19CS6602- CRYPTOGRAPHY AND NETWORK SECURITY

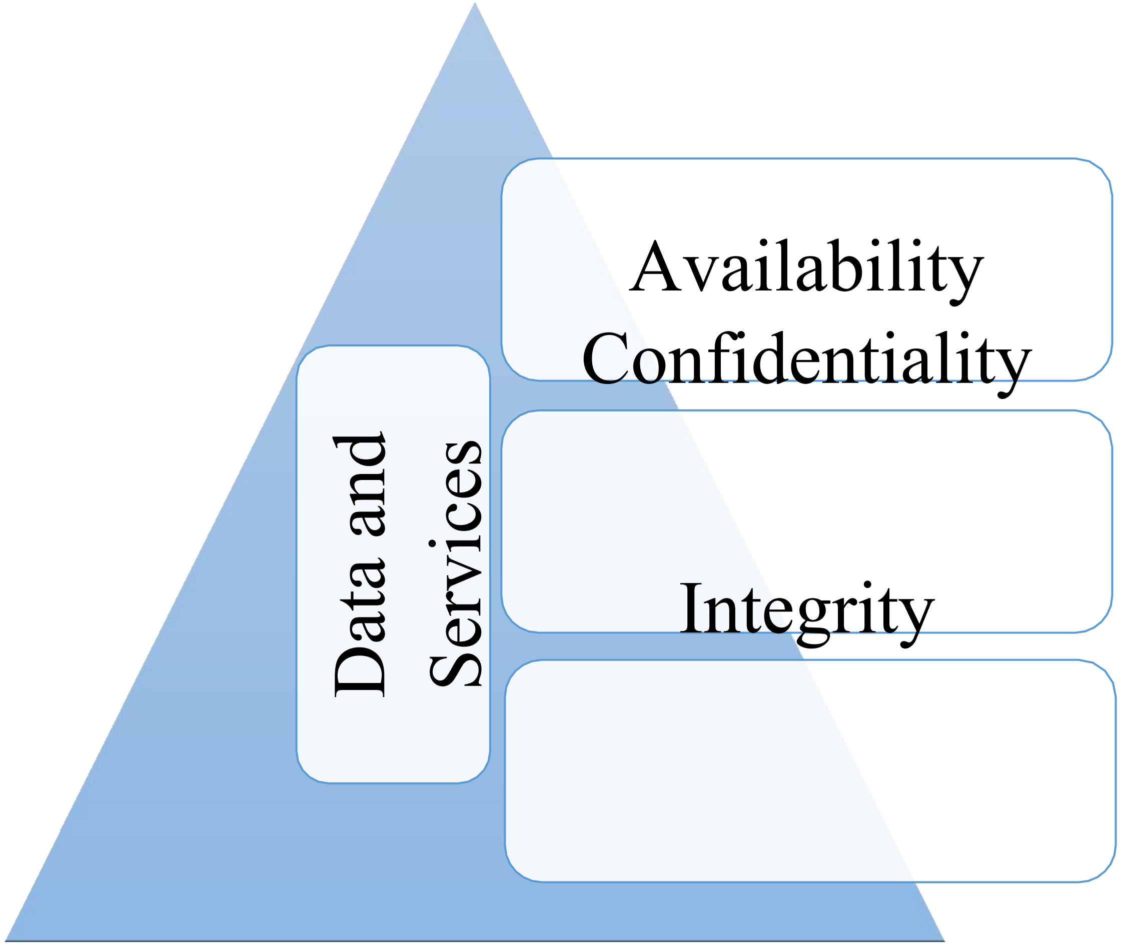
UNIT I

INTRODUCTION

Introduction

Computer Security - The protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability, and confidentiality of information system resources (includes hardware, software, firmware, information/ data and telecommunications).

Introduction



Data and Services

Availability

Confidentiality

Integrity

Need for Security at Multiple levels

- Multilevel security or multiple levels of security (MLS) is the application of a computer system need

  -To process information with incompatible classifications.

  -To permit access by users with different security clearances.

  -To prevent users from obtaining access to information for which they lack authorization.

Security Policies

- Security policies which are the basis of security for the technology infrastructure of a company.
- Policies are divided in two categories.

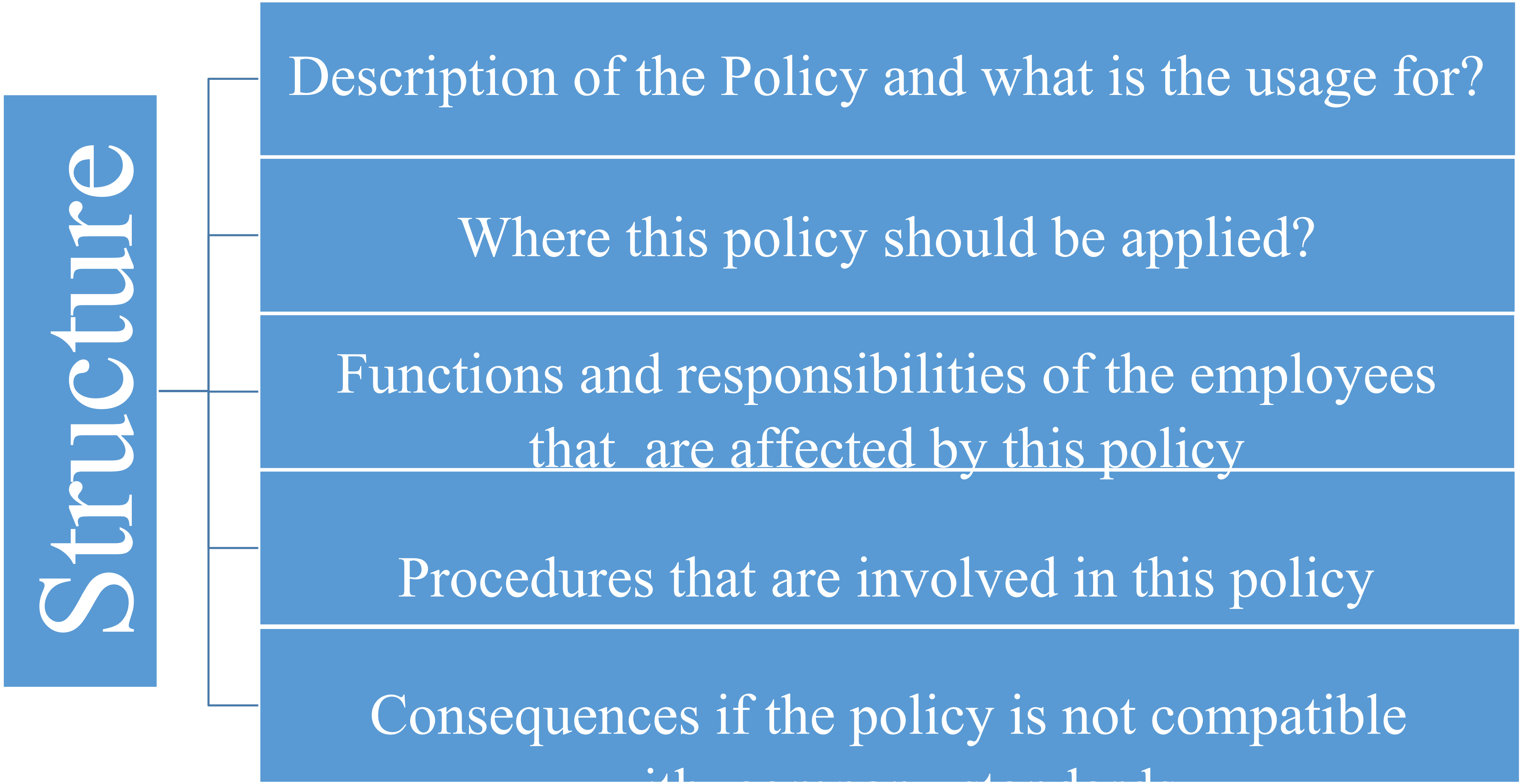
  -User policies

  User policies generally define the limit of the users towards the computer resources in a workplace.

  -IT policies

  IT policies are designed for IT department, to secure the procedures and functions of IT fields.

Security Policies



Structure

Description of the Policy and what is the usage for?

Where this policy should be applied?

Functions and responsibilities of the employees that are affected by this policy

Procedures that are involved in this policy

Consequences if the policy is not compatible

OSI security architecture

- The Open Systems Interconnection (OSI) security architecture provides a systematic framework for defining security attacks, mechanisms, and services.
- To assess effectively the security needs of an organization and to evaluate and choose various security products and policies, the manager responsible for computer and network security needs some systematic way of defining the requirements for security and characterizing the approaches to satisfying those requirements.
- The OSI security architecture is useful to managers as a way of organizing the task of providing security.

Security attacks

- Any action that compromises the security of information owned by an organization.
- It is classified into two types.

  -Passive attacks

  Passive attacks are in the nature of eavesdropping on, or monitoring of, transmissions.

  -Active attacks

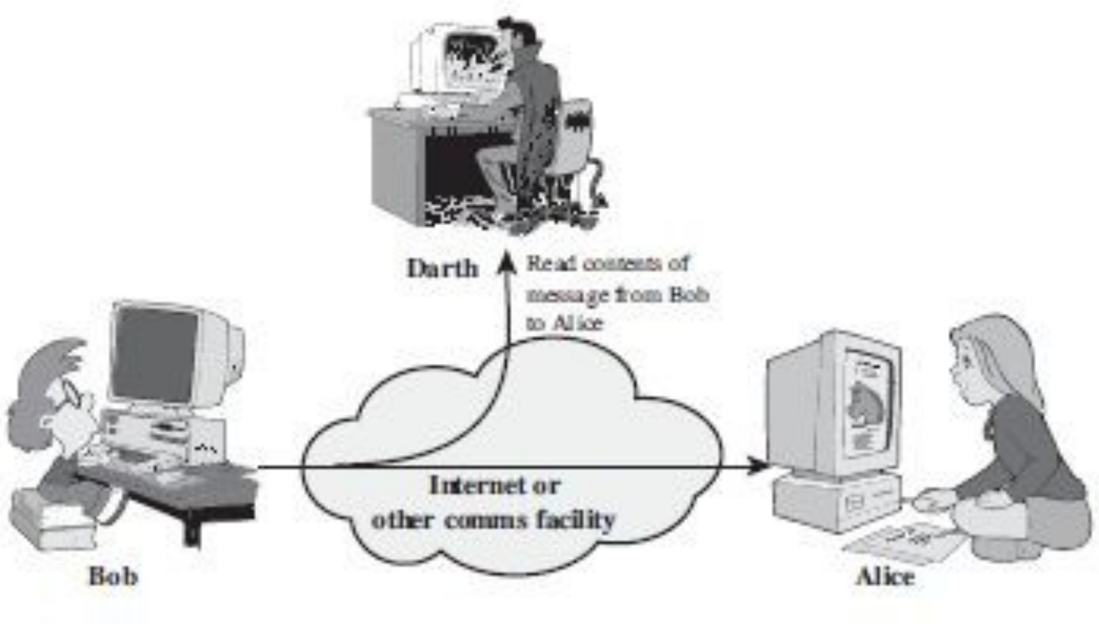
  Active attacks involve some modification of the data stream or the creation of a false stream.

