

Vigenere Algorithm

DATA SECURITY (CS DIPLOMA)

Definition

Vigenere Cipher is a method of encrypting alphabetic text.
It uses a simple form of alphabetic substitution.

Algorithm Formula

Substitute letters as numbers: [A=0, B=1, C=2, ..., Z=25]

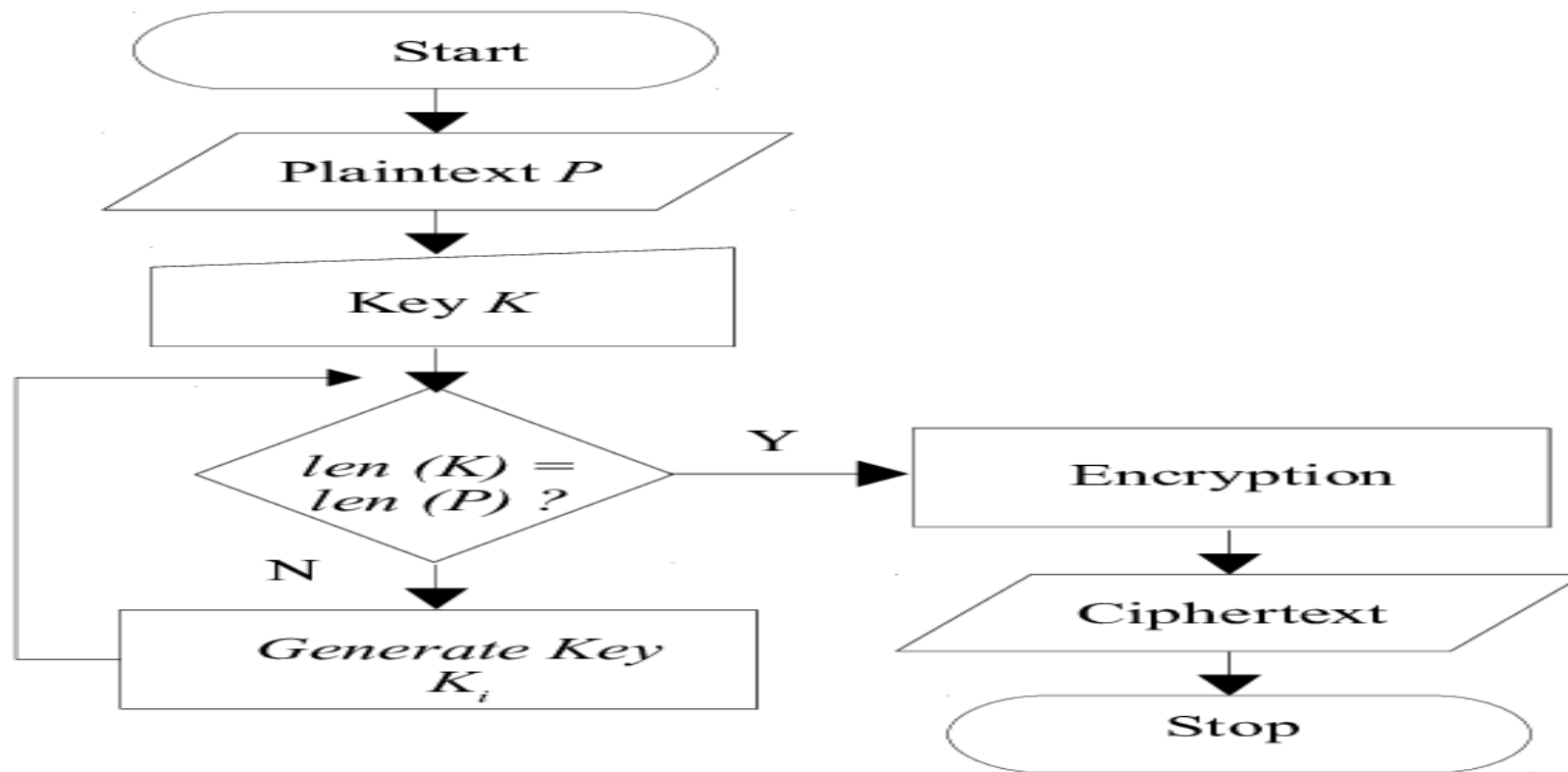
Encryption:

$$C = E(P) = (P+K) \pmod{26}$$

Decryption:

$$P = D(C) = (C-K) \pmod{26}$$

Algorithm Process



Algorithm Process

Encryption:

- 1- Divide message and Key to letters.
- 2- Convert each letter to number as per previous slide.
- 3- Apply Encryption algorithm function on each letter to substitute it with a new letter.

