ECT-434
SECURE COMMUNICATION

Module 1:
Introduction and Classic Encryption Techniques

Bushara A R
AP, ECE
KMEA ENGINEERING COLLEGE

Module 1: Introduction and Classic Encryption Techniques

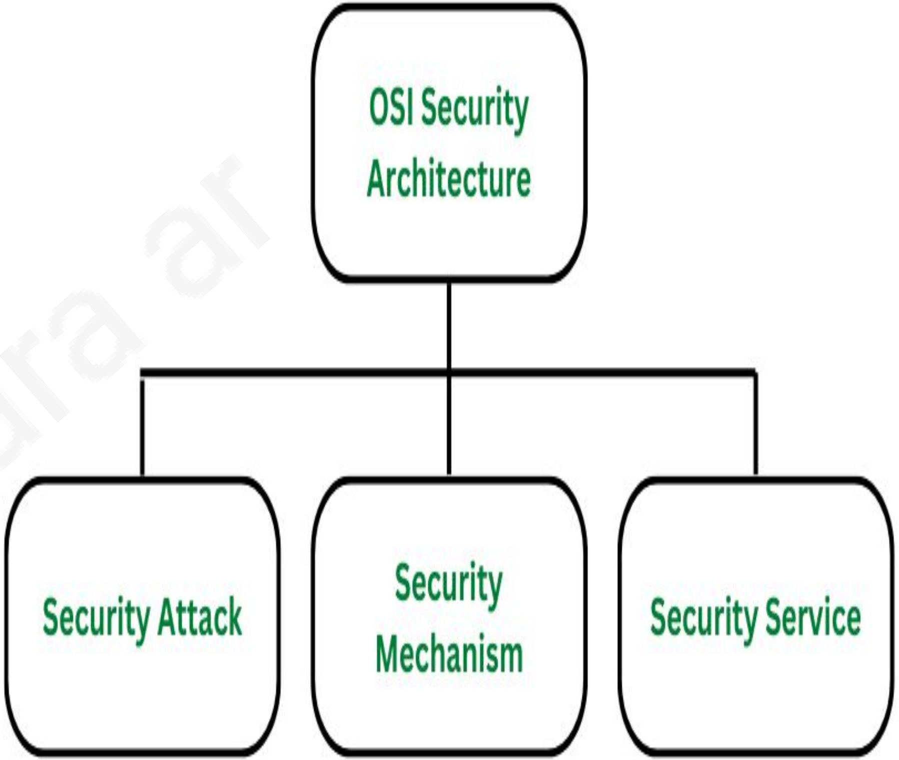
1. OSI security architecture
2. Security attacks – Passive attacks, Active attacks
3. Security services- Authentication, Access Control, Data Confidentiality, Data integrity, Nonrepudiation, Availability service.
4. Model for network security.
5. Symmetric cipher model, Cryptography, Cryptanalysis
6. Substitution techniques- Hill Cipher, One time pad
7. Transposition Techniques

1. OSI security architecture

- The **security of an organization** is the greatest concern of the people working at the organization. **Safety and security** are the pillars of cyber technology.
- It is hard to imagine the cyber world without thinking about security.
- The architecture of security is thus a very important aspect of the organization.
- The **OSI (Open Systems Interconnection)** Security Architecture defines a systematic approach to providing security at each layer.
- It defines **security services and security mechanisms** that can be used at each of the seven layers of the OSI model to provide security for data transmitted over a network.
- These security services and mechanisms help to ensure the **confidentiality, integrity, and availability** of the data.
- OSI architecture is internationally acceptable as it lays the flow of providing safety in an organization.

OSI Security Architecture focuses on these concepts:

- Security Attack
- Security mechanism
- Security Service



OSI Security Architecture is categorized into three broad categories namely **Security Attacks, Security mechanisms, and Security Services.**

1. Security Attacks:

A security attack is an attempt by a person or entity to gain unauthorized access to disrupt or compromise the security of a system, network, or device. These are defined as the actions that put at risk an organization's safety. They are further classified into 2 sub-categories:

A. Passive Attack: B. Active Attacks:

2. Security Mechanism

The mechanism that is built to identify any breach of security or attack on the organization, is called a security mechanism. Security Mechanisms are also responsible for protecting a system, network, or device against unauthorized access, tampering, or other security threats.

3. Security Services:

Security services refer to the different services available for maintaining the security and safety of an organization. They help in preventing any potential risks to security. Security services are divided into 5 types:

Authentication, Access control, Data Confidentiality, Data integrity, Non- repudiation

Benefits of OSI Architecture:

Below listed are the benefits of OSI Architecture in an organization:

1. Providing Security:

- OSI Architecture in an organization provides the needed security and safety, preventing potential threats and risks.
- Managers can easily take care of the security and there is hassle-free security maintenance done through OSI Architecture.

2. Organising Task:

- The OSI architecture makes it easy for managers to build a security model for the organization based on strong security principles.
- Managers get the opportunity to organize tasks in an organization effectively.

3. Meets International Standards:

- Security services are defined and recognized internationally meeting international standards.
- The standard definition of requirements defined using OSI Architecture is globally accepted.

2. Security attacks – Passive attacks, Active attacks

- A passive attack attempts to learn or make use of information from the system but does **not affect system resources.**
- An active attack attempts to **alter system** resources or affect their operation.

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.
- Two types of passive attacks are **release of message contents** and **traffic analysis.**

a. Release of message contents

- The release of message contents is easily understoo (Figure 1). A telephone conversation, an electronic mail message, and a transferred file may contain sensitive or confidential information.
- We would like to prevent an opponent from learning the contents of these transmissions.

