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 ۱۴۰۱/۱۴۰۲

مدرّس: دکتر سیدمحمد دخیل علیان

دستیاران آموزشی: گلاره عودی قدیم

۱

۱.۱ سوال ۷.۱

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

۱.۱.۱ سوال ۱.۷.۱

×	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

۲.۱.۱ سوال ۲.۷.۱

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

×	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

۳.۱.۱ سوال ۳.۷.۱

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

×	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

۴.۱.۱ سوال ۴.۷.۱

طبق جدول، ۲ در $\mathbb{Z}_4$ و ۲، ۳ و ۴ در $\mathbb{Z}_6$ فاقد وارون ضربی‌اند.
شرط لازم و کافی برای اینکه a به پیمانه‌ی m وارون ضربی داشته باشد این است که این دو عدد نسبت به هم اول باشند. از آنجایی که ۵ عدد اول است، همه‌ی اعداد صحیح مثبت کمتر از ۵ نسبت به ۵ اول‌اند. پس وارون ضربی برای تمامی اعضای غیر صفر در $\mathbb{Z}_5$ موجود است.

۲.۱ سوال ۸.۱

×	5
0	0
1	5
2	10
3	4
4	9
5	3
6	8
7	2
8	7
9	1
10	6

×	5
0	0
1	5
2	10
3	3
4	8
5	1
6	6
7	11
8	4
9	9
10	2
11	7

$\times$	5
0	0
1	5
2	10
3	2
4	7
5	12
6	4
7	9
8	1
9	6
10	11
11	3
12	8

وارون ضربی ۵ در $\mathbb{Z}_11$، $\mathbb{Z}_12$ و $\mathbb{Z}_13$ به ترتیب ۹، ۵ و ۸ است.

۲ CrypTool

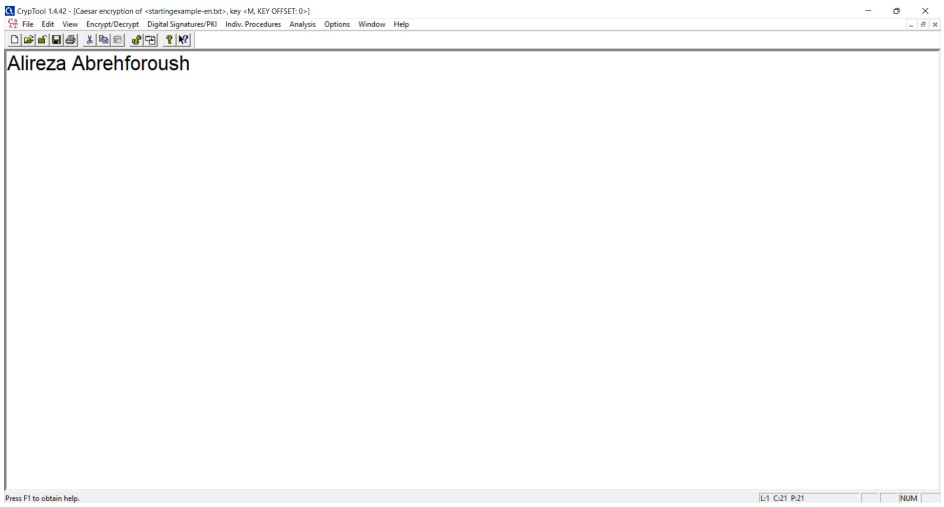
۱.۲

a ۱.۱.۲

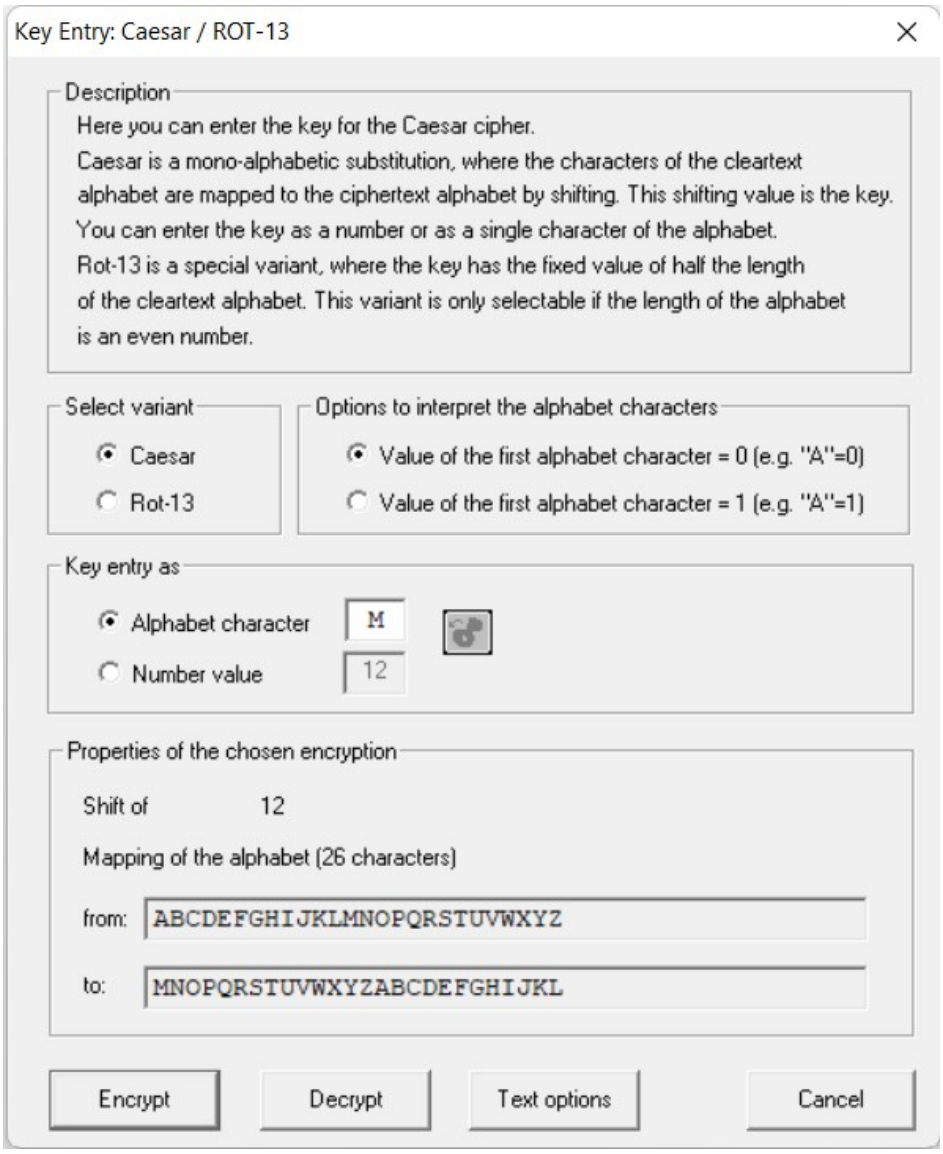
کلید Caesar cipher برابر M است که حرف ۱۳ام الفبای انگلیسی است. پس در واقع هر حرفِ الفبا به صورت حلقوی ۱۲ واحد شیفت می‌خورد. پس در نهایت به صورت زیر رمز می‌شود.

