

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

١

١.١ سوال ٧.١

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	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

٣.١.١ سوال ٣.١.١

+	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

X	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 ۴.۱.۱

طبق جدول، ۲ در \mathbb{Z}_4 و ۲، ۳ و ۴ در \mathbb{Z}_6 فاقد وارون ضربی اند.

شرط لازم و کافی برای اینکه a به پیمانه m وارون ضربی داشته باشد این است که این دو عدد نسبت به هم اول باشند. از آنجایی که a عدد اول است، همه ی اعداد صحیح مثبت کمتر از a نسبت به a اول ند. پس وارون ضربی برای تمامی اعضای غیر صفر در a 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	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.

٣.١ سوال ٩.١

١.٣.١ سوال ١.٣.١

 $3^2 \equiv 9 \mod 13 \Rightarrow x = 9$

۲.۳.۱ سوال ۲.۳.۱

 $7^2 \equiv 10 \mod 13 \Rightarrow x = 10$

٣.٩.١ سوال ٣.٣.١

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

۴.۳.۱ سوال ۴.۳.۱

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

۵.۳.۱ سوال ۵.۳.۱

power	1	2	3	4	5		
7	7	10	5	9	11		

 $\Rightarrow x = 5$

۴.۱ سوال ۴.۱

m=4 1.4.1

(4,1) = 1

(4,3) = 1

m=5 7.4.1

(5,1) = 1

(5,2) = 1

(5,3) = 1

(5,4) = 1

m = 9 r.f.1

(9,1) = 1

(9,2) = 1

(9,4) = 1

(9,5) = 1

(9,7) = 1

(9,8) = 1

m = 26 f.f.1

(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 Δ.۴.\

$$\begin{split} \phi\left(4\right) &= 4 \prod_{p|4} \left(1 - \frac{1}{p}\right) = 2 \\ \phi\left(5\right) &= 5 \prod_{p|5} \left(1 - \frac{1}{p}\right) = 4 \\ \phi\left(9\right) &= 9 \prod_{p|9} \left(1 - \frac{1}{p}\right) = 6 \\ \phi\left(26\right) &= 26 \prod_{p|26} \left(1 - \frac{1}{p}\right) = 12 \end{split}$$

۵.۱ سوال ۱۳.۱

$$(x_1, y_1)$$

$$(x_2, y_2)$$

$$y_1 = e_k(x_1) \equiv ax_1 + b \mod m$$

 $y_2 = e_k(x_2) \equiv ax_2 + b \mod m$

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

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 پیمانه ی (x_1-x_2) وارون خربی داشته باشد این است که این دو عدد نسبت به هم اول باشند. پس Oscar با فرض دانستن m باید (x_1-x_2) به پیمانه (x_1-x_2) وارون خربی داشته باشیم:

$$\left(\left(x_{1}-x_{2}\right),m\right)=1$$

CrypTool 7

1.7

a 1.1.7

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

Х	A	1	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	1	m	M	n	d	q	t	r	a	d	a	g	e	t

در نرم افزار CrypTool به صورت زیر رمز می کنیم.

CrypTool 1.4.42 - [Caesar encryption of <startingexample-en.txt>, key <m, 0="" key="" offset:="">]</m,></startingexample-en.txt>	- o x
₩ File Edit View Encrypt/Decrypt Digital Signatures/PKI Indiv. Procedures Analysis Options Window Help	_ 8 ×
Alireza Abrehforoush	
Allieza Abrelliorousii	
Press F1 to obtain help.	L1 C/21 P/21 NUM
rica i i so successione.	ET CET PET NOM

شکل ۱

Description			
Here you can enter	the key for the Ca	esar cipher.	
Caesar is a mono-al alphabet are mappe	lphabetic substituti ed to the ciphertex	ion, where the characters of the o t alphabet by shifting. This shifting r as a single character of the alph	g value is the key
		key has the fixed value of half th is only selectable if the length of	
Select variant	Options to in	nterpret the alphabet characters-	
Caesar		e of the first alphabet character =	0 (e.g. "A"=0)
C Rot-13	○ Valu	e of the first alphabet character =	1 (e.g. "A"=1)
Key entry as			
Alphabet chaNumber value		8	
Properties of the cho	sen encryption		
Shift of	12		
Mapping of the alp	habet (26 charact	ers)	
from: ABCDEFG	GHIJKLMNOPQ	RSTUVWXYZ	
to: MNOPQRS	STUVWXYZABC	DEFGHIJKL	

