



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 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 اول‌ند. 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

×	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.

۳.۱ سوال ۹.۱

۱.۳.۱ سوال ۱.۹.۱

$$3^2 \equiv 9 \pmod{13} \Rightarrow x = 9$$

۲.۳.۱ سوال ۲.۹.۱

$$7^2 \equiv 10 \pmod{13} \Rightarrow x = 10$$

۳.۳.۱ سوال ۳.۹.۱

$$3^{10} \equiv (3^3)^3 \times 3 \equiv (27)^3 \times 3 \equiv (1)^3 \times 3 \equiv 3 \pmod{13} \Rightarrow x = 3$$

۴.۳.۱ سوال ۴.۹.۱

$$7^{100} \equiv (7^2)^{50} \equiv (-3)^{50} \equiv (3)^{50} \equiv (3^{10})^5 \equiv 3^5 \equiv 3^3 \times 3^2 \equiv 9 \pmod{13} \Rightarrow x = 9$$

۵.۳.۱ سوال ۵.۹.۱

<i>power</i>	1	2	3	4	5
7	7	10	5	9	11

$$\Rightarrow x = 5$$

۴.۱ سوال ۱۰.۱

$$m = 4 \quad ۱.۴.۱$$

$$(4, 1) = 1$$

$$(4, 3) = 1$$

$$m = 5 \quad ۲.۴.۱$$

$$(5, 1) = 1$$

$$(5, 2) = 1$$

$$(5, 3) = 1$$

$$(5, 4) = 1$$

$$m = 9 \quad ۳.۴.۱$$

$$(9, 1) = 1$$

$$(9, 2) = 1$$

$$(9, 4) = 1$$

$$(9, 5) = 1$$

$$(9, 7) = 1$$

$$(9, 8) = 1$$

$$m = 26 \quad ۴.۴.۱$$

$$(26, 1) = 1$$

$$(26, 3) = 1$$

$$(26, 5) = 1$$

$$(26, 7) = 1$$

$$(26, 9) = 1$$

$$(26, 11) = 1$$

$$(26, 15) = 1$$

$$(26, 17) = 1$$

$$(26, 19) = 1$$

$$(26, 21) = 1$$

$$(26, 23) = 1$$

$$(26, 25) = 1$$

Euler's phi function ۵.۴.۱

$$\phi(4) = 4 \prod_{p|4} \left(1 - \frac{1}{p}\right) = 2$$

$$\phi(5) = 5 \prod_{p|5} \left(1 - \frac{1}{p}\right) = 4$$

$$\phi(9) = 9 \prod_{p|9} \left(1 - \frac{1}{p}\right) = 6$$

$$\phi(26) = 26 \prod_{p|26} \left(1 - \frac{1}{p}\right) = 12$$

۵.۱ سوال ۱۳.۱

$$(x_1, y_1)$$

$$(x_2, y_2)$$

$$y_1 = e_k(x_1) \equiv ax_1 + b \pmod{m}$$

$$y_2 = e_k(x_2) \equiv ax_2 + b \pmod{m}$$

$$\Rightarrow y_1 - y_2 \equiv a(x_1 - x_2) \pmod{m}$$

$$\Rightarrow (y_1 - y_2)(x_1 - x_2)^{-1} \equiv a \pmod{m}$$

برای اینکه a وجود داشته باشد، باید $(x_1 - x_2)$ وارون داشته باشد. از آنجایی که شرط لازم و کافی برای اینکه $(x_1 - x_2)$ به پیمانه‌ی m وارون ضربی داشته باشد این است که این دو عدد نسبت به هم اول باشند. پس Oscar با فرض دانستن m باید x_1 و x_2 را طوری انتخاب کند که داشته باشیم:

$$((x_1 - x_2), m) = 1$$

۲ CrypTool

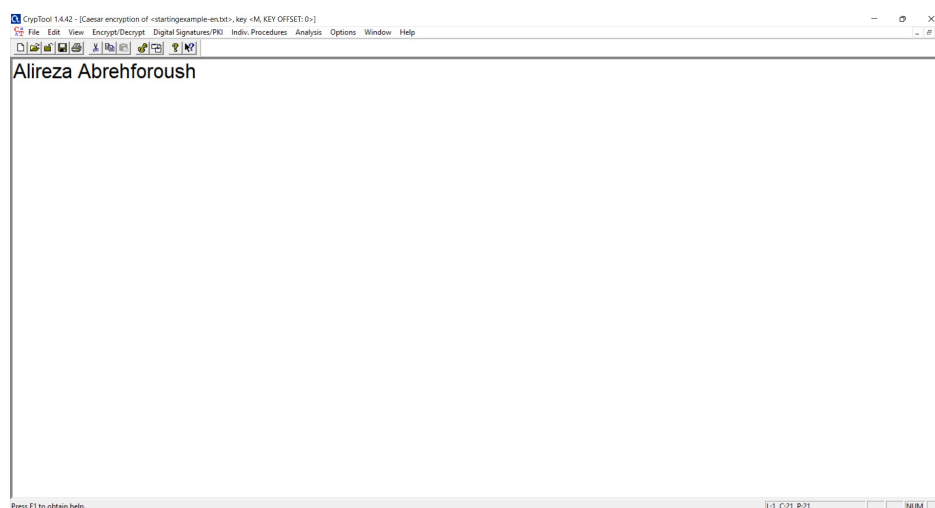
۱.۲

a ۱.۱.۲

کلید Caesar cipher برابر M است که حرف ۱۳ام الفبای انگلیسی است. پس در واقع هر حرف 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