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

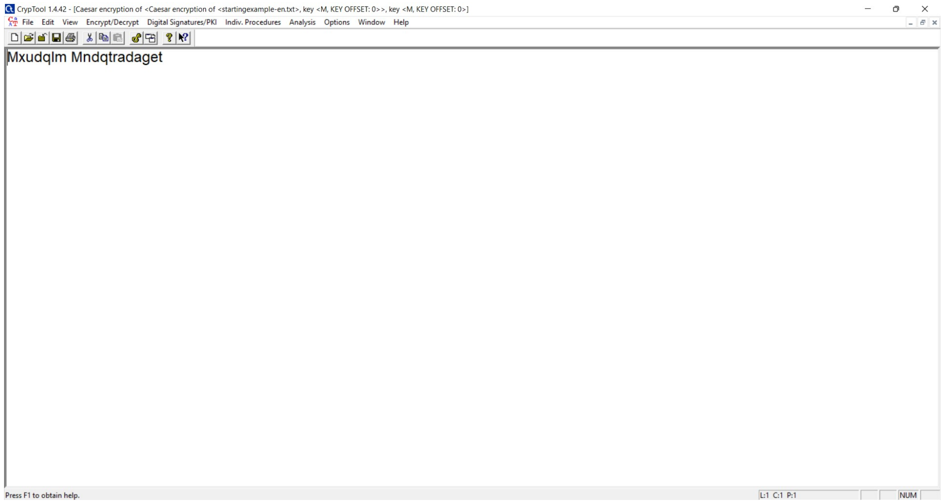
در نرم افزار CrypTool به صورت زیر رمز می‌کنیم.


CrypTool 1.4.42 - [Caesar encryption of <startingexample-en.txt>, key <M, KEY OFFSET: 0>]
File Edit View Encrypt/Decrypt Digital Signatures/PKI Indiv. Procedures Analysis Options Window Help
Alireza Abrehforoush
Press F1 to obtain help.
L:1 C:21 P:21
NUM

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
M
Number value
12
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