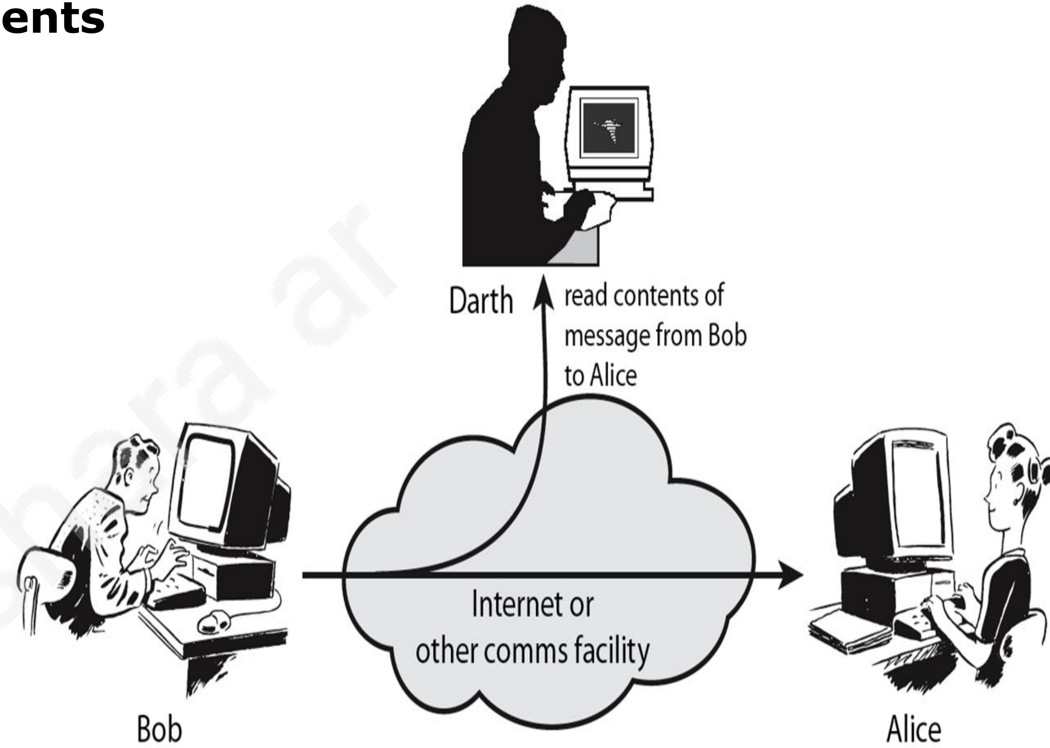

Darth
read contents of message from Bob to Alice
Internet or other comms facility
Bob
Alice

Figure 1. **Release of message contents**

B. Traffic analysis

A second type of passive attack, traffic analysis, is subtler

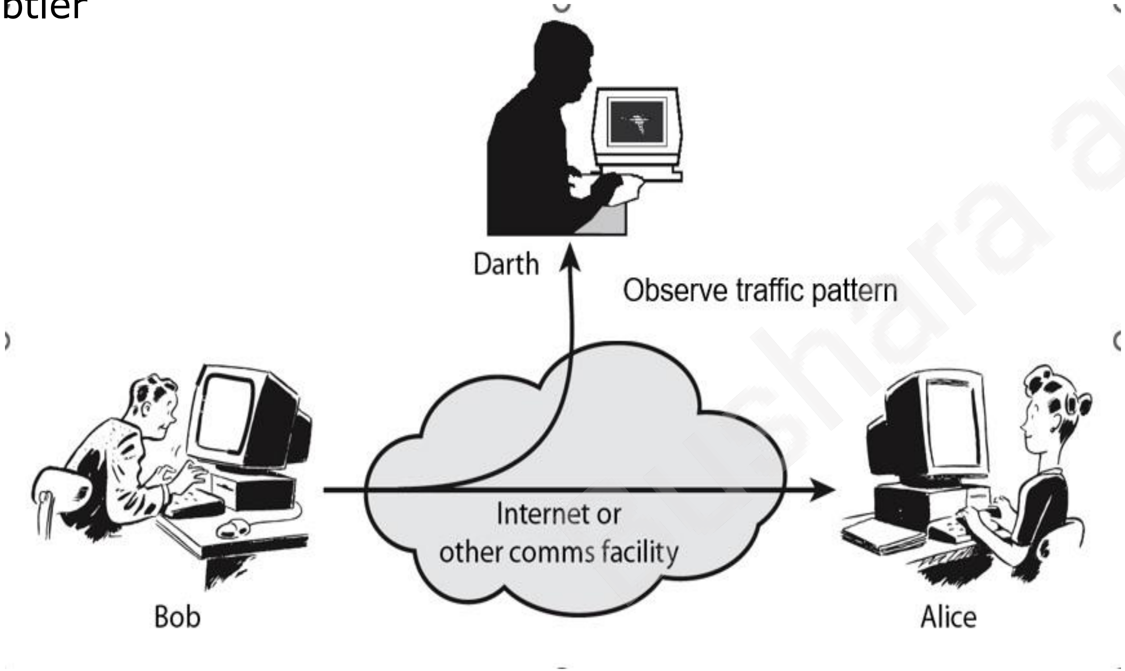


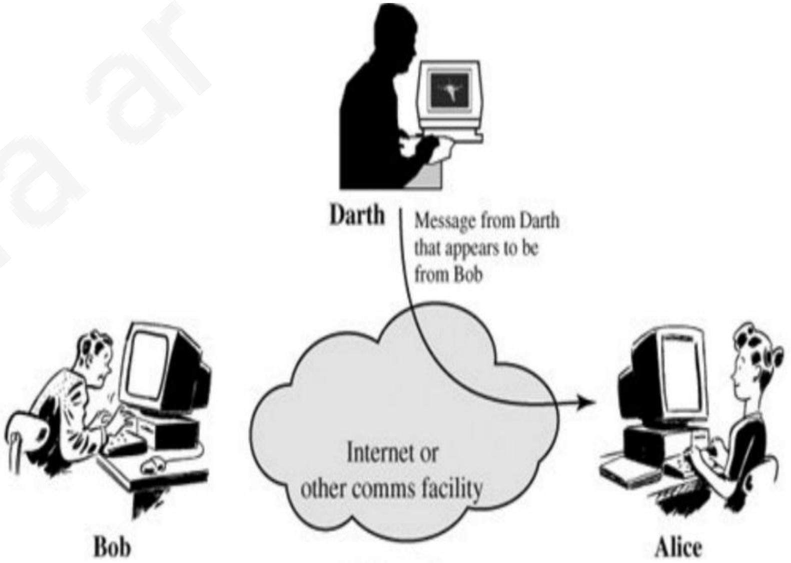
Fig. 2 Traffic analysis

- Passive attacks are very difficult to detect because they **do not involve any alteration of the data**.
- Typically, the message traffic is sent and received in an apparently normal fashion and neither the sender nor receiver is aware that a third party has read the messages or observed the traffic pattern.
- However, it is feasible to prevent the success of these attacks, usually by means of **encryption.**