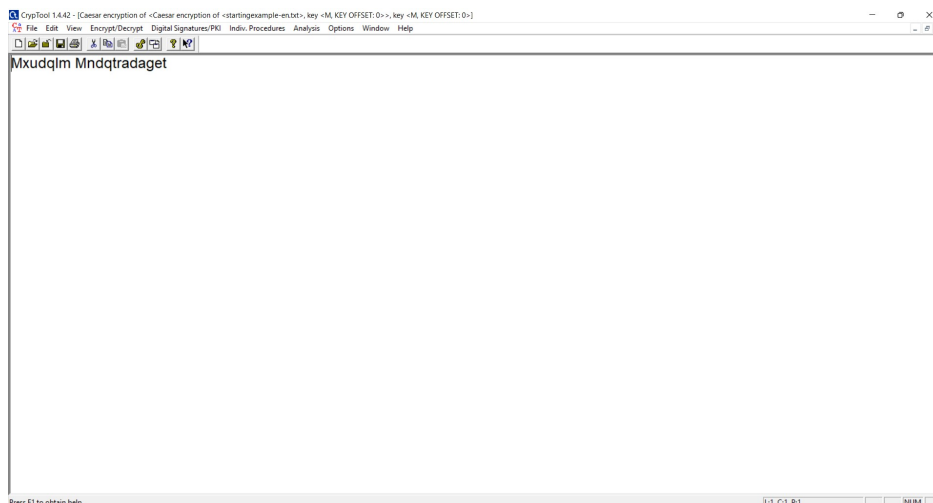
Mapping of the alphabet (26 characters)

from:

to:

Encrypt Decrypt Text options Cancel

شکل ۲



شکل ۳

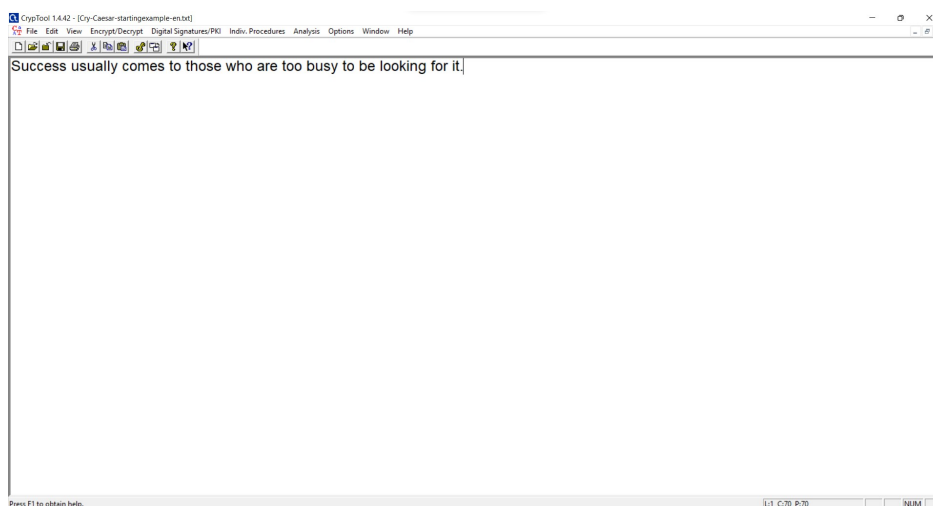
۲.۲

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

کلید Substitution cipher برابر `fhajolyinectzspdbkwxgumvq` 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	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	c	r	h	y	a	m	e	z	x	m	w	h	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

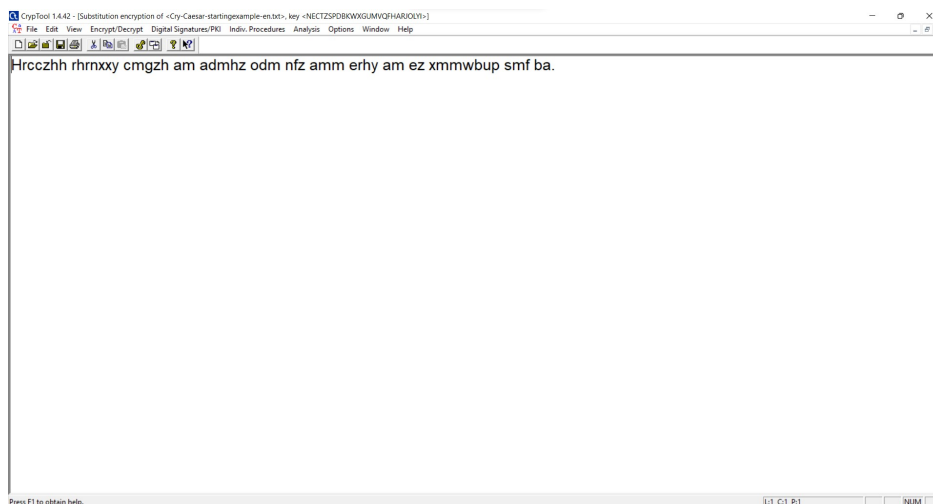
The alphabet (26 characters) will be mapped

from:

to:

