



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

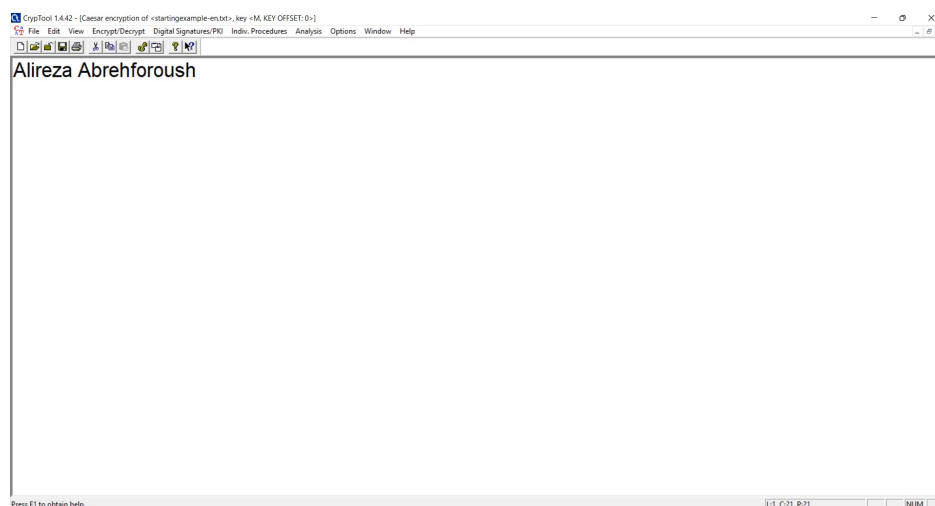
۱

۱.۱ 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

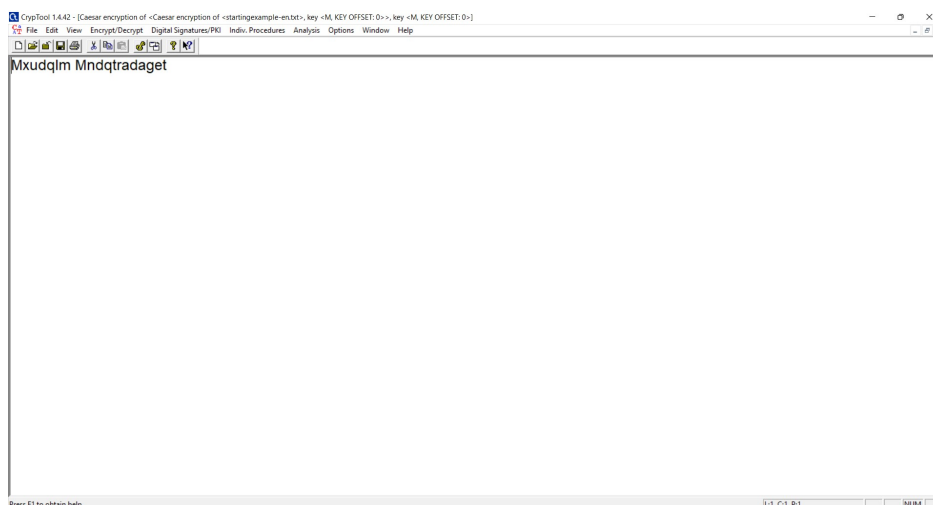
Options to interpret the alphabet characters
☒ Value of the first alphabet character = 0 (e.g. "A"=0)
☐ Value of the first alphabet character = 1 (e.g. "A"=1)

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

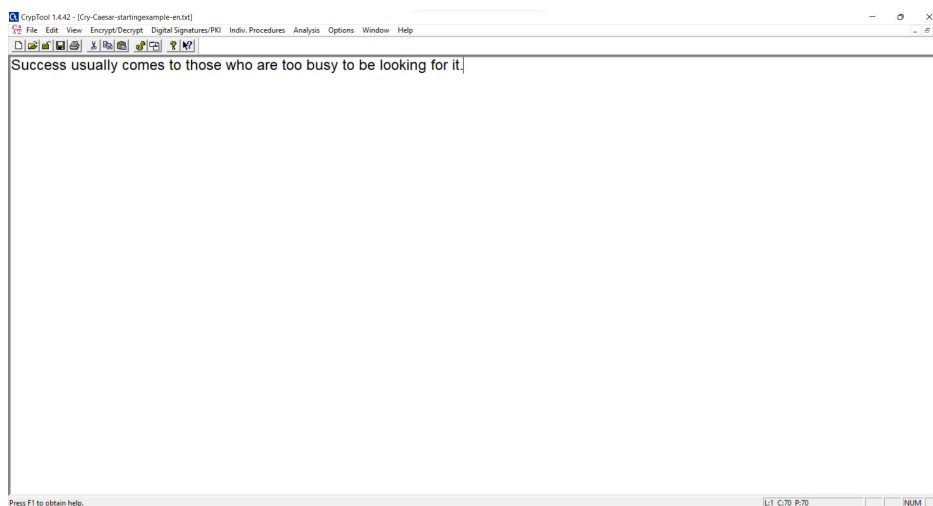
۲

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

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

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

در نرم افزار CrypTool به صورت زیر رمز می‌کنیم.




