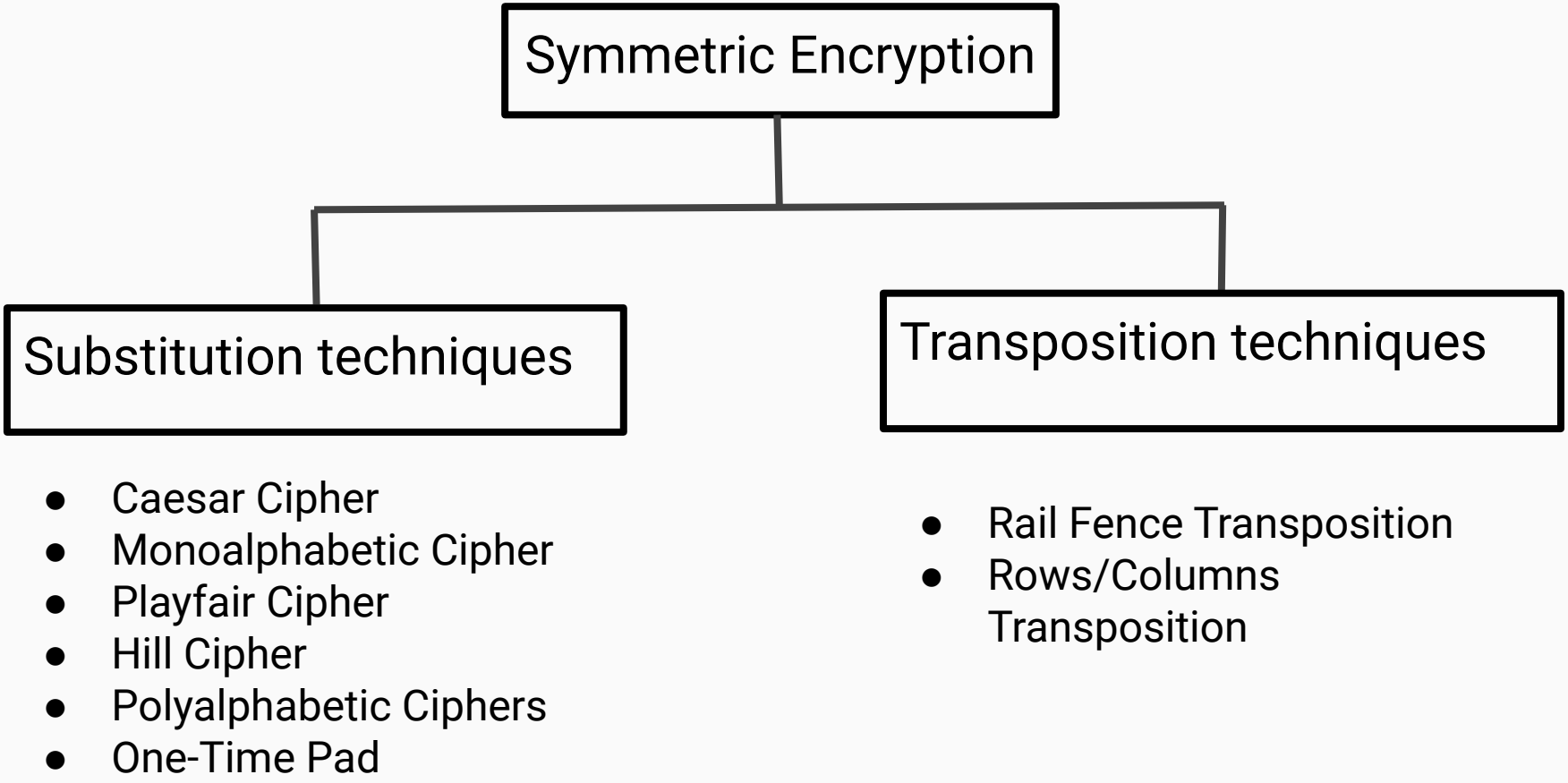
Information and Network Security Chapter - 1

Topic : Substitution and Transposition techniques

Created By:
Axay Sagathya (170210116055)

Difference between Symmetric and asymmetric encryption

The basic difference between these two types of **encryption** is that **symmetric encryption** uses one **key** for both **encryption** and decryption, and the **asymmetric encryption** uses public **key** for **encryption** and a private **key** for decryption.


