Computer Security Assignment

Group Member

1142701102	Wong Zi Xiang
1142701565	Andy Yong Jun Jie
1142701239	Lee Boon Ping
1141328079	Fang Siaw Tung

Background Study

- Caesar Cipher
- Vigenere Cipher
- Advanced Encryption Standard (AES)

Caesar Cipher

- One of the earliest known example of substitution cipher
- Used by Julius Caesar
- Each character of a plaintext message is replaced by a character n position down in the alphebet

Vigenere Cipher

- Effectively multiple Caesar ciphers
- Key is multiple letter long K = k1 k2 …kd
- Use each alphabet in turn
- Repeat from start after d letter in message
- Decryption simply works in reverse

Advanced Encryption Standard (AES)

- Is a symmetric-key block cipher
- Published by the (NIST) in December 2001
- Rijndeal was selected as the AED in OCT-2000
- Variable bit block cipher and user variable key length of 128, 192, 256 bits

Implementation Details

- Caesar Cipher
- Vigenère Cipher
- Advanced Encryption Standard with Cipher Feedback

Caesar Cipher

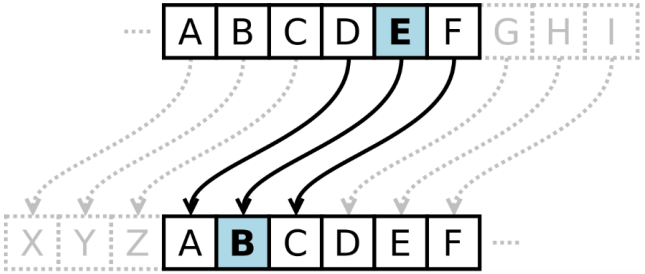
Comparison of results (Caeser Cipher and Vigenere Cipher)

$$E(x) = (x + n)\ mod\ 26$$
$$D(x) = (x - n)\ mod\ 26$$

A	B	C	D	E	F	G	H	I	J	K	L	M
↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕
0	1	2	3	4	5	6	7	8	9	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕
13	14	15	16	17	18	19	20	21	22	23	24	25

Caesar Cipher



Plaintext: h → 07	Encryption: (07 + 15) mod 26	Ciphertext: 22 → W
Plaintext: e → 04	Encryption: (04 + 15) mod 26	Ciphertext: 19 → T
Plaintext: l → 11	Encryption: (11 + 15) mod 26	Ciphertext: 00 → A
Plaintext: l → 11	Encryption: (11 + 15) mod 26	Ciphertext: 00 → A
Plaintext: o → 14	Encryption: (14 + 15) mod 26	Ciphertext: 03 → D

Vigenere Cipher

$\boldsymbol{M} = \boldsymbol{M_1} \ldots \boldsymbol{M_n}$ is the message, $\boldsymbol{C} = \boldsymbol{C_1} \ldots \boldsymbol{C_n}$ is the ciphertext and $\boldsymbol{K} = \boldsymbol{K_1} \ldots \boldsymbol{K_n}$ is the key.

Encryption:

$$C_i = E_K(M_i) = (M_i + K_i) \; mod \; 26$$

Decryption:

$$M_i = D_K(C_i) = (C_i - K_i) \; mod \; 26$$

M is message or plaintext, C is ciphertext and K is key for encryption and decryption.

Vigenere Cipher (Cont.)

A	B	C	D	E	F	G	H	I	J	K	L	M
↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕
0	1	2	3	4	5	6	7	8	9	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕
13	14	15	16	17	18	19	20	21	22	23	24	25

