Question No:1

Monoalphabetic Cipher:

Definition:

Keys for the simple substitution cipher usually consist of 26 letters.

Explanation:

It is easy to see how each character in the plaintext is replaced with the corresponding letter in the cipher alphabet. Decryption is just as easy, by going from the cipher alphabet back to the plain alphabet

Encryption:

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

Plain text:

The sections on quantum cryptography, quantum proper ties of squeezed light, and experimental efforts to measure gravitational waves provide adequate introduction to these exciting applications of quantum optics.

Cipher text:

zsg qgjzatyq ty exlyzxu jwnrztdwlrsn, exlyzxu rwtrgw zagq tf qexggmgh iadsz, lyh gbrgwaugyzli gfftwzq zt uglqxwg dwlcazlzatyli vlcgq rwtcahg lhgexlzg ayzwthxjzaty zt zsgqg gbjazayd lrriajlzatyq tf exlyzxu trzajq.

Question Number 2

Playfair Cipher:

Definition:

The Playfair cipher was the first practical digraph substitution cipher. The scheme was invented in 1854 by Charles Wheatstone, but was named after Lord Playfair who promoted the use of the cipher. The technique encrypts pairs of letters (digraphs), instead of single letters as in the simple substitution cipher.

Encryption:

The 'key' for a playfair cipher is generally a word, for the sake of example we will choose 'sumer'. This is then used to generate a 'key sumer ', e.g.
Note that there is no 'j', it is combined with 'i'.

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

1. Identify any double letters in the plaintext and replace the second occurrence with an 'x' e.g. 'hammer' -> 'hamxer'.
2. If the plaintext has an odd number of characters, append an 'x' to the end to make it even.
3. Break the plaintext into pairs of letters, e.g. 'hamxer' -> 'ha mx er'
4. The algorithm now works on each of the letter pairs.
5. Locate the letters in the key square, (the examples given are using the key square above)
    a. If the letters are in different rows and columns, replace the pair with the letters on the same row respectively but at the other pair of corners of the rectangle defined by the original pair. The order is important – the first encrypted letter of the pair is the one that lies on the same row as the first plaintext letter. 'ha' -> 'bo', 'es' -> 'il'
    b. If the letters appear on the same row of the table, replace them with the letters to their immediate right respectively (wrapping around to the left side of the row if a letter in the original pair was on the right side of the row). 'ma' -> 'or', 'lp' -> 'pq'

c. If the letters appear on the same column of the table, replace them with the letters immediately below respectively (wrapping around to the top side of the column if a letter in the original pair was on the bottom side of the column). 'rk' -> 'dt', 'pv' -> 'vo

Key word : sumer

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

Plain text:

The sections on quantum cryptography, quantum proper ties of squeezed light, and experimental efforts to measure gravitational waves provide adequate introduction to these exciting applications of quantum optics.

Cipher text:

OLRUMDPLPOUNOTSBONMEFMXQNPLSCNKWOEGVORCXUTQMFZKMUNAROEMYYRFKK
HLOGVKDMXRSPCSQNFKRCZTUNRNPERGAMSSKSFXGNFPLPOFGVBYSMNUTXGKDBFDYSB
QRGPZFQBMBPLPONPOLRUMYMILPGPNGXMGKDBPLPOUNDTSBONMEPQPLAM

Question Number 3

Vigenere Cipher:

Definition:

The Vigenere Cipher is a polyalphabetic substitution cipher. The method was originally described by Giovan Battista Bellaso in his 1553.

Encryption:

- The 'key' for a vigenere cipher is a key word. e.g. 'world'
- The Vigenere Cipher uses the following table to encipher the plaintext:
- To encipher a message, repeat the keyword above the plaintext:
- Now we take the letter we will be encoding, 'D', and find it on the first column on the tableau. Then, we move along the 'D' row of the tableau until we come to the column with the 'F' at the top (The 'F' is the keyword letter for the first 'D'), the intersection is our ciphertext character, 'I'.

Key Letter	Plaintext Letter																									
	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

Fig. 1 Vigenere Table

Key Word: World

Plaintext:	The sections on quantum cryptography, quantum proper ties of squeezed light, and experimental efforts to measure gravitational waves provide adequate introduction to these exciting applications of quantum optics.
Key Word	worldworldworldworldworldworldworldworldworldworldworldworldworldworldworldworldworld
Cipher text	Pvvdhyhzzqocebxwbkfpyfpawkuilsdmhfdjhlxsncgpupwvdrbghfhanvooeuyedjrvisafzxhjhrwhbtfcwoh fxhwglchcfrglpoktrjochdrsjaukjzohwrvbxwhvtqpffoxyhzzqpckshosvifehzyjwdgwlyoktrjgfqtqoeexicgelyg

Cipher text:

pvvdhyhzzqocebxwbkfpyfpawkuilsdmhfdjhlxsncgpupwvdrbg
hfhanvooeuyedjrvisafzxhjhrwhbtfcwohfxhwglchcfrglpoktrjo
chdrsjaukjzohwrvbxwhvtqpffoxyhzzqpckshosvifehzyjwdgwly
oktrjgfqtqoeexicgelyg