Symmetric Encryption
Substitution techniques
Transposition techniques
Caesar Cipher
Monoalphabetic Cipher
Playfair Cipher
Hill Cipher
Polyalphabetic Ciphers
One-Time Pad
Rail Fence Transposition
Rows/Columns Transposition

Substitution techniques

Caesar Cipher

- replaces each letter by 3rd letter on

Example:

- meet me after the toga party

  PHHW PH DIWHU WKH WRJD SDUWB

Caesar Cipher

- can define transformation as:

  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

  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

- mathematically give each letter a number

  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

- then have Caesar cipher as:

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

  $= D(c) = (c - k)$

Monoalphabetic Cipher

- rather than just shifting the alphabet, each plaintext letter maps to a different random ciphertext letter.
- hence key is 26 letters long.

Plain: abcdefghijklmnopqrstuvwxyz

Cipher: DKVQFIBJWPESCXHTMYAUOLRGZN

Playfair Cipher

- In this scheme, pairs of letters are encrypted, instead of single letters as in the case of simple substitution cipher.

- In playfair cipher, initially a key table is created. The key table is a 5×5 grid of alphabets that acts as the key for encrypting the plaintext. Each of the 25 alphabets must be unique and one letter of the alphabet (usually J) is omitted from the table as we need only 25 alphabets instead of 26. If the plaintext contains J, then it is replaced by I.

Playfair Cipher (cont ...)

- The sender and the receiver deicide on a particular key, say ‘tutorials’. In a key table, the first characters (going left to right) in the table is the phrase, excluding the duplicate letters. The rest of the table will be filled with the remaining letters of the alphabet, in natural order. The key table works out to be −

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

Process of playfair cipher

- First, a plaintext message is split into pairs of two letters (digraphs). If there is an odd number of letters, a Z is added to the last letter. Let us say we want to encrypt the message “hide money”. It will be written as −

  HI DE MO NE YZ

Process of playfair cipher(Cont ...)

- The rules of encryption are −
  - If both the letters are in the same column, take the letter below each one (going back to the top if at the bottom)

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

‘H’ and ‘I’ are in same column, hence take letter below them to replace. HI → QC

Process of playfair cipher(Cont ...)

- If both letters are in the same row, take the letter to the right of each one (going back to the left if at the farthest right)

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

‘D’ and ‘E’ are in same row, hence take letter to the right of them to replace. DE → EF

Process of playfair cipher(Cont ...)

- If neither of the preceding two rules are true, form a rectangle with the two letters and take the letters on the horizontal opposite corner of the rectangle.

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

'M' and 'O' nor on same column or same row, hence from rectangle as shown, and replace letter by picking up opposite corner letter on same row. MO --> NU

Process of playfair cipher(Cont ...)

Using these rules, the result of the encryption of ‘hide money’ with the key of ‘tutorials’ would be −

QC EF NU MF ZV

Decrypting the Playfair cipher is as simple as doing the same process in reverse. Receiver has the same key and can create the same key table, and then decrypt any messages made using that key.

Hill Cipher

Hill cipher is based on linear algebra

Each letter is represented by numbers from 0 to 25 and calculations are done using modulo 26.

Encryption and decryption can be given by the following formula:

Encription : $C=PK \bmod 26$

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

Hill Cipher(Cont...)

To encrypt a message using the Hill Cipher we must first turn our keyword and plaintext into nXn matrix.

Example: Key = “HILL”,
Plaintext = “EXAM”

a	b	c	d	e	f	g	h	i	j	k	l	m
0	1	2	3	4	5	6	7	8	9	10	11	12

n	o	p	q	r	s	t	u	v	w	x	y	z
13	14	15	16	17	18	19	20	21	22	23	24	25

$$\text{Key Matrix } \begin{pmatrix} H & I \\ L & L \end{pmatrix} = \begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix} \qquad \text{Plaintext } \begin{pmatrix} E \\ X \end{pmatrix} \begin{pmatrix} A \\ M \end{pmatrix} = \begin{pmatrix} 4 \\ 23 \end{pmatrix} \begin{pmatrix} 0 \\ 12 \end{pmatrix}$$

Hill Cipher(Cont...)

$$\text{Plaintext} \begin{pmatrix} E \\ X \end{pmatrix} \begin{pmatrix} A \\ M \end{pmatrix} = \begin{pmatrix} 4 \\ 23 \end{pmatrix} \begin{pmatrix} 0 \\ 12 \end{pmatrix} \qquad \text{Key Matrix} = \begin{pmatrix} H & I \\ L & L \end{pmatrix} = \begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix}$$

