



دانشگاه صنعتی اصفهان  
دانشکده مهندسی برق و کامپیوتر

عنوان: تکلیف اول درس مبانی رمزنگاری

نام و نام خانوادگی: علیرضا ابره فروش

شماره دانشجویی: ۹۸۱۶۶۰۳

نیم سال تحصیلی: بهار ۱۴۰۲/۱۴۰۱

مدرس: دکتر سیدمحمد دخیل علیان

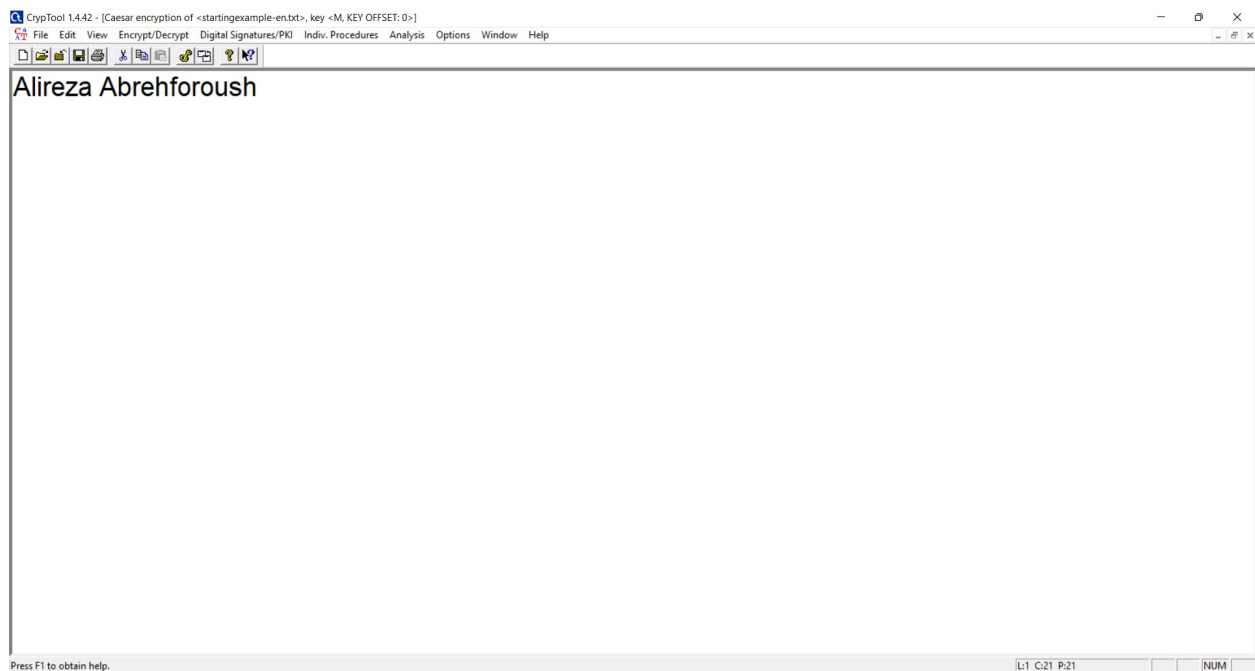
دستیاران آموزشی: گلاره عودی قدیم

## ۱.۱ a

کلید Caesar cipher برابر M است که حرف ۱۳ام الفبای انگلیسی است. پس در واقع هر حرفِ الفبا به صورت حلقوی ۱۲ واحد شیفت می‌خورد. پس در نهایت به صورت زیر رمز می‌شود.

x	A	l	i	r	e	z	a		A	b	r	e	h	f	o	r	o	u	s	h
$E_{12}(x)$	M	x	u	d	q	l	m		M	n	d	q	t	r	a	d	a	g	e	t

در نرم افزار CrypTool به صورت زیر رمز می‌کنیم.




