Seiyun University
Faculty of Applied Science

Computer Science Department

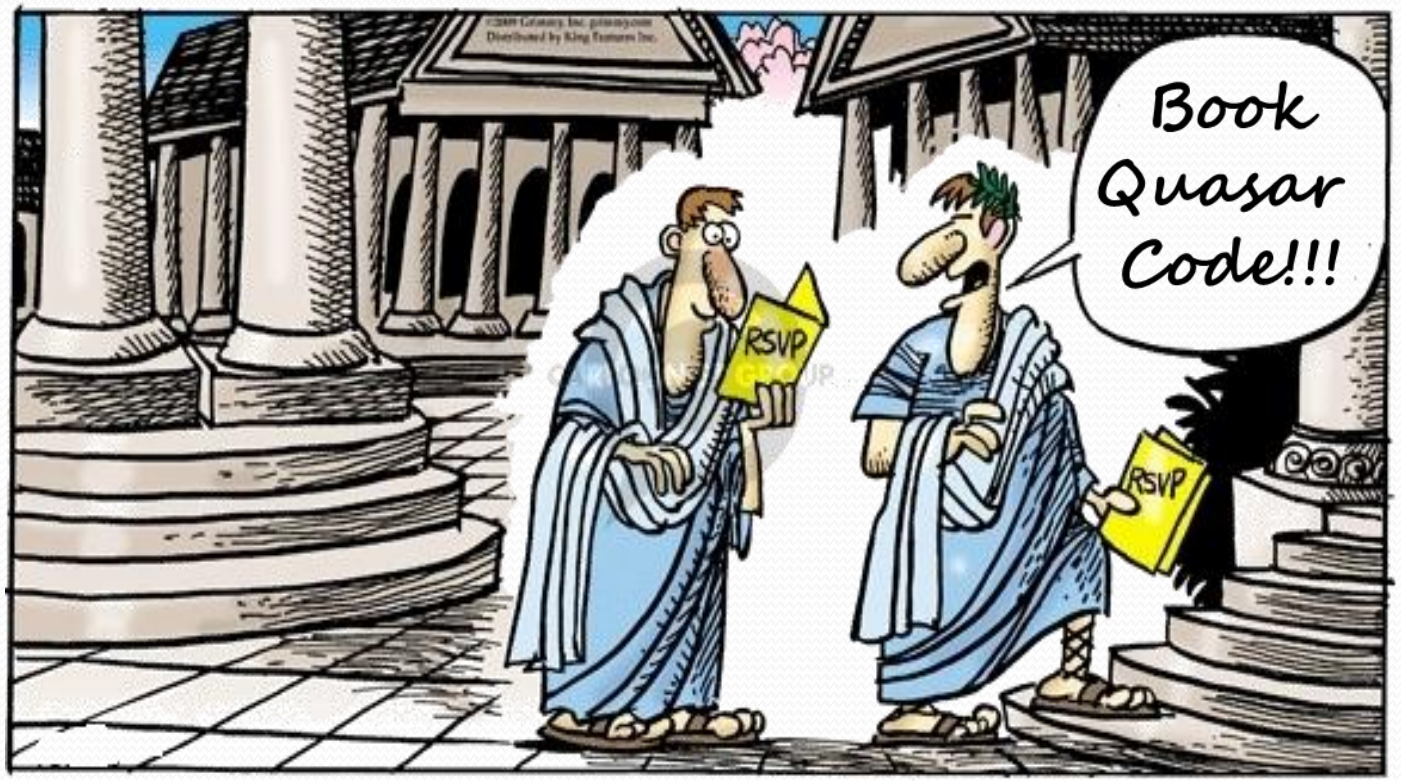
Data Security

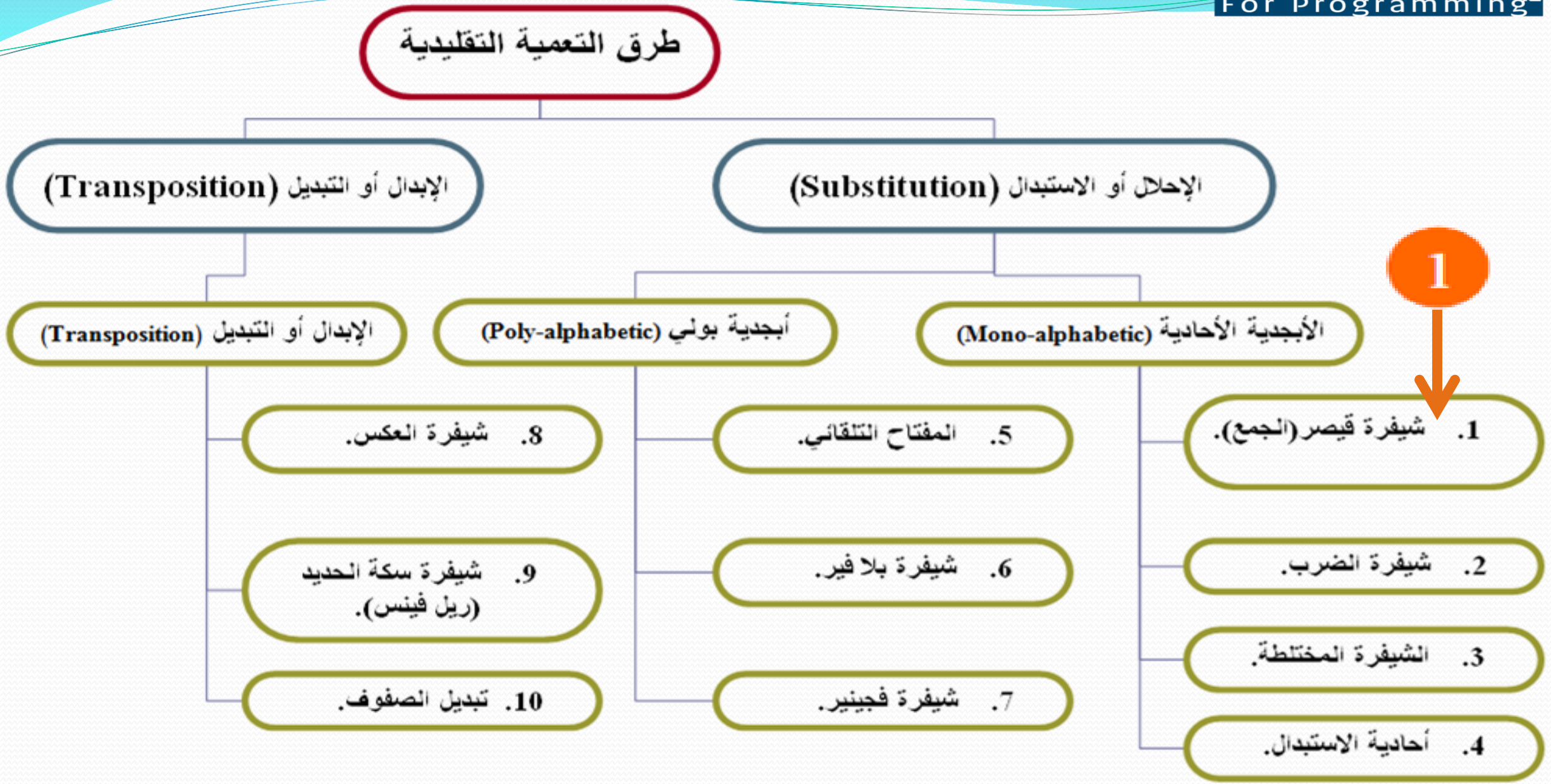
Lab “3”

Prepared by : Dr. Wathq Ahmed Ali Kawelah

Main Points

- **Substitution:**
  - **Mono-alphabetic.**
  - **Quasar Code.**
  - **Examples.**




طرق التعمية التقليدية
الإحلال أو الاستبدال (Substitution)
الإبدال أو التبديل (Transposition)
الأبجدية الأحادية (Mono-alphabetic)
أبجدية بولي (Poly-alphabetic)
الإبدال أو التبديل (Transposition)
1
1. شيفرة قيصر (الجمع).
2. شيفرة الضرب.
3. الشيفرة المختلطة.
4. أحادية الاستبدال.
5. المفتاح التلقائي.
6. شيفرة بلا فير.
7. شيفرة فجينير.
8. شيفرة العكس.
9. شيفرة سكة الحديد (ريل فينس).
10. تبديل الصفوف.

Substitution

- **شيفرة قيصر : يوليوس قيصر (الجمع).**

النص المشفر = النص الأصلي **+** مفتاح التشفير (باقي القسمة) على العدد الكلي للحروف.

- **فك شيفرة قيصر : يوليوس قيصر (الجمع).**

النص الأصلي = النص المشفر **–** مفتاح التشفير (باقي القسمة) على العدد الكلي للحروف.

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
Ciphertext →	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
Value →	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Example “1”

Original Text (Key = D) :

BOOK

Cipher Text = ????