Encrypt Decrypt Text options Cancel

شکل ۵



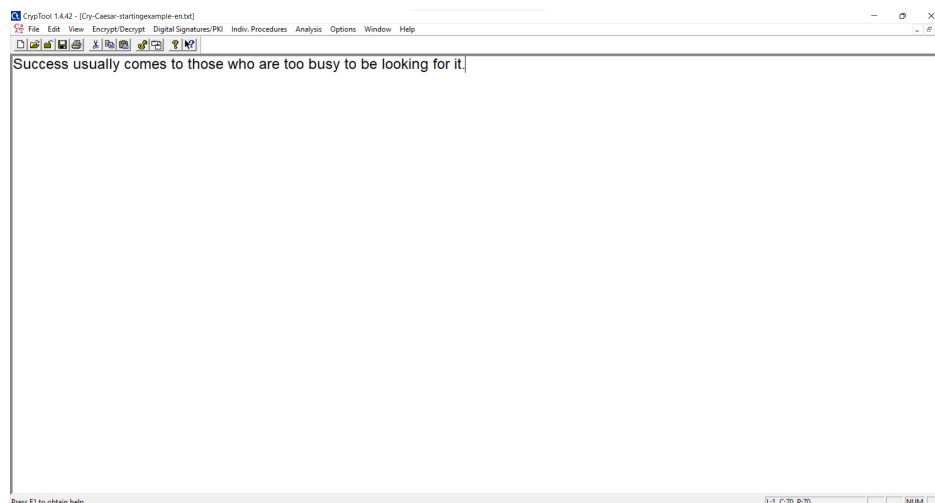
شکل ۶

a 1.3.2

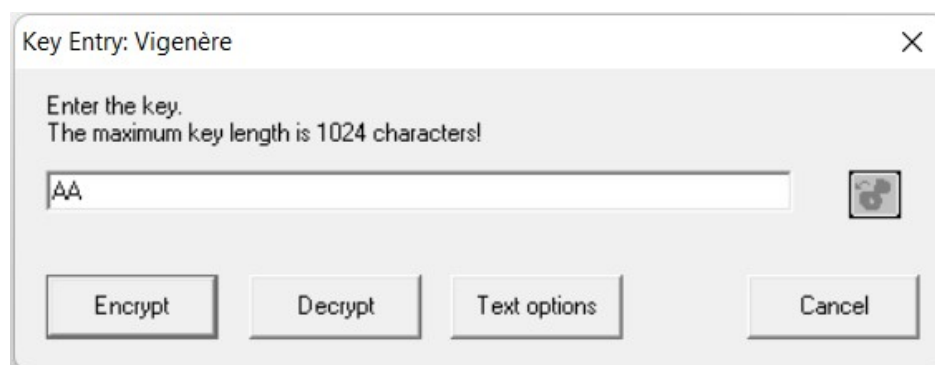
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y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

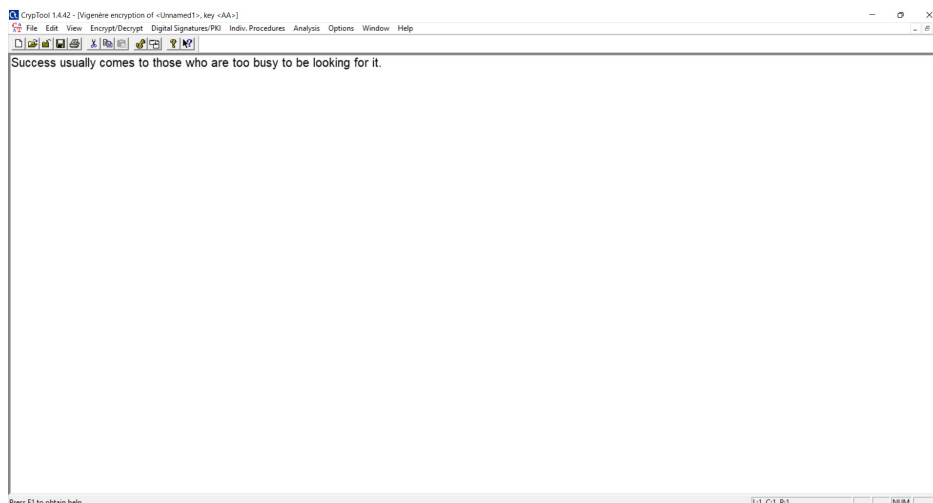
در نرم افزار CrypTool به صورت زیر رمز می کنیم.



شکل ۷



شکل ۸



شکل ۹

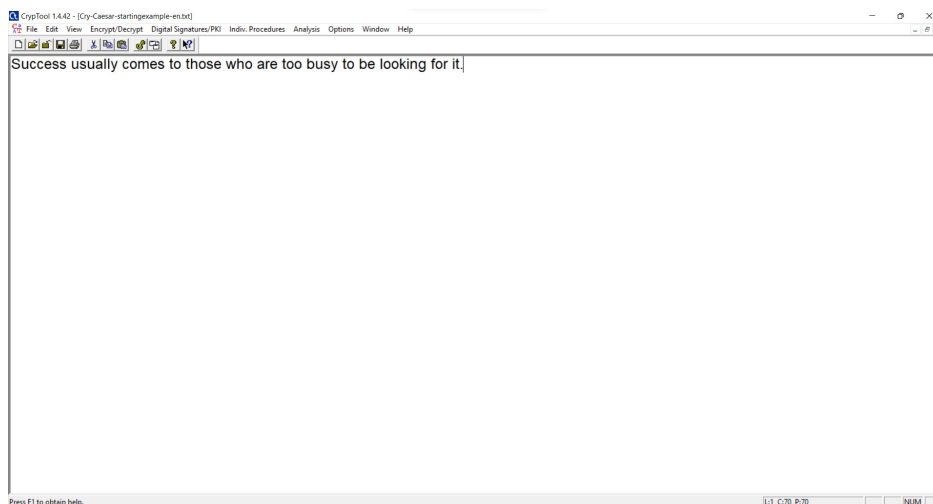
۲.۳.۲ b

مشابه قسمت قبل (صرفاً تغییر کلید) داریم:

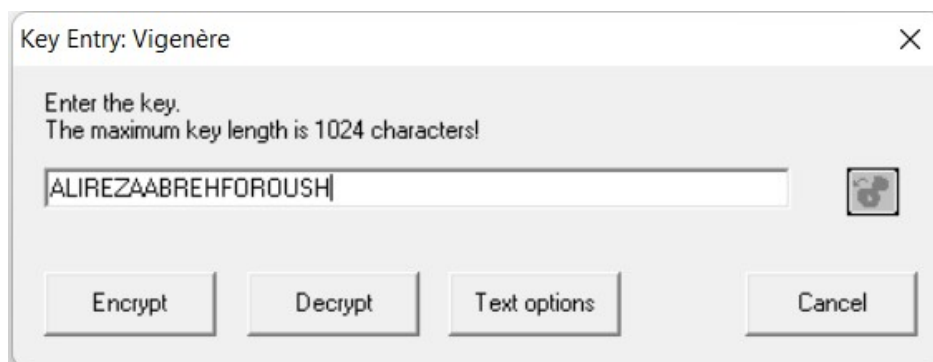
$$ALIREZA ABREHFORUSH \Rightarrow key = ALIREZAABREHFORUSH$$

