Question No:1

Monoalphabetic Cipher:

Definition:

In Monoalphabetic Cipher substitutes one letter of the alphabet with any random letter from the alphabet.

Possible Combination: **26! =24x10^{26}** Possibilities

Plain Text:

In contrast to symmetric cryptosystems, public key cryptography is a form of cryptography which generally allows users to communicate securely without having prior access to a shared secret key.

Encryption Process:

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

Plain text:

In contrast to symmetric cryptosystems public key cryptography is a form of
OF EGFZKQLZ ZG LNDDTZKOE EKNHZGLNLZTDL HXWSOE ATN EKNHZGUQHIN OL Q YGKD GY

cryptography which generally allows users to communicate securely without
EKNHZGUQHIN VIOEI UTFTKQSSN QSSGVL XLTKL ZG EGDDXFOEQZT LTEXKTSN VOZIGXZ

having prior access to a shared secret key
IQCOFU HKOGK QEETLL ZG Q LIQKTR LTEKTZ ATN

Cipher text:

OF EGFZKQLZ ZG LNDDTZKOE EKNHZGLNLZTDL HXWSOE ATN EKNHZGUQHIN OL Q YGKD GY
EKNHZGUQHIN VIOEI UTFTKQSSN QSSGVL XLTKL ZG EGDDXFOEQZT LTEXKTSN VOZIGXZ
IQCOFU HKOGK QEETLL ZG Q LIQKTR LTEKTZ ATN

Question No 2

Playfair Cipher:

- Invented by Charles wheat tone
- It is based on 5x5 matrix table

Rules:

- Chose key word
- The letter I and J count as one letter
- Enter alphabet in matrix table from left to right
- Convert the text into pairs of alphabet

  E.g yellow (ye ll ow)

Encryption Process:

- Broke the plain text in group of two alphabets
  - E,g : yellow (ye ll ow)
- If both alphabets are same (or only one is left) add an X after first alphabet
  - E,g : Tree (Tr ex ex) Alice (Al ic ex)
- If both alphabet is in the pair appear in the same row of matrix replace them with alphabet to their immediate right respective.

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

E,g : LY = AF

- If both the alphabet in the pair appear in the same column replace with alphabet immediately below them respective.

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

E,g : EM = BW

- If the alphabet is not in same row or column replace them with alphabets in the same row respective but at other pair of corner.

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

E,g : IO =TR

Solution:

Keyword: PLAYFIR

Plain text:

In contrast to symmetric cryptosystems, public key cryptography is a form of cryptography which generally allows users to communicate securely without having prior access to a shared secret key.

Making Pairs:

In co nt ra st to sy mx me tr ic cr yp to sy st em sx pu bl ic ke yx cr yp to gr ap hy is ax fo rm of cr yp to gr ap hy wh ic hx ge ne ra lx yx al xo ws us we sx to co mx un ic at ex se cu re ly wi th ou tx ha vi ng pr io rx ac xe sx to ax sh ar ed se cr et ke yx

Cipher text:

RCRGIDELHGOBQFQWIBERNZNLIHGKFQBIQHIPOARIMRFNNLIHBTELIUPNMFLGEKGLIEFLOBOC YLQPUMRISTNCNEYAAFYARKZMZHNEHGGRBKHWCREFBIMCIZENAFUEHUTVHULWRCTFERKO FEINQZOBFMMPENGQNIENOHNA

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

Question Number 3

Vigenere Cipher:

Definition:

Vigenere Cipher is a method of encrypting alphabetic text. It uses a simple form of polyalphabetic substitution.

- The table consists of the alphabets written out 26 times in different rows, each alphabet shifted cyclically to the left compared to the previous alphabet, corresponding to the 26 possible Caesar Ciphers.
- At different points in the encryption process, the cipher uses a different alphabet from one of the rows.
- The alphabet used at each point depends on a repeating keyword.