Decryption:

- 1- Divide Cipher and Key to letters.
- 2- Convert each letter to number as per previous slide.
- 3- Apply Decryption algorithm function on each letter to substitute it with a new letter.

English alphabetic program

- 1- User enter key in Key Field.
- 2- User enter message in Enter Message Field.
- 3- User Press Encrypt.
- 4-Encrypt button has event to do the following:
 - * Get Key and store it keyword.
 - * Get Message and store it str.
 - * For Loop to delete space in str.
 - * Keyword and str send to keygenerator function.
 - * Encrypt message through CipherText Function
- 5- Decrypt button to call original text function.

Enter Message

Key "Key Length Shall be less than message length"

Encrypt

Encrypted Message

Decrypted Message

Example No. 1

Encrypt Message “This Course Name is Data Security” with key “password”.

Solution:

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
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

Encryption:

$$C = E(P) = (P+K) \pmod{26}$$

Message length = 28

Key = “passwordpasswordpasswordpass”

Example No. 1

19	7	8	18	2	14	20	17	18	4	13	0	12	4	8	18	3	0	19	0	18	4	2	20	17	8	19	24
T	H	I	S	C	O	U	R	S	E	N	A	M	E	I	S	D	A	T	A	S	E	C	U	R	I	T	Y
15	0	18	18	22	14	17	3	15	0	18	18	22	14	17	3	15	0	18	18	22	14	17	3	15	0	18	18
P	A	S	S	W	O	R	D	P	A	S	S	W	O	R	D	P	A	S	S	W	O	R	D	P	A	S	S
34	7	26	36	24	28	37	20	33	4	31	18	34	18	25	21	18	0	37	18	40	18	19	23	32	8	37	42
%26																											
8	7	0	10	24	2	11	20	7	4	5	18	8	18	25	21	18	0	11	18	14	18	19	23	6	8	11	16
I	H	A	K	Y	C	L	U	H	E	F	S	I	S	Z	V	S	A	L	S	O	S	T	X	G	I	L	Q