شکل ۴

Key Entry: Monoalphabetic Substitution / Atbash

Choose variant of the monoalphabetic substitution

- ☒ Key entry: Remaining characters are filled in ascending order
- ☐ Key entry: Remaining characters are filled in descending order
- ☐ Atbash (the encryption is using a fixed key)

Key Input

Key: 

Offset:

Information on the substitution encryption

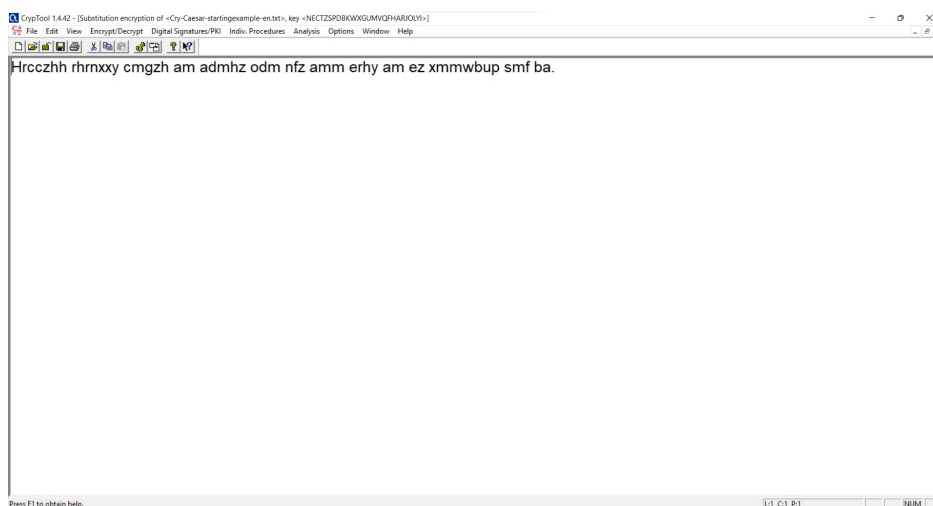
The alphabet (26 characters) will be mapped

from:

to:

Encrypt Decrypt Text options Cancel

شکل ۵

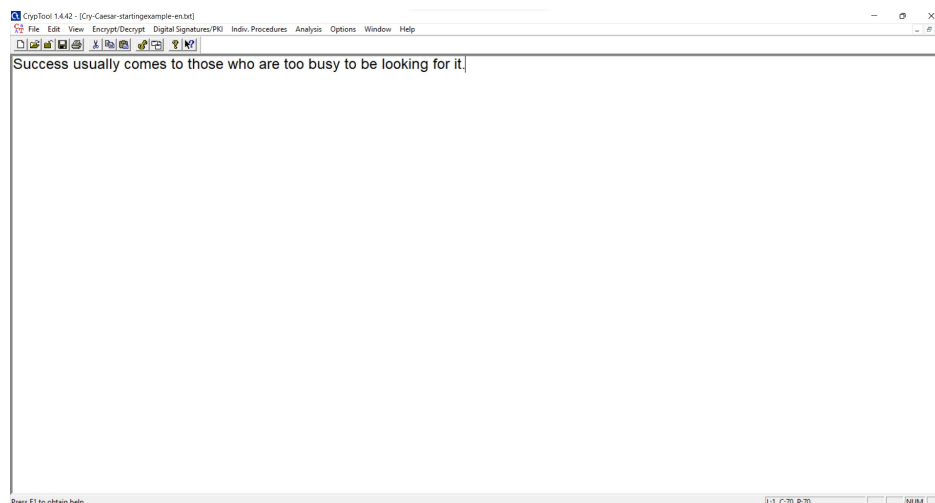


شکل ۶

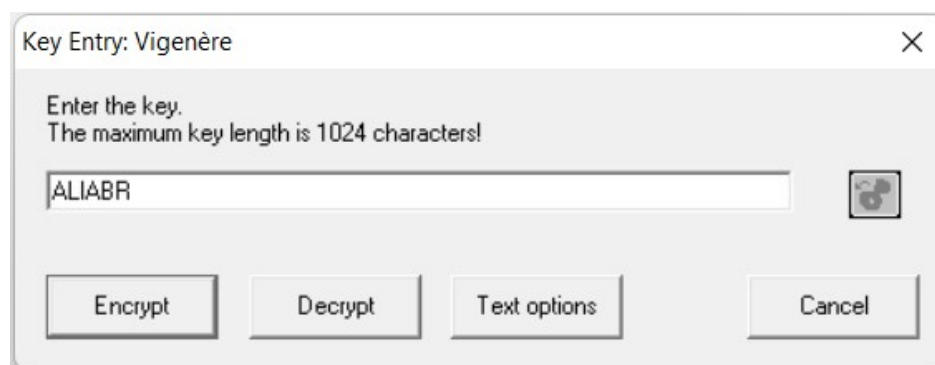
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y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

[illegible]