شکل ۱

Key Entry: Caesar / ROT-13

**Description**  
 Here you can enter the key for the Caesar cipher.  
 Caesar is a mono-alphabetic substitution, where the characters of the cleartext alphabet are mapped to the ciphertext alphabet by shifting. This shifting value is the key. You can enter the key as a number or as a single character of the alphabet.  
 Rot-13 is a special variant, where the key has the fixed value of half the length of the cleartext alphabet. This variant is only selectable if the length of the alphabet is an even number.

**Select variant**  
☒ Caesar  
☐ Rot-13

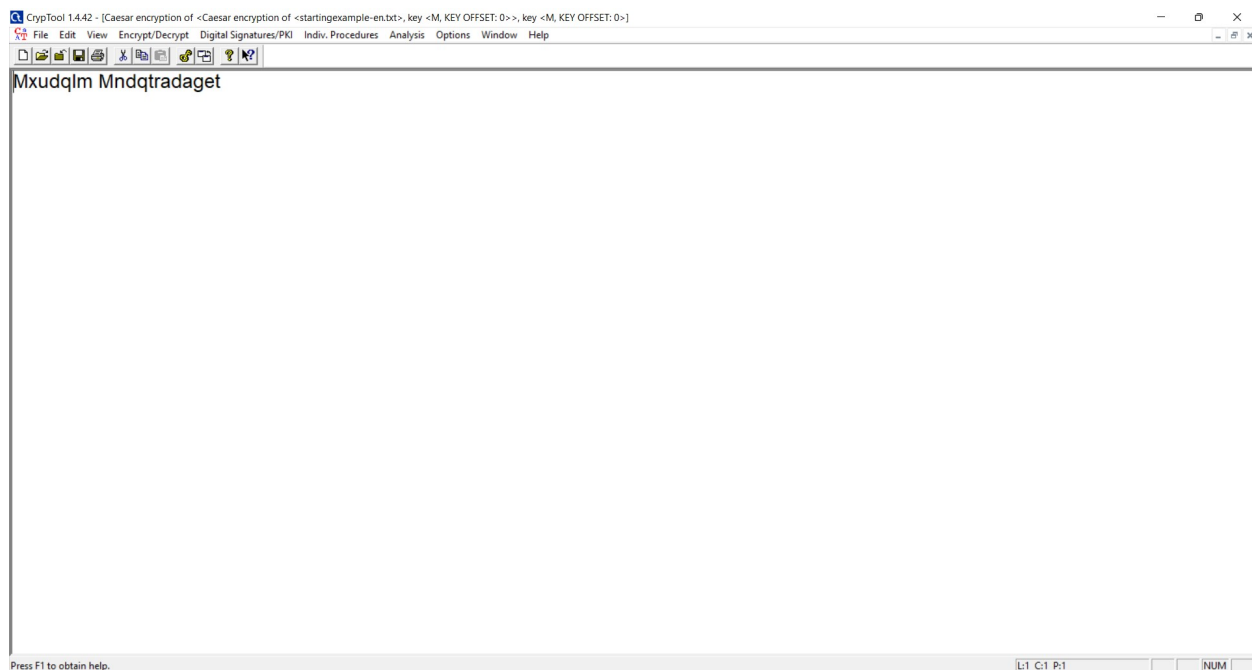
**Options to interpret the alphabet characters**  
☒ Value of the first alphabet character = 0 (e.g. "A"=0)  
☐ Value of the first alphabet character = 1 (e.g. "A"=1)

**Key entry as**  
☒ Alphabet character    
☐ Number value

**Properties of the chosen encryption**  
 Shift of 12  
 Mapping of the alphabet (26 characters)  
 from: ABCDEFGHIJKLMNOPQRSTUVWXYZ  
 to: MNOPQRSTUVWXYZABCDEFGHIJKL

