Polyalphabetic Ciphers

Another way to improve on the simple monoalphabetic technique is to use different monoalphabetic substitutions as one proceeds through the plaintext message. The general name for this approach is **polyalphabetic substitution cipher**. All these techniques have the following features in common:

1. A set of related monoalphabetic substitution rules is used.

2. A key determines which particular rule is chosen for a given transformation.

Vigenère cipher

The best known polyalphabetic substitution cipher, and one of the simplest, such algorithm is referred to as the ***Vigenère cipher***. In this scheme, the set of related monoalphabetic substitution rules consists of the 26 Caesar ciphers, with shifts of 0 through 25. Each cipher is denoted by a key letter.

To aid in understanding the scheme and to aid in its use, a matrix known as the **Vigenère 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 encryption is simple: Given a key letter *x* and a plaintext letter y, the ciphertext letter is at the intersection of the row labeled *x* and the column labeled y; in this case the ciphertext is V.

For example to encrypt a message, a key is needed that is as long as the message. Usually, the key is a repeating keyword. **For example**, if the keyword is **deceptive**, the message "**we are discovered save yourself**" is encrypted as follows:

```
key:            deceptivedeceptivedeceptive
plaintext:       wearediscoveredsaveyourself
ciphertext:     ZICVTWQNGRZGVTWAVZHCQYGLMGJ
```

Security of Computer and Networks

asaad.nayyef@uomus.edu.iq

	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**
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	G
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

Table below shows the cipher text in **Vigenere method**.

Table (1): Mapping Letters To Integers And Back

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

The encryption function seen in Equation 2.

$$E(k, m_i) = m_i + k \pmod{26} \quad .....(2)$$

Plaintext Alphabet	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
Plaintext Value	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Example: encipher the plaintext message: "TO BE OR NOT TO BE THAT IS THE QUESTION", using the keyword SUBSTITUTION?

C=p+k mod 26

A	Keyword:																													
KEY	S	U	B	S	T	I	T	U	T	I	O	N	S	U	B	S	T	I	T	U	T	I	O	N	S	U	B	S	T	I
	As integer																													
Letter Value	18	20	1	18	19	8	19	20	19	8	14	13	18	20	1	18	19	8	19	20	19	8	14	13	18	19	1	18	19	8
	Plaintext:																													
Plaintext	t	o	b	e	o	r	n	o	t	t	o	b	e	t	h	a	t	i	s	t	h	e	q	U	e	s	t	i	o	n
	As integer																													
Letter Value	19	14	1	4	14	17	13	14	19	19	14	1	4	19	7	0	19	8	18	19	7	4	16	20	4	18	19	8	14	13
Sum +	37	34	2	22	33	25	32	34	38	27	28	14	22	39	8	18	38	16	37	39	26	12	30	33	22	37	20	26	33	21
Mod 26	11	8	2	22	7	25	6	8	12	1	2	14	22	13	8	18	12	16	11	13	0	12	4	7	22	11	20	0	7	21
	Cipher text:																													
Cipher	L	I	C	W	H	Z	G	I	M	B	C	O	W	N	I	S	M	Q	L	N	A	M	E	H	W	L	U	A	H	V

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

Example: using vigenere cipher, encrypt and decrypt the word (instruction) with the key (key)

Encryption function: ***C=p+k mod 26***

plaintext	i	n	s	t	r	u	c	t	i	o	n
Letter Value	8	13	18	19	17	20	2	19	8	14	13
key	k	e	y	k	e	y	k	e	y	k	e
Letter Value	10	4	24	10	4	24	10	4	24	10	4
Sum +=P+k	18	17	42	29	21	44	12	23	32	24	17
(P+k)mod26	18	17	16	3	21	18	12	23	6	24	17
ciphertext	S	R	Q	D	V	S	M	X	G	Y	R

Then use decryption function: ***p=C-k mod 26***

ciphertext	S	R	Q	D	V	S	M	X	G	Y	R
C	18	17	16	3	21	18	12	23	6	24	17
key	k	e	y	k	e	y	k	e	y	k	e
k	10	4	24	10	4	24	10	4	24	10	4
C-k	8	13	-8	-7	17	-6	2	19	-18	14	13
(C-k)mod26	8	13	18	19	17	20	2	19	8	14	13
plaintext	i	n	s	t	r	u	c	t	i	o	n