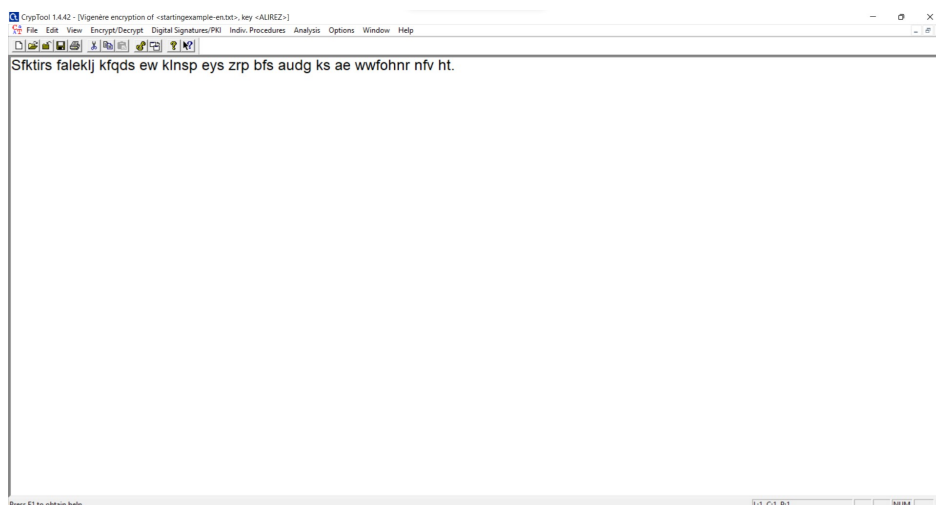
در نرم افزار CrypTool به صورت زیر رمز می کنیم.



شکل ۷



شکل ۸



شکل ۹

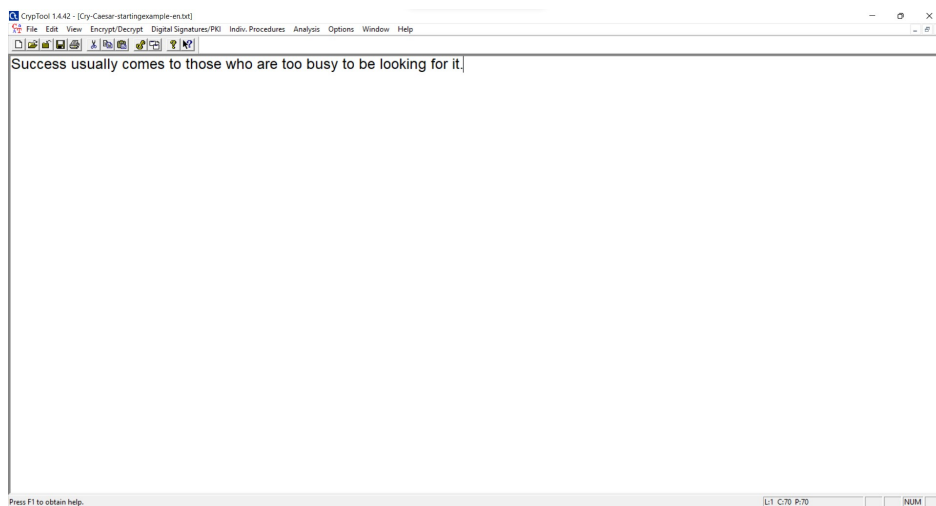
۲.۳ b

مشابه قسمت قبل (صرفاً تغییر کلید) داریم:

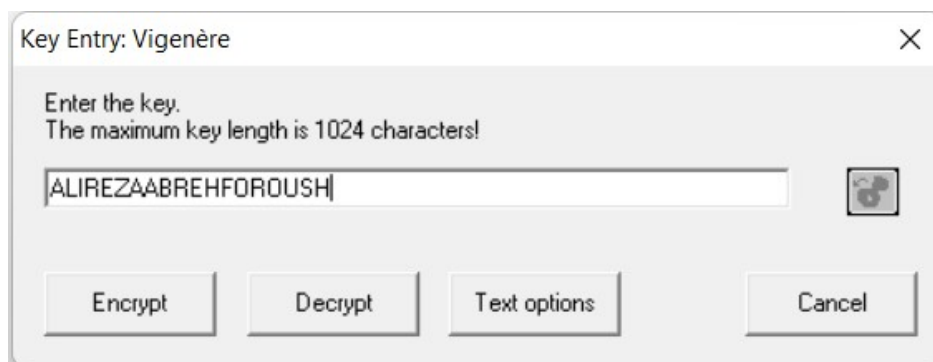
$$ALIREZA ABREHFOROUSH \Rightarrow key = ALIREZAABREHFOROUSH$$