Active Attacks

Active attacks involve some modification of the data stream or the creation of a false stream and can be subdivided into four categories: **masquerade, replay, modification of messages, and denial of service.**

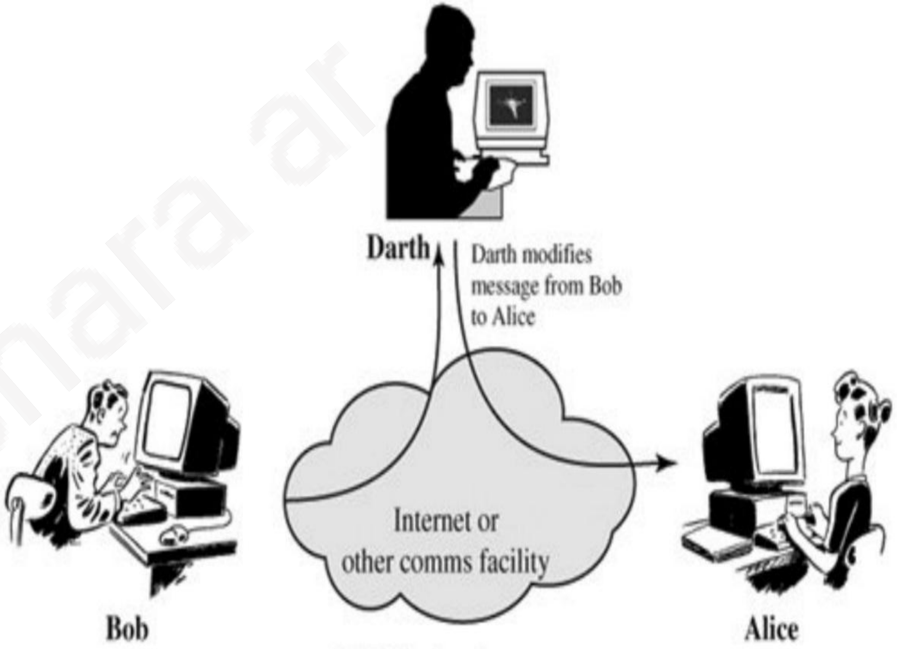
- A **masquerade** takes place when one entity pretends to be a different entity (Figure a).
- A masquerade attack usually includes one of the other forms of active attack.
- For example, authentication sequences can be captured and replayed after a valid authentication sequence has taken place, thus enabling an authorized entity with few privileges to obtain extra privileges by **impersonating** an entity that has those privileges.


Darth
Message from Darth that appears to be from Bob
Internet or other comms facility
Bob
Alice

(a) Masquerade

Modification of messages

- 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 (Figure c).
- 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**."


Darth
Darth modifies message from Bob to Alice
Internet or other comms facility
Bob
Alice

(c) Modification of messages

Replay

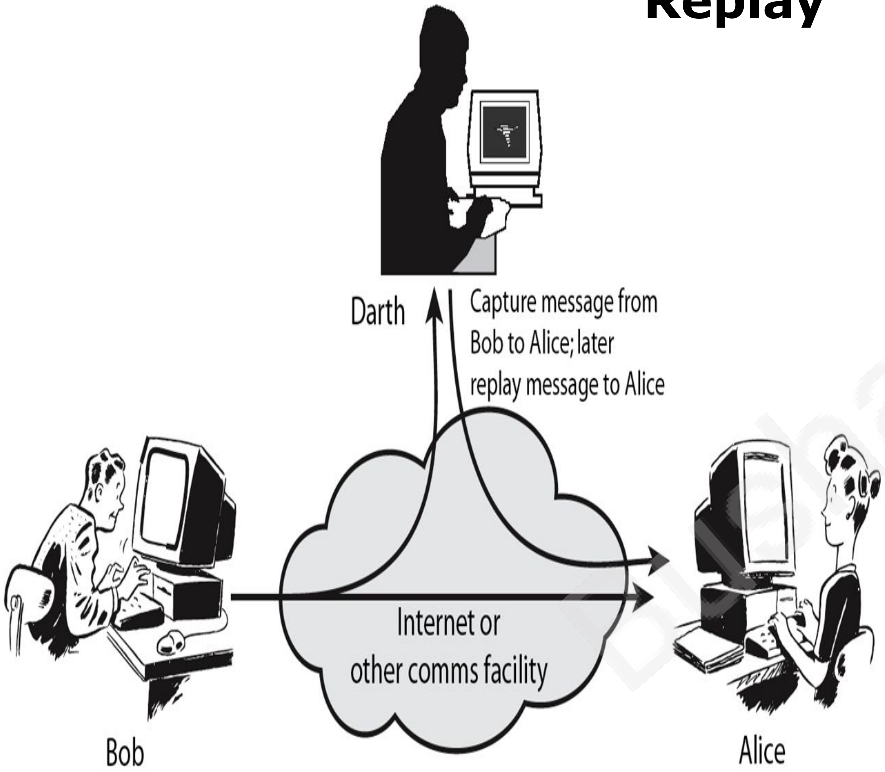
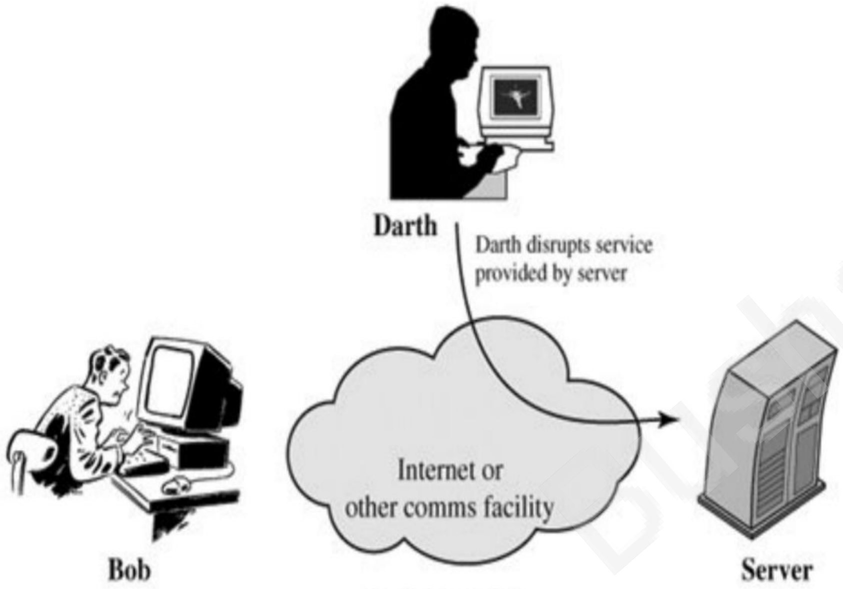

Darth
Capture message from Bob to Alice; later replay message to Alice
Internet or other comms facility
Bob
Alice

Figure b. **Replay**

Replay involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect (Figure b).