Solution "1"

Original Text	B	O	O	K
Original Text Value	1	14	14	10
Key Value	3	3	3	3
Original Text Value + Key Value	4	17	17	13
Cipher Text	E	R	R	N

Key = D = 3

ERRN

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
Ciphertext →	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
Value →	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Cipher Text	E	R	R	N
Cipher Text Value	4	17	17	13
Key Value	3	3	3	3
Cipher Text Value - Key Value	1	14	14	10
Original Text	B	O	O	K

Key = D = 3

BOOK

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
Ciphertext →	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
Value →	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Example "2"

Original Text (Key = U) :

LABONE

Cipher Text = ????

Solution "2"

Original Text	L	A	B	O	N	E
Original Text Value	11	0	1	14	13	4
Key Value	20	20	20	20	20	20
Original Text Value + Key Value	31	20	21	34	33	24
Cipher Text	F	U	V	I	H	Y

Key = U = 20

FUVIHY

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
Ciphertext →	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
Value →	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Cipher Text	F	U	V	I	H	Y
Cipher Text Value	5	20	21	8	7	24
Key Value	20	20	20	20	20	20
Cipher Text Value - Key Value	-15	0	1	-12	-13	4
Original Text	L	A	B	O	N	E

Key = U = 20

LABONE

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
Ciphertext →	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
Value →	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Label

Button

Text Box

```
private void textBox1_TextChanged(object sender, EventArgs e)
{
textBox1.CharacterCasing = CharacterCasing.Upper;
}
```

```
private void textBox2_TextChanged(object sender, EventArgs e)
{ }
```

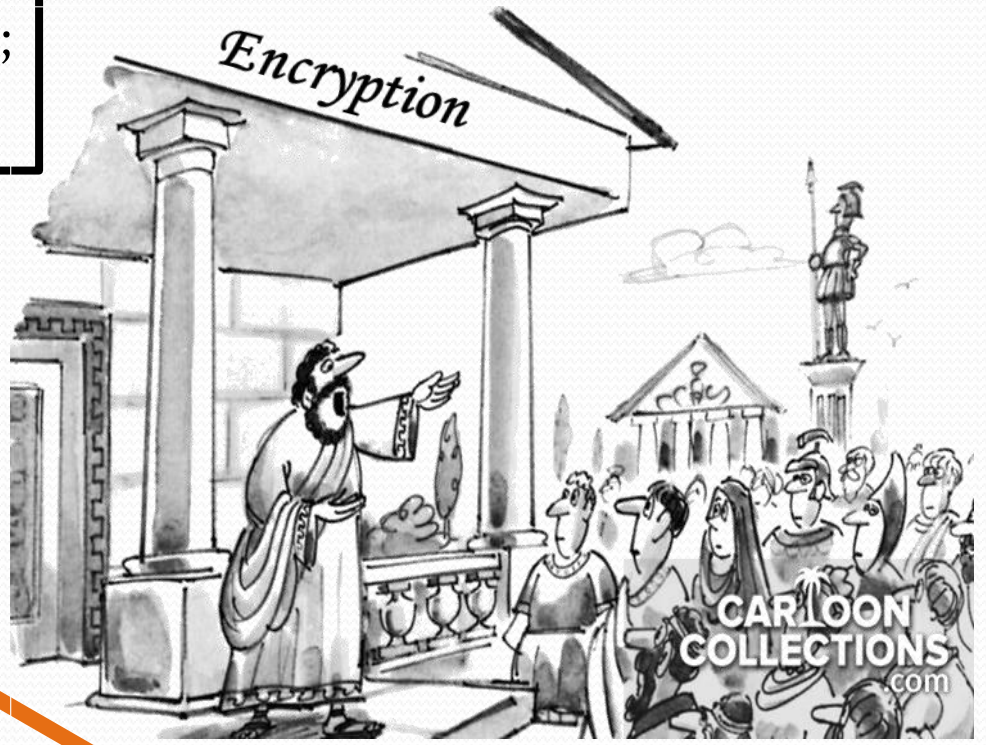
```
private void button1_Click(object sender, EventArgs e)
{       if (Convert.ToInt16(textBox2.Text) <= 25 && Convert.ToInt16(textBox2.Text) >= 1)
        {  textBox3.Text = en(textBox1.Text, Convert.ToInt16(textBox2.Text));   }
        else
        { MessageBox.Show("The key must be between 1 to 25"); }
}
```


```
private void textBox3_TextChanged(object sender, EventArgs e)
{ }
```

