Name: Muhammad Nadeem

Roll no: 201980050

Course name: CS-460-B-Information-Security

Cryptography

Algorithms for Cryptography:

1. Caeser Cipher:

Convert plain text to Cipher text… ENCRYPTION

Given Data:-

Plain Text: NADEEM

Alphabets: ABCDEFGHIJKLMNOPQRSTUVWXYZ

KEY:- 3

Solution: N->K3: Q A->K3: D D->K3: G

E->K3: H E->K3: H M->K3: P

…………Exclude first word…………

CIPHER TEXT= QDGHHP

Convert Cipher text to Plain text… DECRYPTION

GIVEN DATA:-

Cipher text: QDGHHP

Alphabets: ABCDEFGHIJKLMNOPQRSTUVWXYZ

KEY:- 3

Solution:

Q->K3: N D->K3: A G->K3: D

H->K3: E H->K3: E P->K3: M

…………Excluded First Word…………

Plain Text: NADEEM

2. Monoalphabetic

Convert Plain text to Cipher text… ENCRYPTION

Given Data:

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

Key: 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

Plain Text: WAHAB

Solution: W-> H A-> L H-> S A-> L B-> M

Cipher Text: HLSLM

Convert Cipher text to plain text… DECRYPTION

Given Data:

Key: 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

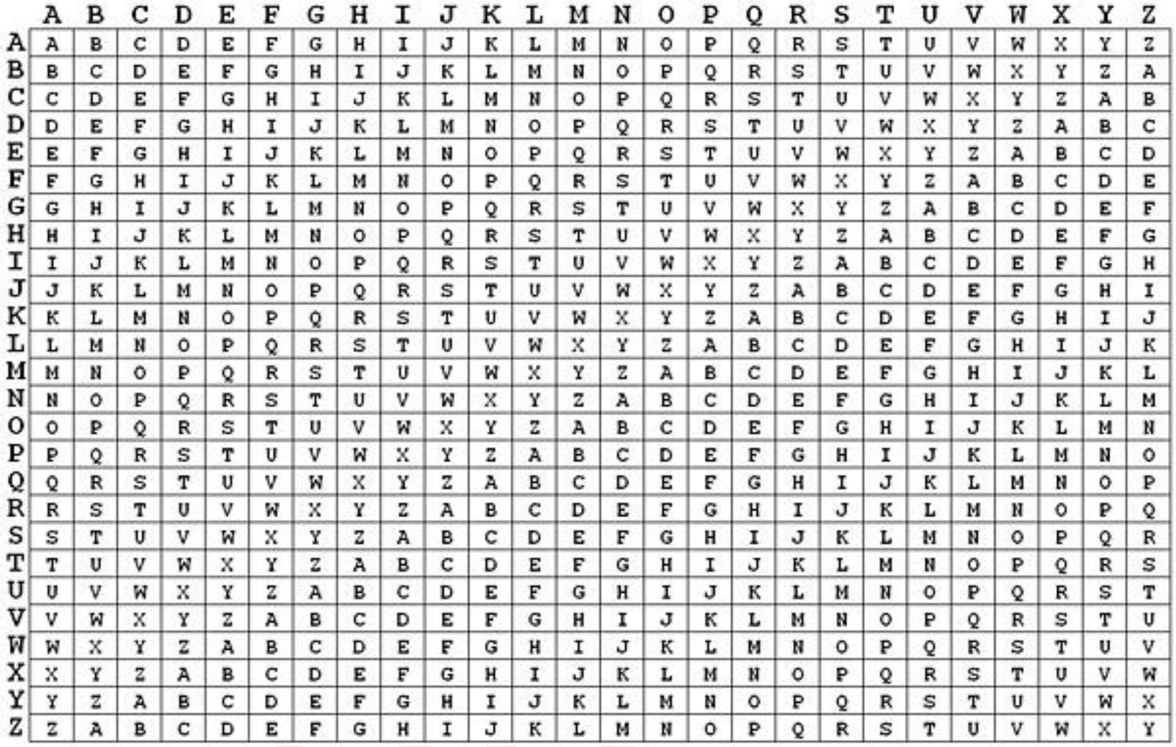
Alphabets: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Cipher Text: HLSLM

Solution: H-> W L-> A S-> H L-> A M-> B

Plain Text: WAHAB

3. VIGENERE CIPHER:



	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

Convert Plain Text to Cipher text… ENCRYPTION

Given Data:

Plain text: GIFTUNI

Key: ML

Solution:

M L M L M L M

G I F T U N I

Now see key in column in table and Plain Text in row.

M->G: S L->I: T M->F: R

L->T: E M->U: G L->N: Y M->I: U

Cipher Text: STREGYU

Convert Cipher text to Plain text... DECRYPTION

Given Data:

Cipher Text: STREGYU

Key: ML

Solution:

Now see key in column and find in those row who has find cipher text.