Denial of service


Darth
Darth disrupts service provided by server
Internet or other comms facility
Bob
Server

(d) Denial of service

- The **denial of service** prevents or inhibits the normal use or management of communications facilities (Figure d).
- This attack may have a specific target; for example, an entity may **suppress all messages directed to a particular destination** (e.g., the security audit service).
- Another form of service denial is the **disruption of an entire network**, either by disabling the network or by overloading it with messages so as to degrade performance.

Masquerade

- Takes place when one entity pretends to be a different entity
- Usually includes one of the other forms of active attack

Replay

- Involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect

Modification of messages

- Some portion of a legitimate message is altered, or messages are delayed or reordered to produce an unauthorized effect

Denial of service

- Prevents or inhibits the normal use or management of communications facilities

3. Security services

3.1 Authentication
3.2 Access Control
3.3 Data Confidentiality
3.4 Data integrity
3.5 Nonrepudiation
3.6 Availability service.

- **X.800** defines a **security service** as a service provided by a protocol layer of communicating open systems, which ensures adequate **security of the systems or of data transfers.**
- A clearer definition is found in **RFC 2828**, which provides the following definition:
  - a processing or communication service that is provided by a system to give a specific kind of protection to system resources;
  - security services implement security policies and are implemented by security mechanisms.

X.800 divides these services into five categories

Authentication

- The authentication service is concerned **with assuring that a communication is authentic**.
- In the case of a single message, such as a warning or alarm signal, the function of the authentication service is to assure the recipient that the message is from the source that it claims to be from.
- In the case of an ongoing interaction, such as the connection of a terminal to a host, two aspects are involved.
- **First**, at the time of connection initiation, the service assures that the two entities are authentic, that is, that each is the entity that it claims to be.
- **Second**, the service must assure that the connection is not interfered with in such a way that a third party can masquerade as one of the two legitimate parties for the purposes of unauthorized transmission or reception.

Two specific authentication services are defined in X.800:

- **Peer entity authentication:** Provides for the corroboration of the **identity of a peer entity in an association**. It is provided for use at the establishment of, or at times during the data transfer phase of, a connection. It attempts to provide confidence that an entity is not performing either a masquerade or an unauthorized replay of a previous connection.
- **Data origin authentication:** Provides for the corroboration of the **source of a data unit.** It does not provide protection against the duplication or modification of data units. This type of service supports applications like electronic mail where there are no prior interactions between the communicating entities.

Access Control

- In the context of network security, access control is the **ability to limit and control the access to host systems and applications via communications links.**
- To achieve this, each entity trying to gain access must first be identified, or authenticated, so that access rights can be tailored to the individual.

Data Confidentiality

- Confidentiality is the **protection of transmitted data from passive attacks.** With respect to the content of a data transmission, several levels of protection can be identified.
- The broadest service protects **all user data transmitted between two users over a period of time.**

- **Connection Confidentiality**
  - The protection of all user data on a connection.
- **Connectionless Confidentiality**
  - The protection of all user data in a single data block
- **Selective-Field Confidentiality**
  - The confidentiality of selected fields within the user data on a connection or in a single data block.
- **Traffic Flow Confidentiality**
  - The protection of the information that might be derived from observation of traffic flows.

Data Integrity

The assurance that data received are exactly as sent by an authorized entity (i.e.,
contain no modification, insertion, deletion, or replay).

Connection Integrity with Recovery

Provides for the integrity of all user data on a connection and detects any modification, insertion, deletion, or replay of any data within an entire data sequence, with recovery attempted.

Connection Integrity without Recovery

As above, but provides only detection without recovery.

Selective-Field Connection Integrity

Provides for the integrity of selected fields within the user data of a data block transferred over a connection and takes the form of determination of whether the selected fields have been modified, inserted, deleted, or replayed.

Connectionless Integrity

Provides for the integrity of a single connectionless data block and may take the form of detection of data modification. Additionally, a limited form of replay detection may be provided.

Selective-Field Connectionless Integrity

Provides for the integrity of selected fields within a single connectionless data block; takes the form of determination of whether the selected fields have been modified.

Nonrepudiation

- Nonrepudiation prevents either sender or receiver **from denying a transmitted message.**
- Thus, when a message is sent, the receiver can prove that the alleged sender in fact sent the message.
- Similarly, when a message is received, the sender can prove that the alleged receiver in fact received the message.

Nonrepudiation, Origin

Proof that the message was sent by the specified party.