key	A	l	i	r	e	z	a	a	b	r	e	h	f	o	r	o	u	s	h	a	l	i	r	e	z	a	a	b	r	e	h	f	o	r	o	u	s	h	a	l	i	r	e	z	a	a	b	r	e	h	f	o	r	o	u	s	h	a	l	i	r	e	z	a	a	b	r	e	h	f	o	r	o	u	s	h	a	l	i	r	e	z	a	a	b	r	e	h	f	o	r	o	u	s	h	a	l	i	r	e	z	a	a	b	r	e	h	f	o	r	o	u	s	h	a	l	i	r	e	z	a	a	b	r	e	h	f	o	r	o	u	s	h	a	l	i	r	e	z	a	a	b	r	e	h	f	o	r	o	u	s	h	a	l	i	r	e	z	a	a	b	r	e	h	f	o	r	o	u	s	h	a	l	i	r	e	z	a	a	b	r	e	h	f	o	r	o	u	s	h	a	l	i	r	e	z	a	a	b	r	e	h	f	o	r	o	u	s	h	a	l	i	r	e	z	a	a	b	r	e	h	f	o	r	o	u	s	h	a	l	i	r	e	z	a	a	b	r	e	h	f	o	r	o	u	s	h	a	l	i	r	e	z	a	a	b	r	e	h	f	o	r	o	u	s	h	a	l	i	r	e	z	a	a	b	r	e	h	f	o	r	o	u	s	h	a	l	i	r	e	z	a	a	b	r	e	h	f	o	r	o	u	s	h	a	l	i	r	e	z	a	a	b	r	e	h	f	o	r	o	u	s	h	a	l	i	r	e	z	a	a	b	r	e	h	f	o	r	o	u	s	h	a	l	i	r	e	z	a	a	b	r	e	h	f	o	r	o	u	s	h	a	l	i	r	e	z	a	a	b	r	e	h	f	o	r	o	u	s	h	a	l	i	r	e	z	a	a	b	r	e	h	f	o	r	o	u	s	h	a	l	i	r	e	z	a	a	b	r	e	h	f	o	r	o	u	s	h	a	l	i	r	e	z	a	a	b	r	e	h	f	o	r	o	u	s	h	a	l	i	r	e	z	a	a	b	r	e	h	f	o	r	o	u	s	h	a	l	i	r	e	z	a	a	b	r	e	h	f	o	r	o	u	s	h	a	l	i	r	e	z	a	a	b	r	e	h	f	o	r	o	u	s	h	a	l	i	r	e	z	a	a	b	r	e	h	f	o	r	o	u	s	h	a	l	i	r	e	z	a	a	b	r	e	h	f	o	r	o	u	s	h	a	l	i	r	e	z	a	a	b	r	e	h	f	o	r	o	u	s	h	a	l	i	r	e	z	a	a	b	r	e	h	f	o	r	o	u	s	h	a	l	i	r	e	z	a	a	b	r	e	h	f	o	r	o	u	s	h	a	l	i	r	e	z	a	a	b	r	e	h	f	o	r	o	u	s	h	a	l	i	r	e	z	a	a	b	r	e	h	f	o	r	o	u	s	h	a	l	i	r	e	z	a	a	b	r	e	h	f	o	r	o	u	s	h	a	l	i	r	e	z	a	a	b	r	e	h	f	o	r	o	u	s	h	a	l	i	r	e	z	a	a	b	r	e	h	f	o	r	o	u	s	h	a	l	i	r	e	z	a	a	b	r	e	h	f	o	r	o	u	s	h	a	l	i	r	e	z	a	a	b	r	e	h	f	o	r	o	u	s	h	a	l	i	r	e	z	a	a	b	r	e	h	f	o	r	o	u	s	h	a	l	i	r	e	z	a	a	b	r	e	h	f	o	r	o	u	s	h	a	l	i	r	e	z	a	a	b	r	e	h	f	o	r	o	u	s	h	a	l	i	r	e	z	a	a	b	r	e	h	f	o	r	o	u	s	h	a	l	i	r	e	z	a	a	b	r	e	h	f	o	r	o	u	s	h	a	l	i	r	e	z	a	a	b	r	e	h	f	o	r	o	u	s	h	a	l	i	r	e	z	a	a	b	r	e	h	f	o	r	o	u	s	h	a	l	i	r	e	z	a	a	b	r	e	h	f	o	r	o	u	s	h	a	l	i	r	e	z	a	a	b	r	e	h	f	o	r	o	u	s	h	a	l	i	r	e	z	a	a	b	r	e	h	f	o	r	o	u	s	h	a	l	i	r	e	z	a	a	b	r	e	h	f	o	r	o	u	s	h	a	l	i	r	e	z	a	a	b	r	e	h	f	o	r	o	u	s	h	a	l	i	r	e	z	a	a	b	r	e	h	f	o	r	o	u	s	h	a	l	i	r	e	z	a	a	b	r	e	h	f	o	r	o	u	s	h	a	l	i	r	e	z	a	a	b	r	e	h	f	o	r	o	u	s	h	a	l	i	r	e	z	a	a	b	r	e	h	f	o	r	o	u	s	h	a	l	i	r	e	z	a	a	b	r	e	h	f	o	r	o	u	s	h	a	l	i	r	e	z	a	a	b	r	e	h	f	o	r	o	u	s	h	a	l	i	r	e	z	a	a	b	r	e	h	f	o	r	o	u	s	h	a	l	i	r	e	z	a	a	b	r	e	h	f	o	r	o	u	s	h	a	l	i	r	e	z	a	a	b	r	e	h	f	o	r	o	u	s	h	a	l	i	r	e	z	a	a	b	r	e	h	f	o	r	o	u	s	h	a	l	i	r	e	z	a	a	b	r	e	h	f	o	r	o	u	s	h	a	l	i	r	e	z	a	a	b	r	e	h	f	o	r	o	u	s	h	a	l	i	r	e	z	a	a	b	r	e	h	f	o	r	o	u	s	h	a	l	i	r	e	z	a	a	b	r	e	h	f	o	r	o	u	s	h	a	l	i	r	e	z	a	a	b	r	e	
-----	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	--