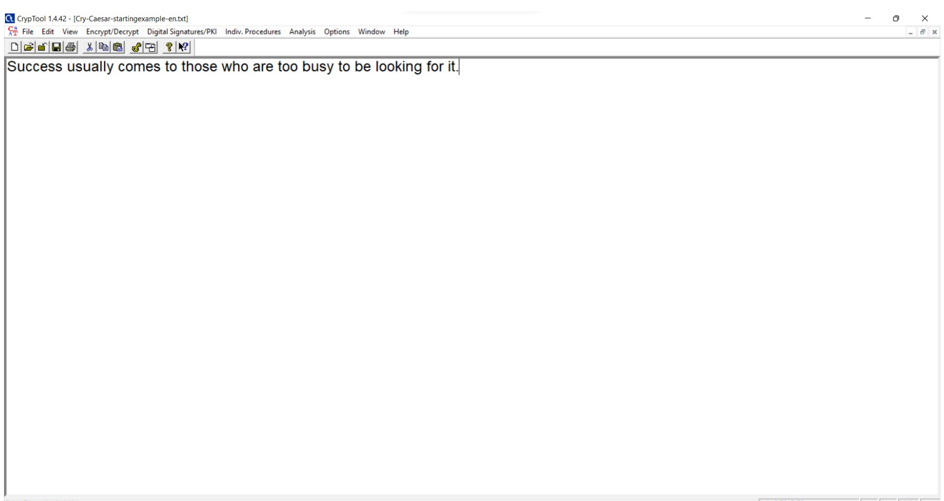
۲.۲

$$9816603 \equiv 17 \quad mod \ 26$$

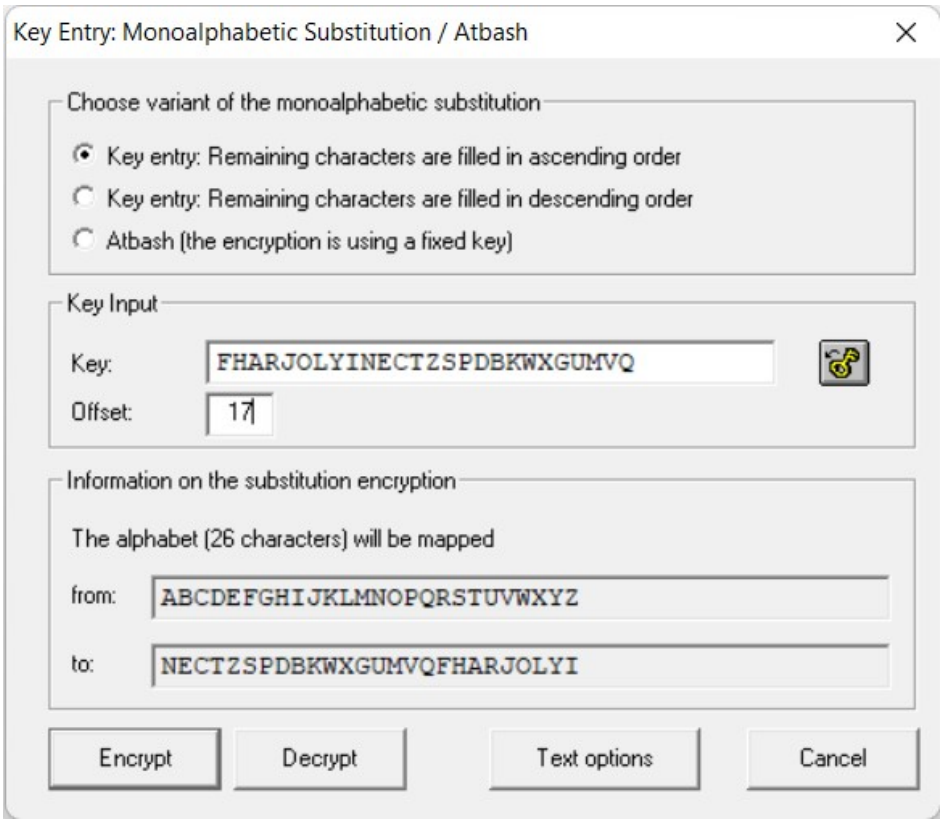
کلید Substitution cipher برابر fharjolyinectzspdbkwxgumvq و offset آن برابر ۱۷ است. در واقع الفبای اگلیسی به ترتیب به NECTZSPDBKWXGUMVQFHARJOLYI map می‌شود. پس در نهایت به صورت زیر رمز می‌شود.

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


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:
FHARJOLYINECTZSPDBKWXGUMVQ
Offset:
17
Information on the substitution encryption
The alphabet (26 characters) will be mapped
from:
ABCDEFGHIJKLMNOPQRSTUVWXYZ
to:
NECTZSPDBKWXGUMVQFHARJOLYI
Encrypt
Decrypt
Text options
Cancel

شکل ۵


File Edit View Encrypt/Decrypt Digital Signatures/PKI Indiv. Procedures Analysis Options Window Help
Hrcczhh rhrnxxy cmgzh am admhz odm nfz amm erhy am ez xmmwbup smf ba.

شکل ۶

۳.۲

۱.۳.۲ a

در Vigenère cipher در الفبای انگلیسی از یک جدول با ابعاد 26×26 استفاده می‌شود که در سطر iام آن حروف انگلیسی به ترتیب به صورت حلقوی با شروع از حرف iام 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

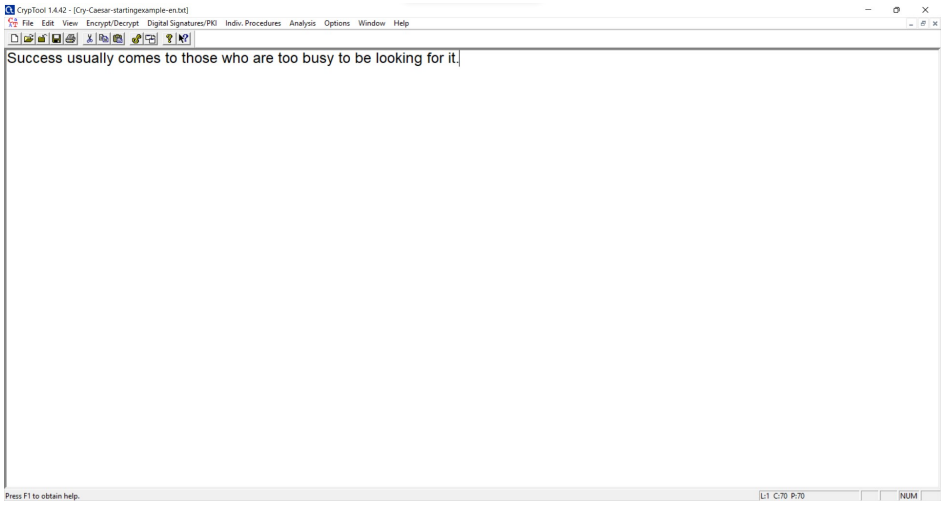
همچنین کلید مورد استفاده در این الگوریتم به صورت زیر (سه حرف اول نام + سه حرف اول نام خانوادگی) ساخته می‌شود.