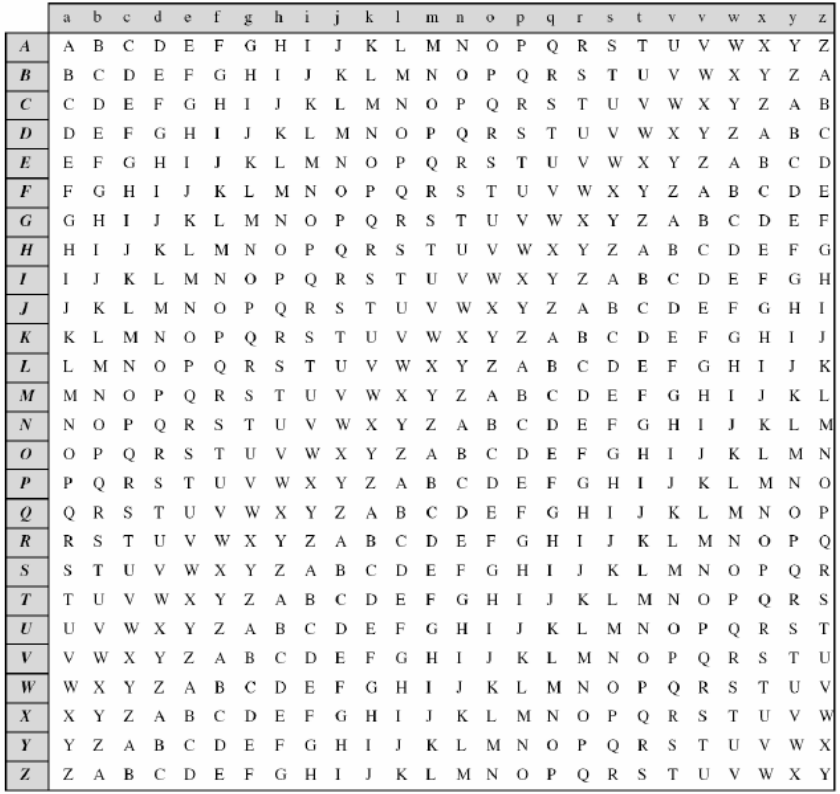
Table of alphabet code for encrypt and decrypt

Vigenere Cipher (Cont.)

Plaintext:	s	h	e	i	s	l	i	s	t	e	n	i	n	g
P's values:	18	07	04	08	18	11	08	18	19	04	13	08	13	06
Key stream:	***15***	***00***	***18***	***02***	***00***	***11***	***15***	***00***	***18***	***02***	***00***	***11***	***15***	***00***
C's values:	**07**	**07**	**22**	**10**	**18**	**22**	**23**	**18**	**11**	**6**	**13**	**19**	**02**	**06**
Ciphertext:	**H**	**H**	**W**	**K**	**S**	**W**	**X**	**S**	**L**	**G**	**N**	**T**	**C**	**G**

Encryption of vigenere cipher

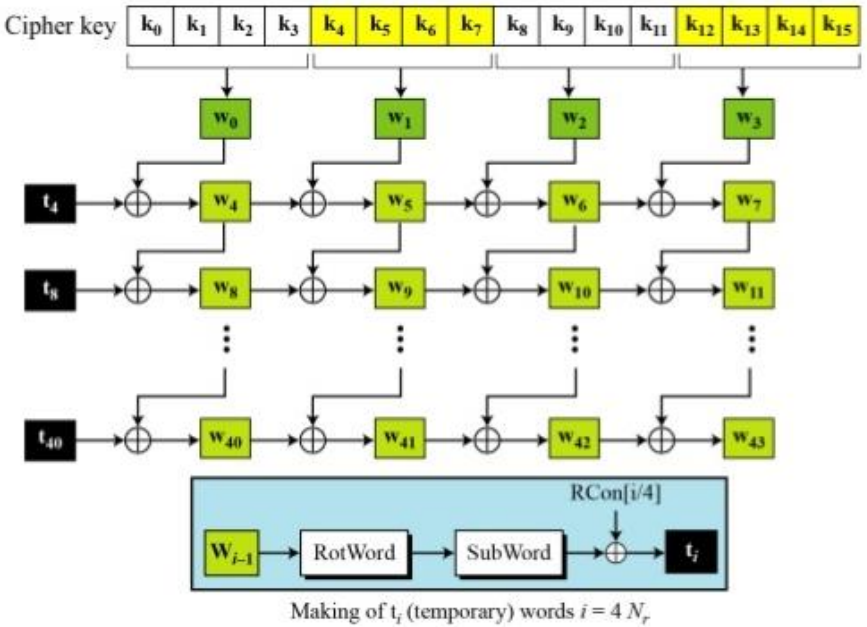
Vigenere Cipher (Cont.)