C=PK mod 26

$$\begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix} \begin{pmatrix} 4 \\ 23 \end{pmatrix}$$

$$\begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix} \begin{pmatrix} 4 \\ 23 \end{pmatrix} = \begin{pmatrix} 212 \\ 297 \end{pmatrix}$$

$$\begin{pmatrix} 212 \\ 297 \end{pmatrix} \bmod 26 = \begin{pmatrix} 4 \\ 11 \end{pmatrix} = \begin{pmatrix} E \\ L \end{pmatrix}$$

$$\begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix} \begin{pmatrix} 0 \\ 12 \end{pmatrix}$$

$$\begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix} \begin{pmatrix} 0 \\ 12 \end{pmatrix} = \begin{pmatrix} 96 \\ 132 \end{pmatrix}$$

$$\begin{pmatrix} 96 \\ 132 \end{pmatrix} \bmod 26 = \begin{pmatrix} 4 \\ 11 \end{pmatrix} = \begin{pmatrix} E \\ L \end{pmatrix}$$

Ciphertext = “ELSC”

Polyalphabetic Cipher

- Monoalphabetic cipher encoded using only one fixed alphabet
- Polyalphabetic cipher is a substitution cipher in which the cipher alphabet for the plain alphabet may be different at different places during the encryption process.
    1. Vigenere cipher
    2. Vernam cipher