$ALIREZA\ ABREHFOROUSH \Rightarrow key = ALIABR$

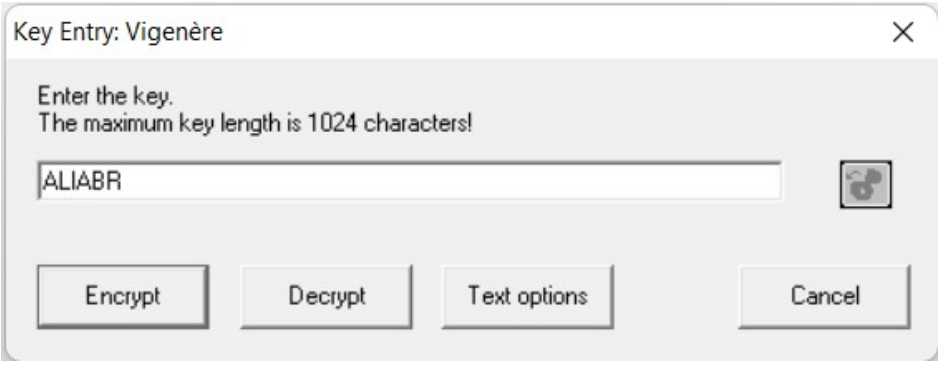
حال key را مکررا تکرار می‌کنیم تا طول آن برابر طول رشته‌ای که می‌خواهیم آن را رمز کنیم بشود (یا به عبارتی کاراکتر نظیر باقیمانده‌ی i به پیمانه‌ی طول کلید (۶) را در کلید به دست آوریم). برای رمز کردن کاراکترِ iام در رشته، کاراکترِ اندیسِ باقیمانده‌ی i به پیمانه‌ی طول کلید (۶) در کلید (key_i) به همراه خود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

key	A	l	i	a	b	r	a		l	i	a	b	r	a	l		i	a	b	r	a		l	i		a	b	r	a	l		i	a	b		r	a	l		i	a	b		r	a	l	i		a	b		r	a		l	i	a	b	r	a	l		i	a	b		r	a	.
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	.
$E(x)$	S	f	k	c	f	j	s		f	a	u	b	c	l	j		k	o	n	v	s		e	w		t	i	f	s	p		e	h	p		r	r	p		b	o	p		s	u	d	g		t	p		s	e		w	w	o	l	z	n	r		n	o	s		z	t	.

در نرم افزار CrypTool به صورت زیر رمز می‌کنیم.



شکل ۷



شکل ۸

شکل ۹

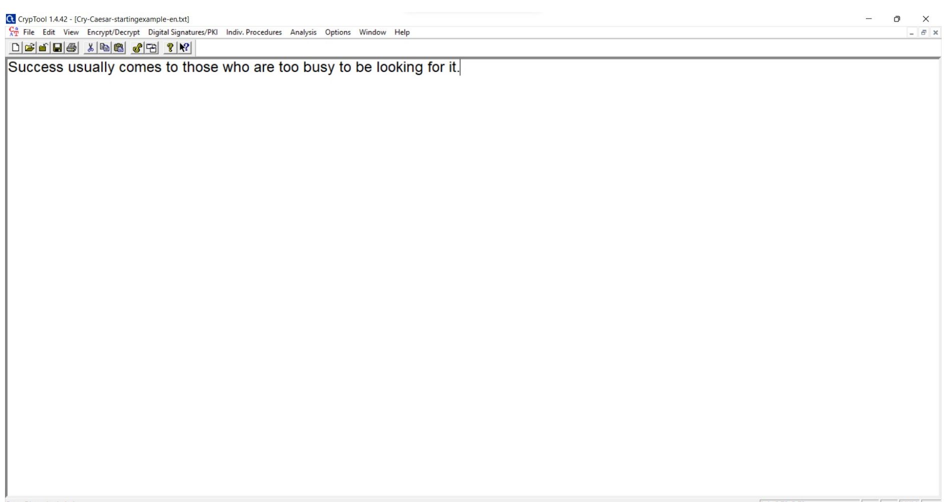
۲.۳.۲ b

مشابه قسمت قبل (صرفا تغییر کلید) داریم:

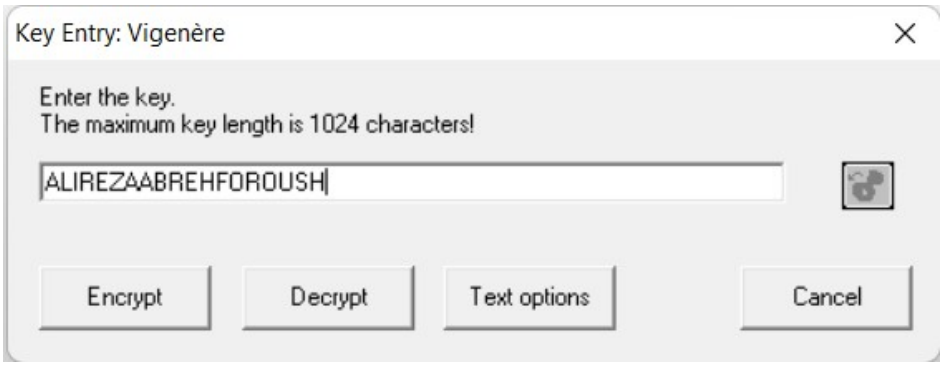
$$ALIREZA\ ABREHFOROUSH \Rightarrow key = ALIREZAABREHFOROUSH$$

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	.
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	.
$E(x)$	S	f	k	t	i	r	s		u	t	l	e	s	q	m		t	c	g	w	z		t	z		b	y	s	r	e		w	i	f		e	y	j		h	f	c		v	m	z	y		e	w		s	i		k	o	o	l	z	r	n		k	c	i		w	n	.