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

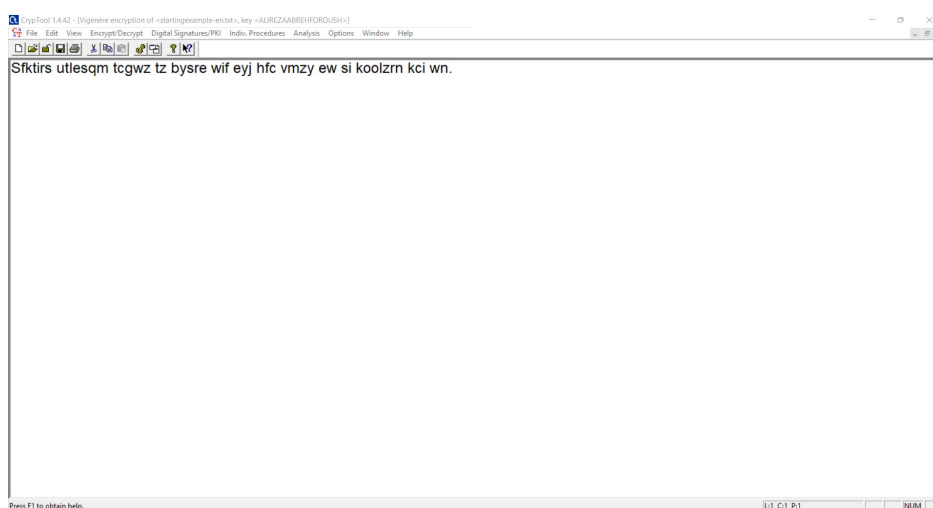
در نرم افزار CrypTool به صورت زیر رمز می کنیم.