	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	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

Table is locate the first letter of plaintext message in the first line of the table and first letter of the key from the left column.

Advanced Encryption Standard with Cipher Feedback



Making of t_i (temporary) words $i = 4\ N_r$

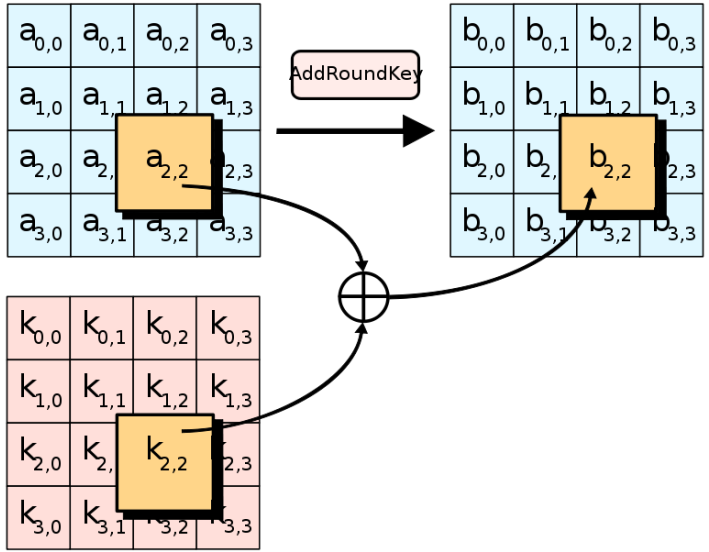
KeyExpansion

A key schedule is used to expand a short key into number of separate round keys. It produces the needed round keys from the initial cipher key.

Advanced Encryption Standard with Cipher Feedback (Cont.)

AddRoundKey

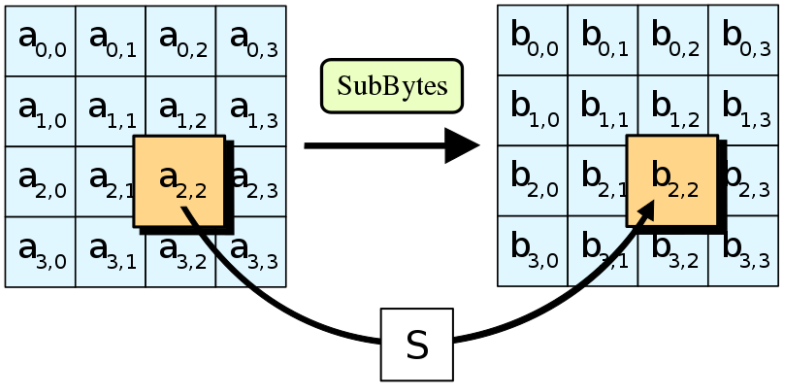
In this step, each byte of the plaintext is combined with respective byte of the round subkey using bitwise XOR.



Advanced Encryption Standard with Cipher Feedback (Cont.)

SubBytes

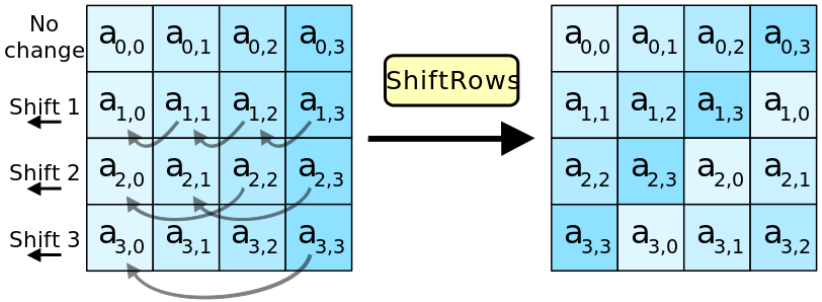
In this step, each byte in the state matrix is replaced with SubByte using an 8-bit substitution box (S-box).



