

15Z704 - CRYPTOGRAPHY AND NETWORK SECURITY

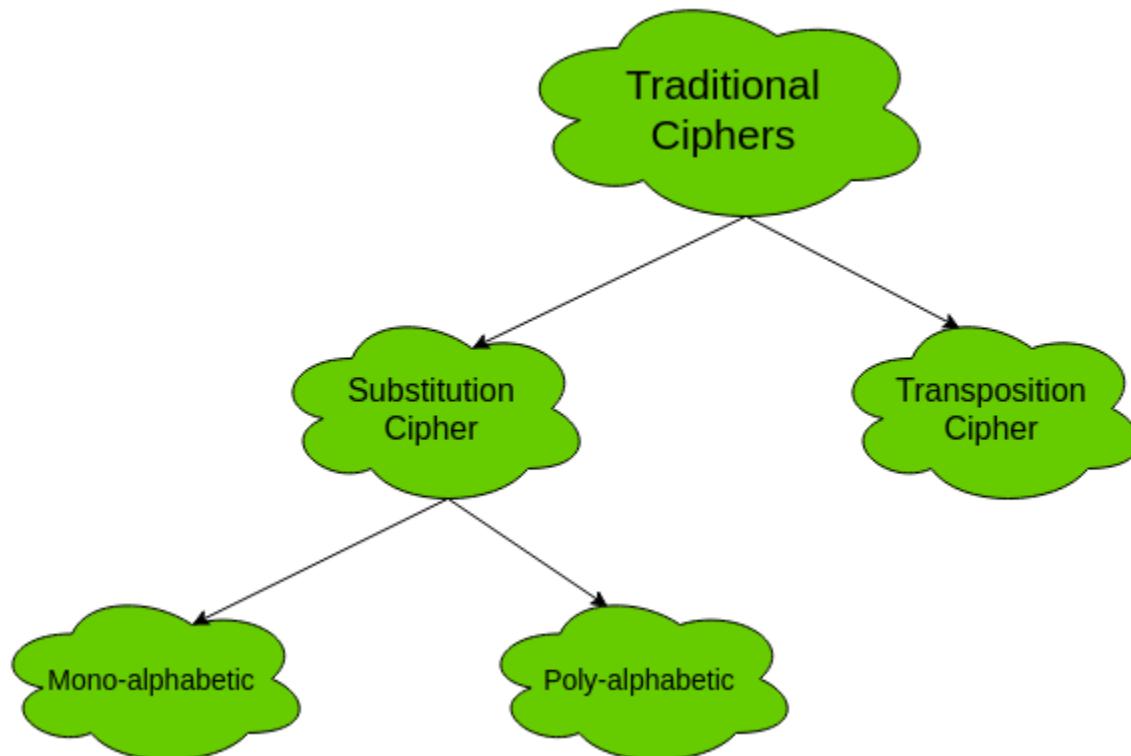
Dr.N.Gopika Rani,

AP-SG,

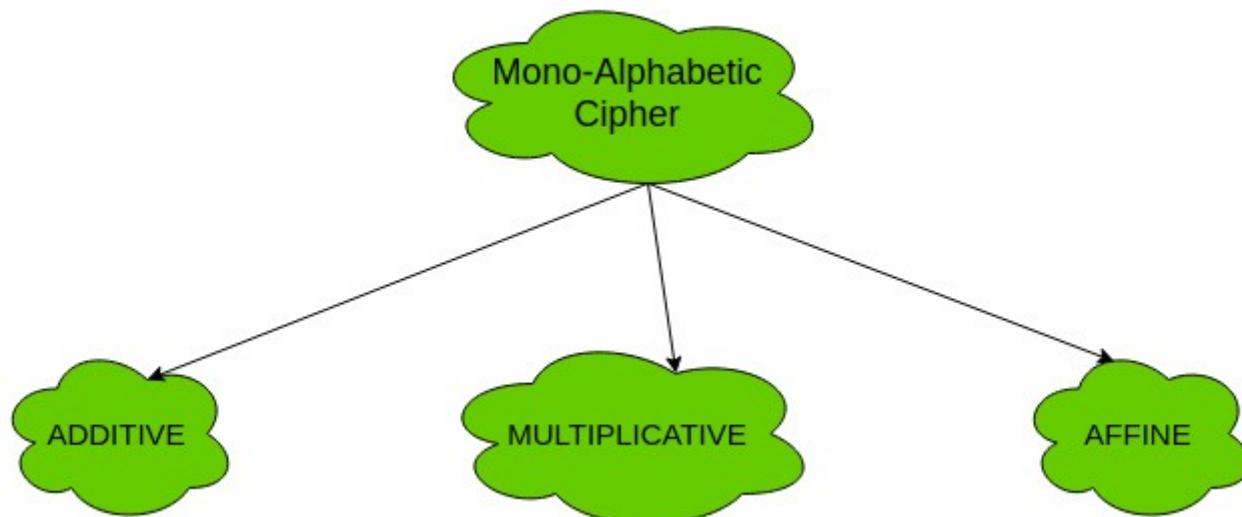
Department of CSE.