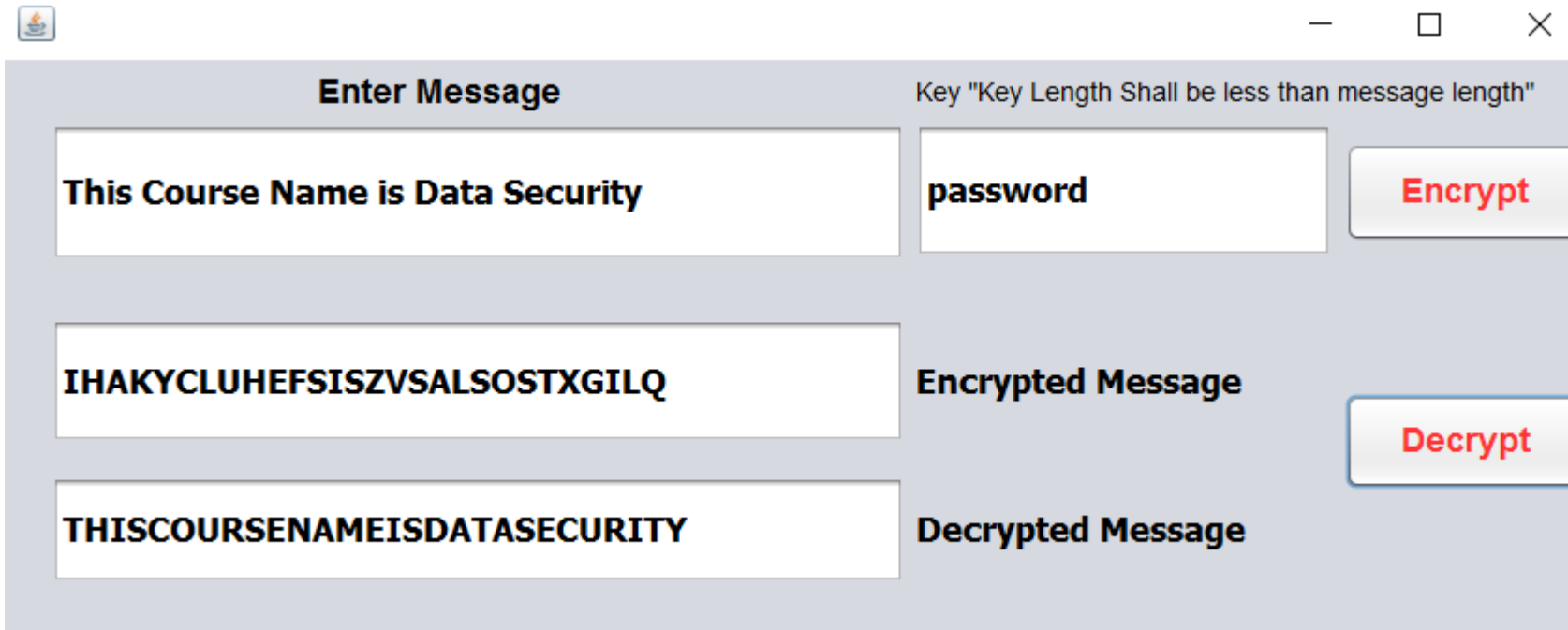
Example No. 1

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

Cipher Message: IHAKYCLUHEFSISZVSALSOSTXGILQ

Example No. 1

If We run Program will see the following Output:



The screenshot shows a Java Swing window titled "Enter Message" with standard window controls (minimize, maximize, close) in the top right corner. The window contains three text input fields on the left and two buttons on the right. The first input field contains the text "This Course Name is Data Security". The second input field contains the text "IHAKYCLUHEFSISZVSALSOSTXGILQ". The third input field contains the text "THISCOURSENAMEISDATASECURITY". The first button is labeled "Encrypt" in red text. The second button is labeled "Decrypt" in red text. Above the "Encrypt" button, there is a label "Key 'Key Length Shall be less than message length'". Below the "Encrypt" button, there is a label "Encrypted Message". Below the "Decrypt" button, there is a label "Decrypted Message".

Input	Output
This Course Name is Data Security	password
IHAKYCLUHEFSISZVSALSOSTXGILQ	Encrypted Message
THISCOURSENAMEISDATASECURITY	Decrypted Message

Example No. 2

Encrypt Message “We Hope to Get A Grade in This Course” with key “Secretpassword”.

Solution:

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
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

Encryption:

$$C = E(P) = (P+K) \pmod{26}$$

Message length = 29

Key = “SecretpasswordSecretpasswordS”

Example No. 2

22	4	7	14	15	4	19	14	6	4	19	6	17	0	3	4	0	8	13	19	7	8	18	2	14	20	17	18	4
W	E	H	O	P	E	T	O	G	E	T	G	R	A	D	E	A	I	N	T	H	I	S	C	O	U	R	S	E
18	4	2	17	4	19	15	0	18	18	22	14	17	3	18	4	2	17	4	19	15	0	18	18	22	14	17	3	18
S	E	C	R	E	T	P	A	S	S	W	O	R	D	S	E	C	R	E	T	P	A	S	S	W	O	R	D	S
40	8	9	31	19	23	34	14	24	22	41	20	34	3	21	8	2	25	17	38	22	8	36	20	36	34	34	21	22
%26																												
14	8	9	5	19	23	8	14	24	22	15	20	8	3	21	8	2	25	17	12	22	8	10	20	10	8	8	21	22
O	I	J	F	T	X	I	O	Y	W	P	U	I	D	V	I	C	Z	R	M	W	I	K	U	K	I	I	V	W

