The implementation of a public key cryptography package needs to ensure that the random number object used in the generation of key pairs cannot be accessed by clients of the package.

Apply the following 3 codes:

(a) Playfair Cipher

(b) Vigenere Cipher

(c) Monoalphabetic Cipher

Playfair cipher

The best known multiple letter encryption cipher is the playfair, which treats digrams in the plaintext as single units and translates these units into cipher text digrams. The playfair algorithm is based on the use of 5x5 matrix of letters constructed using a keyword. Let the keyword be „monarchy". The matrix is constructed by filling in the letters of the keyword (minus duplicates) from left to right and from top to bottom, and then filling in the remainder of the matrix with the remaining letters in alphabetical order. The letter „i" and „j" count as one letter. Plaintext is encrypted two letters at a time According to the following rules: Repeating plaintext letters that would fall in the same pair are separated with a Filler letter such as „x". Plaintext letters that fall in the same row of the matrix are each replaced by the letter to the right, with the first element of the row following the last. Plaintext letters that fall in the same column are replaced by the letter beneath, with the top element of the column following the last. Otherwise, each plaintext letter is replaced by the letter that lies in its own row And the column occupied by the other plaintext letter.

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

Plaintext = meet me at the school house

Splitting two letters as a unit => me et me at th es ch o x ol ho us ex

Corresponding cipher text => CL KL CL RS PD IL HY AV MP HF XL IU

Strength of playfair cipher

Playfair cipher is a great advance over simple mono alphabetic ciphers. Since there are 26 letters, 26x26 = 676 diagrams are possible, so identification of individual diagram is more difficult.

Vigenere cipher

In this scheme, the set of related monoalphabetic substitution rules consisting of 26 Caesar ciphers with shifts of 0 through 25. Each cipher is denoted by a key letter. e.g., Caesar cipher with a shift of 3 is denoted by the key value 'd‟ (since a=0, b=1, c=2 and so on). To aid in understanding the scheme, a matrix known as vigenere tableau is Constructed

Each of the 26 ciphers is laid out horizontally, with the key letter for each cipher to its left. A normal alphabet for the plaintext runs across the top. The process of

	a	b	c	d	e	f	g	h	i	j	k	.....	x	y	z
a	A	B	C	D	E	F	G	H	I	J	K	.....	X	Y	Z
b	B	C	D	E	F	G	H	I	J	K	L	.....	Y	Z	A
c	C	D	E	F	G	H	I	J	K	L	M	.....	Z	A	B
d	D	E	F	G	H	I	J	K	L	M	N	.....	A	B	C
e	E	F	G	H	I	J	K	L	M	N	O	.....	B	C	D
f	F	G	H	I	J	K	L	M	N	O	P	.....	C	D	E
g	G	H	I	J	K	L	M	N	O	P	Q	.....	D	E	F
: :	: :	: :	: :	: :	: :	: :	: :	: :	: :	: :	: :	....	: :	: :	: :
x	X	Y	Z	A	B	C	D	E	F	G	H	.....			W
y	Y	Z	A	B	C	D	E	F	G	H	I	.....			X
z	Z	A	B	C	D	E	F	G	H	I	J	.....			Y

Encryption is simple: Given a key letter X and a plaintext letter y, the cipher text is at the intersection of the row labeled x and the column labeled y; in this case, the cipher text is

To encrypt a message, a key is needed that is as long as the message. Usually, the key is a repeating keyword.

e.g.: key = d e c e p t i v e d e c e p t i v e d e c e p t i v e PT = w e a r e d i s c o v e r e d s a v e y o u r s e l f CT = ZICVTWQNGRZGVTWAVZHCQYGLMGJ

Decryption is equally simple. The key letter again identifies the row. The position of the cipher text letter in that row determines the column, and the plaintext letter is at the top of that column.

Strength of Vigenere cipher

There are multiple cipher text letters for each plaintext letter.

Letter frequency information is obscured

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.

Method:

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