Security attacks

- Passive attacks
  - Release of message contents
  - Traffic analysis
- Active attacks
  - Masquerade
  - Replay
  - Modification of messages
  - Denial of service

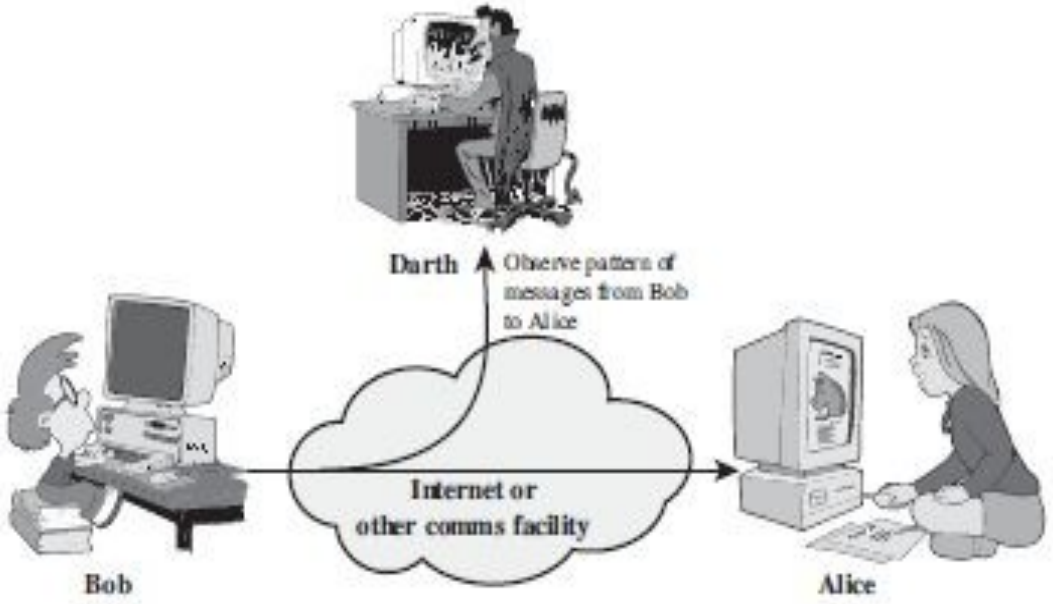
Security attacks

Release of message contents – Attacker reads the contents of message.


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

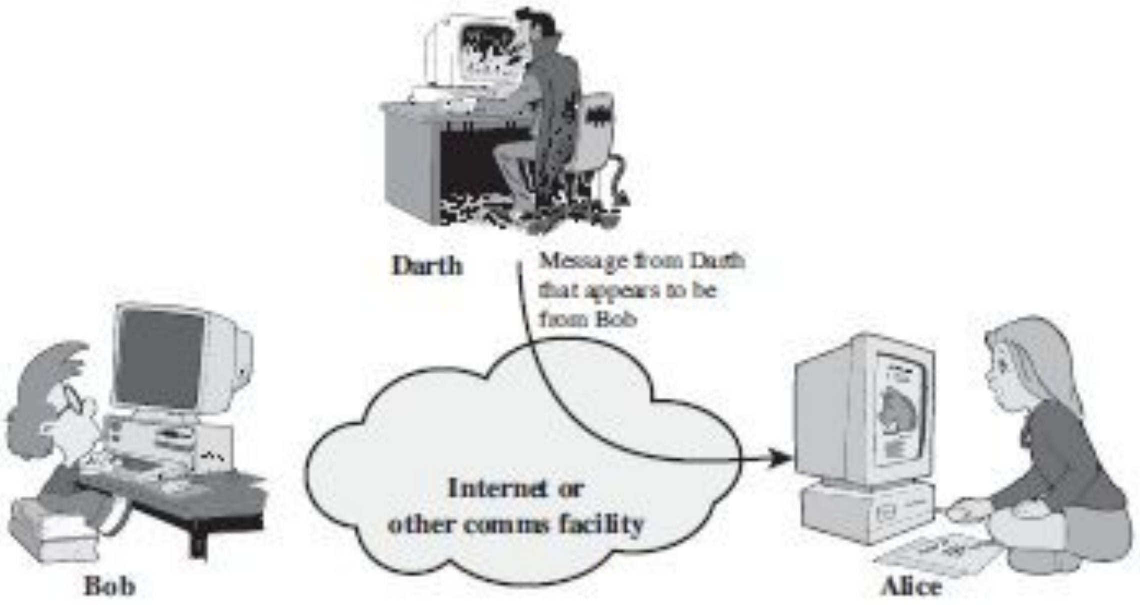
Security attacks

Traffic analysis - Observe the pattern of message and communication.


Darth
Observe pattern of messages from Bob to Alice
Internet or other comms facility
Bob
Alice

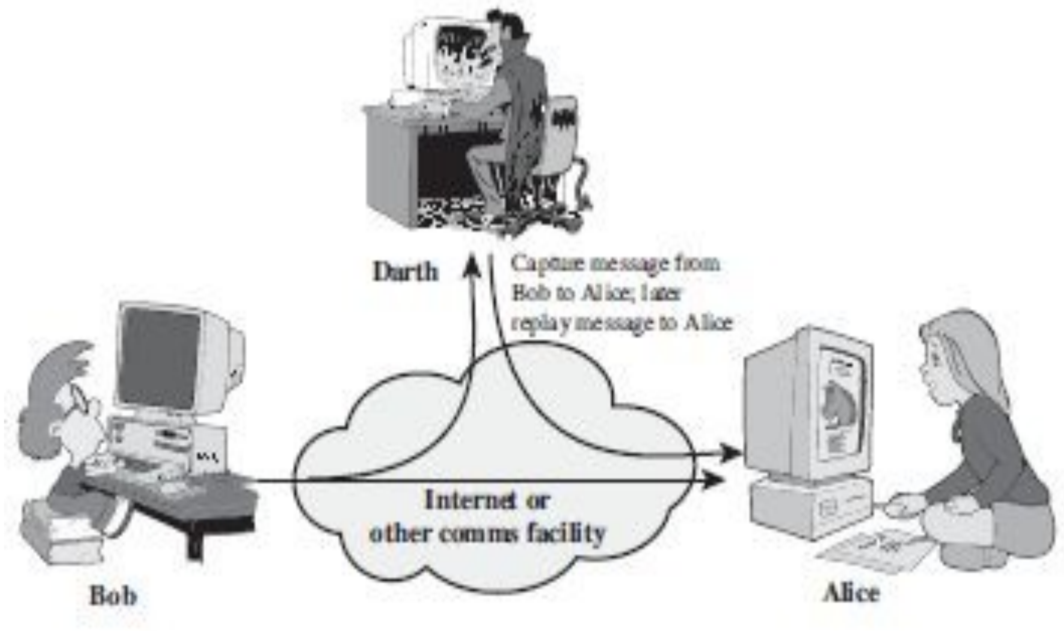
Security attacks

Masquerade - One person pretends to be a another


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

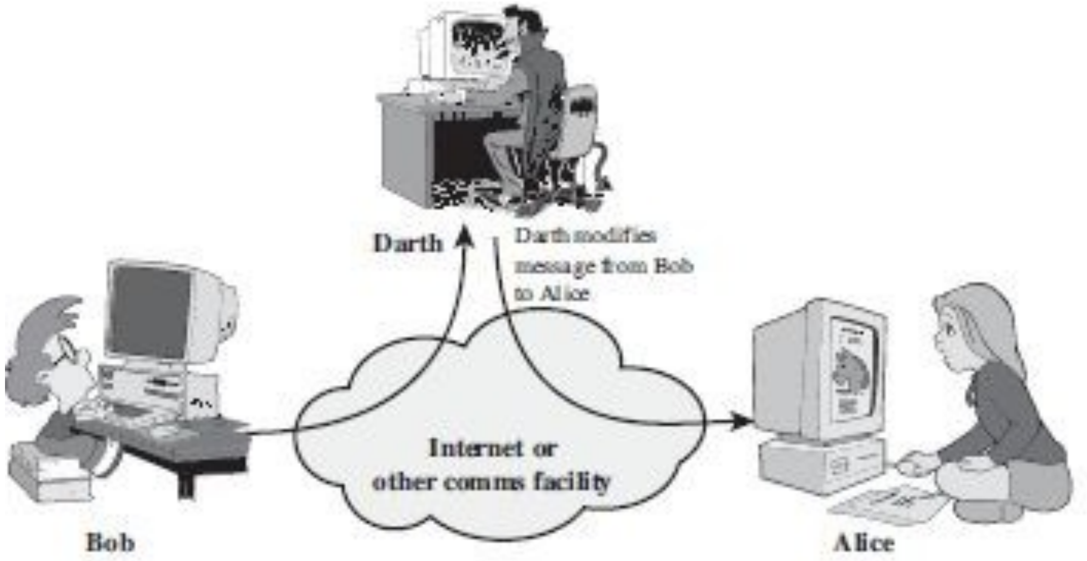
Security attacks

Replay - The passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect.


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

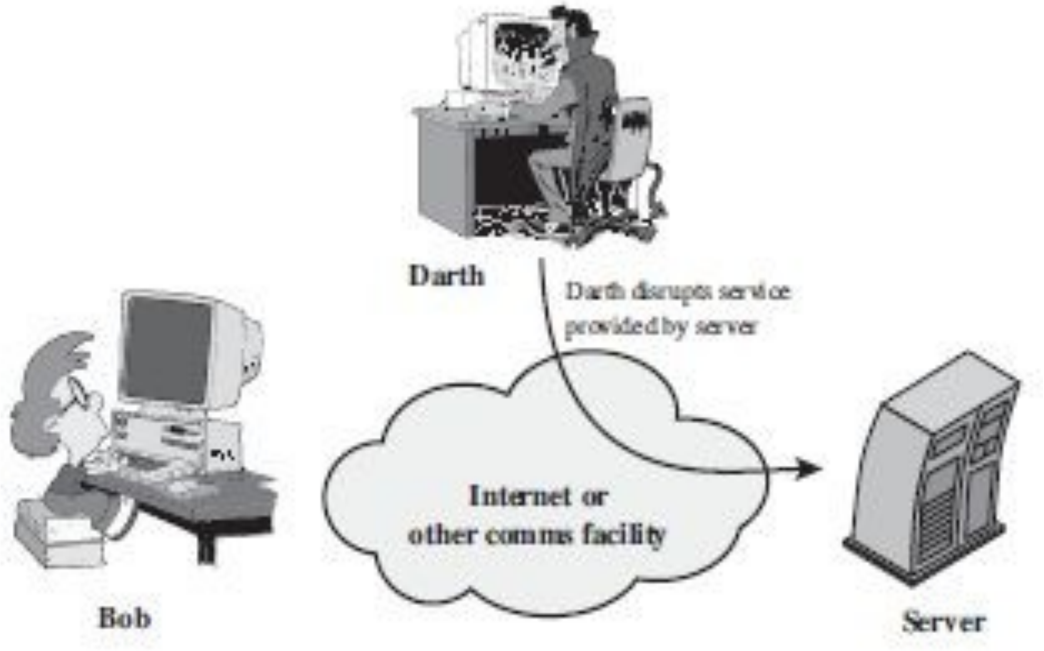
Security attacks

Modification of messages - Some portion of a legitimate message is altered or reordered.