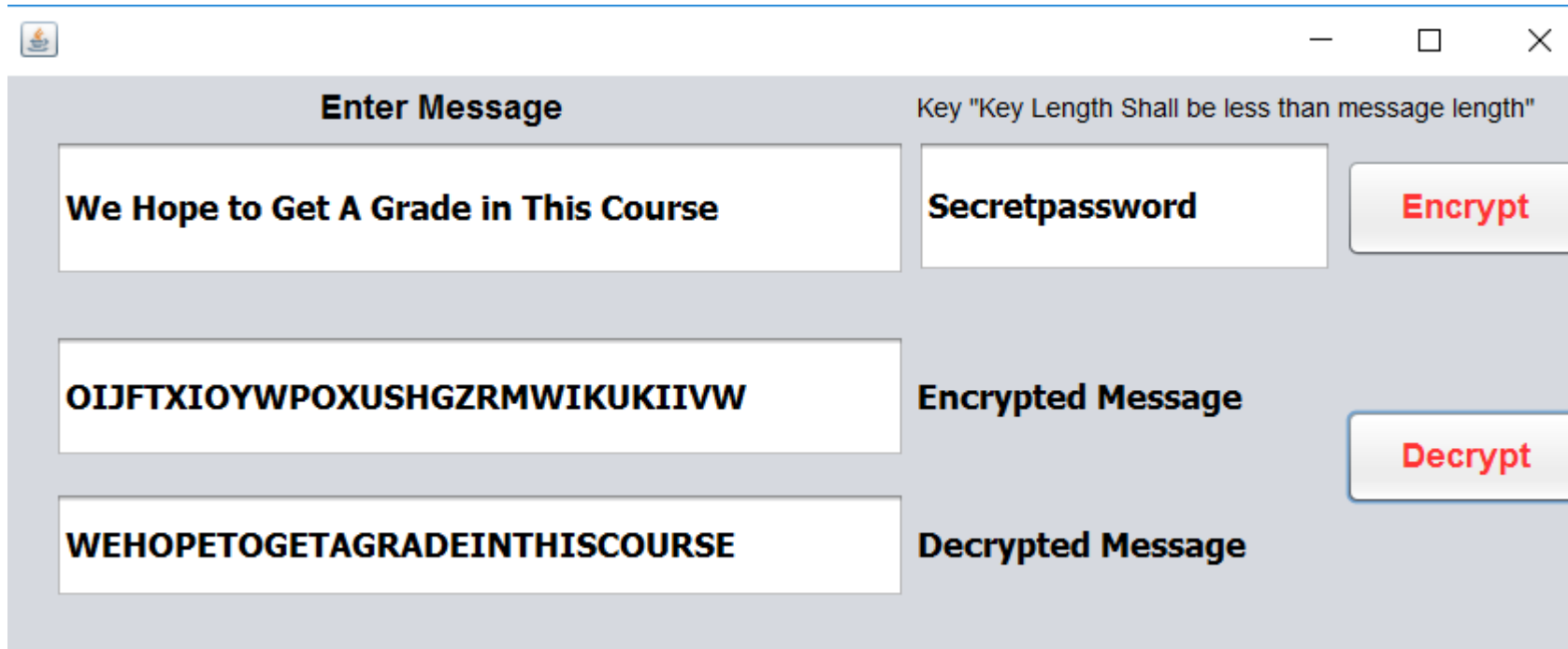
Example No. 2

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

Cipher Message: OIJFTXIOYWPUIDVICZRMWIKUKIIVW

Example No. 2

If We run Program will see the following Output:



The screenshot shows a Java Swing window with a title bar containing a small icon and standard window controls (minimize, maximize, close). The window has a light gray background and contains several text fields and buttons.

Enter Message

Key "Key Length Shall be less than message length"