شکل ۱۰

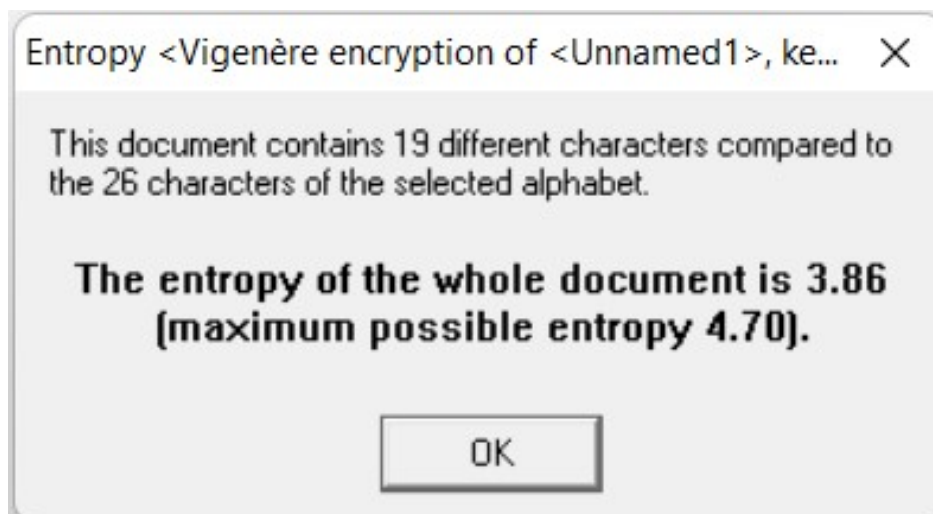


شکل ۱۱

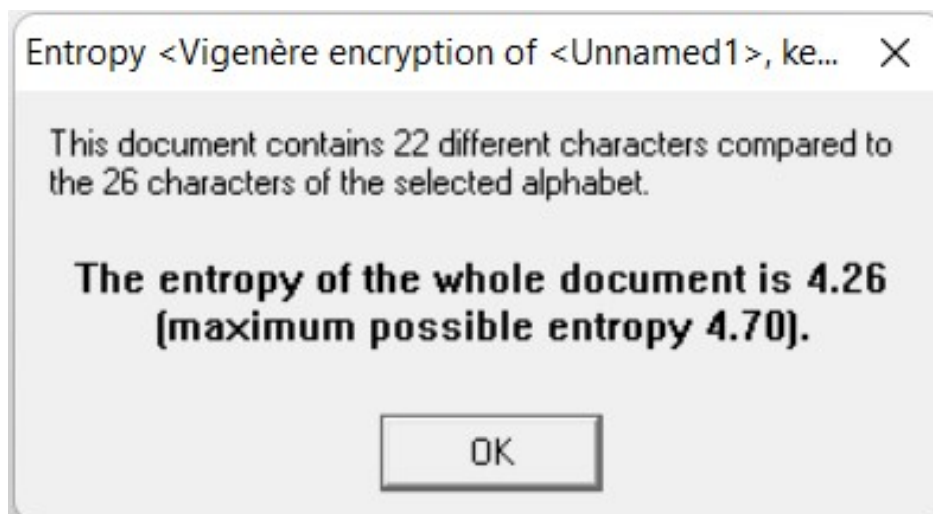


شکل ۱۲

c ۳.۳.۲



شکل ۱۳



شکل ۱۴

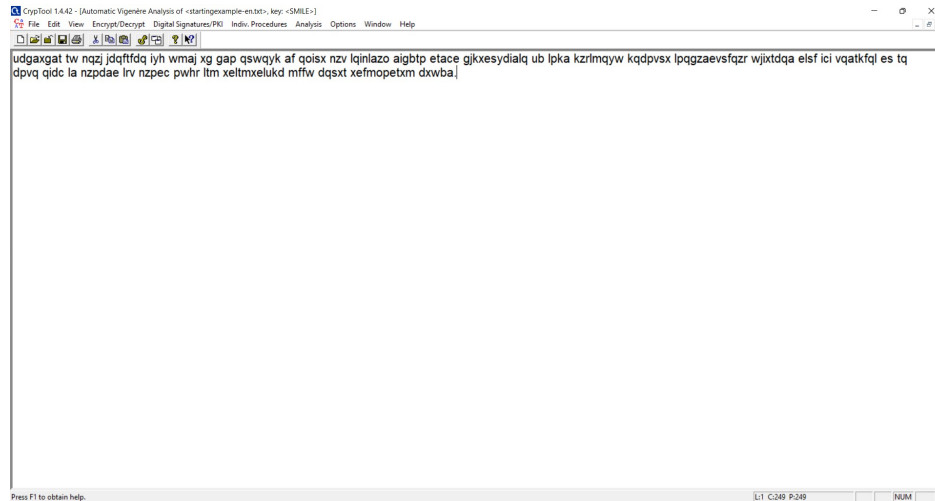
آنتروپی در حالت اول و دوم به ترتیب برابر ۸۶.۳ و ۲۶.۴ است.

Entropy, in the context of cryptography, is related to random number generation, and more precisely, it refers to the “amount of unpredictable randomness” in a physical system. We call an entropy source the physical system that produces random signals.

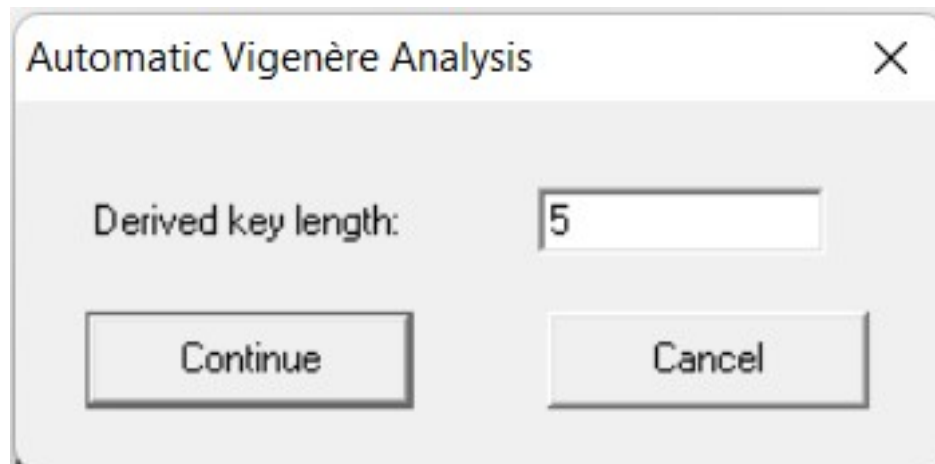
از آنجایی که در حالت دوم که طول کلید بیشتر است (کارکترهای متفاوت‌تری دارد) بی‌نظمی (randomness) بیشتری وجود دارد، رمز امن‌تر است. در حالی که در حالت اول چون دو کاراکتر یکسان بودند صرفاً از یک سطر (سطر اول که بدیهی هم هست) استفاده شده است و عبارت عملاً رمز نشده است.

۴.۲

در نرم افزار CrypTool به صورت زیر رمزگشایی می کنیم. طول کلید (به طور پیش فرض) ۵ است و کلید در Vigenère cipher برابر SMILE به دست می آید.



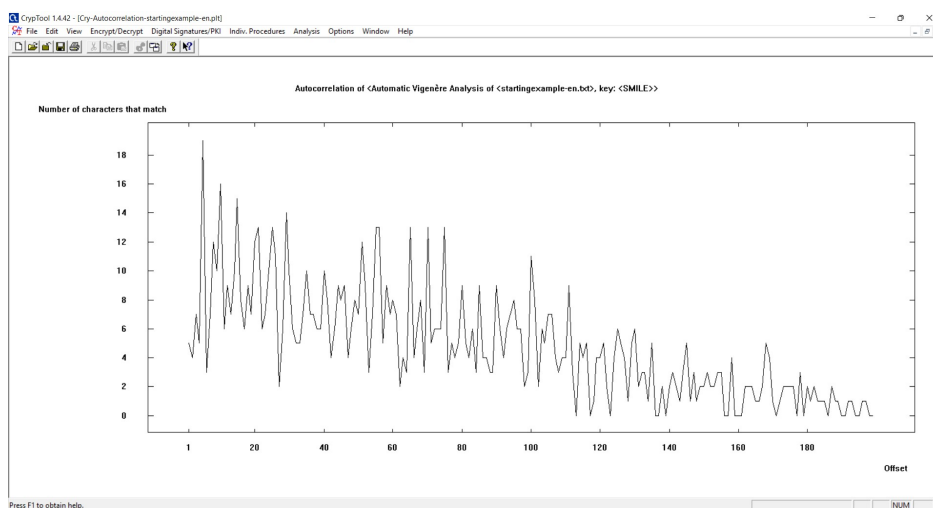
شکل ۱۵



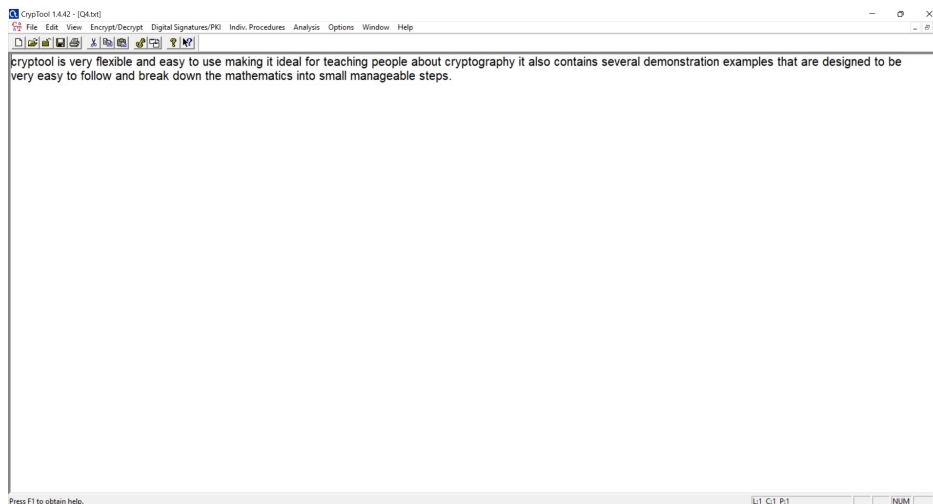
شکل ۱۶



شکل ۱۷



شکل ۱۸



شکل ۱۹

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.