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

Security attacks

Denial of service - Disabling the network or by overloading it with messages so as to degrade performance.


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

Security services

- A processing or communication service that enhances the security of the data processing systems and the information transfers of an organization.
- The services are intended to counter security attacks, and they make use of one or more security mechanisms to provide the service.

Security services

Authentication

- The assurance that the communicating entity is the one that it claims to be.

Access control

- The prevention of unauthorized use of a resource.

Data confidentiality

- The protection of data from unauthorized disclosure.

Data integrity

- The assurance that data received are exactly as sent by an authorized entity.

Nonrepudiation

- Provides protection against denial by one of the entities involved in a communication of having participated in all or part of the communication.

Security services

•Authentication

-Peer Entity Authentication

It is used in association with a logical connection to provide confidence in the identity of the entities connected.

- Data-Origin Authentication

In a connectionless transfer, provides assurance that the source of received data is as claimed.

Security services

- Data confidentiality
  - 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

    Selected fields within the user data

  - Traffic-Flow

    Confidentiality

    Observation of traffic fl

Security services

- Data integrity
  - Connection Integrity with Recovery
    Detects any modification with
    recovery.
  - Connection Integrity without
    Recovery Detection without
    recovery.
  - Selective-Field Connection Integrity
    Selected fields within the user data of a data block.
  - Connectionless Integrity
    Provides for the integrity of a single connectionless data
    block

Security services

- Nonrepudiation
  - Nonrepudiation, Origin

    Proof that the message was sent by the specified party.

  - Nonrepudiation, Destination

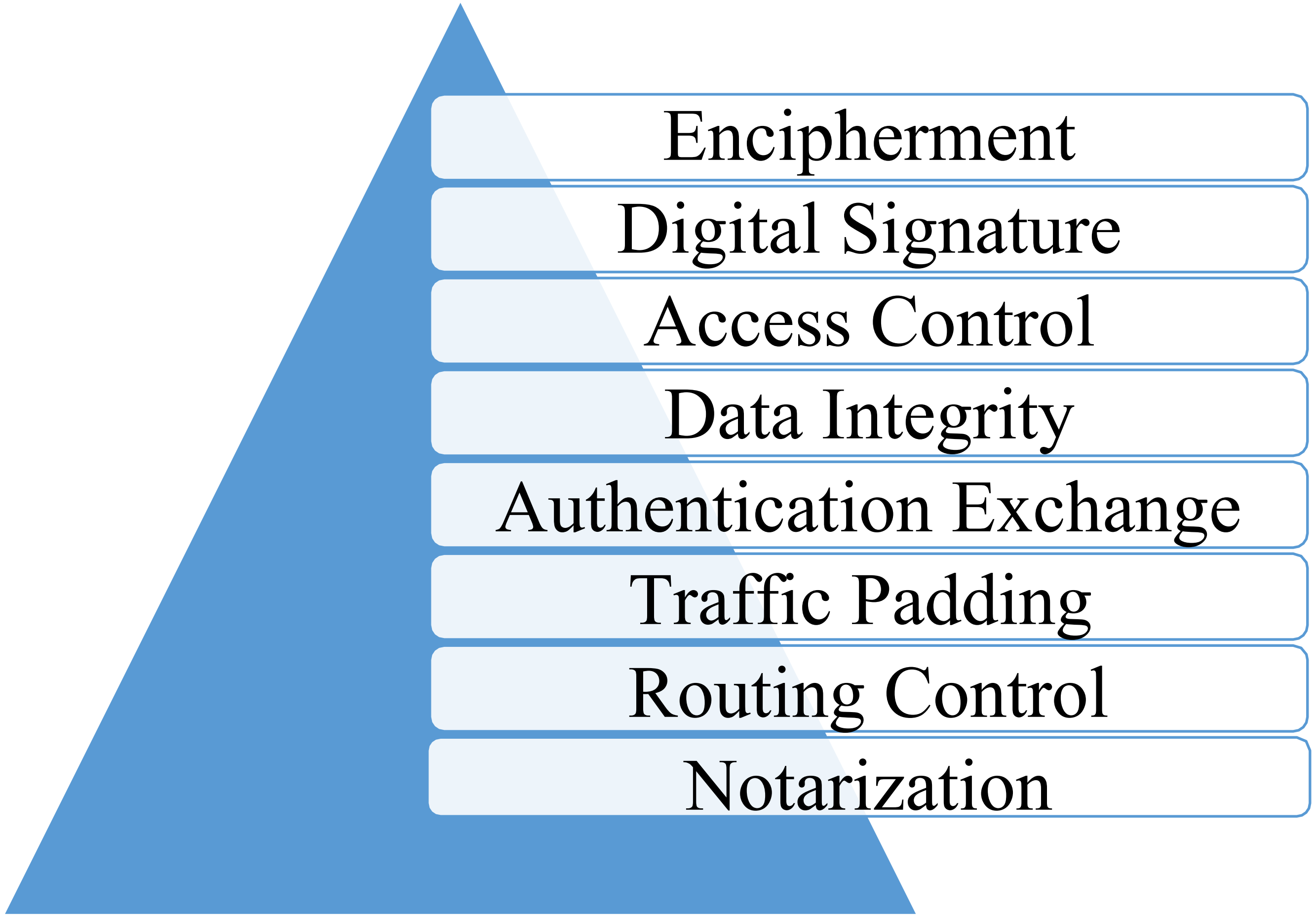
    Proof that the message was received by the specified party.

Security mechanisms

- A process (or a device incorporating such a process) that is designed to detect, prevent, or recover from a security attack.
- The mechanisms are divided into those that are implemented in a specific protocol layer, such as TCP or an application-layer protocol, and those that are not specific to any particular protocol layer or security service.
- Types
  - Specific Security Mechanisms
  - Pervasive Security Mechanisms

Security mechanisms

- Specific Security Mechanisms



Encipherment

Digital Signature

Access Control

Data Integrity

Authentication Exchange

Traffic Padding

Routing Control

Notarization

Security mechanisms

- Specific Security Mechanisms

May be incorporated into the appropriate protocol layer in order to provide some of the OSI security services.

Encipherment

The use of mathematical algorithms to transform data into a form that is not readily intelligible. The transformation and subsequent recovery of the

data depend on an algorithm and zero or more encryption keys.

Digital Signature

Data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery (e.g., by the recipient).

Access Control

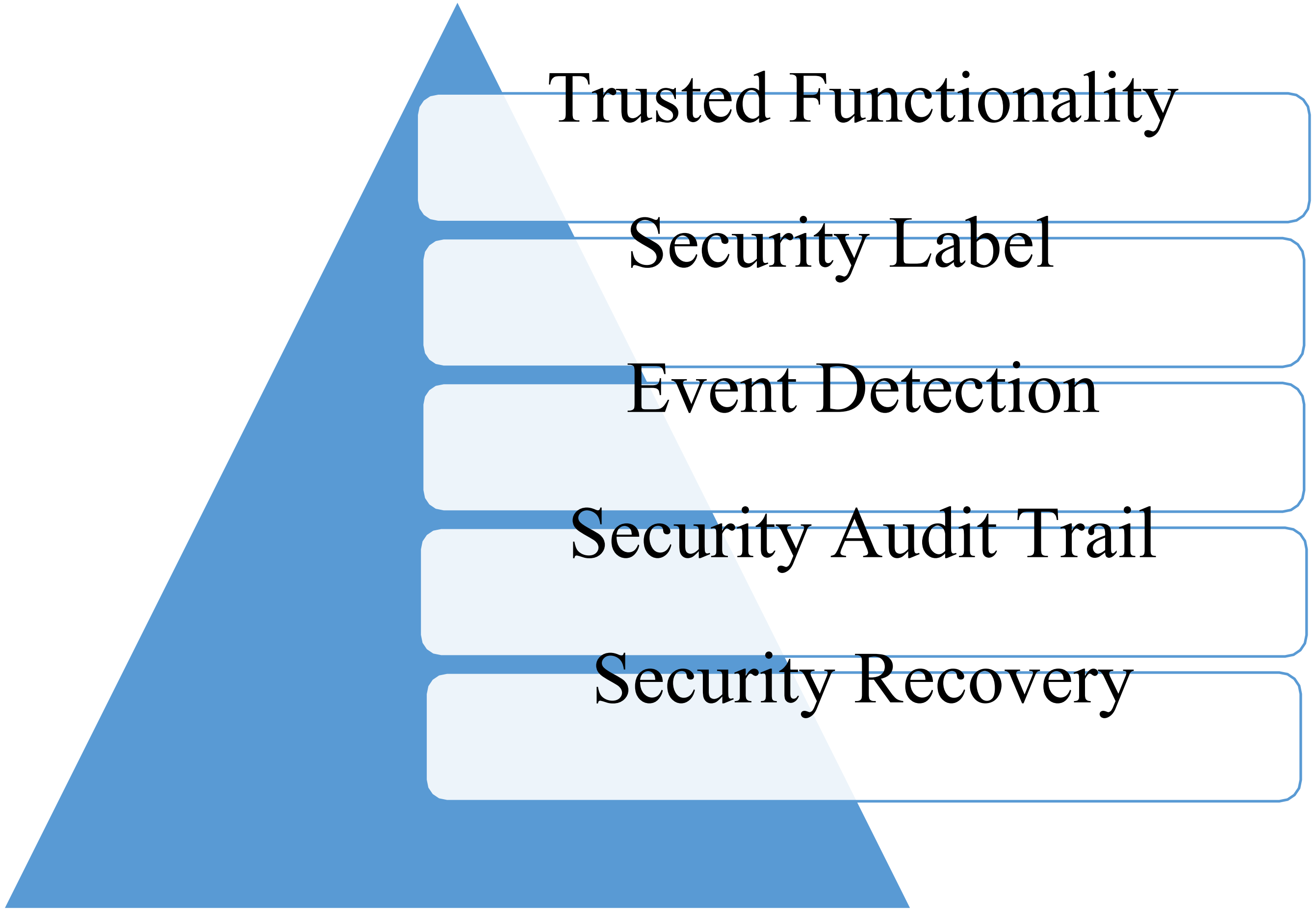
A variety of mechanisms that enforce access rights to resources.

Data Integrity

A variety of mechanisms used to assure the integrity of a data unit or stream of data units.

Security Mechanisms

- Pervasive Security Mechanisms



Trusted Functionality

Security Label

Event Detection

Security Audit Trail

Security Recovery

Security Mechanisms

•Pervasive Security Mechanisms

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

Trusted Functionality

That which is perceived to be correct with respect to some criteria (e.g., as established by a security policy).

Security Label

The marking bound to a resource (which may be a data unit) that names or designates the security attributes of that resource.

Event Detection

Detection of security-relevant events.

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.