1

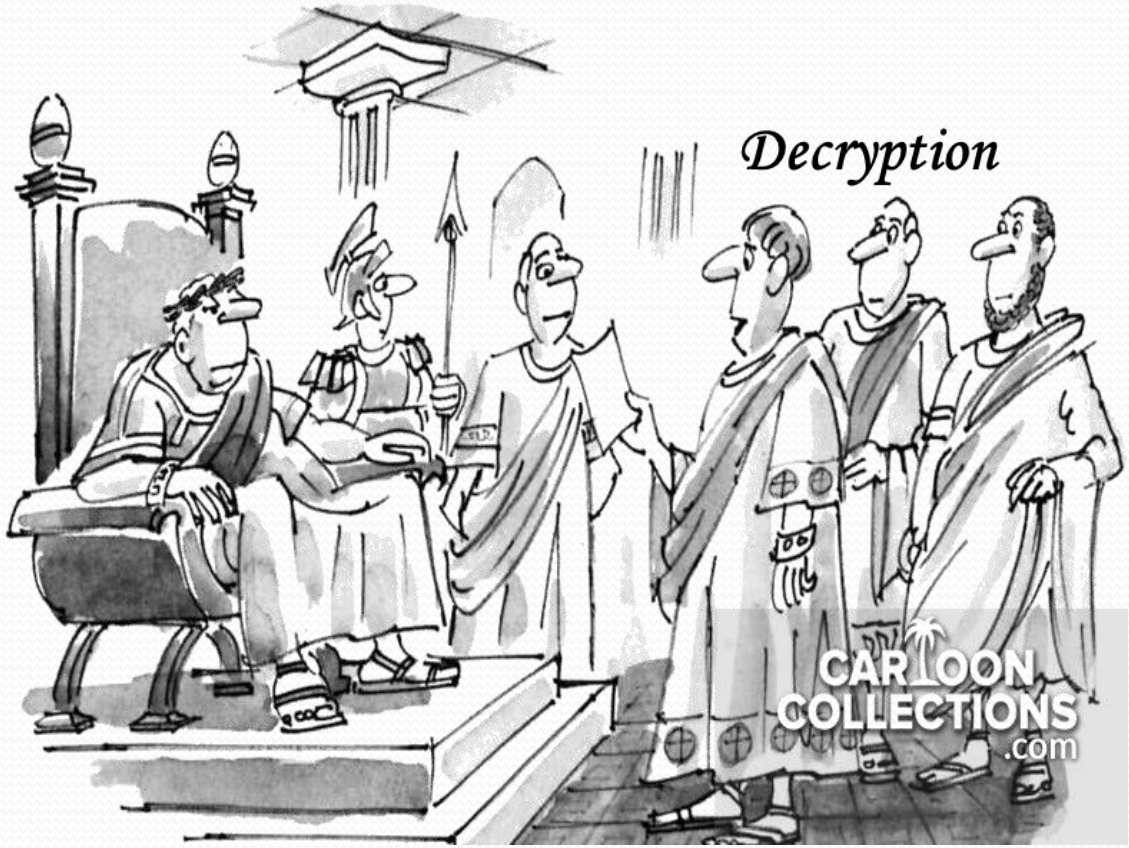
```
string en(string ortext, int k)
{
StringBuilder entext = new StringBuilder();
foreach (char ac in ortext)
{
entext.Append((char)(((int)ac - 65 + k) % 26 + 65));
}
return (entext.ToString());
}
```

```
private void button2_Click(object sender, EventArgs e)
{
textBox4.Text = de(textBox3.Text, Convert.ToInt16(textBox2.Text));
}
```




```
private void button3_Click(object sender, EventArgs e)
        {       Application.Exit();          }
```

```
private void textBox4_TextChanged(object sender, EventArgs e)
                                        { }
```



2

```
string de(string ctext, int k)
{
StringBuilder detext = new StringBuilder();
foreach (char ac in ctext)
{
detext.Append((char)(((int)ac - 65 - (k - 26)) % 26 + 65));
}
return (detext.ToString());
}
```


شفرة قيصر
النص الاصلي
المفتاح
LABONE
20
تشفير
النص المشفر
FUVIHY
فك التشفير
النص الاصلي
LABONE
خروج من البرنامج


شفرة قيصر
النص الاصلي
المفتاح
BOOK
3
تشفير
النص المشفر
ERRN
فك التشفير
النص الاصلي
BOOK
خروج من البرنامج

Thank you for Listening!