در نرم افزار CrypTool به صورت زیر رمز می‌کنیم.



شکل ۱۰



شکل ۱۱

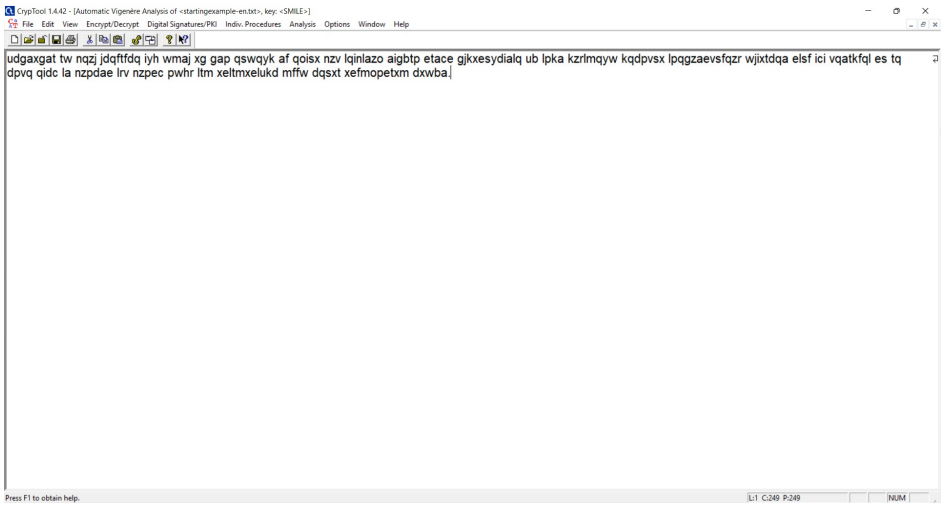
شکل ۱۲

۳.۳.۲

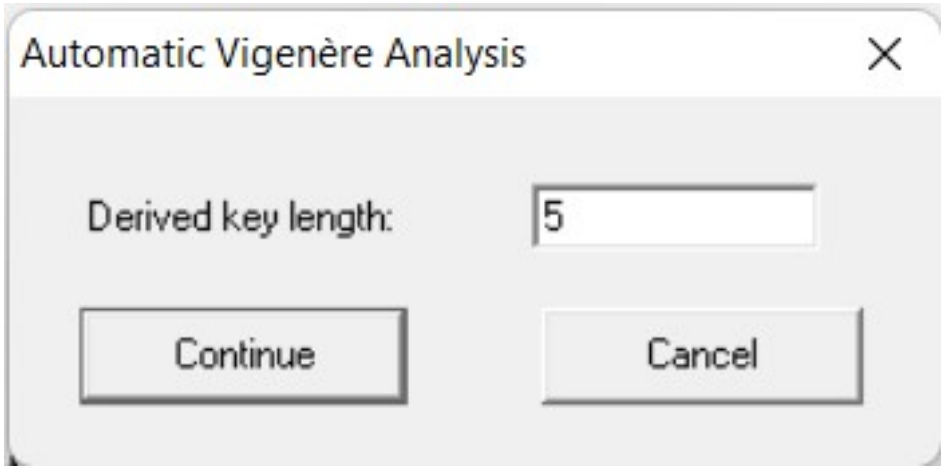
؟؟

۴.۲

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.