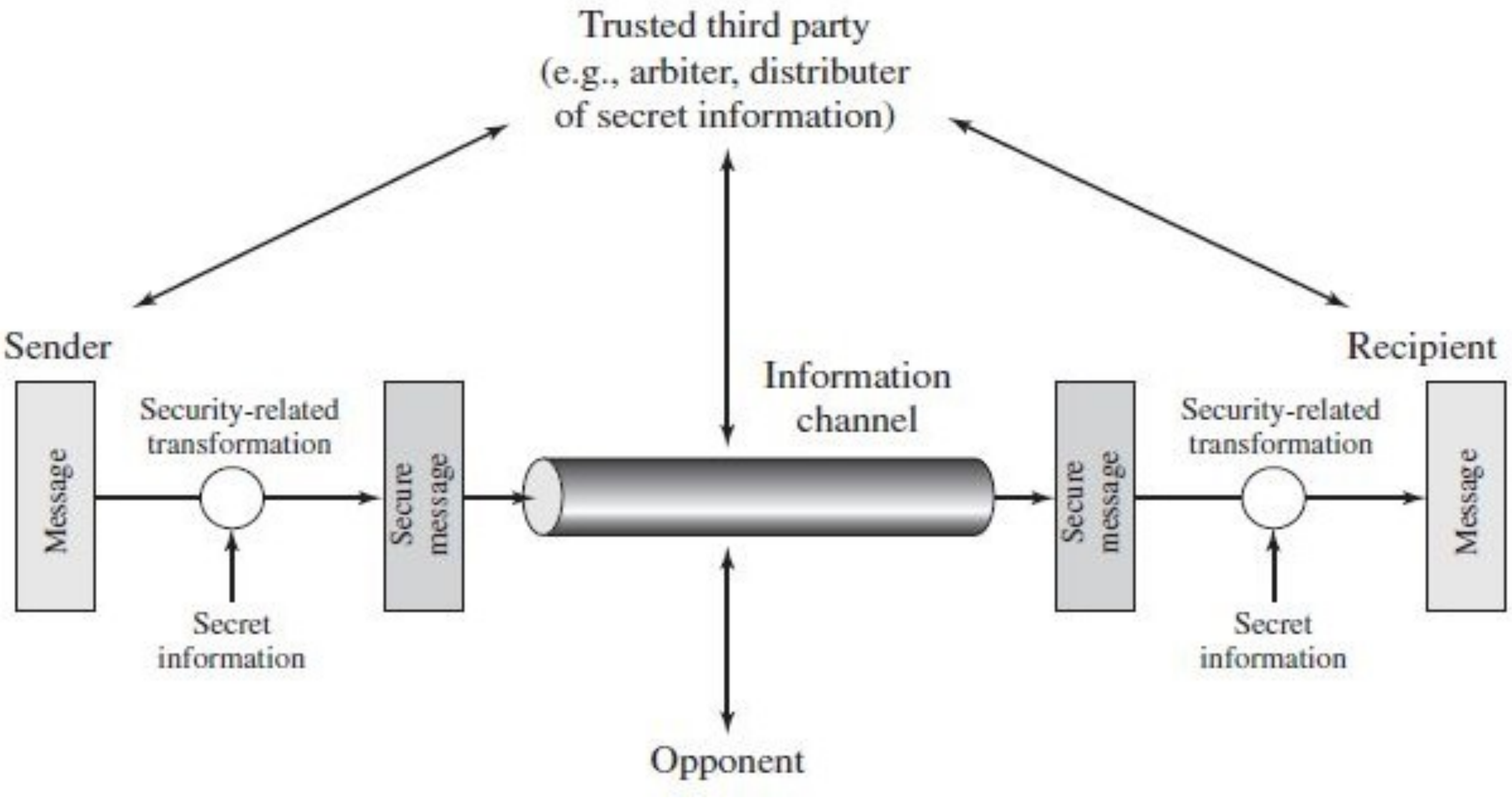
Security Recovery

Deals with requests from mechanisms, such as event handling and management functions, and takes recovery actions.

A Model for Network Security

- A message is to be transferred from one party to another across some sort of Internet service. 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 two principals.
- All the techniques for providing security have two components:
  - A security-related transformation on the information to be sent.
  - Secret information shared by the two parties.

A Model for Network Security



Classical encryption techniques

Plaintext

- Message or data that is fed into the algorithm as input.

Encryption algorithm

- Performs various substitutions and transformations on the plaintext.

Secret key

- The key is a value independent of the plaintext and of the algorithm.

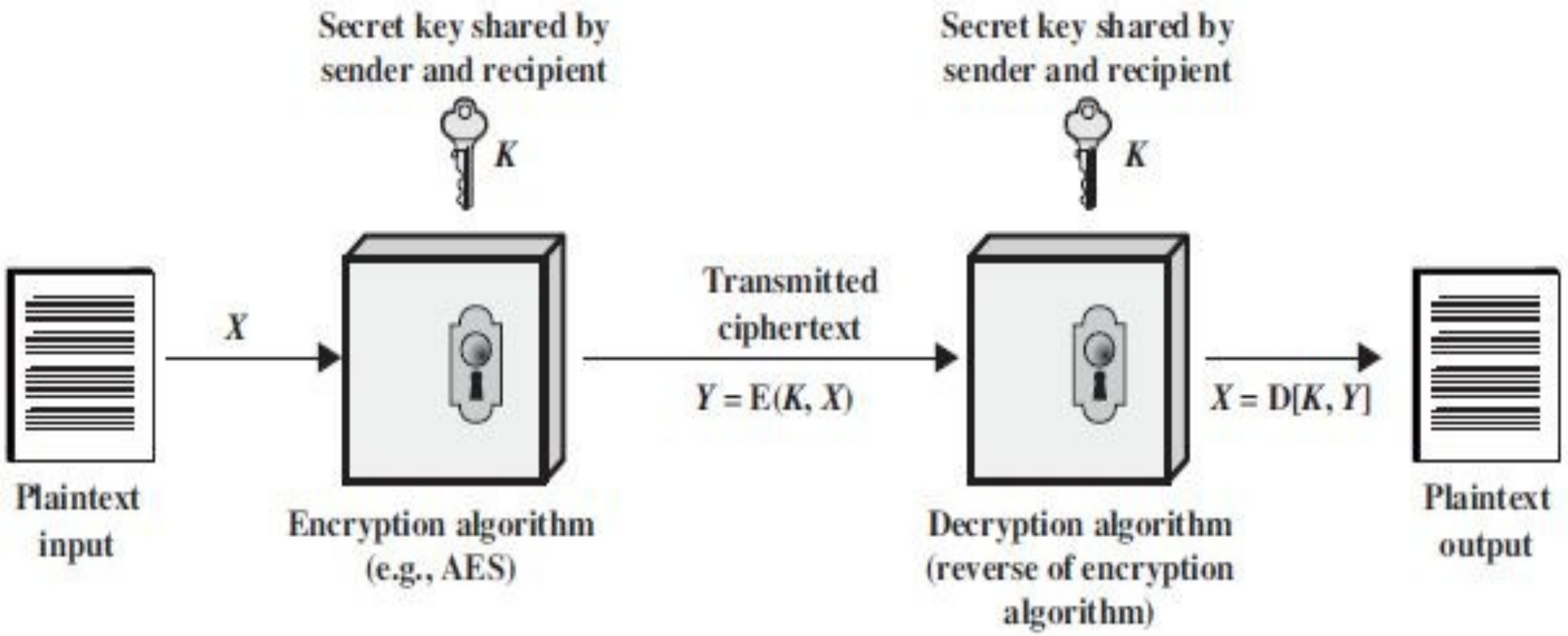
Ciphertext

- This is the scrambled message produced as output.

Decryption algorithm

- It takes the ciphertext and the secret key and produces the original plaintext.

Classical encryption techniques


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

Substitution techniques

- A substitution technique is one in which the letters of plaintext are replaced by other letters or by numbers or symbols.
- The substitution techniques are
  - Caesar cipher
  - Monoalphabetic Ciphers
  - Playfair Cipher
  - Hill Cipher
  - Polyalphabetic Ciphers
  - One-Time Pad

Caesar cipher

- The earliest known, and the simplest, use of a substitution cipher was by Julius Caesar.

- The Caesar cipher involves replacing each letter of the alphabet with the letter standing k^{th} places further down the alphabet.

Caesar cipher

C=(P+K)mod 26 //Encryption

P=(C-K)mod 26 //Decryption

C->Ciphertext

P->Plaintext

K->Key

26->26 alphabets

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
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

Caesar cipher (Encryption)

- Plaintext= hai hello=> 708 74111114
- Key = 3

Encryption

C(h) =(7+3)mod 26 =10 =>k

C(a) =(0+3)mod 26 = 3 =>d

C(i) =(8+3)mod 26 =11=>l

C(h) =(7+3)mod 26 =10 =>k

C(e) =(4+3)mod 26 = 7

=>h

C(l) =(11+3)mod 26 =14 =>o

C(l) =(11+3)mod 26 =14 =>o

C(o) =(14+3)mod 26 =17 =>r

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
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

Ciphertext = kdl khoor

Caesar cipher (Decryption)

- Ciphertext= kdl khoor => 10311 107141417
- Key = 3 Decryption

P(k) =(10-3)mod 26 =7 =>h

P(d) =(3-3)mod 26 =0 =>a

P(l) =(11-3)mod 26 =8 =>i

P(k) =(10-3)mod 26 =7 =>h

P(h) =(7-3)mod 26 = 4

=>e

P(o) =(14-3)mod 26 =11 =>l

P(o) =(14-3)mod 26 =11 =>l

P(r) =(17-3)mod 26 =14 =>o

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
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

Plaintext = hai hello

Monoalphabetic Ciphers

- The process of mapping from plain alphabet to cipher alphabet using permutation is called Monoalphabetic cipher.

- A permutation of a finite set of elements S is an ordered sequence of all the elements of S, with each element appearing exactly once.

Monoalphabetic Ciphers (Encryption)

Plaintext=hai hello

Permutation set (S)

2				5		1, 4	3				6, 7			8											
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
q	w	e	r	t	y	u	i	o	p	a	s	d	f	g	h	j	k	l	z	x	c	v	b	n	m

Ciphertext=iqo itssg

Monoalphabetic Ciphers (Decryption)

Ciphertext=iqo

itssg Permutation

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
q	w	e	r	t	y	u	i	o	p	a	s	d	f	g	h	j	k	l	z	x	c	v	b	n	m
2				**5**		**1, 4**		**3**			**6, 7**			**8**											

Plaintext=hai hello

Playfair Cipher

- Playfair, which treats digrams in the plaintext as single units and translates these units into ciphertext digrams.
- The Playfair algorithm is based on the use of a 5 * 5 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 alphabetic order.

Playfair Cipher

- Plaintext is encrypted two letters at a time.
- Repeating plaintext letters that are in the same pair are separated with a filler letter, such as x, so that balloon would be treated as ba lx lo on.
- Two 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 circularly following the last. For example, ar is encrypted as RM.

Key= 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

Playfair Cipher

- Two plaintext letters that fall in the same column are each replaced by the letter beneath, with the top element of the column circularly following the last. For example, mu is encrypted as CM.
- Otherwise, each plaintext letter in a pair is replaced by the letter that lies in its own row and the column occupied by the other plaintext letter. Thus, hs becomes BP and ea becomes IM (or JM, as the encipherer wishes).