Traditional Symmetric Ciphers

The two types of traditional symmetric ciphers are **Substitution Cipher** and **Transposition Cipher**.
The following flowchart categories the traditional ciphers:



Types of mono-alphabetic ciphers are:



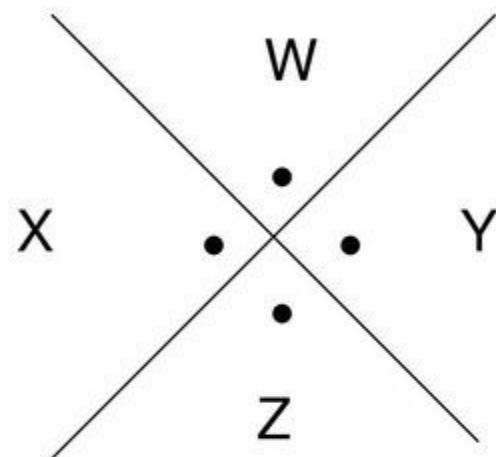
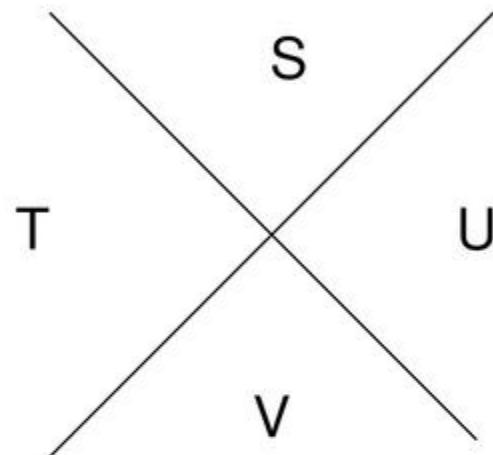
Pigpen Cipher

- Pigpen cipher is a variation on letter substitution
- Alphabets are arranged as follows:

A	B	C
<hr/>		
D	E	F
<hr/>		
G	H	I

J	•	K	•	L
M	•	N	•	O
P	•	Q	•	R

Pigpen Cipher diagram (cont'd)



A =

C =

G =

W =

Pigpen Cipher

- Alphabets will be represented by the corresponding diagram
- E.g., WAG would be A diagram illustrating the Pigpen cipher mapping for the letters W, A, and G. The letter 'W' is represented by a diamond shape with a dot at the top vertex. The letter 'A' is represented by a vertical line segment with a dot at its top end. The letter 'G' is represented by a vertical line segment with a horizontal line segment extending from its right side.
- This is a weak cipher

a	b	c	d	e	f	g	h	i	j
˩	˨	˧	˥	߱	߳	߷	߸	߹	߻
k	l	m	n	o	p	q	r	s	t
܊	܉	܌	܍	܎	܏	ܐ	ܑ	ܒ	ܔ
u	v	w	x	y	z				
ܕ	܈	܌	ܔ	܏	ܐ				

Decode the following pigpen ciphertext:

