms the cipher text Y = [Y1, Y2, YN]. This can be expressed as

$Y = \mathrm{E}_K(X)$

The intended receiver, in possession of the key, is able to invert the transformation:

$X = \mathrm{D}_K(Y)$

If the opponent is interested in only this particular message, then the focus of effort is to recover Xby generating a plaintext estimate. Often if the opponent is interested in being able to read future messages as well, in which case an attempt is made to recover K by generating anestimate.

## 1.10 CLASSICAL ENCRYPTION TECHNIQUES

There are two basic building blocks of all encryption techniques: 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 cipher text bit patterns.

### Caesar cipher (or) shift cipher

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

e.g., plain text : pay more money Cipher text: SDB PRUH PRQHB

Notethatthealphabetiswrappedaround,sothatletterfollowing„z‟is„a‟. For each plaintext letter p, substitute the cipher text letter c suchthat

C = E(p) = (p+3) mod 26

A shift may be any amount, so that general Caesar algorithmis C = E (p) = (p+k) mod26

Where k takes on a value in the range 1 to 25. The decryption algorithm is simply P = D(C) = (C-k) mod26

### PLAYFAIR CIPHER

The best known multiple letter encryption cipher is the playfair, which treats diagrams in plaintextassingleunitsandtranslatestheseunitsintociphertextdigrams.Theplayfairalgorithm is based on the use of 5x5 matrix of letters constructed using a keyword. Let the keyword be „monarchy‟. The matrix is constructed by filling in the letters of the keyword (minus duplicates) from left to right and from top to bottom, and then filling in the remainder of the matrix with the remaining letters in alphabeticalorder.

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

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

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

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

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

| | | | | |
|---|---|---|---|---|
| M | O | N | A | R |
| C | H | Y | B | D |
| E | F | G | I<br>/<br>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 thescho xol ho us ex Correspondingciphertext

=>CL KL CL RS PD IL HY AV MP HF XLIU

**Strength of playfair cipher**

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

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

**POLYALPHABETIC CIPHERS**

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

A set of related monoalphabetic substitution rules are used

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

**Vigenere cipher**

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

26 caesar ciphers with shifts of 0 through 25. Each cipher is denoted by a key letter. e.g., Caesar cipher with a shift of 3 is denoted by the key value 'd‟ (since a=0, b=1, c=2 and so on). Toaid 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 processof

| | PLAIN TEXT | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| K | | a | b | c | D | e | f | g | H | i | j | k | … | x | y | Z |
| | a | A | B | C | D | E | F | G | H | I | J | K | … | X | Y | Z |

| | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| E<br>Y<br>L<br>E<br>T<br>T<br>E<br>R<br>S | b | B | C | D | E | F | G | H | I | J | K | L | … | Y | Z | A |
| | c | C | D | E | F | G | H | I | J | K | L | M | … | Z | A | B |
| | d | D | E | F | G | H | I | J | K | L | M | N | … | A | B | C |
| | e | E | F | G | H | I | J | K | L | M | N | O | … | B | C | D |
| | f | F | G | H | I | J | K | L | M | N | O | P | … | C | D | E |
| | g | G | H | I | J | K | L | M | N | O | P | Q | … | D | E | F |
| | :<br>: | :<br>: | :<br>: | :<br>: | :<br>: | :<br>: | :<br>: | :<br>: | :<br>: | :<br>: | :<br>: | :<br>: | … | :<br>: | :<br>: | :<br>: |
| | x | X | Y | Z | A | B | C | D | E | F | G | H | … | | | W |
| | y | Y | Z | A | B | C | D | E | F | G | H | I | … | | | X |
| | z | Z | A | B | C | D | E | F | G | H | I | J | … | | | Y |

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

V.

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

e.g., key = d e c e p t i v e d e c e p t i v e d e c e p t ivePT = w e a r e d i s c o v e r e d s a v e y o u r s e lfCT =ZICVTWQNGRZGVTWAVZHCQYGLMGJ

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

Strength of Vigenere cipher

- There are multiple cipher text letters for each plaintextletter.
- Letter frequency information isobscured.

## 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 discardedandneverusedagain.Thesystemcanbeexpressedas

Follows:

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

Exclusive OR operation

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

$\oplus$

$P_i$= $C_iK_i$

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

Key = 1 0 1 0 1 1 0 0

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

Advantage:

Encryption method is completely unbreakable for a ciphertext only attack.