Key= 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

Playfair Cipher (Encryption)

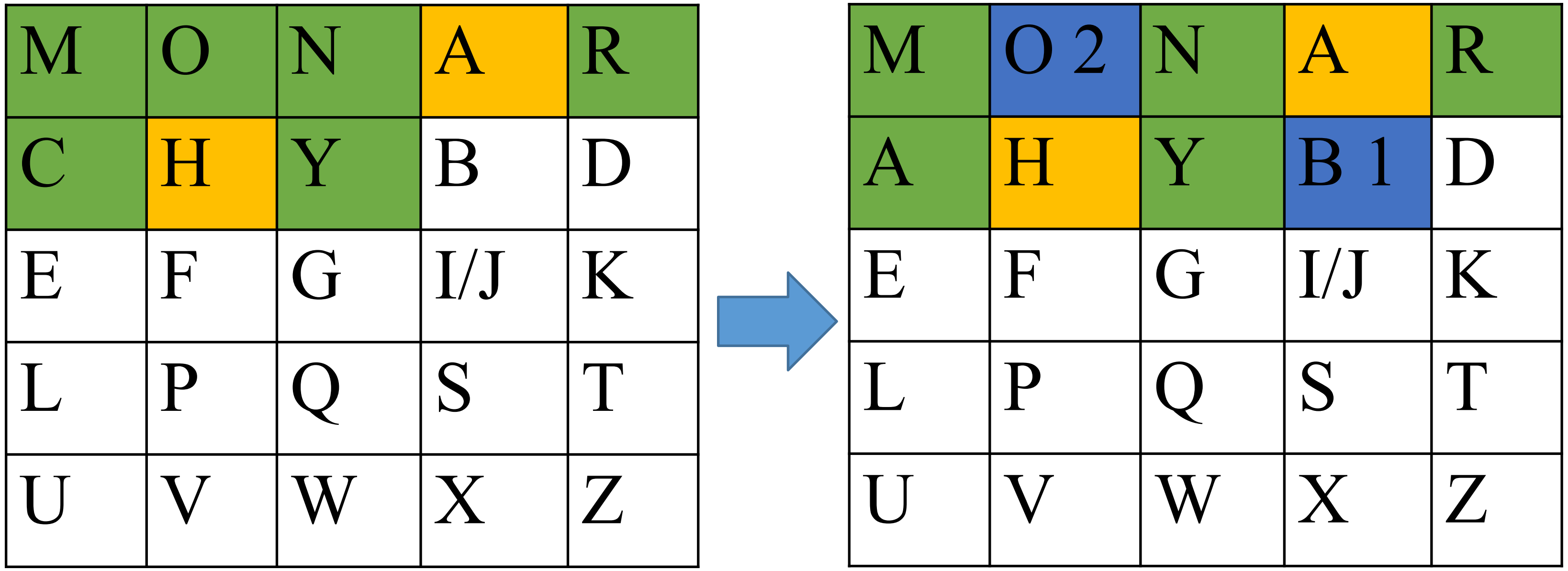
Plaintext =HAI HELLO

=HA IH EL LO

Key =MONARCHY

Ciphertext=BO

Encrypt HA



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

M	O 2	N	A	R
A	H	Y	B 1	D
E	F	G	I/J	K
L	P	Q	S	T
U	V	W	X	Z

Cipher = BO

Playfair Cipher (Encryption)

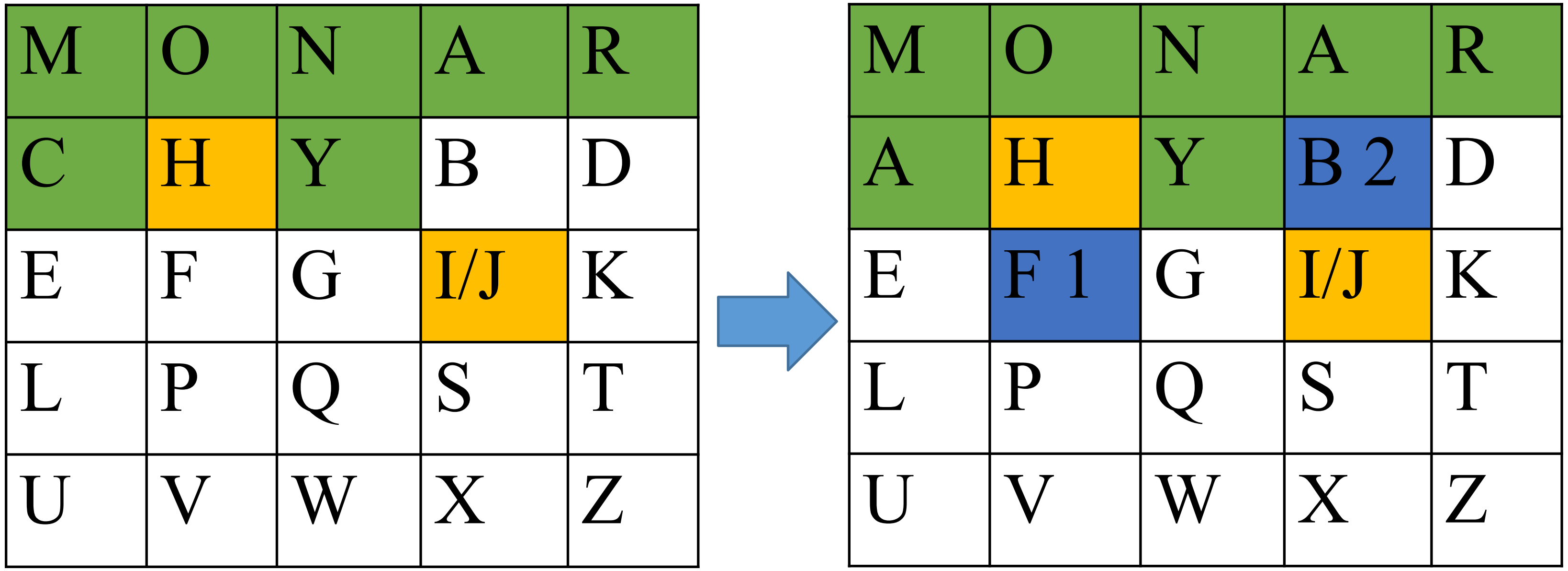
Plaintext =HAI HELLO

=HA IH EL LO

Key =MONARCHY

Ciphertext=BO FB

Encrypt IH



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

M	O	N	A	R
A	H	Y	B 2	D
E	F 1	G	I/J	K
L	P	Q	S	T
U	V	W	X	Z

Cipher = FB

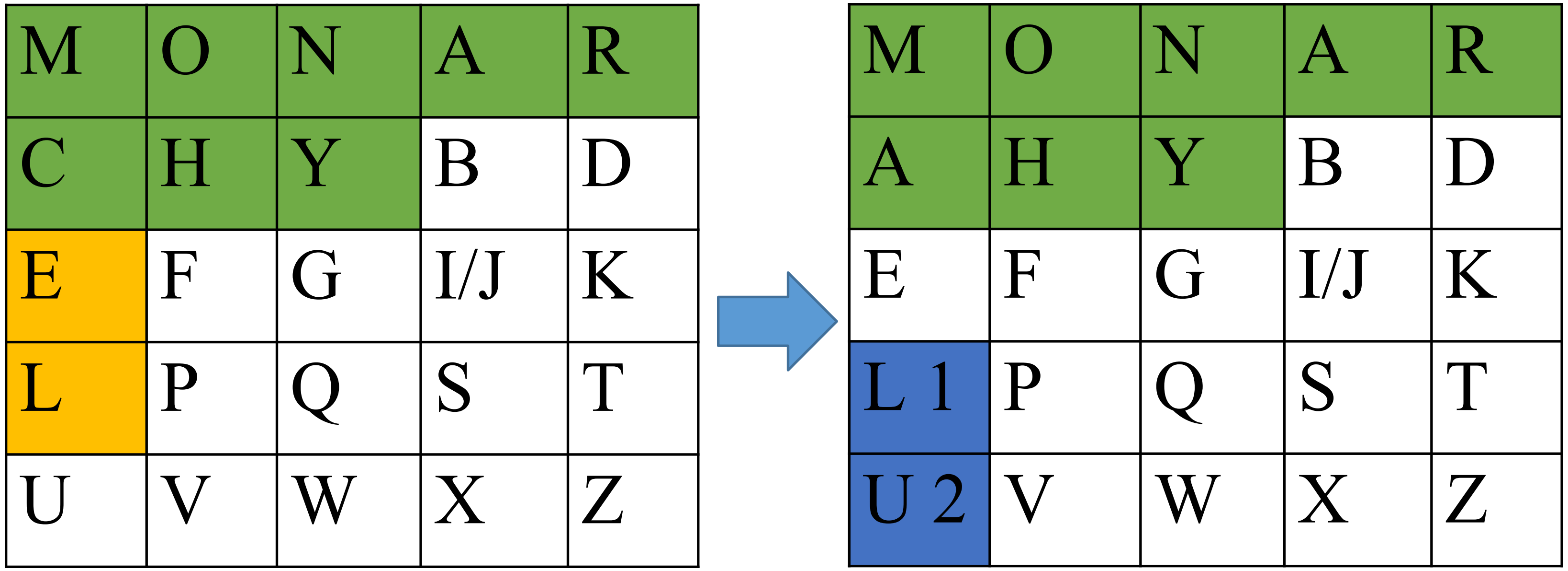
Playfair Cipher (Encryption)

Plaintext =HAI HELLO

=HA IH EL LO

Key =MONARCHY

Encrypt EL



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

M	O	N	A	R
A	H	Y	B	D
E	F	G	I/J	K
L 1	P	Q	S	T
U 2	V	W	X	Z

Cipher = LU

Ciphertext=BO FB LU

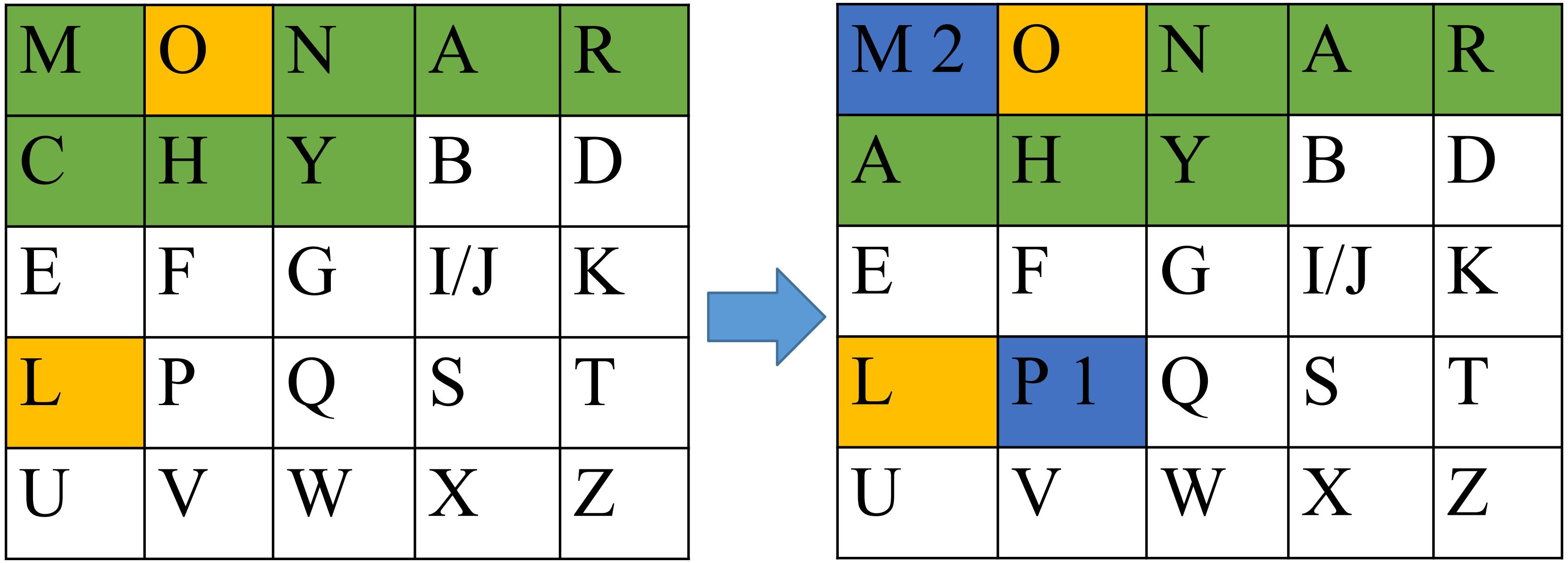
Playfair Cipher (Encryption)