Encrypt Decrypt Text options Cancel

شکل ۲



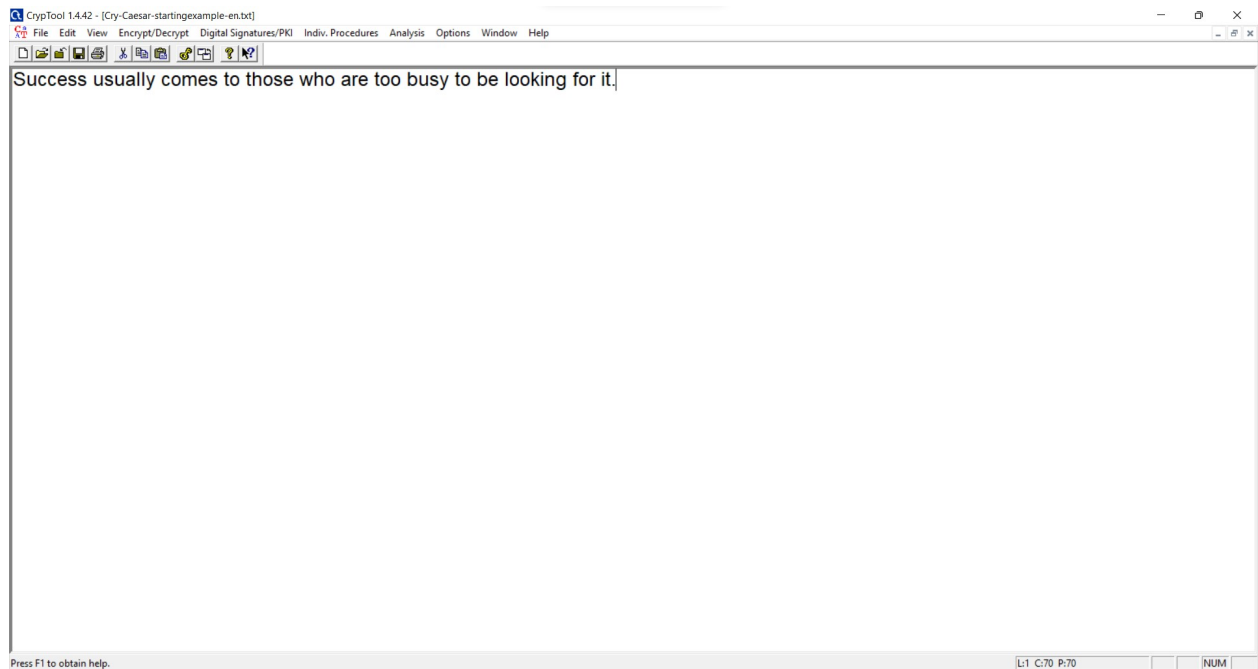
شکل ۳

$$9816603 \equiv 17 \pmod{26}$$

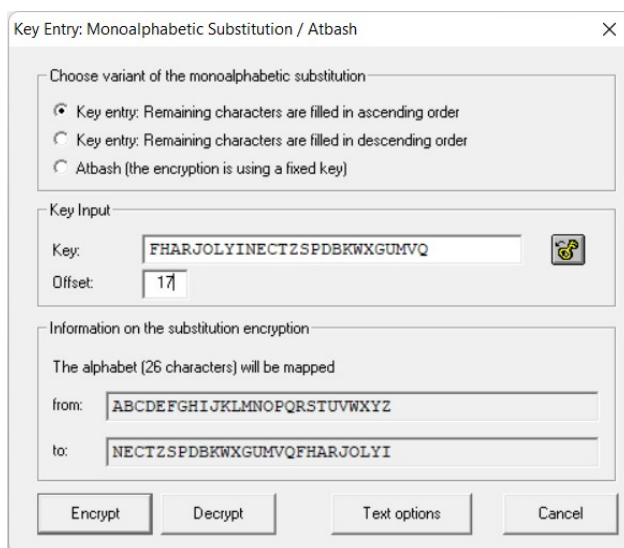
کلید Substitution cipher برابر fharjolyinctzspdbkwxgumvq و offset آن برابر ۱۷ است. در واقع الفبای انگلیسی به ترتیب به NECTZSPDBKWXGUMVQFHARJOLYI map می‌شود. پس در نهایت به صورت زیر رمز می‌شود.

x	S	u	c	c	e	s	s	u	s	u	a	l	l	y	c	o	m	e	s	t	o	t	h	o	s	e	w	h	o	a	r	e	t	o	o	b	u	s	y	t	o	b	e	l	o	o	k	i	n	g	f	o	r	i	t	.
E(x)	H	r	c	c	z	h	h	r	h	r	n	x	x	y	c	m	g	z	h	a	m	a	d	m	h	z	o	d	m	n	f	z	a	m	m	e	r	h	y	a	m	e	z	x	m	m	w	b	u	p	s	m	f	b	a	.