Key:	M	L	M	L	M	L	M
Cipher:	S	T	R	E	G	Y	U

M->S: G L->T: I M->R: F L->E: T

M->G: U L->Y: N M->U: I

Plain Text: GIFTUNI

4.Rail Fence Cipher:

Convert Plain Text to Cipher text... ENCRYPTION

Given Data:

Plain Text: MRNADEEM

KEY: 2

Solution:

M N D E

R A E M

Cipher Text: MNDERAEM

Convert Cipher text to Plain text… DECRYPTION

Given Data:

Cipher Text: MNDERAEM

Key: 2

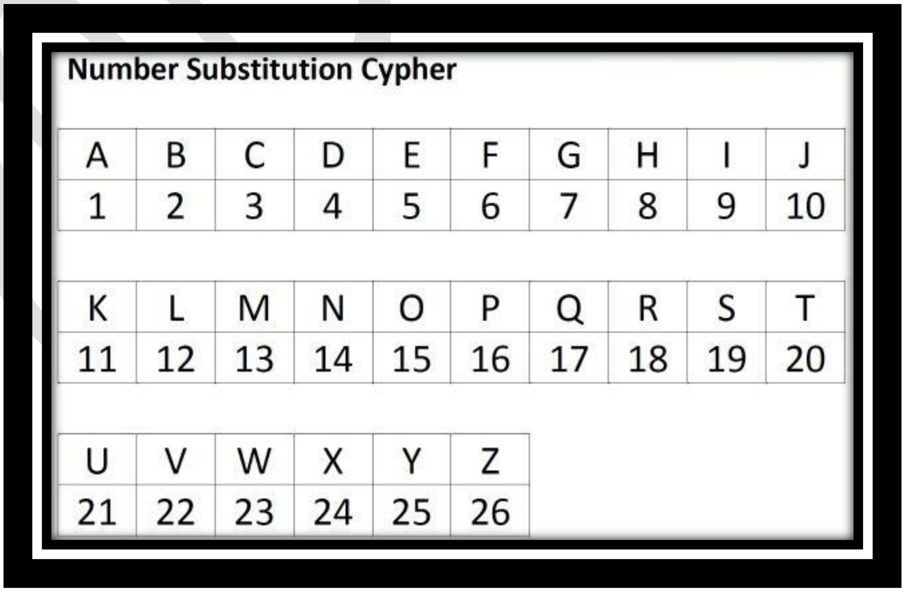
Solution:

M N D E

R A E M

Plain Text: MRNADEEM

5. ONE TIME PASSWORD:



Number Substitution Cypher

A	B	C	D	E	F	G	H	I	J
1	2	3	4	5	6	7	8	9	10

K	L	M	N	O	P	Q	R	S	T
11	12	13	14	15	16	17	18	19	20

U	V	W	X	Y	Z
21	22	23	24	25	26

Convert Plain Text to Cipher text... ENCRYPTION

Given Data:

Plain Text: MRNADEEM

Key: MUGHAL

Solution:

Plain Text:	M	R	N	A	D	E	E	M
No.:	13	18	14	1	4	5	5	13
Key:	M	U	G	H	A	L		
No.:	13	21	7	8	1	12		

Now add Plain text no. and key no. and write sum no.

SUM:	26	39	21	9	5	17

Now write alphabets w.r.t its no.

Alphabets:	Z	M	U	I	E	Q

Cipher Text: ZMUIEQ

Convert Cipher text to Plain text... DECRYPTION

Given Data:

Cipher Text: ZMUIEQ

KEY: MUGHAL

Solution:

Cipher text:	Z	M	U	I	E	Q
No.:	26	13	21	9	5	17

Key:	M	U	G	H	A	L
No.:	13	21	7	8	1	12
Subtraction:	13	-8	14	1	4	5
Alphabets:	M	R	N	A	D	E

Plain Text: MRNADE

6. Column Transposition Cipher:

Convert Plain Text to Cipher text… ENCRYPTION

Given Data:

Plain Text: MUHAMMADNADEEMMUGHAL

Key: 195362

Solution:

Key:	1	9	5	3	6	2
Plain Text:	M	U	H	A	M	M
	A	D	N	A	D	E
	E	M	M	U	G	H
	A	L	X	X	X	X

Cipher Text: MAEAUDMLHNMXAAUXMDGXMEHX

Convert Cipher text to Plain text… DECRYPTION

Given Data:

Cipher Text: MAEAUDMLHNMXAAUXMDGXMEHX

Key: 195362

Solution:

1	9	5	3	6	2

M	U	H	A	M	M
A	D	N	A	D	E
E	M	M	U	G	H
A	L	X	X	X	X

Plain text: MUHAMMADNADEEMMUGHALXXXX