Plaintext =HAI HELLO

=HA IH EL LO

Key =MONARCHY

Encrypt LO



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

M 2	O	N	A	R
A	H	Y	B	D
E	F	G	I/J	K
L	P 1	Q	S	T
U	V	W	X	Z

Ciphertext=BO FB LU PM

=BOF BLUPM

Cipher = PM

Playfair Cipher (Decryption)

Ciphertext =BOF BLUPM

=BO FB LU PM

Key =MONARCHY

Plaintext =HA

Decrypt BO

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

M	O	N	A 2	R
A	H 1	Y	B	D
E	F	G	I/J	K
L	P	Q	S	T
U	V	W	X	Z

Message = HA

Playfair Cipher (Decryption)

Ciphertext =BOF BLUPM

=BO FB LU PM

Key =MONARCHY

Plaintext =HA IH

Decrypt FB

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

M	O	N	A	R
A	H 2	Y	B	D
E	F	G	I/J 1	K
L	P	Q	S	T
U	V	W	X	Z

Message = IH

Playfair Cipher (Decryption)

Ciphertext =BOF BLUPM

=BO FB LU PM

Key =MONARCHY

Plaintext =HA IH EL

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

Decrypt LU

M	O	N	A	R
A	H	Y	B	D
E 1	F	G	I/J	K
L 2	P	Q	S	T
U	V	W	X	Z

Message = EL

Playfair Cipher (Decryption)

Ciphertext =BOF BLUPM

=BO FB LU PM

Key =MONARCHY

Plaintext =HA IH EL LO

=HAI HELLO

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

Decrypt PM

M	O 2	N	A	R
A	H	Y	B	D
E	F	G	I/J	K
L 1	P	Q	S	T
U	V	W	X	Z

Message = LO

Hill cipher

- Hill cipher, developed by the mathematician Lester Hill in 1929. This encryption algorithm takes m successive plaintext letters and substitutes for them m ciphertext letters.

- The substitution is determined by m linear equations in which each character is assigned a numerical value (a = 0, b = 1,……z = 25).

Hill cipher

- For m = 3, the system can be described as
- $c_1 = (k_{11}p_1 + k_{21}p_2 + k_{31}p_3) \bmod 26$
- $c_2 = (k_{12}p_1 + k_{22}p_2 + k_{32}p_3) \bmod 26$
- $c_3 = (k_{13}p_1 + k_{23}p_2 + k_{33}p_3) \bmod 26$
- This can be expressed in terms of row vectors and matrices:

- $(c_1\ c_2\ c_3) = (p_1\ p_2\ p_3) \begin{pmatrix} k_{11} & k_{12} & k_{13} \\ k_{21} & k_{22} & k_{23} \\ k_{31} & k_{32} & k_{33} \end{pmatrix} \bmod 26$

Or $C = PK \bmod 26$

$P = CK^{-1} \bmod 26$

Hill cipher (Encryption)

Plaintext=hai emy

$$\text{Key} =^{5} \begin{pmatrix} 7 & 9 & & \\ = & 6 & 8 & 3 \\ 11 & 2 & 1 & \end{pmatrix}$$

Step-1: Split the characters (3 as a block)

=hai emy

Step-2: Assign numerical equivalent to each letter: 701 41224

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
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

Hill cipher (Encryption)

Step-3: Formation of enciphering matrix

$$P_{1=>} \begin{matrix} h \\ a \\ i \end{matrix} \begin{pmatrix} 7 \\ 0 \\ 8 \end{pmatrix} \qquad P_{2=>} \begin{matrix} e \\ m \\ y \end{matrix} = \begin{pmatrix} 4 \\ 12 \\ 24 \end{pmatrix}$$

Step-4: Multiply the above matrix with the key (B_1=Block 1, B_2= Block 2)

$$B_1 = \begin{pmatrix} 5 & 7 & 9 \\ 6 & 8 & 3 \\ 11 & 2 & 1 \end{pmatrix} * \begin{pmatrix} 7 \\ 0 \\ 8 \end{pmatrix} = \begin{pmatrix} 107 \\ 66 \\ 85 \end{pmatrix} \qquad B_2 = \begin{pmatrix} 5 & 7 & 9 \\ 6 & 8 & 3 \\ 11 & 2 & 1 \end{pmatrix} * \begin{pmatrix} 4 \\ 12 \\ 24 \end{pmatrix} = \begin{pmatrix} 320 \\ 192 \\ 92 \end{pmatrix}$$

Hill cipher (Encryption)

Step-5: Replace each value in matrix with modulo 26

$$B_{1=>} \begin{pmatrix} 107 \\ 66 \\ 85 \end{pmatrix} \text{mod } 26 = \begin{pmatrix} 3 \\ 14 \\ 7 \end{pmatrix} \qquad B_{2=>} \begin{pmatrix} 320 \\ 192 \\ 92 \end{pmatrix} \text{mod } 26 = \begin{pmatrix} 8 \\ 10 \\ 14 \end{pmatrix}$$

Step-6: Assign alphabet for the values in the matrix by referring the table

$$C_1 = B_1 = \begin{pmatrix} 3 \\ 14 \\ 7 \end{pmatrix} = \begin{pmatrix} d \\ o \\ h \end{pmatrix} \qquad C_2 = B_2 = \begin{pmatrix} 8 \\ 10 \\ 14 \end{pmatrix} = \begin{pmatrix} i \\ k \\ o \end{pmatrix}$$

Ciphertext = doh iko

Hill cipher (Decryption)

Ciphertext=doh iko

Key 5 7 $\left(\begin{matrix} 9 & & \\ 6 & 8 & 3 \\ 2 & 1 & \end{matrix}\right)$
=
11

Step-1: Split the characters (3 as a block) =doh iko

Step-2: Assign numerical equivalent to each letter: 3147 81014

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
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

Hill cipher (Decryption)

Step-3: Formation of enciphering matrix

$$C_{1=>} \begin{matrix} d \\ o \\ i \end{matrix} = \begin{pmatrix} 3 \\ 14 \\ 7 \end{pmatrix} o \quad C_{2=>} \qquad k = \begin{pmatrix} i & 8 \\ & \\ & \end{pmatrix}$$

10

14

Step-4: Find K^{-1}

$K^{-1} = 1/\det(K)*\mathrm{adj}(K) = \det^{-1}(K)*\mathrm{adj}(K)$

1. Calculate $\det^{-1}(K)$
2. Calculate adj(K)
3. Calculate K^{-1}

Hill cipher (Decryption)

Step-4.1: Calculate $\det^{-1}(K)$

$\det(K) = \begin{vmatrix} 5 & 7 & 9 \\ 6 & 8 & 3 \\ 11 & & \end{vmatrix}$ = 5(8-6)-7(6-33)+9(12-88) = -485

= -485 mod 26 = 485 mod 26 =17

2 1 = 26-17=9 (If numerator is –ve and > denominator)

$\det(K)*\det^{-1}(K) \equiv 1 \bmod 26$ => $\det(K)*\det^{-1}(K) \bmod 26 = 1$

$9*\det^{-1}(K) \bmod 26=1$

$9*3 \bmod 26 =1$

$\det^{-1}(K) = 3$

Hill cipher (Decryption)

Step-4.2: Calculate adj(K)

$$K = \begin{pmatrix} 5 & 7 & 9 \\ 6 & 8 & 3 \\ 11 & 2 & 1 \end{pmatrix}$$

→

Find cofactors of each entry k_{mn}

$k_{11} = 8-6 = 2$

$k_{12} = 6-33 = -27$

$k_{13} = 12-88 = -76$

$k_{21} = 7-18 = -11$

$k_{22} = 5-99 = -94$

$k_{23} = 10-77 = -67$

$k_{31} = 21-72 = -51$

$k_{32} = 15-54 = -39$

$k_{33} = 40-42 = -2$

Hill cipher (Decryption)

Step-4.2: Calculate adj(K)

Substitute the values and put sign according to $(-1)^{m+n}$

$$\begin{pmatrix} 2 & -27 & -76 \\ -11 & -9 & -67 \\ -51 & -39 & -2 \end{pmatrix} \Rightarrow \begin{pmatrix} 2 & 27 & -76 \\ 11 & -94 & 67 \\ -51 & 39 & -2 \end{pmatrix}$$

Take transpose for the above matrix

$$\text{adj}(K) = \begin{pmatrix} 2 & 11 & -51 \\ 27 & -94 & 39 \\ -76 & 67 & -2 \end{pmatrix}$$

Hill cipher (Decryption)

Step-4.3: Calculate K^{-1}

$$K^{-1} = \det{}^{-1}(K) * \mathrm{adj}(K)$$

$$= 3 * \begin{pmatrix} 2 & 11 & -51 \\ 27 & -94 & 39 \\ -76 & 67 & -2 \end{pmatrix} = \begin{pmatrix} 6 & 33 & -153 \\ 81 & -282 & 117 \\ -228 & 201 & -6 \end{pmatrix}$$

Take modulo 26 for all the values

$$K^{-1} = \begin{pmatrix} 6 & 7 & 3 \\ 3 & 4 & 13 \\ 6 & 19 & 20 \end{pmatrix}$$

Hill cipher (Decryption)

Step-5: Multiply the C_1 and C_2 with K^{-1} (B_1=Block 1, B_2= Block 2)

$$B_1 = \begin{pmatrix} 6 & 7 & 3 \\ 3 & 4 & 13 \\ 6 & 19 & 20 \end{pmatrix} * \begin{pmatrix} 3 \\ 14 \\ 7 \end{pmatrix} = \begin{pmatrix} 137 \\ 156 \\ 424 \end{pmatrix} \qquad B_2 = \begin{pmatrix} 6 & 7 & 3 \\ 3 & 4 & 13 \\ 6 & 19 & 20 \end{pmatrix} * \begin{pmatrix} 8 \\ 10 \\ 14 \end{pmatrix} = \begin{pmatrix} 160 \\ 246 \\ 514 \end{pmatrix}$$