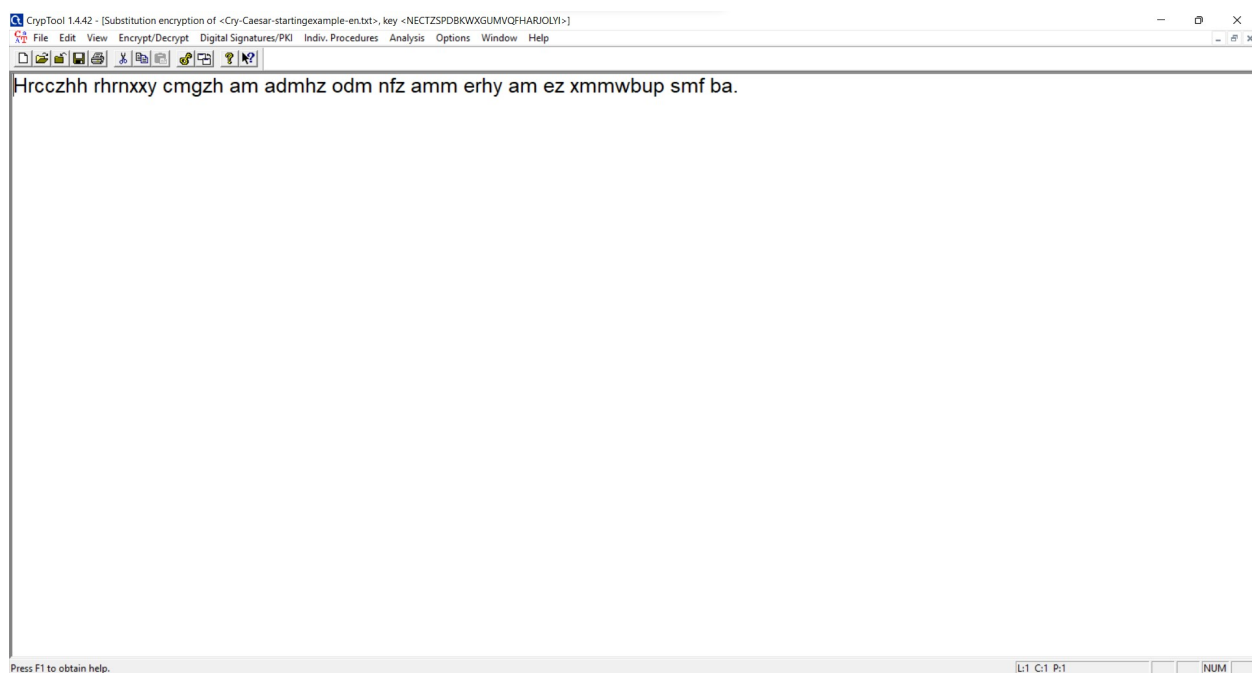
در نرم افزار CrypTool به صورت زیر رمز می‌کنیم.



شکل ۴



شکل ۵



شکل ۶

۳

۱.۳ a

در Vigenère cipher در الفبای انگلیسی از یک جدول با ابعاد  $26 \times 26$  استفاده می‌شود که در سطر  $i$ ام آن حروف انگلیسی به ترتیب به صورت حلقوی با شروع از حرف  $i$ ام الفبا نوشته شده است.