Encryption Process:

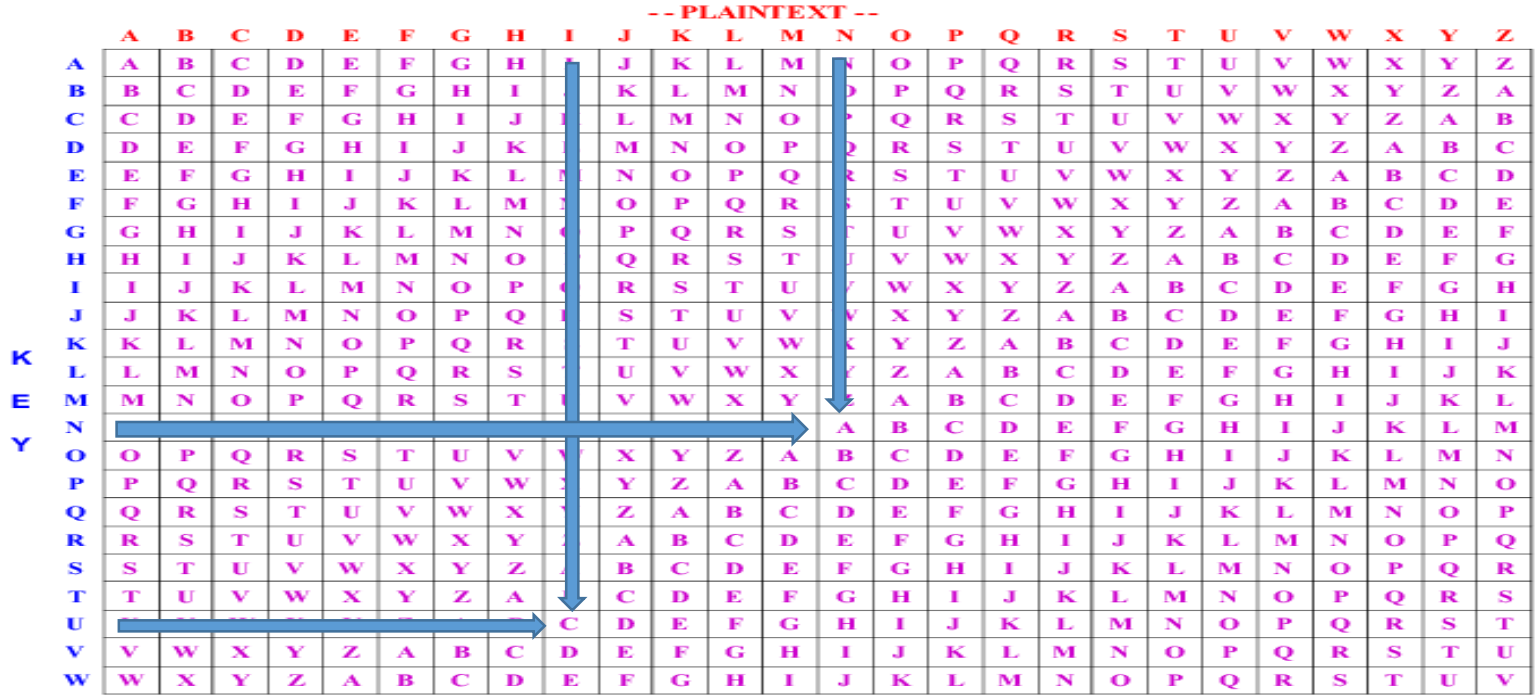
- Using the table
- Keyword
- The first letter of the plaintext is paired with the first letter of the key.
- So use row and column of the Vigenere square, namely
- Similarly, for the second letter of the plaintext, the second letter of the key is used, the letter at row and column
- The rest of the plaintext is enciphered in a similar fashion.

		-- PLAINTEXT --																								
		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
K	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
E	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
Y	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

Solution
Key Word: university

Formula: $E_i = (P_i + K_i) \bmod 26$

Plaintext:	In contrast to symmetric cryptosystems, public key cryptography is a form of cryptography which generally allows users to communicate securely without having prior access to a shared secret key.
Key Word	universityuniversityuniversityuniversityuniversityuniversityuniversityuniversityuniversity
Cipher text	Cakjrkjilrnbatqdwbkgwpzttkgarqnruntlttbaergxvphbhelnxcczkiymlzwagiqxmmaeiklpopbabtmiiistewuy tjajmaxpmgwxsdecggwnbzwvuckcfledxygcmfuiqikgjqhpupkzwjlwtqbnzzhjwkkcnxmt



Cipher Text:

cakjrkjilrnbatqdwbkgwpzttkgarqnruntlttbaergxvphbhelnxcczkiy
mlzwagiqxmmaeiklpopbabtmiiistewuytjajmaxpmgwxsdecggwn
bzwvuckcfledxygcmfuiqikgjqhpupkzwjlwtqbnzzhjwkkcnxmt