We Hope to Get A Grade in This Course

Secretpassword

Encrypt

OIJFTXIOYWPOXUSHGZRMWIKUKIIVW

Encrypted Message

Decrypt

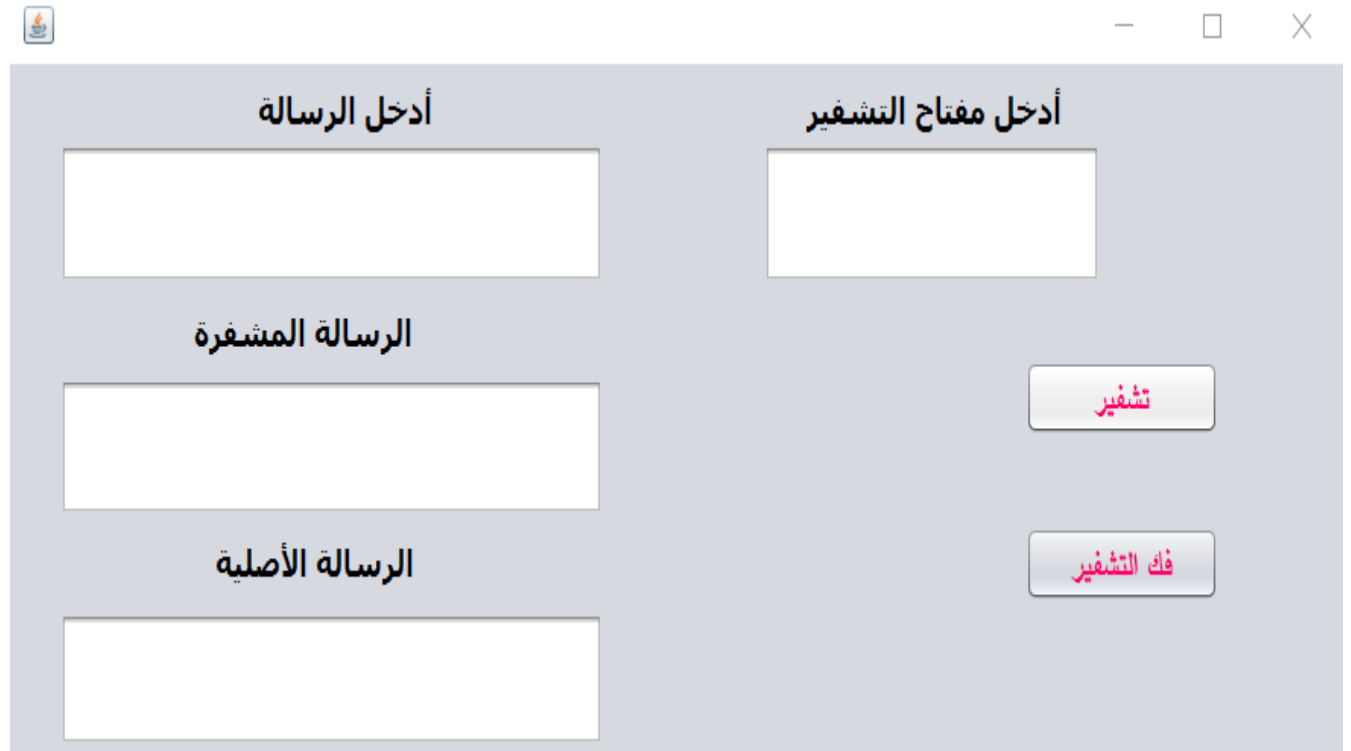
WEHOPETOGETAGRADEINTHISCOURSE

Decrypted Message

Arabic alphabetic program

In This Code we define all Arabic letters in array

We use modulus 31 to accept all Arabic letters and its shapes.



The screenshot shows a web application interface with a light gray background. At the top right, there are standard window control buttons: a minus sign, a square, and an 'X'. The interface is divided into two main sections. The left section is titled 'أدخل الرسالة' (Enter the message) and contains three input fields: the first is empty, the second is labeled 'الرسالة المشفرة' (The encrypted message), and the third is labeled 'الرسالة الأصلية' (The original message). The right section is titled 'أدخل مفتاح التشفير' (Enter the encryption key) and contains one input field. Below the input fields, there are two buttons: 'تشفير' (Encrypt) and 'فك التشفير' (Decrypt), both with red text. The entire interface is enclosed in a light gray border.

Example No. 1

Encrypt Message “أرسلت لك رسالة مهمة” with key “تشفير”.

