Muhammad
Anshad P A / -36

Practice Questions on Classical Encryption Techniques

Q.1 "All the world's a stage, and all the men and women merely players" — Encrypt the message with caesar Cipher with Shift 5.

solution →

Numbers - Alphabets

0	1	2	3	4	5	6	7	8	9	10	11	12	13
A	B	C	D	E	F	G	H	I	J	K	L	M	N

14	15	16	17	18	19	20	21	22	23	24	25
O	P	Q	R	S	T	U	V	W	X	Y	Z

Encryption

$$C = E(P,k) \bmod 26 = (P+k) \bmod 26$$

key = 5

plaintext
ciphertext

PT	A	L	L	T	H	E	W	O	R	L	D	S	A	S	T	A	G	E
CT	F	Q	Q	Y	M	J	B	T	W	Q	I	X	F	X	Y	F	L	J
PT	A	N	D	A	L	L	T	H	E	M	E	N	A	N	D	W	O	M
CT	F	S	I	F	Q	Q	Y	M	J	R	J	S	F	S	I	B	T	R
PT	E	N	M	E	R	E	L	Y	P	L	A	Y	E	R	S
CT	J	S	R	J	W	J	Q	D	U	Q	F	D	J	W	X

$$C = (P+k) \bmod 26$$

A	$C = 0+5 \bmod 26$	= 5 → F
L	$C = 11+5 \bmod 26$	= 16 → Q
T	$C = 19+5 \bmod 26$	= 24 → Y
H	$C = 7+5 \bmod 26$	= 12 → M

E	$C = 4+5 \mod 26 = 9 \to J$
W	$C = 22+5 \mod 26 = 1 \to B$
O	$C = 14+5 \mod 26 = 19 \to T$
R	$C = 17+5 \mod 26 = 22 \to W$
D	$C = 3+5 \mod 26 = 8 \to I$
S	$C = 18+5 \mod 26 = 23 \to X$
G	$C = 6+5 \mod 26 = 11 \to L$
N	$C = 13+5 \mod 26 = 18 \to S$
M	$C = 12+5 \mod 26 = 17 \to R$
L	$C = 11+5 \mod 26 = 16 \to Q$
Y	$C = 24+5 \mod 26 = 3 \to D$
P	$C = 15+5 \mod 26 = 20 \to U$

Q.2 A short cryptic message was received from a friend:
" Xs fi, sv rsy xs fi, xlex mw xli uyiwxmsr".
Assuming Caesar Cipher **Decrypt** the message with
shift 4

Solution ⇒ Decryphon

$$P = D(C, k) \mod 26 = C - k \mod 26$$

key = 4

Ciphertext	CT	X	S	F	I	S	V	R	S	Y	X	S	F	I	X	L	E	X
plaintext	PT	T	O	B	E	O	R	N	O	U	T	O	B	E	T	H	A	T
	CT	M	W	X	L	I	U	Y	I	W	X	M	S	R				
	PT	I	S	T	H	E	Q	U	E	S	T	I	O	N				

$$P = C - k \mod 26$$

X	$P = 23 - 4 \mod 26 = 19 \rightarrow T$	
S	$P = 18 - 4 \mod 26 = 14 \rightarrow O$	
F	$P = 5 - 4 \mod 26 = 1 \rightarrow B$	
I	$P = 8 - 4 \mod 26 = 4 \rightarrow E$	
Y	$P = 21 - 4 \mod 26 = 17 \rightarrow R$	
R	$P = 17 - 4 \mod 26 = 13 \rightarrow N$	
Y	$P = 24 - 4 \mod 26 = 20 \rightarrow U$	
L	$P = 11 - 4 \mod 26 = 7 \rightarrow H$	
E	$P = 4 - 4 \mod 26 = 0 \rightarrow A$	
M	$P = 12 - 4 \mod 26 = 8 \rightarrow I$	
W	$P = 22 - 4 \mod 26 = 18 \rightarrow S$	
U	$P = 20 - 4 \mod 26 = 16 \rightarrow Q$	

2. So, Decrypted Message =>

To be or Nou To Be That Is The Question.

Q.3 Encrypt the following phrase using the Playfair Cipher with the key "SECURITY". The message to be converted is "KEEP IT SAFE".

Solution.

Plaintext → KEEP IT SAFE

keyword → SECURITY

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

Diagrams : KE | EP | IT | SA | FE

Encryption

KE	EP	IT	SA	FE
FR	RM	TY	UI	MT

Q.4 Decrypt the following message which was encrypted using the playfair Cipher with the key "HARMONY". Encrypted Message : "LCZTRTCFXNCG"

Solution

Encrypted message = LCZTRT

keyword → HARMONY

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

Decryption	LC	ZT	RT	CF	XN	CG
	SN	TK	OQ	YI	UC	BI

Q5 Encrypt the phrase " GOOD MORNING " using the Monoalphabetic Cipher with give Substitution:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
M	N	B	V	C	X	Z	L	K	J	H	G	F	D	S	A

Q	R	S	T	U	V	W	X	Y	Z
P	O	I	U	Y	T	R	E	W	Q

Solution

Plaintext → GOOD MORNING

PT	G	O	O	D	M	O	R	N	I	N	G
CT	Z	S	S	V	F	S	O	D	K	D	Z

Q-6 Decrypt the message: " SZEV Z MRMX WVZ " using the monoalphabetic Cipher with the given Substitution:

A	B	C	D	E	F	G	H	I	J	K	L	M	N

P	Q	R	S	T	U	V	W	X	Y	Z

[Q-6] Decrypt the message : " SZEV Z MRMX WVZ"
using monoalphabetic Cipher with the given Substitution.

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

Solution →

Decryption.

S	Z	E	V	Z	M	R	M	X	W	Y	Z
H	A	V	E	A	N	I	N	C	D	E	A

[Q-7] Encrypt the phrase using Vernam Cipher with the given
key . Message: "SECURITY IS IMPORTANT"
key : "ZEBRASKS VF MQKGXYHZO"

Solution ⇒

$$C_i = (P_i + k_i) \bmod 26$$

PT	S	E	C	U	R	I	T	Y	I	S	I	M	P	O	R	T	A	N	T
	18	4	2	20	17	8	19	24	8	18	8	12	15	14	17	19	0	13	19
Key	Z	E	B	R	A	S	K	S	V	F	M	Q	K	G	X	Y	H	Z	O
	25	4	1	17	0	18	10	18	21	5	12	16	10	6	23	24	7	25	14
$(P_i + k_i)$ mod 26	17	8	3	11	17	0	3	16	3	23	20	2	25	20	14	17	7	12	7
CT ⇒	R	I	D	L	R	A	D	Q	D	X	U	C	Z	U	O	R	H	M	H

Q-8 Decrypt the following message which was encrypted using Vernam Cipher with the given key.

Encrypted message : " DLAY F YLCE CZG "

key : " LIMNQ BYXPT JZZ "

Solution.

$$P_i = (C_i - K_i) \bmod 26$$

CT

D	L	A	Y	F	Y	L	C	E	C	Z	G
3	11	0	24	5	24	11	2	4	2	25	6

key.

L	I	M	N	Q	B	Y	X	P	T	J	Z	Z
11	8	12	13	16	1	24	23	15	19	9	25	

$(C_i - K_i) \bmod 26$

18	3	14	11	15	23	13	5	15	9	16	7
S	D	O	L	P	X	N	F	P	J	Q	H