Q#1:

MONOALPHABETIC CIPHER:

Monoalphabetic cipher is a substitution cipher in which for a given key, the cipher alphabet for each plain alphabet is fixed throughout the encryption process. For example, if 'A' is encrypted as 'D', for any number of occurrence in that plaintext, 'A' will always get encrypted to 'D'.

Table for monoalphabetic cipher

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

PLAIN TEXT: Within those developments, we must ensure confidentiality and integrity in transaction, And the new science of cryptography using secret codes to keep messages secure-will be vital.

CIPHER TEXT: EQBPQV BPWAM LMDMTWXUMVBA,EM UCAB MVACZM KWVNQLMVBQITQBG IVL QVBMOZQBG QV BZINAIKBQWV IVL BPM VME AKQMVKM WN KZGXBWOZIXPG CAQVO AMKZMB KWLMA BW SMMX UMTTIOMA AMKCZM-EQTT JM DQBIT.

Q#2:

Playfair Cipher:

Lets we are selecting a key: "Playfair Example"

Plain Text: Within those developments we must ensure confidentiality and integrity in transaction and the new science of cryptography – using secret codes to keep messages secure-will be vital

Note: *If there is nothing given except plane text then we will choose 5x5 matrixes for this.*

Solution:

Step I: We have choosen a key which is "Playfair Example"

Step II: Create a 5x5 matrix

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

Step III: Plain Text Pairs

Hints: If there is any consecutive alphabets then we will add ‘X’.

WI	TH	IN	TH	OS	ED	EV	EL	OP	ME	NT	SW	EM	US	TE
NS	UR	EC	ON	FI	DE	NT	IA	LI	TY	AN	DI	NT	EG	RI
TY	IN	TR	AN	SA	CT	IO	NA	ND	TH	EN	EW	SC	IE	NC
EO	FC	RY	PT	OG	RA	PH	YU	SI	NG	SE	CR	ET	CO	DE
ST	OK	EX	EP	ME	SX	SA	GE	SX	SE	CU	RE	WI	LX	LB
EV	IT	AL												

Step IV: Cipher Text after applying playfair

Q#3:

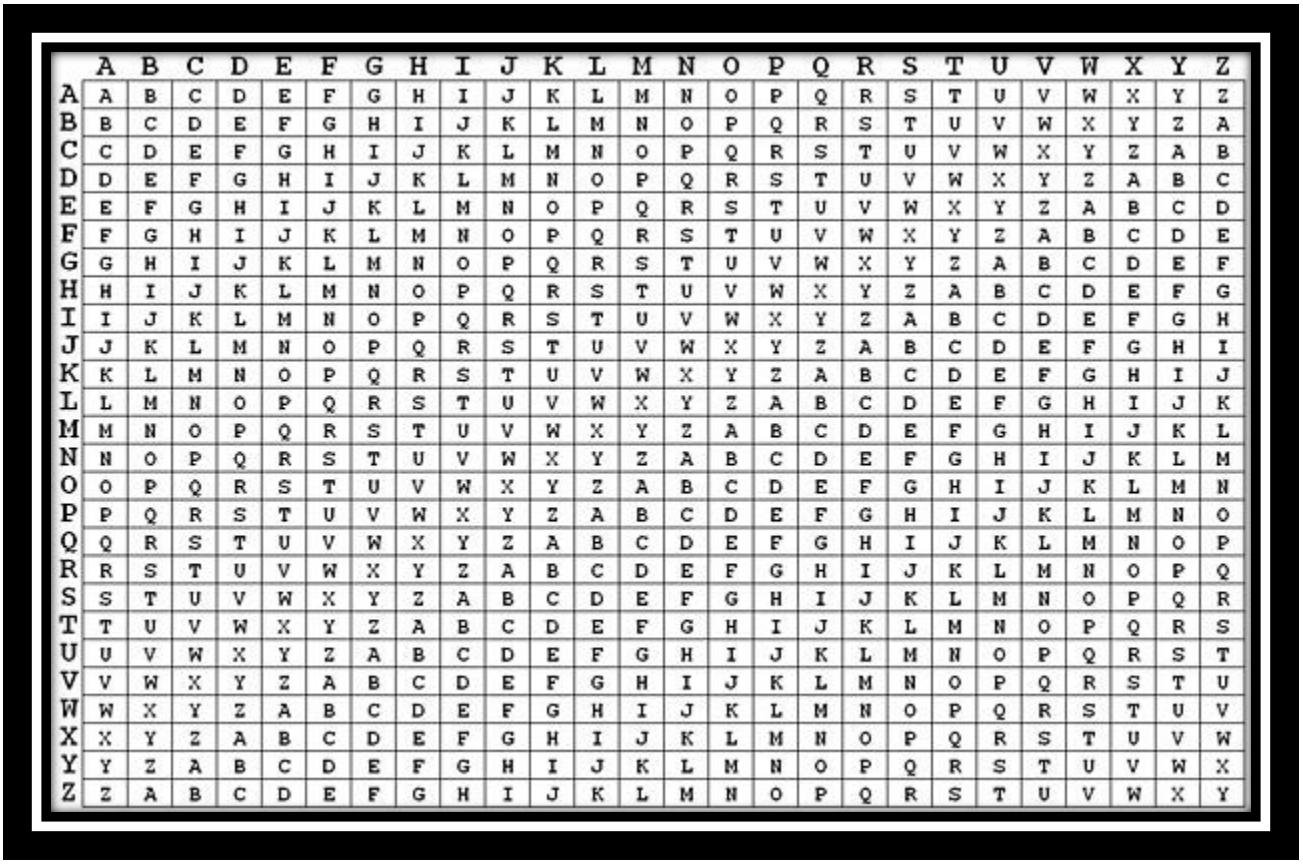
Vigenere Cipher

Description

The Vigenere cipher is an example of a polyalphabetic substitution cipher. A polyalphabetic substitution cipher is similar to a monoalphabetic substitution except that the cipher alphabet is changed periodically while enciphering the message. This makes the cipher less vulnerable to cryptanalysis using letter frequencies.

Blaise de Vigenere developed what is now called the Vigenere cipher in 1585. He used a table known as the Vigenere square, to encipher messages. This page discusses two different versions of the Vigenere cipher, the autokey method and the keyword method.

The Vigenere square



	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

In order to encipher a message using the Vigenere autokey method it uses a keyword. The keyword can be of any length greater than one, which provides an unlimited number of possible keys. To form the key, the sender writes the keyword repeatedly on the line underneath the plaintext. The sender will encrypt the message by writing the plaintext on one line and writing the key on the line beneath it. The sender will use the plaintext and key letters to select a row and a column in the Vigenere square. The selected row is the row in which the plaintext letter is in the first column and the selected column is the column in which the key letter is in the first row. A ciphertext letter will be the letter that appears in the Vigenere square at the position corresponds to the selected row and column. In the following example, to find the ciphertext letter, first locate the row in the Vigenere square that corresponds to plaintext letter w. Next locate the column that corresponds to the key letter r. The letter at which they intersect is the ciphertext letter, in this case b. Continue to do this for each pair of letters to form the compete ciphertext.

Plain text: within those development we must ensure confidentiality and integrity in transactions and the new science of cryptography using secret codes to keep message secure will be vital.

Keyword: friend

Process:

Plain text	w	i	t	h	i	n	t	h	o	s	e	d	e	v	e	l	o	p	m	e	n	t	w	e	m	u	s	t
Key	f	e	i	e	n	d	f	r	i	e	n	d	f	r	i	e	n	d	f	r	i	e	n	d	f	r	i	e
Cipher text	b	z	b	l	v	q	y	y	i	w	r	g	j	m	m	p	b	s	r	v	v	x	j	h	r	l	a	x

Plain text	e	n	s	u	r	e	c	o	n	f	i	d	e	n	t	i	a	l	i	t	y	a	n	d	i	n	t	e
Key	n	d	f	r	i	e	n	d	f	r	i	e	n	d	f	r	i	e	n	d	f	r	i	e	n	d	f	r
Cipher text	r	q	x	l	z	i	p	r	s	w	q	h	r	s	y	z	i	p	v	w	d	r	v	h	v	q	y	u

Plain text	g	r	i	t	y	i	n	t	r	a	n	s	a	c	t	i	o	n	s	a	n	d	t	h	e	n	e	w
Key	i	e	n	d	f	r	i	e	n	d	f	r	i	e	n	d	f	r	i	e	n	d	f	r	i	e	n	d
Cipher text	o	v	v	w	d	z	v	x	e	d	s	j	i	g	g	l	t	e	a	e	a	g	y	y	m	r	r	z

Plain text	s	c	i	e	n	c	e	o	f	c	r	y	p	t	o	g	r	a	p	h	y	u	s	i	n	g	s	e
Key	f	r	i	e	n	d	f	r	i	e	n	d	f	r	i	e	n	d	f	r	i	e	n	d	f	r	i	e
Cipher text	x	t	q	i	a	f	j	f	n	g	e	b	a	k	w	o	e	d	u	y	g	y	f	l	s	x	a	i