L F A O L E B N J D C T F E V T O F

Encode the following message using the pigpen cipher:

the truth is out there

ADFGVX Cipher

- This is a variation on substitution cipher and is a strong cipher

	A	D	F	G	V	X
A	8	p	3	d	1	n
D	I	t	4	o	a	h
F	7	k	b	c	5	z
G	j	u	6	w	g	m
V	x	s	v	i	r	2
X	9	e	y	0	f	q

ADFGVX Cipher

- Rules:
 - Remove spaces and punctuation marks from message
 - For each letter or number substitute the letter pair from the column and row heading
 - Next, use a transposition operation on the pair of letters using a key word (which the receiver knows)
 - Rearrange the columns of the new arrangement in alphabetical order
 - Finally, arrange the letters from consecutive columns

ADFGVX Cipher

- E.g., Message = SEE ME IN MALL
 - SEEMEINMALL
 - VDXDXDGXXDVGAXGXDV DADA
 - Use keyword of INFOSEC
 - Arrange the stage 1 ciphertext characters in a fresh grid with keyword as the column heading
 - Ciphertext is written in column order from left to right

ADFGVX Cipher

I	N	F	O	S	E	C
V	D	X	D	X	D	C
X	X	D	V	G	A	
G	X	D	V	D	A	

ADFGVX Cipher

C	E	F	I	N	O	S
G	D	X	V	D	D	X
X	A	D	X	X	V	G
V	A	D	G	X	V	D

ADFGVX Cipher

- Ciphertext is:

GXVDAAXDDVXGDXDVVXGD

- Recipient reverses the process using the same keyword and gets the plaintext
- Reason for this cipher using the name ADFGVX is that in Morse code these characters all have dissimilar patterns of dots and dashes

Multiplicative Cipher

- The multiplicative cipher is similar to additive cipher except the fact that the key bit is multiplied to the plain-text symbol during encryption. Likewise, the cipher-text is multiplied by the multiplicative inverse of key for decryption to obtain back the plain-text.

$$C = (M * k) \bmod n$$

$$M = (C * k^{-1}) \bmod n$$

- where,
 k^{-1} -> multiplicative inverse of k (key)
- The key space of multiplicative cipher is 12. Thus, it is also not very secure.

Multiplicative Cipher

If multiplication is used to convert to cipher text, it is called a **wrap-around** situation. Consider the letters and the associated numbers to be used as shown below –

0	1	2	3	4	5	6	7	8	9	10	11	12
A	B	C	D	E	F	G	H	I	J	K	L	M
13	14	15	16	17	18	19	20	21	22	23	24	25
N	O	P	Q	R	S	T	U	V	W	X	Y	Z

The numbers will be used for multiplication procedure and the associated key is 7. The basic formula to be used in such a scenario to generate a multiplicative cipher is as follows –

(Alphabet Number * key) mod (total number of alphabets)

Plaintext Symbol	Number	Encryption with Key 7	Ciphertext Symbol
A	0	(0 * 7) % 26 = 0	A
B	1	(1 * 7) % 26 = 7	H
C	2	(2 * 7) % 26 = 14	O
D	3	(3 * 7) % 26 = 21	V
E	4	(4 * 7) % 26 = 2	C
F	5	(5 * 7) % 26 = 9	J
G	6	(6 * 7) % 26 = 16	Q
H	7	(7 * 7) % 26 = 23	X
I	8	(8 * 7) % 26 = 4	E
J	9	(9 * 7) % 26 = 11	L
K	10	(10 * 7) % 26 = 18	S
L	11	(11 * 7) % 26 = 25	N
M	12	(12 * 7) % 26 = 6	G
N	13	(13 * 7) % 26 = 13	Z
O	14	(14 * 7) % 26 = 20	U
P	15	(15 * 7) % 26 = 1	B
Q	16	(16 * 7) % 26 = 8	I
R	17	(17 * 7) % 26 = 15	P
S	18	(18 * 7) % 26 = 22	W
T	19	(19 * 7) % 26 = 3	D
U	20	(20 * 7) % 26 = 10	K
V	21	(21 * 7) % 26 = 17	R
W	22	(22 * 7) % 26 = 24	Y
X	23	(23 * 7) % 26 = 5	F
Y	24	(24 * 7) % 26 = 12	M
Z	25	(25 * 7) % 26 = 19	T