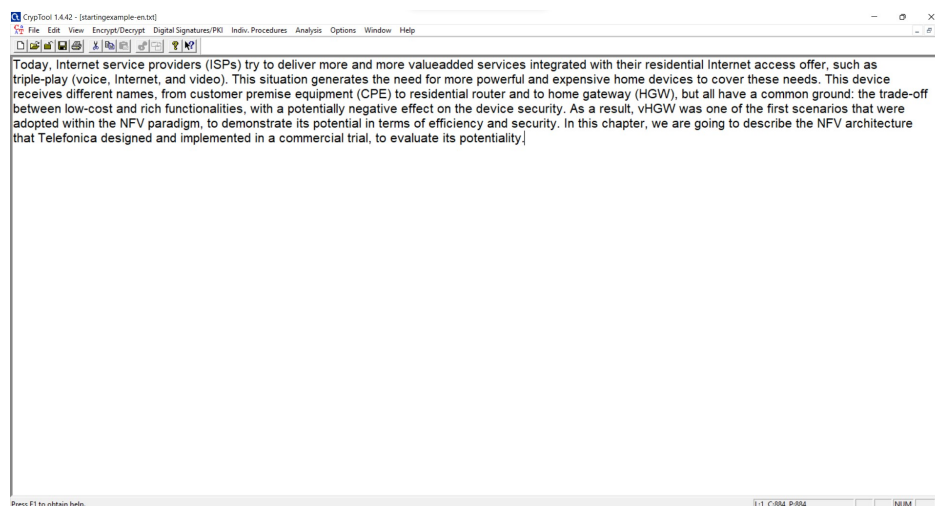
Original text	S	u	c	c	e	s	s	u	s	u	a	l	l	y	c	o	m	e	s	t	o	t	h	e	s	e	w	h	o	a	r	e	t	o	o	b	u	s	y	t	o	b	e	l	o	o	k	i	n	g	f	o	r	i	t	.
Modified	S	u	c	c	e	s	s	u	s	u	a	l	l	y	c	o	m	e	s	t	o	t	h	e	s	e	w	h	o	a	r	e	t	o	o	b	u	s	y	t	o	b	e	l	o	o	k	i	n	g	f	o	r	i	t	.
Shifted by 6	S	u	c	c	e	s	s	u	s	u	a	l	l	y	c	o	m	e	s	t	o	t	h	e	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 شیف ۶ واحد، تعداد کاراکترهای match شده برابر ۸ است.

