Assignment 1

Name: Umamah Hussain

Roll Number: 21L-1858

Section: 7A

Plaintext: 21L1858-Murrawat Hussain-37405-8879993-4

Caesar Cipher

Key: 4

2	1	L	1	8	5	8
6	5	P	5	2	9	2

M	u	r	r	a	w	a	t	H	u	s	s	a	i	n
Q	y	v	v	e	a	e	x	L	y	w	w	e	m	r

3	7	4	0	5	8	8	7	9	9	9	3	4
7	1	8	4	9	2	2	1	3	3	3	7	8

Caesar Cipher: 65P5292-Qyvveaex Lywwemr-71849-2213337-8

Monoalphabetic Cipher

Alphabet Key:

a	b	c	d	e	f	g	h	i	j	k	l	m	n
h	j	l	n	p	r	t	v	w	z	y	x	a	d

o	p	q	r	s	t	u	v	w	x	y	z
e	b	f	s	i	c	g	k	m	o	q	u

Number Key:

1	2	3	4	5	6	7	8	9	0
5	8	2	1	7	3	0	4	6	9

Special Character Key:

-	space
&	^

Encryption:

2	1	L	1	8	5	8
8	5	X	5	4	7	4

M	u	r	r	a	w	a	t	H	u	s	s	a	i	n
A	g	s	s	h	m	h	c	V	g	i	i	h	w	d

3	7	4	0	5	8	8	7	9	9	9	3	4
2	0	1	0	7	4	4	0	6	6	6	2	1

Monoalphabetic Cipher: 85X5474&Agsshmhc^
Vgiihwd&20107&4406662&1

Vignere Cipher

Alphabet Key:

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

2	1	L	1	8	5	8
		M				

M	u	r	r	a	w	a	t	H	u	s	s	a	i	n
U	r	r	a	w	a	t	H	u	s	s	a	i	n	M

3	7	4	0	5	8	8	7	9	9	9	3	4

Encryption:

	Plaintext	2	1	L	1	8	5	8
	Plaintext index			11				
	Key			M				
	Key index			12				
	Calculation			23				

Ciphertext			X			

Plaintext	M	u	r	r	a	w	a	t	H	u	s	s	a	i	n
Plaintext index	12	20	17	17	0	22	0	19	7	20	18	18	0	8	13
Key	U	r	r	a	w	a	t	H	u	s	s	a	i	n	M
Key index	20	17	17	0	22	0	19	7	20	18	18	0	8	13	12
Calculation	32=6	37=11	34=8	17	22	22	19	26=0	27=1	20	36=10	18	8	21	25
Ciphertext	g	l	i	r	w	w	t	a	b	u	k	s	i	v	z

3	7	4	0	5	8	8	7	9	9	9	3	4

Vignere Cipher: 21X1858-glirwwtabuksivz-37405-8879993-4

One Time Pad

Alphabet Key:

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

2	1	L	1	8	5	8

M	u	r	r	a	w	a	t	H	u	s	s	a	i	n
a	h	b	e	j	a	p	c	d	o	f	i	x	o	g

3	7	4	0	5	8	8	7	9	9	9	3	4

Encryption:

Plaintext	2	1	L	1	8	5	8
Plaintext index			**11**				
Key			M				
Key index			12				
Calculation			23				
Ciphertext			X				

Plaintext	M	u	r	r	a	w	a	t	H	u	s	s	a	i	n
Plaintext index	12	20	17	17	0	22	0	19	7	20	18	18	0	8	13
Key	a	h	b	e	j	a	p	c	d	o	f	i	x	o	g
Key index	0	7	1	4	9	0	15	2	3	14	5	8	23	14	6
Calculation	12	27=1	18	21	9	22	15	21	10	8	23	26=0	23	22	19
Ciphertext	m	b	s	v	j	w	p	v	k	i	x	a	x	w	t

3	7	4	0	5	8	8	7	9	9	9	3	4

One Time Pad Cipher: 21X1858-mbsvjwpvkixaxwt-37405-8879993-4

Limitations

1. Caesar Cipher:

- Cannot encrypt spaces, numbers, or special characters.
- Only shifts alphabetic characters.
- Can be extended to include numbers, but still weak due to limited security.

2. Monoalphabetic Cipher:

- Can be extended to encrypt spaces, numbers, and special characters by assigning a substitution for each.
- Still vulnerable to frequency analysis attacks.

3. Vigenère Cipher:

- Only encrypts alphabetic characters.
- Spaces, numbers, and special characters are left unchanged.
- Could be modified to include a larger character set.

4. One-Time Pad:

- Encrypts only alphabetic characters perfectly.
- Cannot natively handle spaces, numbers, or special characters.
- Can be extended using ASCII values or a custom character set for full encryption.