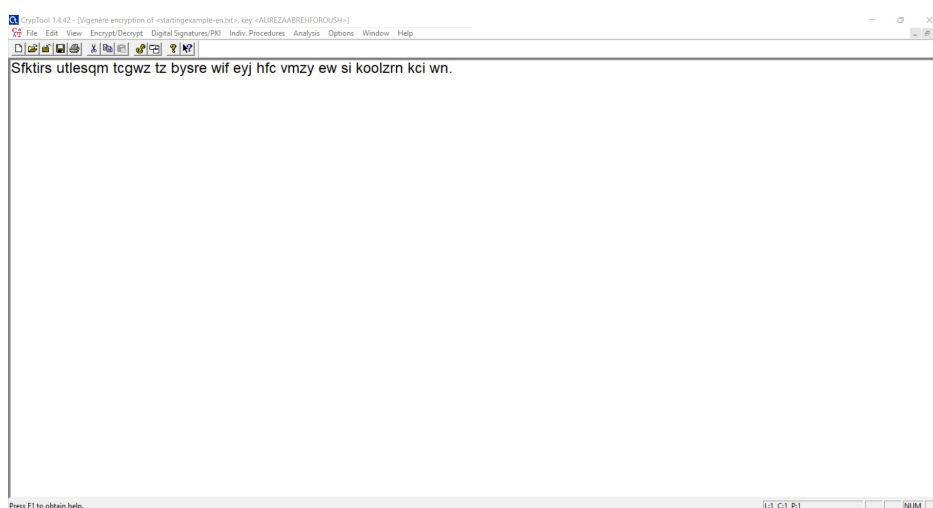
در نرم افزار CrypTool به صورت زیر رمز می کنیم.



شکل ۱۰



شکل ۱۱



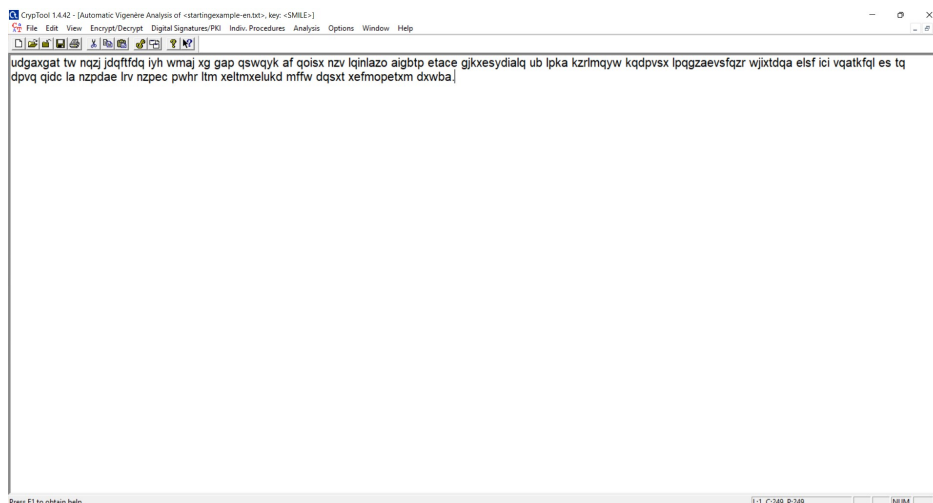
شکل ۱۲

۳.۳

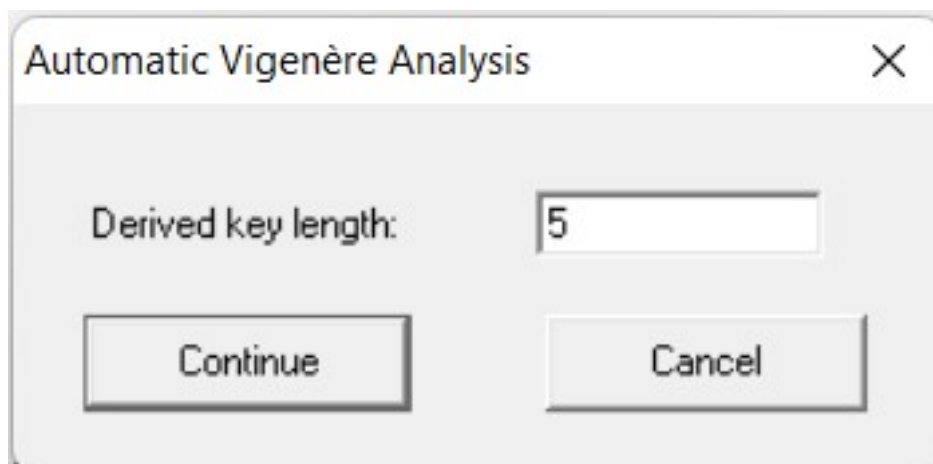
؟؟

۴

در نرم افزار CrypTool به صورت زیر رمزگشایی می‌کنیم. طول کلید (به طور پیشفرض) ۵ است و کلید در Vigenère cipher برابر SMILE به دست می‌آید.