Advanced Encryption Standard with Cipher Feedback (cont.)

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

Advanced Encryption Standard with Cipher Feedback (cont.)



ShiftRows

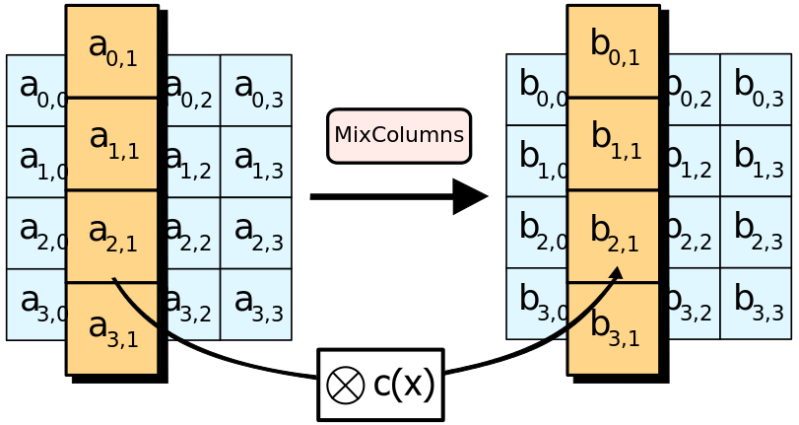
This step operates on the rows of the state. Bytes in each row is cyclically shifted by a certain offset. The first row is unchanged. The second row is shifted one to the left. Third and fourth row is shifted two and three to the left respectively.

Advanced Encryption Standard with Cipher Feedback (cont.)

MixColumns

In this step, each column is transformed using a fixed matrix. Each column of the state is multiplied with the fixed matrix

$$\begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix}$$



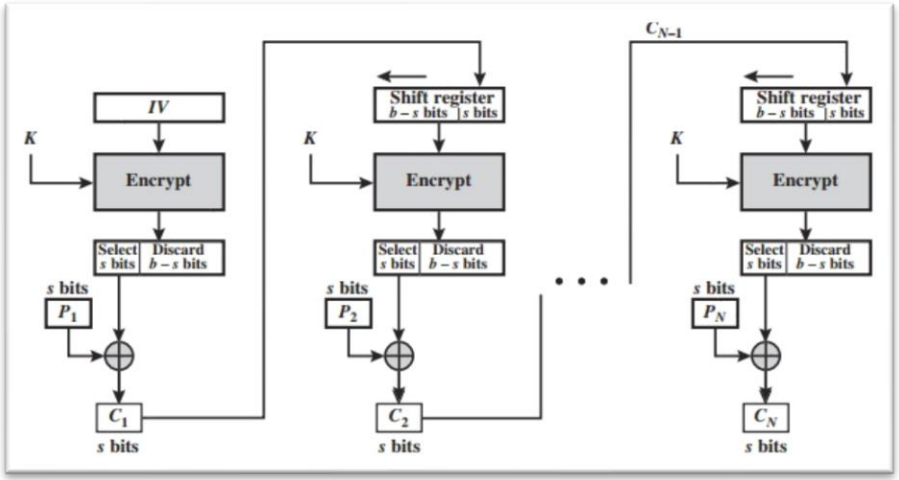
Advanced Encryption Standard with Cipher Feedback (cont.)