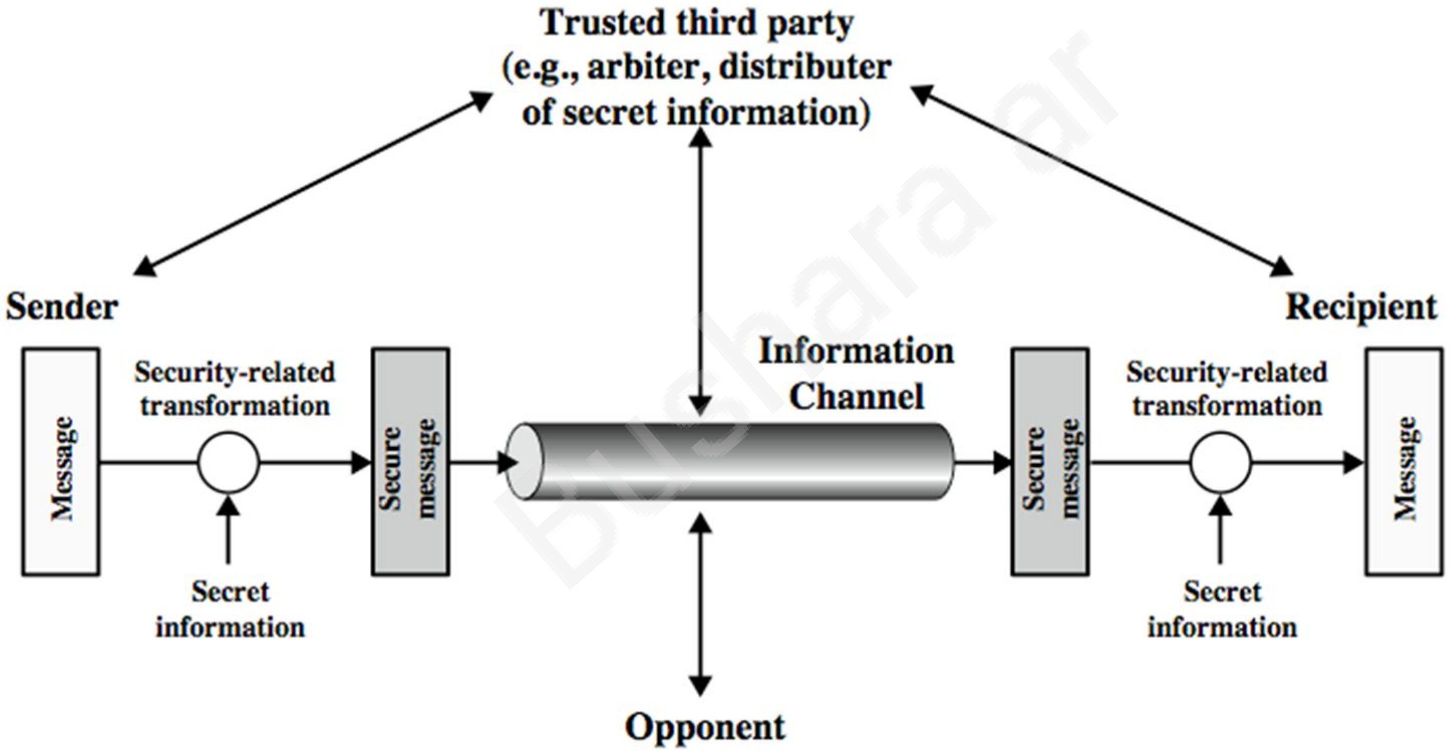
Nonrepudiation, Destination

Proof that the message was received by the specified party.

Availability Service

- Both X.800 and RFC 2828 define availability to be **the property of a system or a system resource** being accessible and usable upon demand by an authorized system entity, according to performance specifications for the system (i.e., a system is available if it provides services according to the system design whenever users request them).
- A variety of attacks can result in the loss of or reduction in availability.
- X.800 treats availability as a property to be associated with various security services.
- However, it makes sense to call out specifically an availability service. An availability service is one that protects a system to ensure its availability.
- This service addresses the security concerns raised by denial-of-service attacks.
- It depends on proper management and control of system resources and thus depends on access control service and other security services.

4. Model for network security.

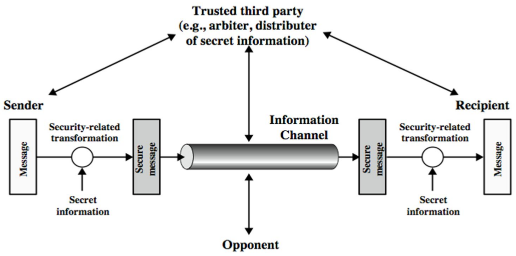


★ Security aspects come into play when it is necessary or desirable to protect the information transmission from an opponent who may present a threat to confidentiality, authenticity, and so on. All the techniques for providing security have two components:

❖ A security-related transformation on the information to be sent. Examples include the encryption of the message, which scrambles the message so that it is unreadable by the opponent, and the addition of a code based on the contents of the message, which can be used to verify the identity of the sender

❖ Some secret information shared by the two principals and, it is hoped, unknown to the opponent. An example is an encryption key used in conjunction with the transformation to scramble the message before transmission and unscramble it on reception.

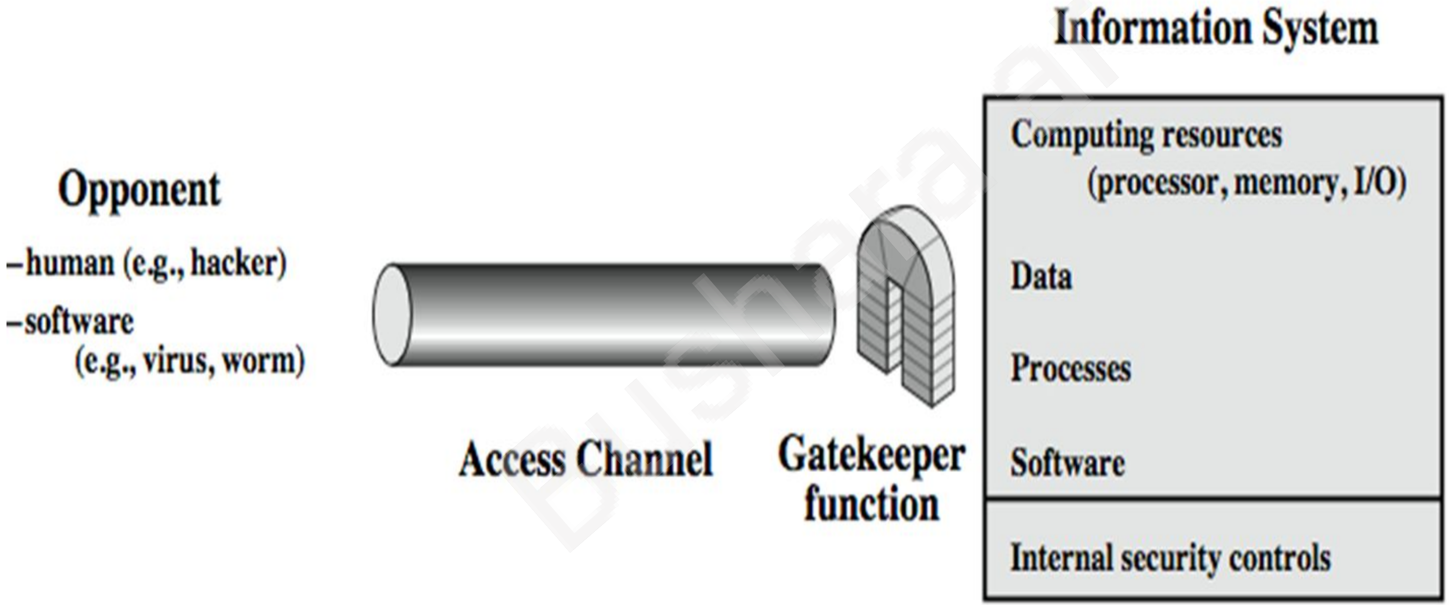
- ➔ message is to be transferred from one party to another across some sort of internet.
- ➔ The two parties, who are the **principals** in this transaction, must cooperate for the exchange to take place.