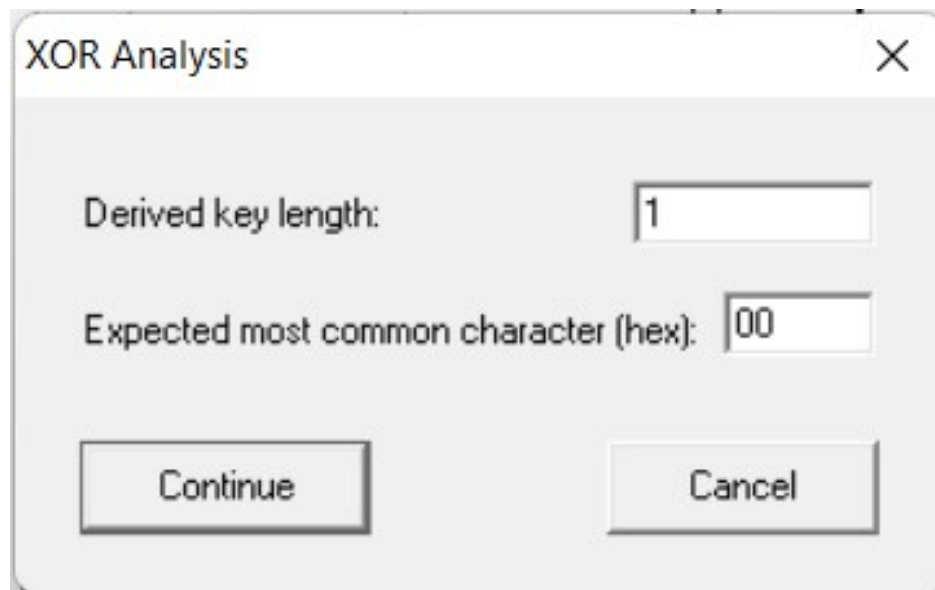
5.2

a 1.5.2

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



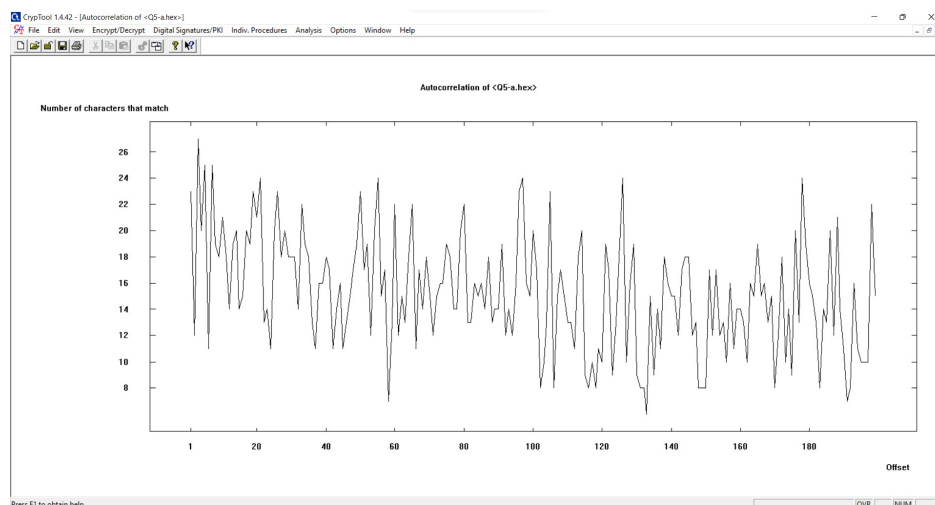
شكل ٢٠



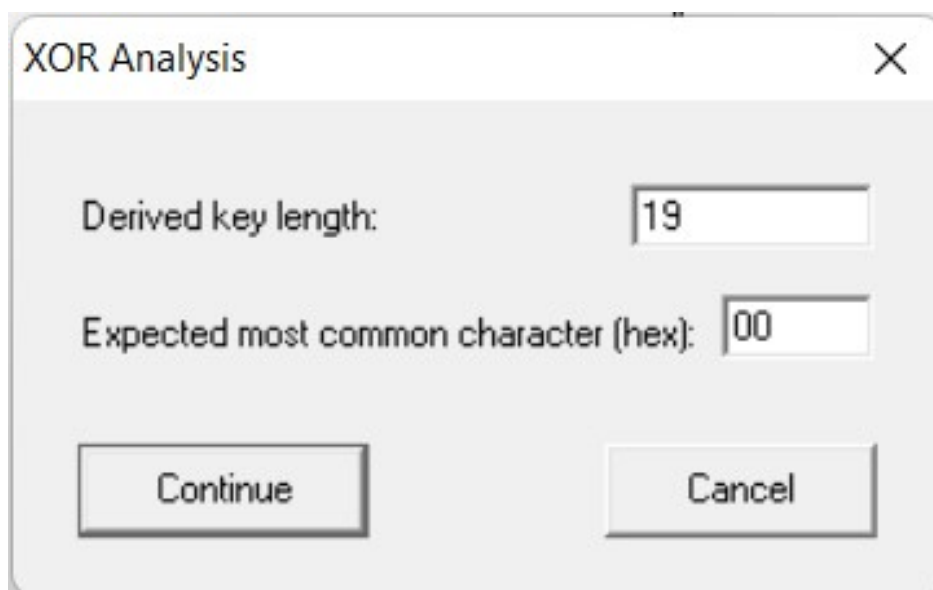
شکل ۲۳



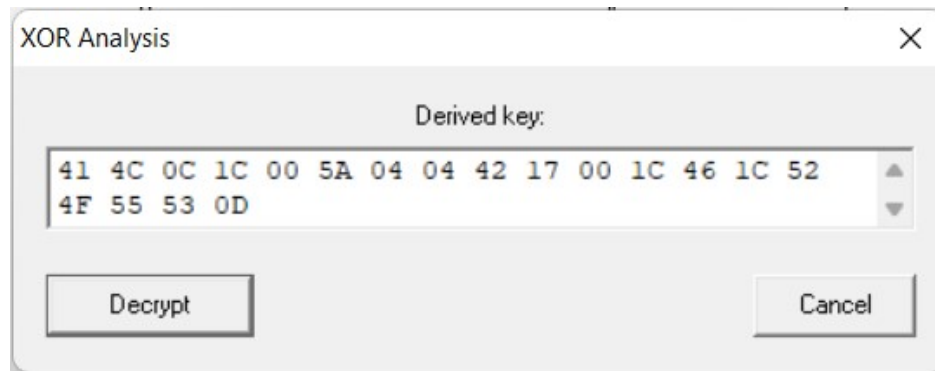
شکل ۲۴



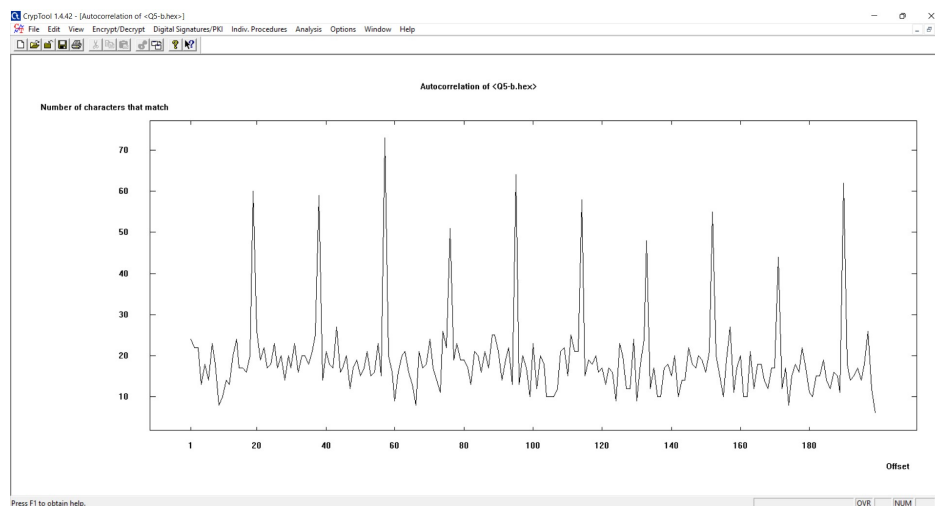
شکل ۲۵



شکل ۲۶



شکل ۲۷

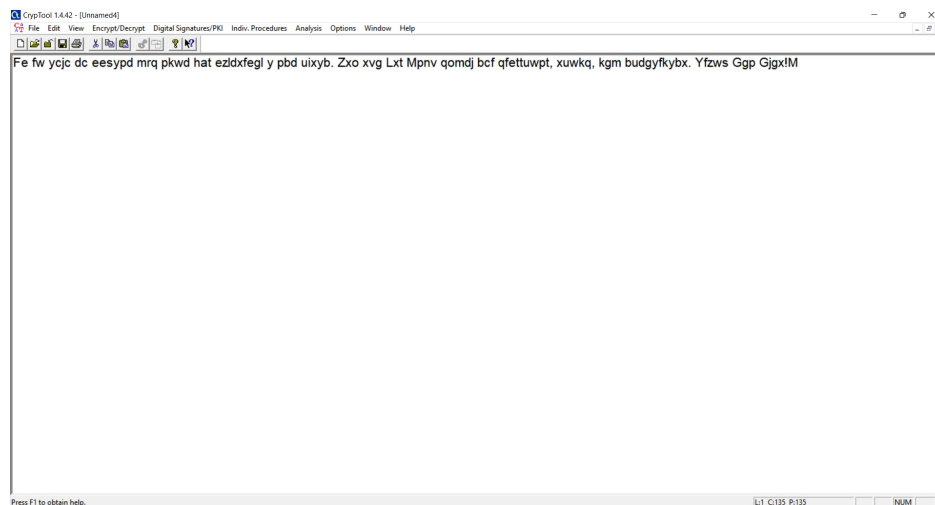


شکل ۲۸

همانطور که مشاهده می‌کنیم در حالت دوم که کلید دارای عبارات و کاراکترهای تکراری است طول کلید به درستی حدس زده شده است و همچنین قسمت‌هایی از کلید به درستی تشخیص داده شده است. پس امنیت پایین‌تری دارد.

۶.۲

در نرم افزار CrypTool به صورت زیر رمزگشایی می‌کنیم.



شکل ۲۹

Hill Analysis (Known Plaintext)

This is a known-plaintext analysis of Hill encryption. If the plaintext is available along with the ciphertext, the Hill key can be recomputed.

Plaintext Ciphertext

fh efuonw dhpe iegrmhkudgf. Bonsruc hgppk ubmy jwwvi woghdedpf.IK

[Please select a document.]

Hill encryption variants

Multiplication variant

☒ (row vector) * (matrix)

☐ (matrix) * (column vector)

Options

Search through the dimensions from 1 to 10

Continue Text options Cancel

شکل ۳۰

Display Hill Key Matrix

Selected alphabet (26 characters)
 ABCDEFGHIJKLMNOPQRSTUVWXYZ Value of the first alphabet character 0

Hill key matrix

Alphabet characters

R	K	P	A	L
H	L	B	L	L
F	R	V	A	M
Y	L	S	X	P
J	Q	E	Y	U

Number values

17	10	15	00	11
07	11	01	11	11
05	17	21	00	12
24	11	18	23	15