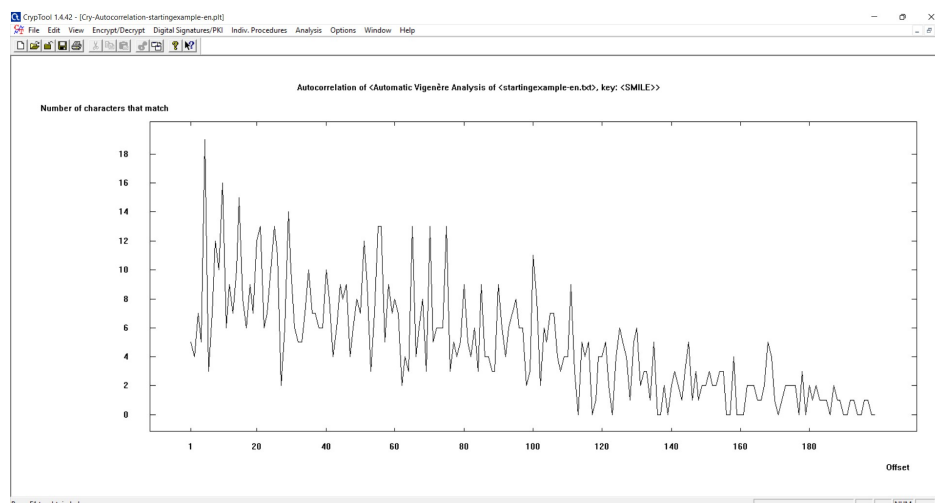
شکل ۱۳



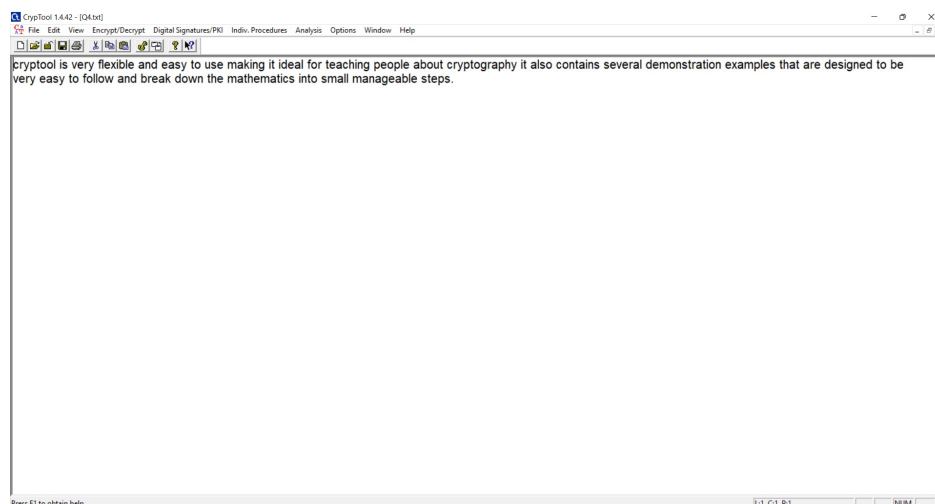
شکل ۱۴



شکل ۱۵



شکل ۱۶



شکل ۱۷

نمودار رسم شده autocorrelation را نشان می‌دهد. autocorrelation یک متن را با نسخه‌های مختلف شیفت یافته‌ی آن (به طول یکسان) مقایسه می‌کند. در هر حالت کاراکترهایی که باهم match می‌شوند (یکسان‌اند) را تعیین می‌کنیم. در نمودار رسم شده، تعداد کاراکترهای match شده بر اساس تعداد واحد شیفت داده شده نمایش داده شده است. توجه شود که فقط حروف الفبای انتخاب شده (انگلیسی یا آلمانی برای مثال) تجزیه و تحلیل می‌شوند. همچنین تعداد جابجایی‌ها به طول متن بستگی دارد (شما می‌توانید متنی متشکل از n کاراکتر را حداکثر n واحد جابجا کنید، سپس آن‌ها به نوعی زیر یکدیگر قرار می‌گیرند). به مثال زیر توجه کنید.