Using this model requires us to:

- ❖ design a **suitable algorithm** for the **security transformation**
- ❖ generate the **secret information** (**keys**) used by the algorithm
- ❖ develop **methods** to distribute and share the secret information
- ❖ specify **a protocol enabling the principals** to use the transformation and secret information for a security service

Network Access Security Model



- ★ using this model requires us to: **select appropriate gatekeeper functions to identify users**
- ★ It includes password-based login procedures that are designed to deny access to all but authorized users and screening logic that is designed to detect and reject worms, viruses, and other similar attacks.
- ★ Also a variety of internal controls that monitor activity and analyze stored information in an attempt to detect the presence of unwanted intruders.

5. Symmetric cipher model, Cryptography, Cryptanalysis

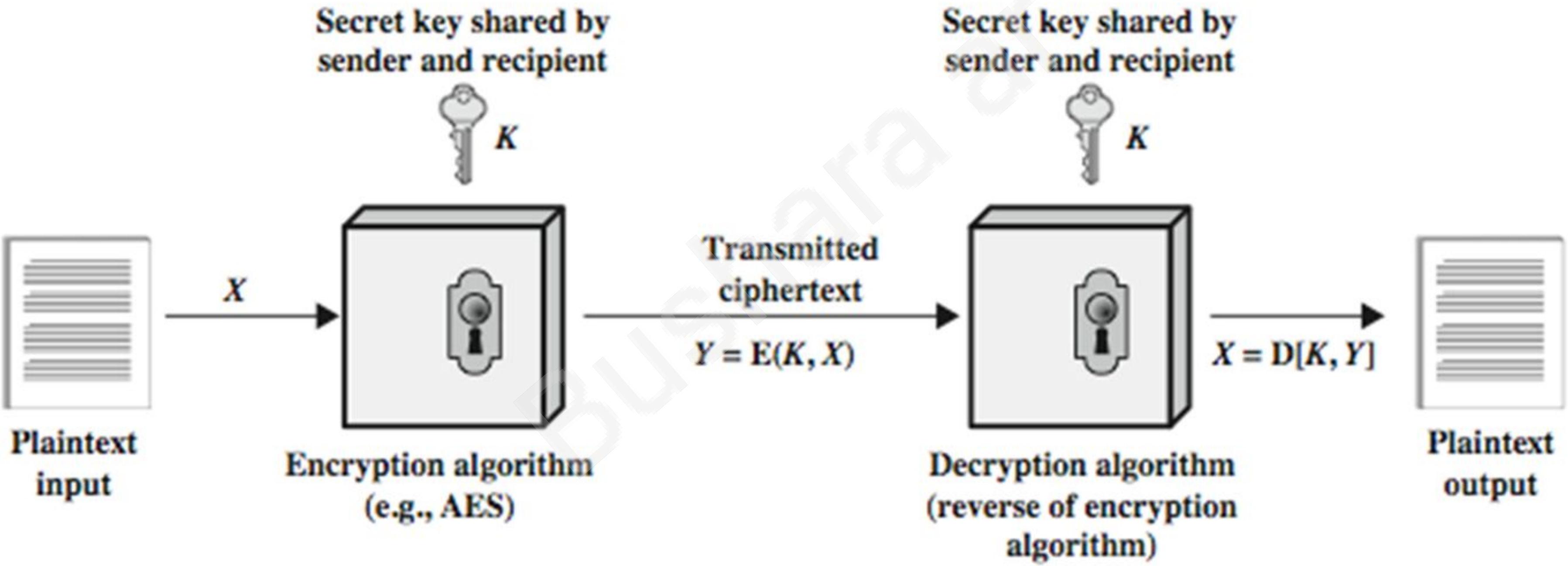

Secret key shared by sender and recipient
K
Secret key shared by sender and recipient
K
X
Transmitted ciphertext
$Y = E(K, X)$
$X = D[K, Y]$
Plaintext input
Encryption algorithm (e.g., AES)
Decryption algorithm (reverse of encryption algorithm)
Plaintext output

Fig: Symmetric cipher model

A symmetric encryption scheme has five ingredients

1. **Plaintext**: This is the **original message** or data that is fed into the algorithm as input.
2. **Encryption algorithm:** The encryption algorithm performs various **substitutions and transformations** on the plaintext.
3. **Secret key:** The secret key is also input to the encryption algorithm. The key is a value independent of the plaintext and of the algorithm. The algorithm will produce a different output depending on the specific key being used at the time.
4. **Ciphertext:** This is the **scrambled message** produced as **output**. It depends on the plaintext and the secret key. For a given message, two different keys will produce two different ciphertexts.
5. **Decryption algorithm:** This is essentially the **encryption algorithm run in reverse**. It takes the ciphertext and the secret key and produces the original plaintext.

Cryptography : study of encryption principles/methods

Cryptographic systems are characterized along three independent dimensions:

1. **The type of operations used for transforming plaintext to ciphertext.**

   All encryption algorithms are based on two general principles: **substitution**, in which each element in the plaintext (bit, letter, group of bits or letters) is mapped into another element, and **transposition**, in which elements in the plaintext are rearranged.

2. **The number of keys used.**

   If both sender and receiver use the **same key**, the system is referred to as symmetric, single-key, secret-key, or conventional encryption. If the sender and receiver use **different keys,** the system is referred to as asymmetric, two-key, or public-key encryption.

3. **The way in which the plaintext is processed.**

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

Cryptanalysis: study of principles/ methods of deciphering ciphertext without knowing key

The objective of attacking an encryption system is to **recover the key** in use rather then simply to recover the plaintext of a single ciphertext. There are two general approaches to attacking a conventional encryption scheme:

- **Cryptanalysis:** Cryptanalytic attacks **depend on the algorithm** and maybe some knowledge of the **plaintext's general characteristics** or sample plaintext-ciphertext combinations. This attack utilizes the algorithm's properties to derive a plaintext or the key.