Solution:

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

م ل ك ق ف غ ع ظ ط ض ص ش س ز ر ن د خ ح ج ث ت ب ا ا

26 27 28 29 30

ي و ه ن

Encryption:

$$C = E(P) = (P+K) \pmod{31}$$

Message length = 16

Key = “تشفير تشفير تشفيرت”

Example No. 1

4	25	27	25	4	24	1	13	11	23	24	3	24	13	11	0
ة	م	ه	م	ة	ل	ا	س	ر	ك	ل	ت	ل	س	ر	أ
3	11	30	21	14	3	11	30	21	14	3	11	30	21	14	3
ت	ر	ي	ف	ش	ت	ر	ي	ف	ش	ت	ر	ي	ف	ش	ت
7	36	57	46	18	27	12	43	32	37	27	14	54	34	25	3
%31															
7	5	26	15	18	27	12	12	1	6	27	14	23	3	25	3
ح	ث	ن	ص	ظ	ه	ز	ز	ا	ج	ه	ش	ك	ت	م	ت

Example No. 1

ة	م	ه	م	ة	ل	ا	س	ر	ك	ل	ت	ل	س	ر	أ
ت	ر	ي	ف	ش	ت	ر	ي	ف	ش	ت	ر	ي	ف	ش	ت
ح	ث	ن	ص	ظ	ه	ز	ز	ا	ج	ه	ش	ك	ت	م	ت

Cipher Message: تمتكشهاز ز هظصنثح

Example No. 1

If We run Program will see the following Output:



The screenshot shows a Windows-style application window with a title bar containing a small icon and standard minimize, maximize, and close buttons. The window is divided into two main sections. The left section is titled 'أدخل الرسالة' (Enter the message) and contains three text input fields. The first field contains the text 'أرسلت لك رسالة مهمة' (I sent you an important message). The second field is titled 'الرسالة المشفرة' (The encrypted message) and contains the text 'تمتكنش جهاز زهظ صنتح' (I couldn't get the device). The third field is titled 'الرسالة الأصلية' (The original message) and contains the text 'أرسلتلك رسالة مهمة' (I sent you an important message). The right section is titled 'أدخل مفتاح التشفير' (Enter the encryption key) and contains a single text input field with the text 'تشفير' (Encryption). Below this field are two buttons: 'تشفير' (Encrypt) and 'فك التشفير' (Decrypt).

Section	Field Title	Field Content
Left Panel	أدخل الرسالة	أرسلت لك رسالة مهمة
	الرسالة المشفرة	تمتكنش جهاز زهظ صنتح
	الرسالة الأصلية	أرسلتلك رسالة مهمة
Right Panel	أدخل مفتاح التشفير	تشفير
Buttons		تشفير, فك التشفير

Example No. 2

Encrypt Message "حافظ على نظافة بلدك" with key "سرية".

Solution:

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

م ل ك ق ف غ ع ظ ط ض ص ش س ز ر ن د خ ح ج ث ت ب ا ا

26 27 28 29 30

ي و ه ن

Encryption:

$$C = E(P) = (P+K) \pmod{31}$$

Message length = 16

Key = "سريةسريةسريةسرية"

Example No. 2

23	9	24	2	4	21	1	18	26	29	24	19	18	21	1	7
ك	د	ل	ب	ة	ف	ا	ظ	ن	ى	ل	ع	ظ	ف	ا	ح
4	30	11	13	4	30	11	13	4	30	11	13	4	30	11	13
ة	ي	ر	س	ة	ي	ر	س	ة	ي	ر	س	ة	ي	ر	س
27	39	35	15	8	51	12	31	30	59	35	32	22	51	12	20
%31															
27	8	4	15	8	20	12	0	30	28	4	1	22	20	12	20
ه	خ	ة	ص	خ	غ	ز	أ	ي	و	ة	ا	ق	غ	ز	غ