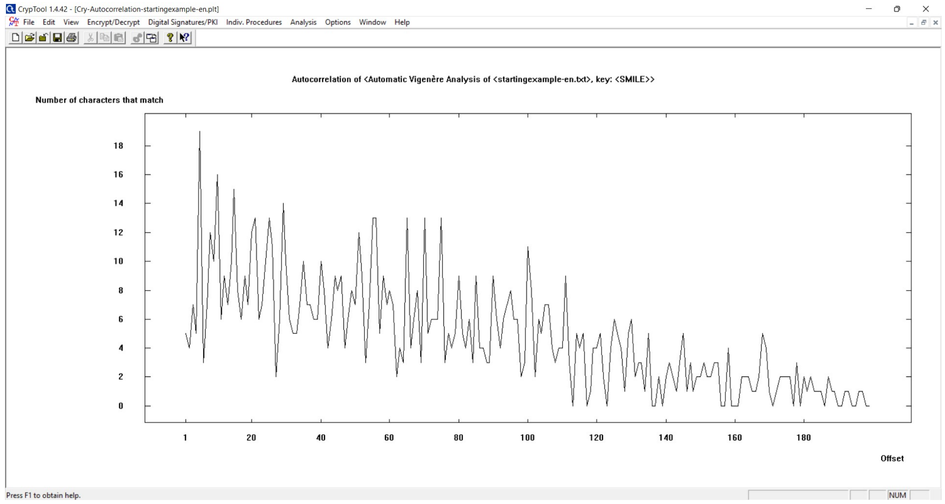


شکل ۱۳

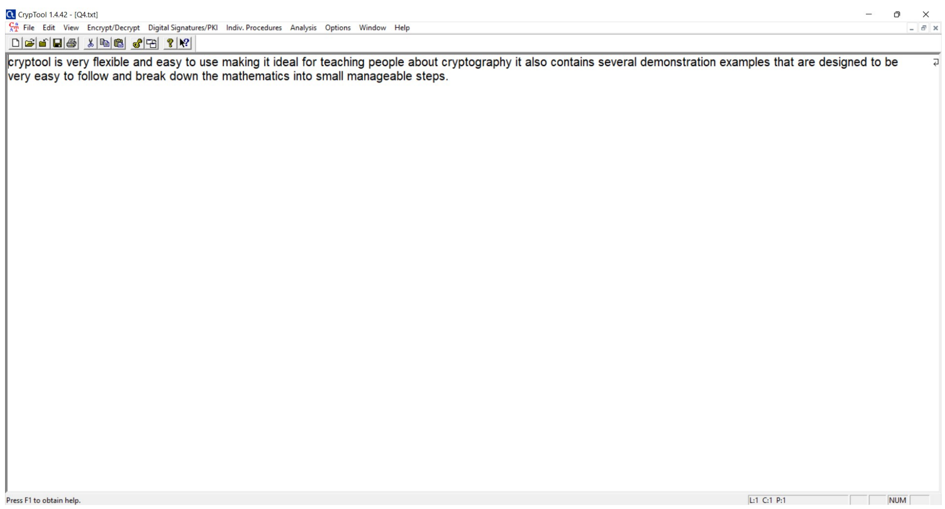


شکل ۱۴

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 matchشده 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 جابه‌جایی‌ها 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.

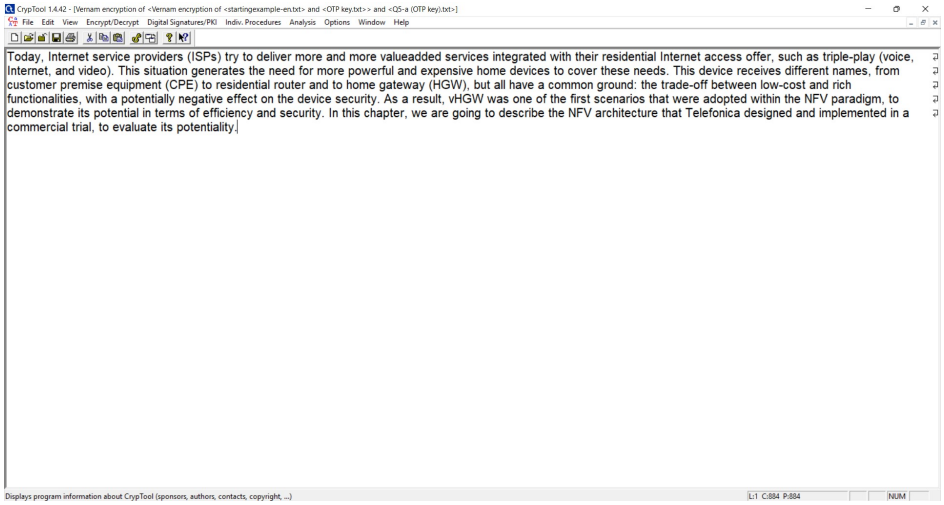
Orginal text	S	u	c	c	e	s	s		u	s	u	a	l	l	y		c	o	m	e	s		t	o		t	h	o	s	e		w	h	o		a	r	e		t	o	o		b	u	s	y		t	o		b	e		l	o	o	k	i	n	g		f	o	r		i	t	.
Modified	S	u	c	c	e	s	**s**	**u**	**s**	u	a	l	l	y	c	o	m	e	s	t	o	t	h	o	**s**	e	w	h	o	a	r	**e**	t	o	**o**	b	u	s	y	t	**o**	**b**	e	l	o	o	k	i	n	g	f	**o**	r	**i**	t	.		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