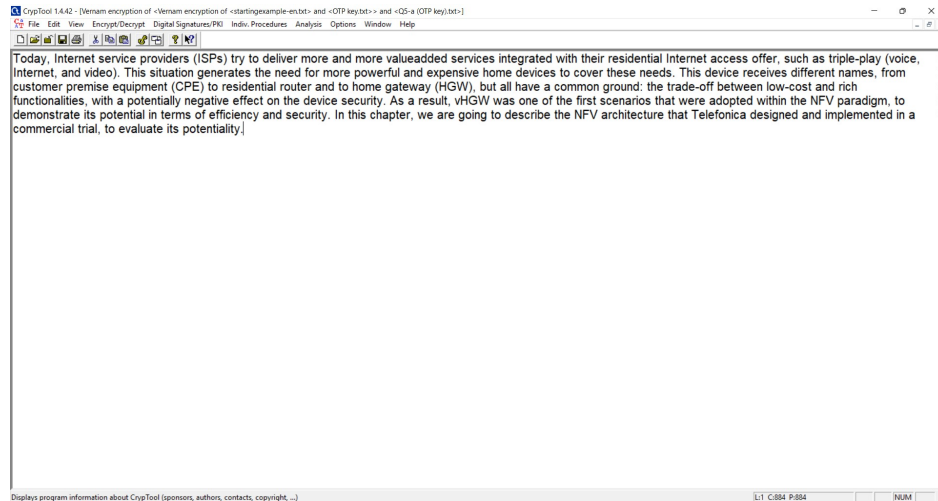
Original text	S	u	c	c	e	s	s	u	s	a	a	l	i	y	c	o	m	e	s	t	o	t	h	o	s	e	w	h	o	a	r	e	t	o	o	b	u	s	y	t	o	b	e	l	o	o	k	i	n	g	f	o	r	i	t	.							
Modified	S	u	c	c	e	s	s	u	s	a	a	l	i	y	c	o	m	e	s	t	o	i	t	h	o	s	e	w	h	o	a	r	e	t	o	o	b	u	s	y	t	o	b	e	l	o	o	k	i	n	g	f	o	r	i	t	.						
Shifted by 6							S	u	c	c	e	s	s	u	s	a	a	l	i	y	c	o	m	e	s	t	o	i	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	.

در این مثال در شیفت ۶ واحد، تعداد کاراکترهای match شده برابر ۸ است.

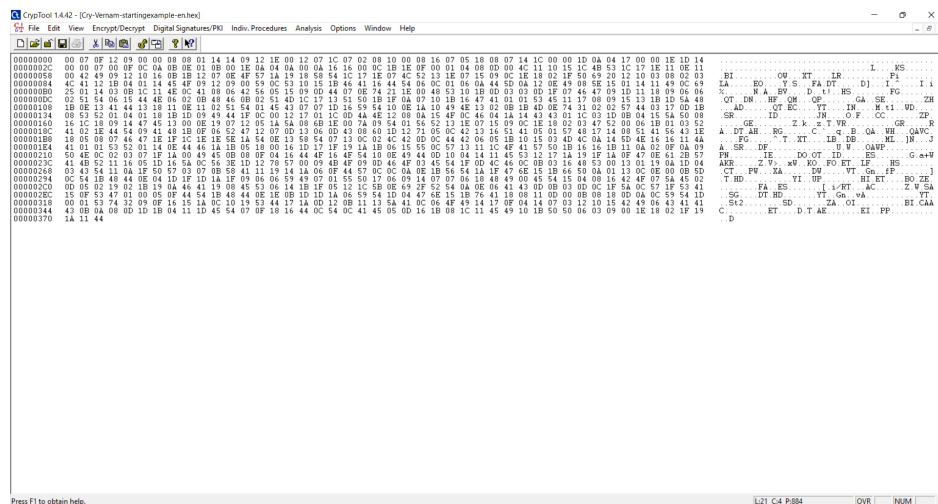
۵

a ۱.۵

plaintext مذکور را با OTP Key مذکور به شکل زیر با تکنیک one-time pad رمز می‌کنیم.



شکل ۱۸



شکل ۱۹

b ۲.۵

plaintext مذکور را به شکل زیر با تکنیک one-time pad رمز می‌کنیم (از آنجایی که طول کلید OTP بایستی بزرگتر مساوی طول رشته‌ای که می‌خواهیم رمز کنیم باشد؛ کلید OTP را برابر تکرار رشته‌ی Alireza Abrehforoush قرار می‌دهیم).

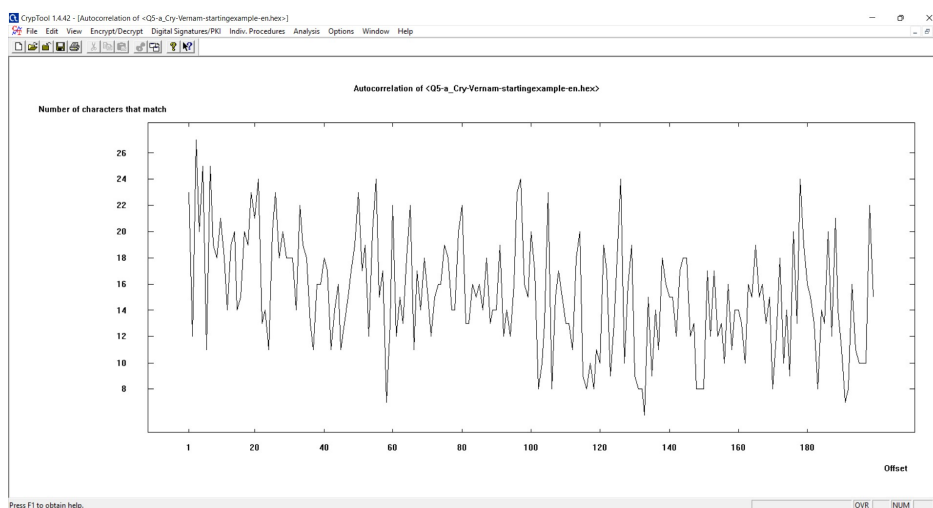


به شکل زیر تحلیل برای کشف کلید OTP به ترتیب برای قسمت a و b انجام می‌شود.