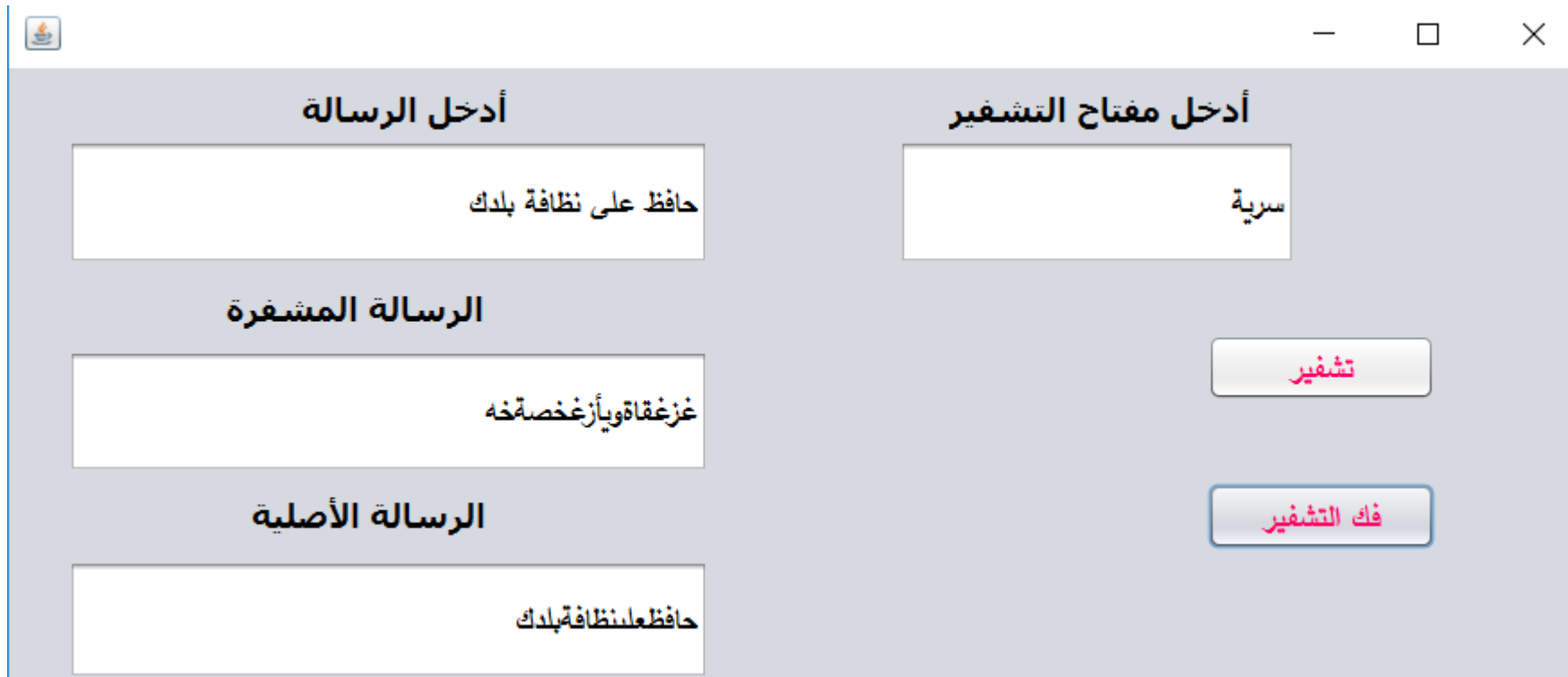
Example No. 2

ك	د	ل	ب	ة	ف	ا	ظ	ن	ى	ل	ع	ظ	ف	ا	ح
ة	ي	ر	س	ة	ي	ر	س	ة	ي	ر	س	ة	ي	ر	س
ه	خ	ة	ص	خ	غ	ز	أ	ي	و	ة	ا	ق	غ	ز	غ

Cipher Message: غز غقاةويأز غخصةه

Example No. 2

If We run Program will see the following Output:



The screenshot shows a Windows-style application window with a title bar containing a small icon and standard minimize, maximize, and close buttons. The window is divided into two main sections. The left section is titled 'أدخل الرسالة' (Enter the message) and contains three text input fields. The first field contains the text 'حافظ على نظافة بلدك' (Keep your country clean). The second field is titled 'الرسالة المشفرة' (Encrypted message) and contains the text 'غزغقة ويا ز غخصة ذه' (Gzegha and ya z ghassha dha). The third field is titled 'الرسالة الأصلية' (Original message) and contains the text 'حافظ على نظافة بلدك' (Keep your country clean). The right section is titled 'أدخل مفتاح التشفير' (Enter the encryption key) and contains a single text input field with the text 'سرية' (Secret). Below this field are two buttons: 'تشفير' (Encrypt) and 'فك التشفير' (Decrypt).

Section	Field Title	Field Content
Left Panel (Message)	أدخل الرسالة	حافظ على نظافة بلدك
	الرسالة المشفرة	غزغقة ويا ز غخصة ذه
	الرسالة الأصلية	حافظ على نظافة بلدك
Right Panel (Key)	أدخل مفتاح التشفير	سرية
	Buttons	تشفير, فك التشفير