Step-6: Replace each value in matrix with modulo 26

$$B_{1=>} \begin{pmatrix} 137 \\ 156 \\ 424 \end{pmatrix} \text{mod } 26 = \begin{pmatrix} 7 \\ 0 \\ 8 \end{pmatrix} \qquad B_{2=>} \begin{pmatrix} 160 \\ 246 \\ 514 \end{pmatrix} \text{mod } 26 = \begin{pmatrix} 4 \\ 12 \\ 24 \end{pmatrix}$$

Hill cipher (Decryption)

Step-6: Assign alphabet for the values in the matrix by referring the table.

$$P_1 = B_1 = \begin{pmatrix} 7 \\ 0 \\ 8 \end{pmatrix} = \begin{pmatrix} h \\ a \\ i \end{pmatrix} \qquad P_2 = B_2 = \begin{pmatrix} 4 \\ 12 \\ 24 \end{pmatrix} = \begin{pmatrix} e \\ m \\ y \end{pmatrix}$$

Plaintext = hai emy

Polyalphabetic Ciphers

- Different monoalphabetic substitutions as one proceeds through the plaintext message.
- A set of related monoalphabetic substitution rules is used.
- A key determines which particular rule is chosen for a given transformation.
- Two types of Ciphers

  A. Vigenere Cipher - The key is used as a repeating keyword as long as the message.

  B. Vernam Cipher - The ciphertext is generated by performing the bitwise XOR of the plaintext and the key.

Vigenere Cipher (Encryption)

Plaintext : hai hello

Key   : wish

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
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

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
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

Vigenere Cipher (Encryption)

P	h	a	i	h	e	l	l	o	
	7	0	8	7	4	11	11	14	
K	w	i	s	h	w	i	s	h	
	22	8	18	7	22	8	18	7	(P+K)
C	29	8	26	14	26	19	29	21	(mod 26)
	3	8	0	14	0	19	3	21	
	d	i	a	o	a	t	d	v	

Ciphertext : dia oatdv

Vigenere Cipher (Decryption)

Ciphertext : dia oatdv

Key : wish

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
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

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
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

Vigenere Cipher (Decryption)

C	d	i	a	o	a	t	d	v	
	3	8	0	14	0	19	3	21	
K	w	i	s	h	w	i	s	h	
	22	8	18	7	22	8	18	7	(C-K)
P	-19	0	-18	7	-22	11	-15	14	(mod 26)
	7	0	8	7	4	11	11	14	
	h	a	i	h	e	l	l	o	

Plaintext : hai hello

Vigenere Cipher (Encryption)
Autokey system

Another method that uses the plaintext, in a repetitive nature that fills after the key for encryption to produce the ciphertext. It is called **Autokey system**.

Plaintext : hai hello

Key : wish

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
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

↓

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
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

Vigenere Cipher (Encryption)

P	h	a	i	h	e	l	l	o	
	7	0	8	7	4	11	11	14	
K	w	i	s	h	h	a	i	h	
	22	8	18	7	7	0	8	7	(P+K)
C	29	8	26	14	11	11	19	21	(mod 26)
	3	8	0	14	11	11	19	21	
	d	i	a	o	l	l	t	v	

Ciphertext : dia olltv

Vigenere Cipher (Decryption)

Ciphertext : dia olltv

Key : wish

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
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

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
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

Vigenere Cipher (Decryption)

C	d	i	a	o	l	l	t	v	
	3	8	0	14	11	11	19	21	
K	w	i	s	h	h	a	i	h	
	22	8	18	7	7	0	8	7	(C-K)
P	-19	0	-18	7	4	11	11	14	(mod 26)
	7	0	8	7	4	11	11	14	
	h	a	i	h	e	l	l	o	

Plaintext : hai hello

Vernam Cipher

The ciphertext is generated by performing the bitwise XOR of the plaintext and the key. The plaintext can be retrieved by performing the bitwise XOR of the ciphertext and the key.

$C_i = P_i \oplus K_i$ //Encryption

$P_i = C_i \oplus K_i$ // Decryption

where

P_i =i^{th} binary digit of plaintext.

K_i =i^{th} binary digit of key.

C_i =i^{th} binary digit of ciphertext.

$\oplus$ =exclusive-or (XOR) operation.

Vernam Cipher (Encryption)

Plaintext = hai hello

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
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

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
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

Plaintext = 7 0 8 7 4 11 11 14

Key = 100 =>Max. no of binary digits in plaintext=4=> 100 1 (Key repeat)

Vernam Cipher (Encryption)

$C_1=P_1 \oplus K_1$

$P_1=7=0111$; $K_1=1001$

$=0111 \oplus 1001$

$=1110$

$=14=$o

$C_2=P_2 \oplus K_2$

$P_2=0=0000$; $K_2=1001$

$=0000 \oplus 1001$

$=1001$

$=9=$j

Representing in binary form

0	=	0000	11	=	1011
1	=	0001	12	=	1100
2	=	0010	13	=	1101
3	=	0011	14	=	1110
4	=	0100	15	=	1111
5	=	0101			
6	=	0110			
7	=	0111			
8	=	1000			
9	=	1001			
10	=	1010			

Vernam Cipher (Encryption)

$C_3=P_3\oplus K_3$

$P_3=8=1000;\ K_3=1001$

$=1000\oplus1001$

$=0001=1=b$

$C_4=P_4\oplus K_4$

$P_4=7=0111;\ K_4=1001$

$=0111\oplus1001$

$=1110$

$=14=o$

Representing in binary form

0 = 0000	11 = 1011
1 = 0001	12 = 1100
2 = 0010	13 = 1101
3 = 0011	14 = 1110
4 = 0100	15 = 1111
5 = 0101	
6 = 0110	
7 = 0111	
8 = 1000	
9 = 1001	
10 = 1010	

Vernam Cipher (Encryption)

$C_5=P_5\oplus K_5$

$P_5=4=0100;\ K_5=1001$

$=0100\oplus 1001$

$=1101$

$=13=n$

$C_6=P_6\oplus K_6$

$P_6=11=1011;\ K_6=1001$

$=1011\oplus 1001$

$=0010$

$=2=c$

Representing in binary form

0	=	0000	11	=	1011
1	=	0001	12	=	1100
2	=	0010	13	=	1101
3	=	0011	14	=	1110
4	=	0100	15	=	1111
5	=	0101			
6	=	0110			
7	=	0111			
8	=	1000			
9	=	1001			
10	=	1010			

Vernam Cipher (Encryption)

$C_7=P_7 \oplus K_7$

$P_7=11=1011$; $K_7=1001$

$=1011 \oplus 1001$

$=0010$

$=2=$c

$C_8=P_8 \oplus K_8$

$P_8=14=1110$; $K_8=1001$

$=1110 \oplus 1001$

$=0111$

$=7=$h **Ciphertext=ojb oncch**

Representing in binary form

0	=	0000	11	=	1011
1	=	0001	12	=	1100
2	=	0010	13	=	1101
3	=	0011	14	=	1110
4	=	0100	15	=	1111
5	=	0101			
6	=	0110			
7	=	0111			
8	=	1000			
9	=	1001			
10	=	1010			

Vernam Cipher (Decryption)

Ciphertext = ojb oncch

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
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

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
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

Ciphertext= 14 9 1 14 13 2 2 7

Key = 100 =>Max. no of binary digits in ciphertext=4=> 100 1 (Key repeat)

Vernam Cipher (Decryption)

$P_1 = C_1 \oplus K_1$

$C_1 = 14 = 1110;\ K_1 = 1001$

$= 1110 \oplus 1001$

$= 0111$

$= 7 = h$

$P_2 = C_2 \oplus K_2$

$C_2 = 9 = 1001;\ K_2 = 1001$

$= 1001 \oplus 1001$

$= 0$

$= 0 = a$

Representing in binary form

0	=	0000	11 =	1011
1	=	0001	12 =	1100
2	=	0010	13 =	1101
3	=	0011	14 =	1110
4	=	0100	15 =	1111
5	=	0101		
6	=	0110		
7	=	0111		
8	=	1000		
9	=	1001		
10	=	1010		

Vernam Cipher (Decryption)

$P_3=C_3 \oplus K_3$

$C_3=1=0001$; $K_3=1001$

$=0001\oplus1001$

$=1000=8=i$

$P_4=C_4 \oplus K_4$

$C_4=14=1110$; $K_4=1001$

$=1110\oplus1001$

$=0111$

$=7=h$

Representing in binary form

0	=	0000	11	=	1011
1	=	0001	12	=	1100
2	=	0010	13	=	1101
3	=	0011	14	=	1110
4	=	0100	15	=	1111
5	=	0101			
6	=	0110			
7	=	0111			
8	=	1000			
9	=	1001			
10	=	1010			

Vernam Cipher (Decryption)

$P_5 = C_5 \oplus K_5$

$C_5 = 13 = 1101$; $K_5 = 1001$

$= 1101 \oplus 1001$

$= 0100$

$= 4 = e$

$P_6 = C_6 \oplus K_6$

$C_6 = 02 = 0010$; $K_6 = 1001$

$= 0010 \oplus 1001$

$= 1011$

$= 11 = l$

Representing in binary form

0 =	0000	11 =	1011
1 =	0001	12 =	1100
2 =	0010	13 =	1101
3 =	0011	14 =	1110
4 =	0100	15 =	1111
5 =	0101		
6 =	0110		
7 =	0111		
8 =	1000		
9 =	1001		
10 =	1010		

Vernam Cipher (Decryption)

$P_7 = C_7 \oplus K_7$

$C_7 = 02 = 0010;\ K_7 = 1001$

$= 0010 \oplus 1001$

$= 1011$

$= 11 = \mathrm{l}$

$P_8 = C_8 \oplus K_8$

$C_8 = 7 = 0111;\ K_8 = 1001$

$= 0111 \oplus 1001$

$= 1110$

$= 14 = \mathrm{o}$ **Plaintext=hai hello**

Representing in binary form

0	=	0000	11	=	1011
1	=	0001	12	=	1100
2	=	0010	13	=	1101
3	=	0011	14	=	1110
4	=	0100	15	=	1111
5	=	0101			
6	=	0110			
7	=	0111			
8	=	1000			
9	=	1001			
10	=	1010			

One-Time Pad

- It is a improved version of Vernam cipher.
- Using a random key that is as long as the message, so that the key need not be repeated.
- In addition, the key is to be used to encrypt and decrypt a single message, and then is discarded.
- Each new message requires a new key of the same length as the new message.