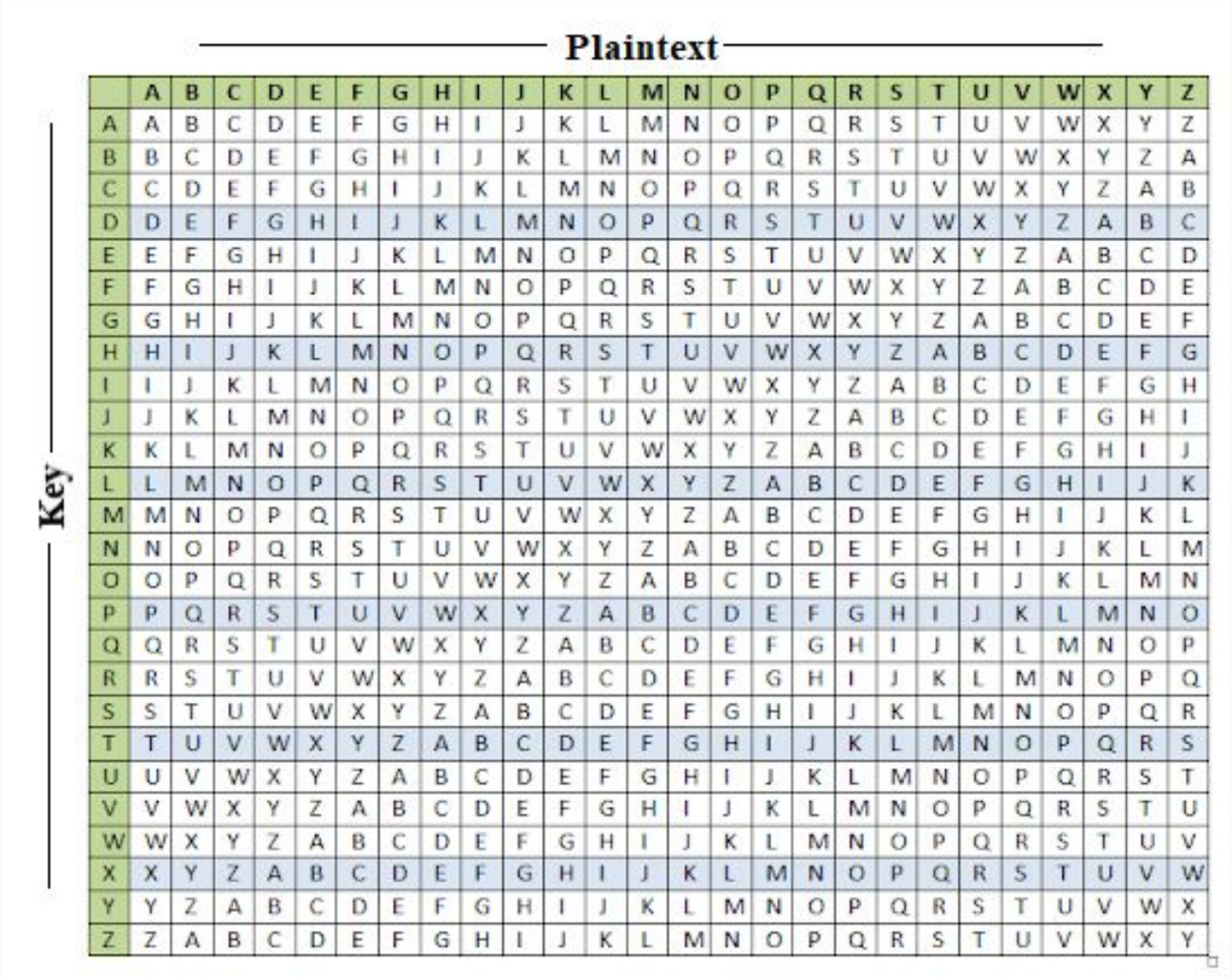
Vigenere cipher

- Polyalphabetic cipher
- Uses vigenere,s table (shown in next slide)

- Let plain text be GIVEMONEY
- Let key be LOCK

- Repeat the letters of key so that number of letters in plain text and key becomes equal.

ie,. G I V E M O N E Y
L O C K L O C K L



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

Vigenere cipher (Cont...)

- Find the Intersection of the letter of plain text and key will be the letter of cipher text.

Plain text : G I V E M O N E Y

Key : L O C K L O C K L

Cipher text : RWXOXCPOJ

Vernam cipher / One - Time Pad

- Similar to Vigenere, but use random key as long as plaintext
- Two practical limitations:
  - Difficult to provide large number of random keys
  - Distributing unique long random keys is difficult
- The ciphertext is generated by applying the logical XOR operation to the individual bits of plaintext and the key stream

Vernam cipher / One - Time Pad (Cont ...)

a	b	c	d	e	f	g	h	i	j	k	l	m
0	1	2	3	4	5	6	7	8	9	10	11	12
n	o	p	q	r	s	t	u	v	w	x	y	z
13	14	15	16	17	18	19	20	21	22	23	24	25

Plain Text : **RAMSWARUPK**
Key : **RANCHOBABA**

Plain Text =>	17	0	12	18	22	0	17	20	15	10
Key =>	17	0	13	2	7	14	1	0	1	0
(PT + Key) =>	34	0	25	20	29	14	18	20	16	10
(PT + Key) % 26 =>	8	0	25	20	3	14	18	20	16	10

Cipher Text = IAZUDOSUQK

Transposition Techniques

- A transposition cipher does not substitute one symbol for another, instead it changes the location of the symbols.

rail fence technique

- the plaintext is written down as a sequence of diagonals and then read off as a sequence of rows.
- Easy to break: letter frequency analysis to determine depth

Example :

Plain text : MEET ME AT THE PARK

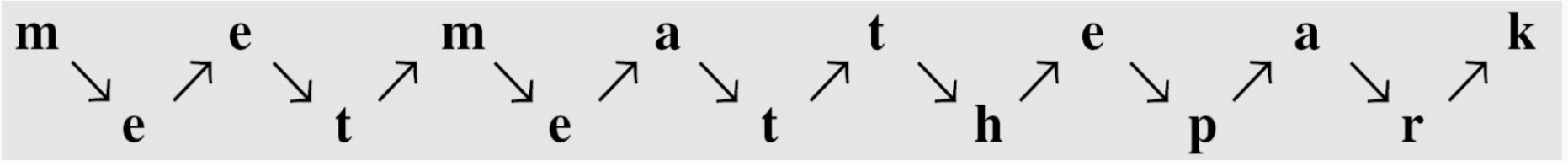
Depth : 2

rail fence technique (cont ...)

Example :

Plain text : MEET ME AT THE PARK

Depth : 2



Cipher text : MEMATEAK ETETHPR

Rows/Columns Transposition

- Write the plain text row by row
- Ciphertext will be obtained by reading column-by-column, but re-arranged.
- Key determines order of columns to read
- Transposition ciphers can be made stronger by using multiple stages of transposition

Rows/Columns Transposition (Cont ...)

Key : 4312567
Plain text : ATTACK POSTPONED UNTIL TWO AM

Key ==>	4	3	1	2	5	6	7	
Plain Text ==>	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**	**Y**	<== Dummy letters

Cipher text : TTNA APTM TSUO AODW COIX KNLY PETZ

Thank You...