	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	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

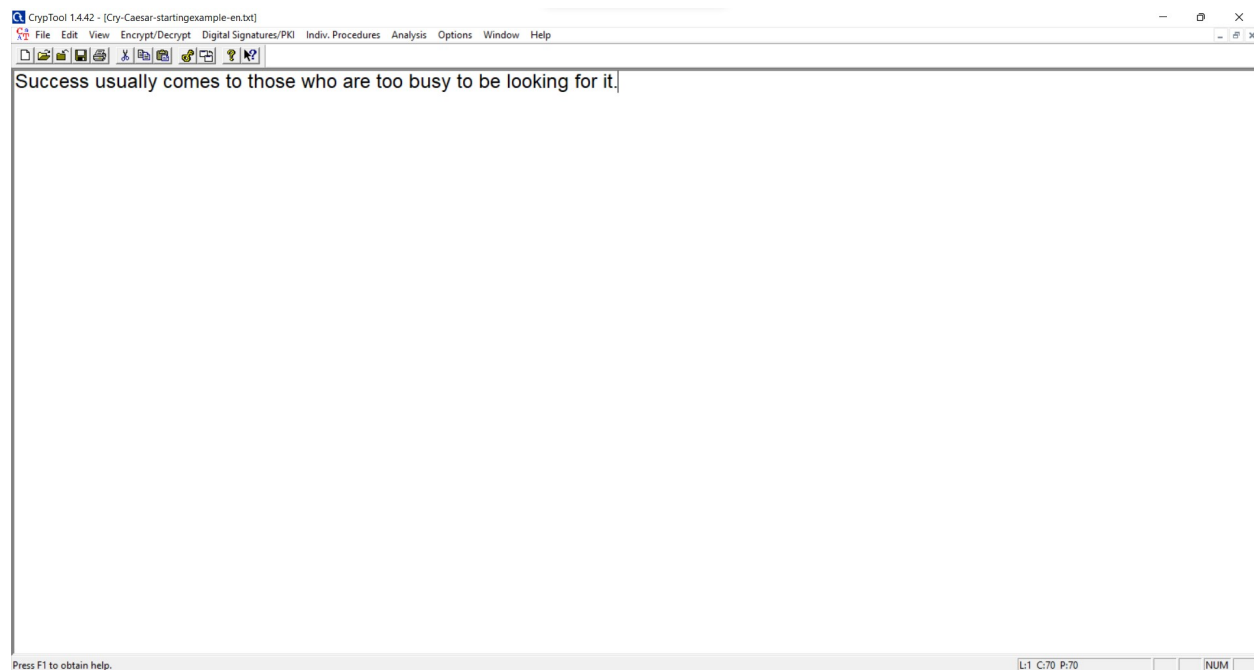
همچنین کلید مورد استفاده در این الگوریتم به صورت زیر (سه حرف اول نام + سه حرف اول نام خانوادگی) ساخته می‌شود.

$$ALIREZA\ ABREHFOROUSH \Rightarrow key = ALIABR$$

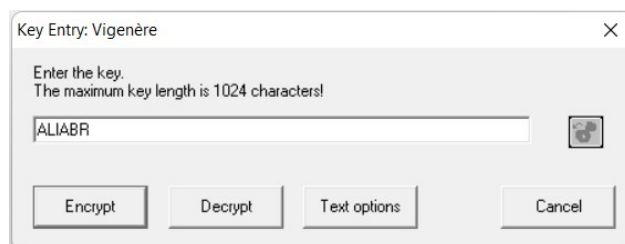
حال  $key$  را مکرراً تکرار می‌کنیم تا طول آن برابر طول رشته‌ای که می‌خواهیم آن را رمز کنیم بشود (یا به عبارتی کاراکتر نظیر باقیمانده‌ی  $i$  به پیمانه‌ی طول کلید (۶) را در کلید به دست آوریم). برای رمز کردن کاراکتر  $ham$  در رشته، کاراکترِ اندیسِ باقیمانده‌ی  $i$  به پیمانه‌ی طول کلید (۶) در کلید ( $key_i$ ) به همراه خود کاراکترِ  $ham$  ( $x_i$ ) به دست می‌آوریم.  $cipher_i$  نظیر  $x_i$  برابر کاراکتر قرار گرفته در سطر  $key_i$  و ستون  $x_i$  است.

[illegible]

در نرم افزار CrypTool به صورت زیر رمز می کنیم.



شکل ۷



شکل ۸



شکل ۹

منابع