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

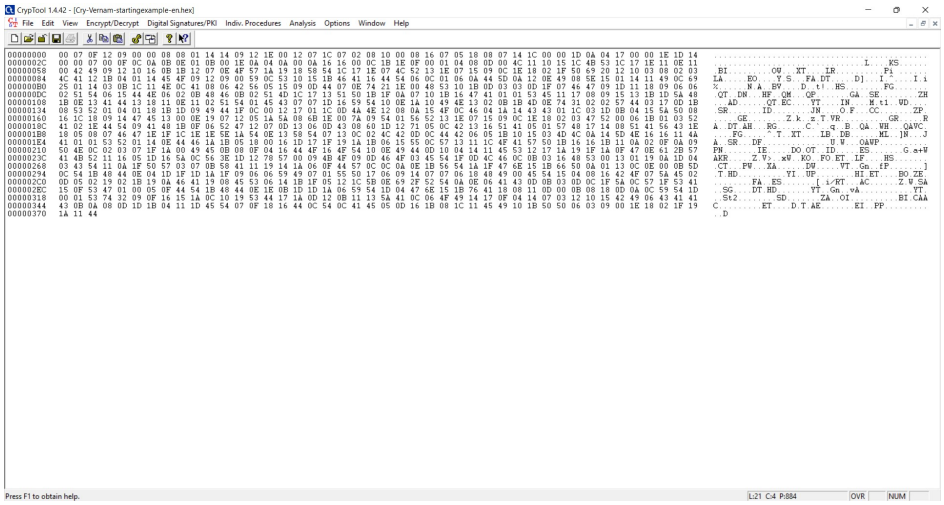
۵.۲

a ۱.۵.۲

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



شکل ۱۸



شکل ۱۹

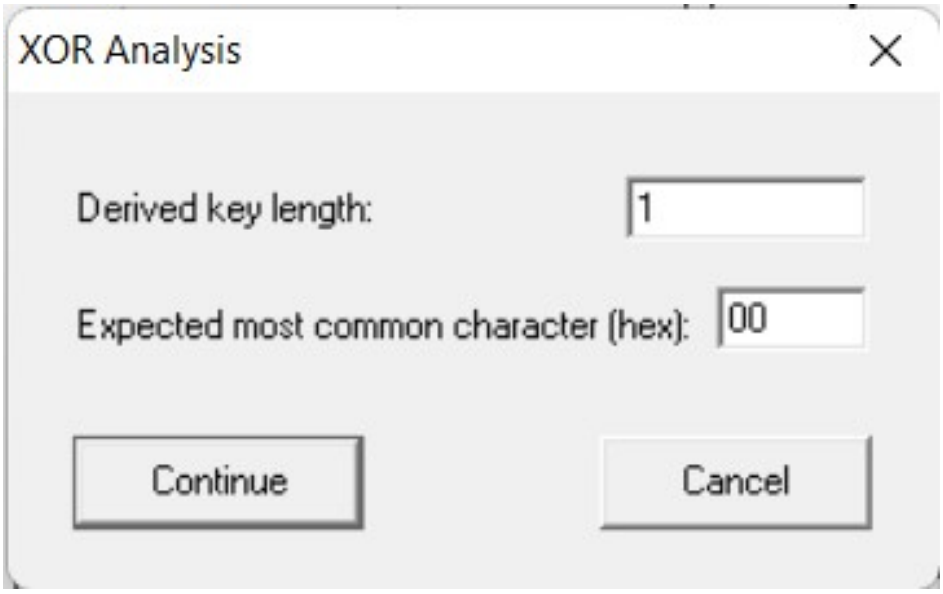
b ۲.۵.۲

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).

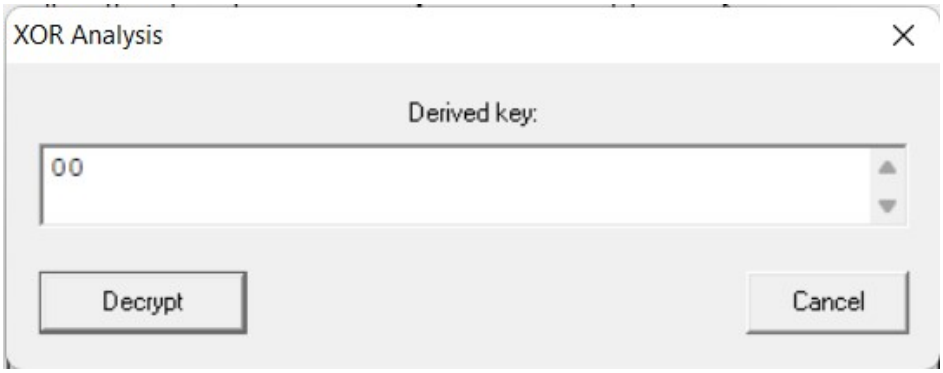
شکل ۲۰

c ۳.۵.۲

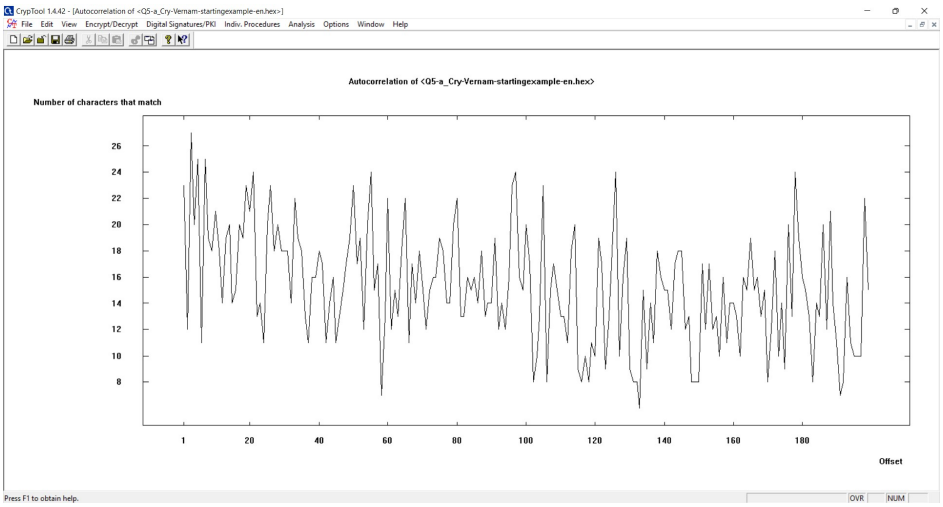
به شکل زیر تحلیل برای کشف کلید OTP به ترتیب برای قسمت a و b انجام می‌شود.