Disadvantages

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

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

**TRANSPOSITION TECHNIQUES**

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

**Rail fence**

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

Plaintext= meet at the schoolhouse

To encipher this message with a rail fence of depth 2, we write the message as follows: m e a t e c o l os

e t t h s h o h u e The encrypted message is MEATECOLOSETTHSHOHUE

**Row TranspositionCiphers-**

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

e.g., plaintext = meet at the schoolhouse

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 eCT =ESOTCUEEHMHLAHSTOETO

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

## Symmetric key Cryptography

Symmetric key cryptography plays a crucial role in Cryptography and Network Security (CNS). It is one of the fundamental pillars for securing data in various applications, including secure communications, data storage, and authentication systems. Below is an overview of symmetric key cryptography within the context of CNS

Symmetric key cryptography involves the use of a single secret key for both encryption and decryption of data. Both the sender and receiver must possess the same key and keep it confidential to ensure secure communication.

## Asymmetric key Cryptography

Asymmetric key cryptography, also known as public-key cryptography, is a critical component of Cryptography and Network Security (CNS). It addresses some of the limitations of symmetric key cryptography, particularly in the areas of secure key distribution and authentication. Here’s an overview of asymmetric key cryptography within the context of CNS

Asymmetric key cryptography uses a pair of keys—a public key and a private key—that are mathematically related. The public key can be freely distributed and used by anyone to encrypt data or verify a digital signature, while the private key is kept secret and is used to decrypt data or create a digital signature.

## 1.11 STEGANOGRAPHY

A plaintext message may be hidden in any one of the two ways. The methods of steganography conceal the existence of the message, whereas the methods of cryptography render the message unintelligible to outsiders by various transformations of thetext.

A simple form of steganography, but one that is time consuming to construct is one in which an arrangement of words or letters within an apparently innocuous text spells out the realmessage.

e.g., (i) the sequence of first letters of each word of the overall message spells out the real (Hidden)message.

(ii) Subset of the words of the overall message is used to convey the hidden message.

Various other techniques have been used historically, some of them are

Character marking – selected letters of printed or typewritten text are overwritten in pencil. The

marks are ordinarily not visible unless the paper is held to an angle to bright light.

Invisible ink – a number of substances can be used for writing but leave no visible trace until heat or some chemical is applied to the paper.

Pin punctures – small pin punctures on selected letters are ordinarily not visible unless the paper is held in front of the light. Typewritten correction ribbon – used between the lines typed with a black ribbon, the results of typing with the correction tape are visible only under a strong light.

Drawbacks of steganography

Requires a lot of overhead to hide a relatively few bits of information. Once the system is discovered, it becomes virtually worthless.

## 1.12 KEY RANGE AND KEY SIZE

The encrypted message can be attacked and the crypt analyst may have the following information:

1) The encryption Decryption algorithm

2) The Encrypted Message

3) Key

The attack may be in terms of following types:

a) Plain Text only attack(Known plain text  attack)

b) Cipher text only attack(known cipher text attack)

c) Chosen plain text attack

d) Chosen cipher text attack

The simplest type of attack is brute force attack in which all types of substitution techniques are used to fetch original message .A Brute force attack works on a principal of trying everything possible key from the key range. Key range may contain individual single arbitrary quantity whereas key size defines the total or maximum capacity of all the keys.

**EXHAUSTIVE KEY SEARCH:**

It is basically used by the side of cryptanalyst. Basically the procedure for exhaustive keys search becomes more complex as the key size that means number of bits are increased. The time required for single encryption message and entire message would be automatically increased.

All encryption algorithm are having two main criteria for encryption-

1) The cost of breaking the cipher exceeds the value of encryption information.

**2)** The time required to break the cipher exceeds the useful timeline of the information.

An encryption scheme is said to be comparatively secure if the above criteria are met

## 1.13 POSSIBLE TYPES OF ATTACKS

Without security measures and controls in place, your data might be subjected to an attack. Some attacks are passive, meaning information is monitored; others are active, meaning the information is altered with intent to corrupt or destroy the data or the network itself.

Your networks and data are vulnerable to any of the following types of attacks if you do not have a security plan in place.