Cipher Feedback Mode

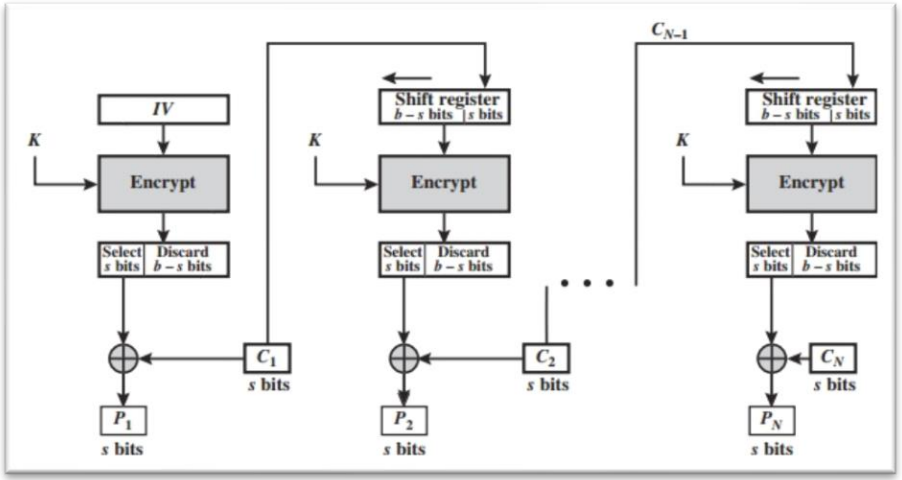
Previous ciphertext is used to encrypt the next block of data. Often used to encrypt individual characters (Terminals)

$$C_i = head(E_K(S_{i-1}), x) \oplus P_i$$
$$P_i = head(E_K(S_{i-1}), x) \oplus C_i$$
$$S_i = \left((S_{i-1} << x) + C_i\right) mod\ 2^n$$
$$S_0 = IV$$

Advanced Encryption Standard with Cipher Feedback (cont.)



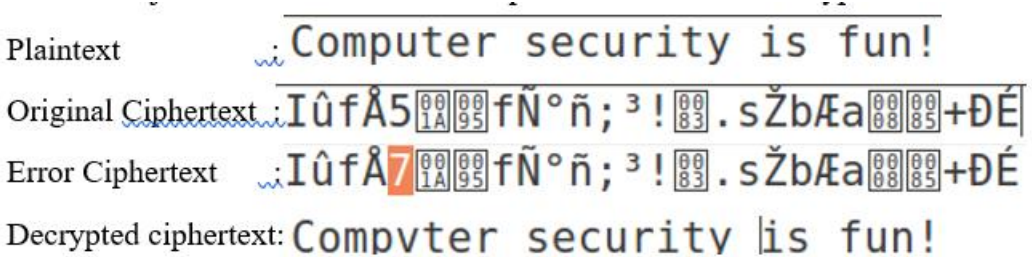
Cipher Feedback Mode Encryption



Cipher Feedback Mode Decryption

Comparison of results

Cipher Feedback Mode Bit-error Propagation



Comparison of results (Cont.)

Comparison of results (Caeser Cipher and Vigenere Cipher)

```
 Caesar Cipher
 What do you want to perform:
 1. Encryption
 2. Decryption
==>1

 Enter Key(0 until 25):23
Time : 62.0096 microseconds
Total bytes : 52
Total plaintext in bytes encrypted/Encryption Time : 0.83858bytes/microseconds

 Done
```

```
 Vigenere Cipher
 What do you want to perform:
 1. Encryption
 2. Decryption
 3. Encryption Time
 4. Decryption Time
==>3

 Enter Key:happy
Time : 53.4565 microseconds
Total bytes : 44 bytes
Total plaintext in bytes encrypted/Encryption Time : 0.823098bytes/microseconds

 Done
D:\Degree IT\Trimester 1 (Y3)\TSN3251 - COMPUTER SECURITY\Assignment\Monocipher\
Polyalphabetic Cipher>
```

Comparison of results (Cont.)

```
 Caesar Cipher
 What do you want to perform:
 1. Encryption
 2. Decryption
==>2

 Enter Key(0 until 25):23
Time : 53.0289 microseconds
Total bytes : 52
Total ciphertext in bytes decrypted/Decryption Time : 0.980598bytes/microseconds

 Done
```

```
 Vigenere Cipher
 What do you want to perform:
 1. Encryption
 2. Decryption
 3. Encryption Time
 4. Decryption Time
==>4

 Enter Key:happy
Time : 54.3118 microseconds
Total bytes : 48 bytes
Total ciphertext in bytes decrypted/Decryption Time : 0.883785bytes/microseconds

 Done
D:\Degree IT\Trimester 1 (Y3)\TSN3251 - COMPUTER SECURITY\Assignment\Monocipher\
Polyalphabetic Cipher>
```

The End