One-Time Pad (Encryption)

Plaintext = hai hello

Key = klm iopce

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
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

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
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

Plaintext = 7 0 8 7 4 11 11 14

Key = 10 11 12 8 14 15 2 4

One-Time Pad (Encryption)

$C_1=P_1\oplus K_1$

$P_1=7=0000\ 0111;\ K_1=10=0000\ 1010$

$=0000\ 0111\oplus 0000\ 1010$

$=0000\ 1101$

$=13=n$

$C_2=P_2\oplus K_2$

$P_2=0=0000\ 0000;\ K_2=11=0000\ 1011$

$=0000\ 0000\oplus 0000\ 1011$

$=0000\ 1011$

$=11=l$

Representing in binary form

0	=	0000	11	=	1011
1	=	0001	12	=	1100
2	=	0010	13	=	1101
3	=	0011	14	=	1110
4	=	0100	15	=	1111
5	=	0101			
6	=	0110			
7	=	0111			
8	=	1000			
9	=	1001			
10	=	1010			

One-Time Pad (Encryption)

$C_3=P_3 \oplus K_3$

$P_3=8=0000\ 1000;\ K_3=12=0000\ 1100$

$=0000\ 1000 \oplus 0000\ 1100$

$=0000\ 0100$

$=4=e$

$C_4=P_4 \oplus K_4$

$P_4=7=0000\ 0111;\ K_4=8=0000\ 1000$

$=0000\ 0111 \oplus 0000\ 1000$

$=0000\ 1111$

$=15=p$

Representing in binary form

0	=	0000	11	=	1011
1	=	0001	12	=	1100
2	=	0010	13	=	1101
3	=	0011	14	=	1110
4	=	0100	15	=	1111
5	=	0101			
6	=	0110			
7	=	0111			
8	=	1000			
9	=	1001			
10	=	1010			

One-Time Pad (Encryption)

$C_5=P_5 \oplus K_5$

$P_5=4=0000\ 0100;\ K_5=14=0000\ 1110$

$=0000\ 0100 \oplus 0000\ 1110$

$=0000\ 1010$

$=10=$k

$C_6=P_6 \oplus K_6$

$P_6=11=0000\ 1011;\ K_6=15=0000\ 1111$

$=0000\ 1011 \oplus 0000\ 1111$

$=0000\ 0100$

$=4=$e

Representing in binary form

0	=	0000	11	=	1011
1	=	0001	12	=	1100
2	=	0010	13	=	1101
3	=	0011	14	=	1110
4	=	0100	15	=	1111
5	=	0101			
6	=	0110			
7	=	0111			
8	=	1000			
9	=	1001			
10	=	1010			

One-Time Pad (Encryption)

$C_7=P_7\oplus K_7$

$P_7=11=0000\ 1011;\ K_7=2=0000\ 0010$

$=0000\ 1011\oplus 0000\ 0010$

$=0000\ 1001$

$=9=j$

$C_8=P_8\oplus K_8$

$P_8=14=0000\ 1110;\ K_8=4=0000\ 0100$

$=0000\ 1110\oplus 0000\ 0100$

$=0000\ 1010$

$=10=k$

Ciphertext=nle pkejk

Representing in binary form

0	=	0000	11	=	1011
1	=	0001	12	=	1100
2	=	0010	13	=	1101
3	=	0011	14	=	1110
4	=	0100	15	=	1111
5	=	0101			
6	=	0110			
7	=	0111			
8	=	1000			
9	=	1001			
10	=	1010			

One-Time Pad (Decryption)

Ciphertext = nle pkejk

Key = klm iopce

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
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

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
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

Ciphertext = 13 11 4 15 10 4 9 10

Key = 10 11 12 8 14 15 2 4

One-Time Pad (Encryption)

$P_1=C_1 \oplus K_1$

$C_1=13=0000\ 1101$; $K_1=10=0000\ 1010$

$=0000\ 1101 \oplus 0000\ 1010$

1

$=0000\ 0111$

$=7=h$

$P_2=C_2 \oplus K_2$

$C_2=11=0000\ 1011$; $K_2=11=0000\ 1011$

$=0000\ 01011 \oplus 0000\ 1011$

$=0000\ 0000$

$=0=a$

Representing in binary form

0	=	0000	11	=	1011
	=	0001	12	=	1100
2	=	0010	13	=	1101
3	=	0011	14	=	1110
4	=	0100	15	=	1111
5	=	0101			
6	=	0110			
7	=	0111			
8	=	1000			
9	=	1001			
10	=	1010			

One-Time Pad (Encryption)

$P_3 = C_3 \oplus K_3$

$C_3 = 4 = 0000\ 0100;\ K_3 = 12 = 0000\ 1100$

$= 0000\ 0100 \oplus 0000\ 1100$

$= 0000\ 1000$

$= 8 = i$

$P_4 = C_4 \oplus K_4$

$C_4 = 15 = 0000\ 1111;\ K_4 = 8 = 0000\ 1000$

$= 0000\ 1111 \oplus 0000\ 1000$

$= 0000\ 0111$

$= 7 = h$

Representing in binary form

0	=	0000	11	=	1011
1	=	0001	12	=	1100
2	=	0010	13	=	1101
3	=	0011	14	=	1110
4	=	0100	15	=	1111
5	=	0101			
6	=	0110			
7	=	0111			
8	=	1000			
9	=	1001			
10	=	1010			

One-Time Pad (Encryption)

$P_5=C_5 \oplus K_5$

$C_5=10=0000\ 1010$; $K_5=14=0000\ 1110$

$=0000\ 1010 \oplus 0000\ 1110$

1

$=0000\ 0100$

$=4=$e

$P_6=C_6 \oplus K_6$

$C_6=4=0000\ 0100$; $K_6=15=0000\ 1111$

$=0000\ 0100 \oplus 0000\ 1111$

$=0000\ 1011$

$=11=$l

Representing in binary form

0	=	0000	11	=	1011
	=	0001	12	=	1100
2	=	0010	13	=	1101
3	=	0011	14	=	1110
4	=	0100	15	=	1111
5	=	0101			
6	=	0110			
7	=	0111			
8	=	1000			
9	=	1001			
10	=	1010			

One-Time Pad (Encryption)

$P_7 = C_7 \oplus K_7$

$C_7 = 9 = 0000\ 1001$; $K_7 = 2 = 0000\ 0010$

$= 0000\ 1001 \oplus 0000\ 0010$

$= 0000\ 1011$

$= 11 = l$

$P_8 = C_8 \oplus K_8$

$C_8 = 10 = 0000\ 1010$; $K_8 = 4 = 0000\ 0100$

$= 0000\ 1010 \oplus 0000\ 0100$

$= 0000\ 1110$

$= 14 = o$

Plaintext=hai hello

Representing in binary form

0	=	0000	11	=	1011
1	=	0001	12	=	1100
2	=	0010	13	=	1101
3	=	0011	14	=	1110
4	=	0100	15	=	1111
5	=	0101			
6	=	0110			
7	=	0111			
8	=	1000			
9	=	1001			
10	=	1010			

Transpositional techniques

- The process of rearranging the letters in plaintext using key to form the ciphertext is called Transpositional technique.
- It is classified into two types.

1. Rail fence
   - The plaintext is written down as a sequence of diagonals and then read off as asequence of rows.
2. Columnar transposition
   - Write the message in a rectangle, row by row, and read the message off, column by column, but permute the order of the columns.

Rail fence (Encryption)

Plaintext = hai hello

depth (Key) = 2

No .of chars = 8

Step-1: Create a table with 2 rows and 8 columns

Step-2: Fill the table with characters of plaintext in Zig Zag format

h		i		e		l	
	a		h		l		o

Ciphertext=hie lahlo

Rail fence (Decryption)

Ciphertext = hie lahlo

depth (Key) = 2

No .of chars = 8

Step-1: Create a table with 2 rows and 8 columns

Step-2: Fill the table with characters of ciphertext sequentially and leave a cell blank between characters.

h		i		e		l	
	a		h		l		o

Plaintext=hai hello (Read in Zig Zag order)

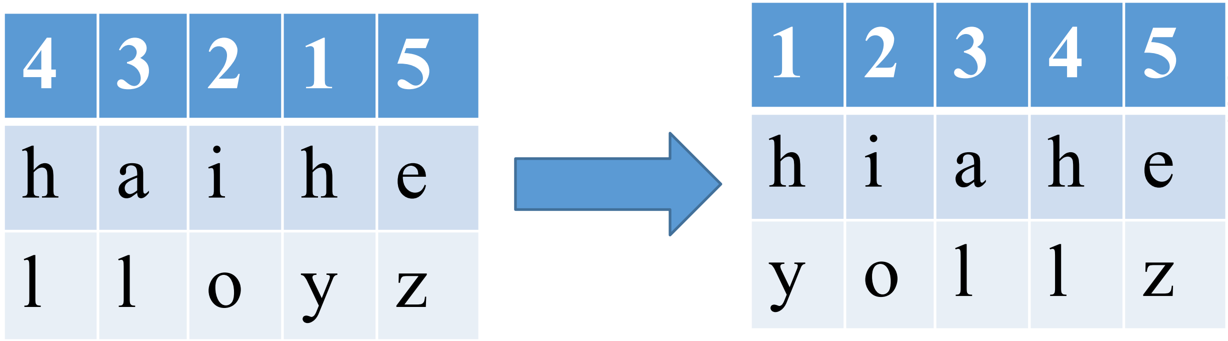
Columnar transposition (Encryption)

Plaintext=hai hello

Rectangle formation (Row wise)

Length of Key=5

Key (Order) =



4	3	2	1	5
h	a	i	h	e
l	l	o	y	z

1	2	3	4	5
h	i	a	h	e
y	o	l	l	z

phertext

Ciphertext= hyi oalhlez

Columnar transposition (Decryption)

Ciphertext= hyi oalhlez

Rectangle formation (Column wise)

Length of Key=5

Key (Order) =

4	3	2	1	5
h	i	a	h	e
y	o	l	l	z

1	2	3	4	5
h	a	i	h	e
l	l	o	y	z

phertext

Plaintext= hai hello (yz can ignored with knowledge of user)

Steganography

- 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 the text.
- For example, the sequence of first letters of each word of the overall message spells out the hidden message (Key).
- Message = Strike Now.
- Ciphertext = She takes revenge in king’s exile. No option would.

Steganography

- Character marking: Selected letters of printed or typewritten text are overwritten in pencil. The marks are ordinarily not visible unless the paper is held at 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 up in front of a light.
- Typewriter correction ribbon: Used between lines typed with a black ribbon, the results of typing with the correction tape are visible only under a strong light.

Foundations of modern security: Perfect security

- It operates on binary bit sequences.
- It relies on publicly known mathematical algorithms for coding the information.
- Secrecy is obtained through a secret key which is used as the seed for the algorithms. The computational difficulty of algorithms, absence of secret key, etc., make it impossible for an attacker to obtain the original information even if he knows the algorithm used for coding.
- Modern cryptography requires parties interested in secure communication to possess the secret key only.

Cryptosystem and Cryptanalysis

- A product cryptosystem is a block cipher that repeatedly performs substitutions and permutations, one after the other, to produce ciphertext.
- Example. DES (Data Encryption Standard), AES (Advanced Encryption Standard)
- The art and science of breaking the cipher text is known as cryptanalysis.
- It involves the study of cryptographic mechanism with the intention to break them. Cryptanalysis is also used during the design of the new cryptographic techniques to test their security strengths.

Summary

- Security trends, aspects and needs has been studied.
- Security attacks, services and mechanisms has been explored.
- The working of classical encryption techniques has been studied with example.

Thank You