Plain text	c	r	e	t	c	o	d	e	s	t	o	k	e	e	p	m	e	s	s	a	g	e	s	s	e	c	u	r
Key	n	d	f	r	i	e	n	d	f	r	i	e	n	d	f	r	i	e	n	d	f	r	i	e	n	d	f	r
Cipher text	p	u	j	k	k	s	q	h	x	k	w	o	r	h	u	d	m	w	f	d	l	v	a	w	r	f	z	i

Plain text	e	w	i	l	l	b	e	v	i	t	a	l																
Key	i	e	n	d	f	r	i	e	n	d	f	r																
Cipher text	m	a	v	o	q	s	m	z	v	w	f	c																

Cipher text:

bzblvqyyiwrgjmmpbsrvvxjhrlaxrqxlziprswqhzsyzipvwdrvhvqyuovvwdzvxedsjigglteaeagyymrrZxt
qiafjfngebakwoeduygyflsxaIpujkksqhxkworhudmwfdlvawrfzImavoqsmzvwfc

Decipher

To decrypt a message, the row is selected using the priming key. Next, the receiver locates the first letter of the ciphertext in the selected row. The letter at the top of the column that contains the ciphertext letter is the first letter of the plaintext. Add the first letter of the plaintext to the key and use it with next ciphertext letter to continue decipherment.

Cipher text:
bzblvqyyiwrgjmmpbsrvvxjhrlaxrqxlziprswqhzsyzipvwdrvhvqyuovvwdzvxedsjigglteaeagyymrrZxt
qiafjfngebakwoeduygyflsxaIpujkksqhxkworhudmwfdlvawrfzImavoqsmzvwfc

Keyword: friend

Process:

Key	f	e	i	e	n	d	f	r	i	e	n	d	f	r	i	e	n	d	f	r	i	e	n	d	f	r	i	e
Cipher text	b	z	b	l	v	q	y	y	i	w	r	g	j	m	m	p	b	s	r	v	v	x	j	h	r	l	a	x
Plain text	w	i	t	h	i	n	t	h	o	s	e	d	e	v	e	l	o	p	m	e	n	t	w	e	m	u	s	t

Key	n	d	f	r	i	e	n	d	f	r	i	e	n	d	f	r	i	e	n	d	f	r	i	e	n	d	f	r
Cipher text	r	q	x	l	z	i	p	r	s	w	q	h	r	s	y	z	i	p	v	w	d	r	v	h	v	q	y	u
Plain text	e	n	s	u	r	e	c	o	n	f	i	d	e	n	t	i	a	l	i	t	y	a	n	d	i	n	t	e

Key	i	e	n	d	f	r	i	e	n	d	f	r	i	e	n	d	f	r	i	e	n	d	f	r	i	e	n	d
Cipher text	o	v	v	w	d	z	v	x	e	d	s	j	i	g	g	l	t	e	a	e	a	g	y	y	m	r	r	z
Plain text	g	r	i	t	y	i	n	t	r	a	n	s	a	c	t	i	o	n	s	a	n	d	t	h	e	n	e	w

Key	f	r	i	e	n	d	f	r	i	e	n	d	f	r	i	e	n	d	f	r	i	e	n	d	f	r	i	e
Cipher text	x	t	q	i	a	f	j	f	n	g	e	b	a	k	w	o	e	d	u	y	g	y	f	l	s	x	a	i
Plain text	s	c	i	e	n	c	e	o	f	c	r	y	p	t	o	g	r	a	p	h	y	u	s	i	n	g	s	e

Key	n	d	f	r	i	e	n	d	f	r	i	e	n	d	f	r	i	e	n	d	f	r	i	e	n	d	f	r
Cipher text	p	u	j	k	k	s	q	h	x	k	w	o	r	h	u	d	m	w	f	d	l	v	a	w	r	f	z	i
Plain text	c	r	e	t	c	o	d	e	s	t	o	k	e	e	p	m	e	s	s	a	g	e	s	s	e	c	u	r

Key	i	e	n	d	f	r	i	e	n	d	f	r																
Cipher text	m	a	v	o	q	s	m	z	v	w	f	c																
Plain text	e	w	i	l	l	b	e	v	i	t	a	l																

Plain text: within those development we must ensure confidentiality and integrity in transactions and the new science of cryptography using secret codes to keep message secure will be vital.

END