- **Brute-force attack:** The attacker tries every possible key on a piece of ciphertext until an intelligible translation into plaintext is obtained. On average, half of all possible keys must be tried to achieve success.

cryptology - field of both cryptography and cryptanalysis

6. Substitution techniques- Hill Cipher, One time pad

- 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.**

- Eg: Caesar cipher, Monoalphabetic cipher, Playfair cipher, **Hill cipher, one time pad** etc

CAESAR CIPHER

- Earliest known substitution cipher
- Invented by Julius Caesar
- Each letter is replaced by the letter **three positions further down** the alphabet.
- 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
- Example: ohio state □ RKLR VWDWH

Monoalphabetic cipher

- Replace an alphabet in a plain text message with an alphabet that is k positions up or down the order, based upon some key.

- Replace all the other alphabets in the plain text with the same technique.

A can be replaced by-(B through Z)
B can be replaced by-(A or C through)
No relation between replacement of A & B.

Monoalphabetic Substitution Cipher

- Shuffle the letters and map each plaintext letter to a different random ciphertext letter:

Plain letters: abcdefghijklmnopqrstuvwxyz
Cipher letters: DKVQFIBJWPESCXHTMYAUOLRGZN

Plaintext: ifwewishtoreplaceletters
Ciphertext: WIRFRWAJUHYFTSDVFSFUUFYA

HILL CIPHER

- ➔ It is works on multiple letters at the same time.
- ➔ Lester Hill invented this in 1929.

1. Treat every letter in the **plain text message as a number**, so that A=0, B=1,....Z=25

2. The plain text message is organized as a matrix of numbers, based on the above conversion.

3. Plain text matrix is **multiplied by randomly chosen keys.** The key matrix consists of size **n*n** , where n is the number of rows in our plain text matrix.

4.Now **multiply two matrices to get cipher text**

For **decryption**, take the ciphertext matrix and multiply it by the **inverse of our original key matrix.**

Encryption: C = K P mod 26

Decryption: P = K^{-1}C mod 26

xample: Encrypt the plaintext “attack”, using Hill cipher for the given key = $\begin{bmatrix} 2 & 3 \\ 3 & 6 \end{bmatrix}$.

ns. :

ince the key is a 2x2 Matrix, plaintext should be converted into vectors of length 2. So, $\begin{bmatrix} a \\ t \end{bmatrix}_{2x1} \begin{bmatrix} t \\ a \end{bmatrix}_{2x1} \begin{bmatrix} c \\ k \end{bmatrix}_{2x1}$

ncryption:

Plaintext Alphabet	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
Plaintext Value	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

) **1st Vector** $\begin{bmatrix} a \\ t \end{bmatrix}_{2x1} = \begin{bmatrix} 0 \\ 19 \end{bmatrix}$, **key =** $\begin{bmatrix} 2 & 3 \\ 3 & 6 \end{bmatrix}$,

$$\mathbf{C = K\,P \bmod 26} = \begin{bmatrix} 2 & 3 \\ 3 & 6 \end{bmatrix} \begin{bmatrix} 0 \\ 19 \end{bmatrix} \bmod 26 = \begin{bmatrix} 2(0) + 3\,(19) \\ 3(0) + 6\,(19) \end{bmatrix} \bmod 26 = \begin{bmatrix} 57 \\ 114 \end{bmatrix} \bmod 26 = \begin{bmatrix} 5 \\ 10 \end{bmatrix} = \begin{bmatrix} F \\ K \end{bmatrix}$$

) **2nd Vector** $\begin{bmatrix} t \\ a \end{bmatrix}_{2x1} = \begin{bmatrix} 19 \\ 0 \end{bmatrix}$

$$\mathbf{C = K\,P \bmod 26} = \begin{bmatrix} 2 & 3 \\ 3 & 6 \end{bmatrix} \begin{bmatrix} 19 \\ 0 \end{bmatrix} \bmod 26 = \begin{bmatrix} 2(19) + 3\,(0) \\ 3(19) + 6\,(0) \end{bmatrix} \bmod 26 = \begin{bmatrix} 38 \\ 57 \end{bmatrix} \bmod 26 = \begin{bmatrix} 12 \\ 5 \end{bmatrix} = \begin{bmatrix} M \\ F \end{bmatrix}$$

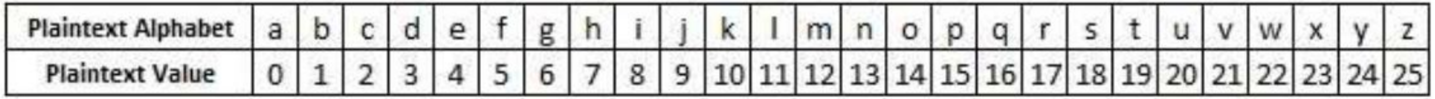
) **3rd Vector** $\begin{bmatrix} c \\ k \end{bmatrix}_{2x1} = \begin{bmatrix} 2 \\ 10 \end{bmatrix}$

$$\mathbf{C = K\,P \bmod 26} = \begin{bmatrix} 2 & 3 \\ 3 & 6 \end{bmatrix} \begin{bmatrix} 2 \\ 10 \end{bmatrix} \bmod 26 = \begin{bmatrix} 2(2) + 3\,(10) \\ 3(2) + 6\,(10) \end{bmatrix} \bmod 26 = \begin{bmatrix} 34 \\ 66 \end{bmatrix} \bmod 26 = \begin{bmatrix} 8 \\ 14 \end{bmatrix} = \begin{bmatrix} I \\ O \end{bmatrix}$$

Ciphertext: “FKMFIO”.

Example: Decrypt the ciphertext**“FKMFIO”**, using Hill cipher for the given key = $\begin{bmatrix} 2 & 3 \\ 3 & 6 \end{bmatrix}$.

Ans. :



Plaintext Alphabet	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
Plaintext Value	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

P = K^{-1} C mod 26

Inverse of Key Matrix $K^{-1} = \frac{1}{|K|}\text{ adj }(K) = K^{-1}\text{ adj }(K) = \frac{1}{|D|}\text{ adj }(K) = D^{-1}\text{ adj }(K)$

determinant of Matrix $D = \begin{vmatrix} a & b \\ c & d \end{vmatrix} = |ad - bc|,\ \text{where } D \neq 0$

$D = \begin{vmatrix} 2 & 3 \\ 3 & 6 \end{vmatrix} = |12 - 9| = 3$

Now, find multiplicative inverse of determinant $D\,D^{-1} = 1 \bmod 26$

Using hit and trial method $3\ D^{-1} \equiv 1\ mod\ 26 = 3\ D^{-1} \text{mod } 26 = 1$

$3 \times 9 \bmod 26 = 27 \bmod 26 = 1$, $D^{-1} = 9$.