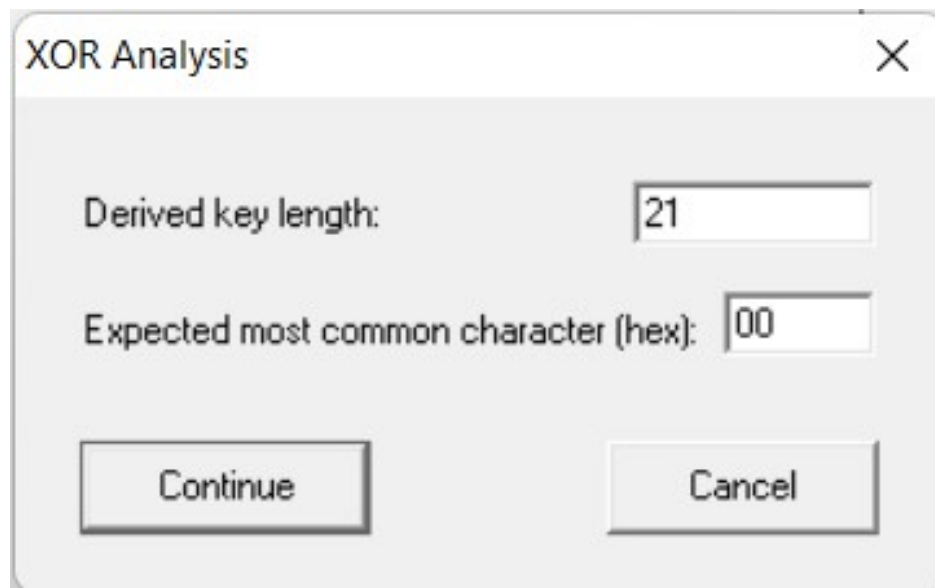




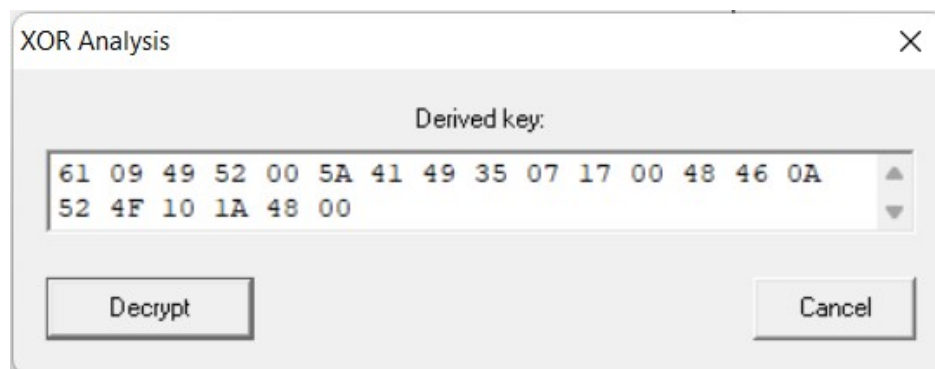
شکل ۲۲



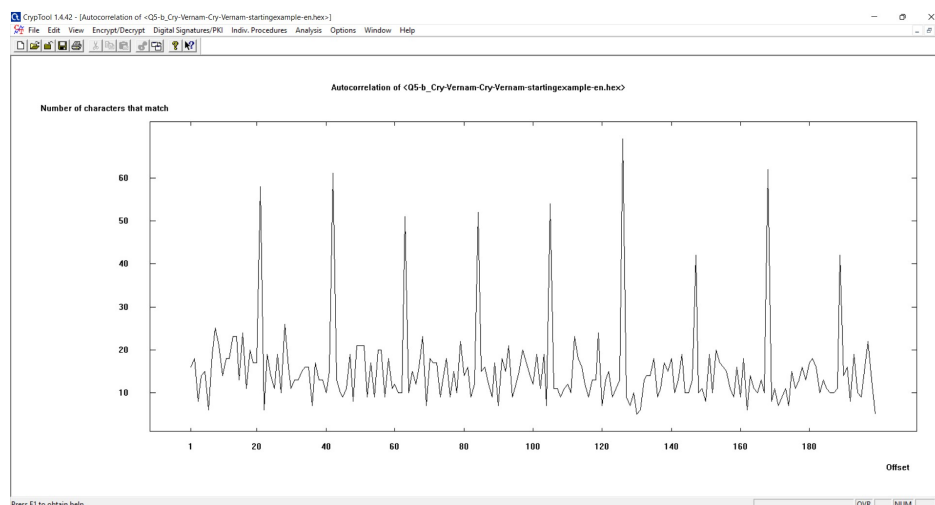
شکل ۲۳



شکل ۲۴



شکل ۲۵



شکل ۲۶

منابع