### Eavesdropping

In general, the majority of network communications occur in an unsecured or "cleartext" format, which allows an attacker who has gained access to data paths in your network to "listen in" or interpret (read) the traffic. When an attacker is eavesdropping on your communications, it is referred to as sniffing or snooping. The ability of an eavesdropper to monitor the network is generally the biggest security problem that administrators face in an enterprise. Without strong encryption services that are based on cryptography, your data can be read by others as it traverses the network.

### Data Modification

After an attacker has read your data, the next logical step is to alter it. An attacker can modify the data in the packet without the knowledge of the sender or receiver. Even if you do not require confidentiality for all communications, you do not want any of your messages to be modified in transit. For example, if you are exchanging purchase requisitions, you do not want the items, amounts, or billing information to be modified.

### Identity Spoofing (IP Address Spoofing)

Most networks and operating systems use the IP address of a computer to identify a valid entity. In certain cases, it is possible for an IP address to be falsely assumed— identity spoofing. An attacker might also use special programs to construct IP packets that appear to originate from valid addresses inside the corporate intranet.

After gaining access to the network with a valid IP address, the attacker can modify, reroute, or delete your data. The attacker can also conduct other types of attacks, as described in the following sections.

### Password-Based Attacks

A common denominator of most operating system and network security plans is password-based access control. This means your access rights to a computer and network resources are determined by who you are, that is, your user name and your password.

Older applications do not always protect identity information as it is passed through the network for validation. This might allow an eavesdropper to gain access to the network by posing as a valid user.

When an attacker finds a valid user account, the attacker has the same rights as the real user. Therefore, if the user has administrator-level rights, the attacker also can create accounts for subsequent access at a later time.

After gaining access to your network with a valid account, an attacker can do any of the following:

- Obtain lists of valid user and computer names and network information.
- Modify server and network configurations, including access controls and routing tables.
- Modify, reroute, or delete your data.

### Denial-of-Service Attack

Unlike a password-based attack, the denial-of-service attack prevents normal use of your computer or network by valid users.

After gaining access to your network, the attacker can do any of the following:

- Randomize the attention of your internal Information Systems staff so that they do not see the intrusion immediately, which allows the attacker to make more attacks during the diversion.
- Send invalid data to applications or network services, which causes abnormal termination or behavior of the applications or services.
- Flood a computer or the entire network with traffic until a shutdown occurs because of the overload.
- Block traffic, which results in a loss of access to network resources by authorized users.

### Man-in-the-Middle Attack

As the name indicates, a man-in-the-middle attack occurs when someone between you and the person with whom you are communicating is actively monitoring, capturing, and controlling your communication transparently. For example, the attacker can re-route a data exchange. When computers are communicating at low levels of the network layer, the computers might not be able to determine with whom they are exchanging data.

Man-in-the-middle attacks are like someone assuming your identity in order to read your message. The person on the other end might believe it is you because the attacker might be actively replying *as you* to keep the exchange going and gain more information. This attack is capable of the same damage as an application-layer attack, described later in this section.

**Compromised-Key Attack**

A key is a secret code or number necessary to interpret secured information. Although obtaining a key is a difficult and resource-intensive process for an attacker, it is possible. After an attacker obtains a key, that key is referred to as a compromised key.

An attacker uses the compromised key to gain access to a secured communication without the sender or receiver being aware of the attack.With the compromised key, the attacker can decrypt or modify data, and try to use the compromised key to compute additional keys, which might allow the attacker access to other secured communications.

**Sniffer Attack**

A *sniffer* is an application or device that can read, monitor, and capture network data exchanges and read network packets. If the packets are not encrypted, a sniffer provides a full view of the data inside the packet. Even encapsulated (tunneled) packets can be broken open and read unless they are encrypted *and* the attacker does not have access to the key.

Using a sniffer, an attacker can do any of the following:

- Analyze your network and gain information to eventually cause your network to crash or to become corrupted.
- Read your communications.

**Application-Layer Attack**

An application-layer attack targets application servers by deliberately causing a fault in a server's operating system or applications. This results in the attacker gaining the ability to bypass normal access controls. The attacker takes advantage of this situation, gaining control of your application, system, or network, and can do any of the following:

- Read, add, delete, or modify your data or operating system.
- Introduce a virus program that uses your computers and software applications to copy viruses throughout your network.
- Introduce a sniffer program to analyze your network and gain information that can eventually be used to crash or to corrupt your systems and network.

- Abnormally terminate your data applications or operating systems.
- Disable other security controls to enable future attacks.