To find the adjoint of the Matrix $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$, **adj (A) =** $\begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$

Here, $K = \begin{bmatrix} 2 & 3 \\ 3 & 6 \end{bmatrix}$, **adj (K) =** $\begin{bmatrix} 6 & -3 \\ -3 & 2 \end{bmatrix} = \begin{bmatrix} 6 & 23 \\ 23 & 2 \end{bmatrix}$

Inverse of Key Matrix $K^{-1} = \frac{1}{|K|}\,\text{adj}\,(K) = K^{-1}\,\text{adj}\,(K) = \frac{1}{|D|}\,\text{adj}\,(K) = D^{-1}\,\text{adj}\,(K)$

$$K^{-1} = 9\begin{bmatrix} 6 & 23 \\ 23 & 2 \end{bmatrix} \text{mod } 26 = \begin{bmatrix} 54 & 207 \\ 207 & 18 \end{bmatrix} \text{mod } 26 = \begin{bmatrix} 2 & 25 \\ 25 & 18 \end{bmatrix}$$

Now, we will decrypt the cipher: FK MF IO

$$C = \begin{bmatrix} F \\ K \end{bmatrix}_{2x1} = \begin{bmatrix} 5 \\ 10 \end{bmatrix}, C = \begin{bmatrix} M \\ F \end{bmatrix}_{2x1} = \begin{bmatrix} 12 \\ 5 \end{bmatrix}, C = \begin{bmatrix} I \\ O \end{bmatrix}_{2x1} = \begin{bmatrix} 8 \\ 14 \end{bmatrix}$$

$$P = K^{-1}\,C \text{ mod } 26 = \begin{bmatrix} 2 & 25 \\ 25 & 18 \end{bmatrix}\begin{bmatrix} 5 \\ 10 \end{bmatrix} \text{mod } 26 = \begin{bmatrix} 2(5) + 25\,(10) \\ 25(5) + 18\,(10) \end{bmatrix} \text{mod } 26 = \begin{bmatrix} 260 \\ 305 \end{bmatrix} \text{mod } 26 = \begin{bmatrix} 0 \\ 19 \end{bmatrix} = \begin{bmatrix} a \\ t \end{bmatrix}$$

$$P = K^{-1}\,C \text{ mod } 26 = \begin{bmatrix} 2 & 25 \\ 25 & 18 \end{bmatrix}\begin{bmatrix} 12 \\ 5 \end{bmatrix} \text{mod } 26 = \begin{bmatrix} 2(12) + 25\,(5) \\ 25(12) + 18\,(5) \end{bmatrix} \text{mod } 26 = \begin{bmatrix} 149 \\ 390 \end{bmatrix} \text{mod } 26 = \begin{bmatrix} 19 \\ 0 \end{bmatrix} = \begin{bmatrix} t \\ a \end{bmatrix}$$

$$P = K^{-1}\,C \text{ mod } 26 = \begin{bmatrix} 2 & 25 \\ 25 & 18 \end{bmatrix}\begin{bmatrix} 8 \\ 14 \end{bmatrix} \text{mod } 26 = \begin{bmatrix} 2(8) + 25\,(14) \\ 25(8) + 18\,(14) \end{bmatrix} \text{mod } 26 = \begin{bmatrix} 366 \\ 452 \end{bmatrix} \text{mod } 26 = \begin{bmatrix} 2 \\ 10 \end{bmatrix} = \begin{bmatrix} c \\ k \end{bmatrix}$$

Plaintext: “attack”

ONE TIME PAD (OTP)

- Also called VERNAM cipher.
- It is implemented using **a random set of non repeating characters as the input cipher text.**
- Most significant point is that once an input cipher text is used, **it is never used again for any other message.** Hence the name **one time Pad**.

Encryption

h	e	l	l	o	message
7 (h)	4 (e)	11 (l)	11 (l)	14 (o)	message
+ 23 (X)	12 (M)	2 (C)	10 (K)	11 (L)	key
= 30	16	13	21	25	message + key
= 4 (E)	16 (Q)	13 (N)	21 (V)	25 (Z)	(message + key) mod 26
E	Q	N	V	Z	→ ciphertext

Decryption

E	Q	N	V	Z	ciphertext
4 (E)	16 (Q)	13 (N)	21 (V)	25 (Z)	ciphertext
– 23 (X)	12 (M)	2 (C)	10 (K)	11 (L)	key
= −19	4	11	11	14	ciphertext – key
= 7 (h)	4 (e)	11 (l)	11 (l)	14 (o)	ciphertext – key (mod 26)
h	e	l	l	o	→ message

-19 mod 26
-19 = 26*-1 + 7

7. 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.**
- these **hide the message** by **rearranging the letter order**
- without altering the actual letters used
- Eg: rail fence technique, simple columnar technique, columnar technique with multiple rounds

Rail Fence cipher

- **write** message letters out **diagonally** over a number of rows
- use a “W” pattern
- then read off cipher **row by row**

eg. example, to encipher the message "meet me after the toga party" with a rail fence of depth 2,

m e m a t r h t g p r y

e t e f e t e o a a t

Ciphertext =

MEMATRHTGPRYETEFETEOAAT

- Simple Columnar Technique

- 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 the columns then becomes the key to the algorithm. For example,**attack postponed until two am**

Key:	4	3	1	2	5	6	7
Plaintext:	a	t	t	a	c	k	p
	o	s	t	p	o	n	e
	d	u	n	t	i	l	t
	w	o	a	m	x	y	z

Ciphertext: TTNAAPTMTSUOAODWCOIXKNLYPETZ

- Columnar Technique with multiple rounds

- The transposition cipher can be made significantly more secure by performing **more than one stage of transposition**.
- The result is a more complex permutation that is not easily reconstructed.
- Thus, if the foregoing message is re-encrypted using the same algorithm,

Key:	4	3	1	2	5	6	7
Input:	t	t	n	a	a	p	t
	m	t	s	u	o	a	o
	d	w	c	o	i	x	k
	n	l	y	p	e	t	z

Output: NSCYAUOPTTWLTMDNAOIEPAXTTOKZ