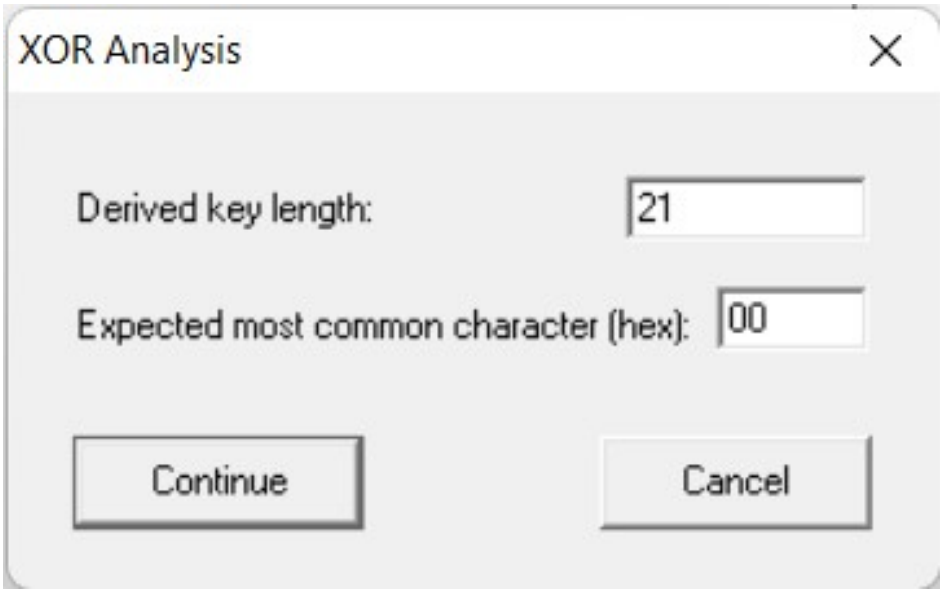
شکل ۲۱


XOR Analysis
Derived key:
00
Decrypt
Cancel

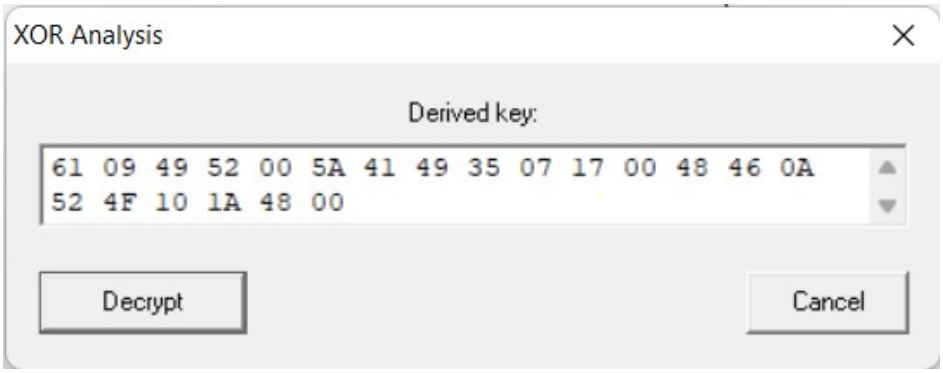
شکل ۲۲


Autocorrelation of <Q5-a_Cry-Vernam-startingexample-en.hex>
Number of characters that match
Offset

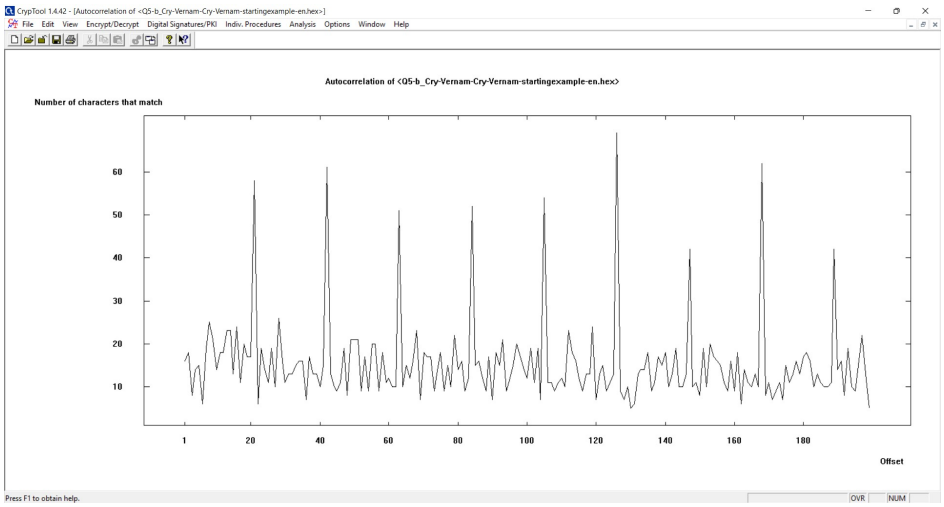
شکل ۲۳


XOR Analysis
Derived key length:
21
Expected most common character (hex):
00
Continue
Cancel

شکل ۲۴


XOR Analysis
Derived key:
61 09 49 52 00 5A 41 49 35 07 17 00 48 46 0A
52 4F 10 1A 48 00
Decrypt
Cancel

شکل ۲۵


CrypTool 1.4.42 - [Autocorrelation of <Q5-b_Cry-Vernam-Cry-Vernam-startingexample-en.hex>]
File Edit View Encrypt/Decrypt Digital Signatures/PKI Indiv. Procedures Analysis Options Window Help
Autocorrelation of <Q5-b_Cry-Vernam-Cry-Vernam-startingexample-en.hex>
Number of characters that match
60
50
40
30
20
10
1
20
40
60
80
100
120
140
160
180
Offset
Press F1 to obtain help.
OVR
NUM

شکل ۲۶

منابع