09	16	04	24	20

☒ Hill key matrix (encrypt)
☐ Inverse Hill key matrix (decrypt)

Multiplication variant

☒ (row vector) * (matrix)
☐ (matrix) * (column vector)

Value of the first alphabet character

☒ 0 (e.g. "A"=0)
☐ 1 (e.g. "A"=1)

Copy key Close

شکل ۳۱

Key Entry: Hill

Description

The Hill cipher is a polygraphic substitution cipher based on linear algebra. This was the first polygraphic cipher in which it was practical to operate on groups of more than three letters (blocks) at once. The key is a quadratic matrix. Its dimension is the length of the group of letters.

Selected alphabet (26 characters)

ABCDEFGHIJKLMNOPQRSTUVWXYZ

Value of the first alphabet character 0

Hill key matrix

☒ Alphabet characters ☐ Number values

Alphabet characters

R	K	P	A	L
H	L	B	L	L
F	R	V	A	M
Y	L	S	X	P
J	Q	E	Y	U

Number values

17	10	15	00	11
07	11	01	11	11
05	17	21	00	12
24	11	18	23	15
09	16	04	24	20

Generate random key

Reset key

Multiplication variant

☐ (row vector) * (matrix)

☒ (matrix) * (column vector)

Size of matrix

☐ 1 x 1

☐ 2 x 2

☐ 3 x 3

☐ 4 x 4

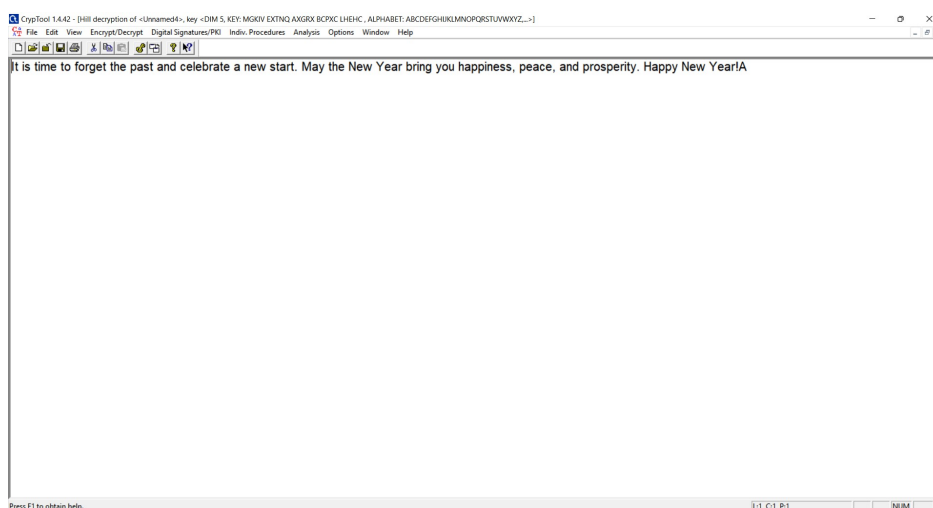
☒ 5 x 5

Larger matrix

☐ Show details and single steps of the Hill cipher

Encrypt Decrypt Further Hill options Text options Cancel

شکل ۳۲



شکل ۳۳

پیام محرمانه , peace, happiness, prosperity. Happy New Year!A”
”It is time to forget the past and celebrate a new start. May the New Year bring you and است.

منابع

□□□□□□□□□□