شکل ۲



شکل ۳

۲.۲

 $9816603 \equiv 17 \mod 26$

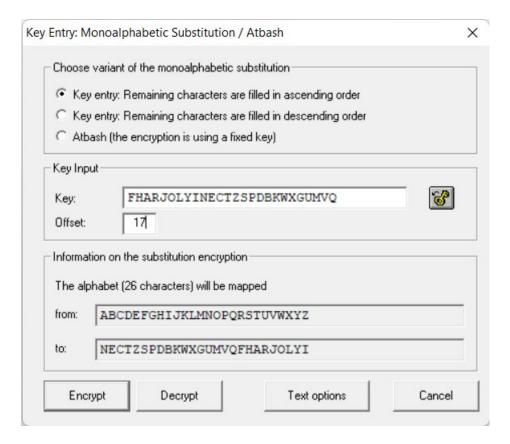
کلید Substitution cipher برابر Substitution cipher و offset و fharjolyinectzspdbkwxgumvq برابر ۱۷ است. در واقع الفبای انگلیسی به ترتیب به map NECTZSPDBKWXGUMVQFHARJOLYI می شود.



در نرم افزار CrypTool به صورت زیر رمز می کنیم.



شکل ۴



شکل ۵

(CypTool 1.4.42 - [Substitution exception of <cyp-caesar-startingexample-en.txt ,="" <nectzspobkyngumvqfharuquy-]="" analysis.="" deccypt.="" digital="" edit.="" encypt="" fig.="" file.="" help<="" indiv.="" key="" options.="" procedures.="" signature:pro.="" th="" view="" window.=""><th>- o x</th></cyp-caesar-startingexample-en.txt>	- o x
The cold view Encryptocetype Organisal Signature Pro Indiv. Procedure Analysis Options Window Prep	= D A
Hrcczhh rhrnxxy cmgzh am admhz odm nfz amm erhy am ez xmmwbup smf ba.	
Press F1 to obtain help.	L:1 C:1 P:1 NUM

شکل ۶

٣.٢

a 1.7.7

در Vigenère cipher در الفبای انگلیسی از یک جدول با ابعاد 26×26 استفاده می شود که در سطر iام آن حروف انگلیسی به ترتیب به صورت حلقوی با شروع از حرف iام الفبا نوشته شده است.

	A	В	C	D	E	F	G	Н	I	J	K	L	M	N	o	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	В	С	D	E	F	G	Н	I	J	K	L	M	N	О	P	Q	R	S	T	U	V	W	X	Y	Z
В	В	С	D	E	F	G	Н	I	J	K	L	M	N	О	P	Q	R	S	T	U	V	W	X	Y	Z	Α
C	С	D	Е	F	G	Н	I	J	K	L	M	N	О	P	Q	R	S	T	U	V	W	X	Y	Z	A	В
D	D	Е	F	G	Н	I	J	K	L	M	N	О	P	Q	R	S	T	U	V	W	X	Y	Z	A	В	C
E	Е	F	G	Н	I	J	K	L	M	N	0	P	Q	R	S	T	U	V	W	X	Y	Z	A	В	C	D
F	F	G	Н	I	J	K	L	M	N	О	P	Q	R	S	T	U	V	W	X	Y	Z	A	В	С	D	Е
G	G	Н	I	J	K	L	M	N	О	P	Q	R	S	T	U	V	W	X	Y	Z	A	В	С	D	Е	F
Н	Н	I	J	K	L	M	N	О	P	Q	R	S	T	U	V	W	X	Y	Z	A	В	С	D	Е	F	G
I	I	J	K	L	M	N	О	P	Q	R	S	T	U	V	W	X	Y	Z	A	В	С	D	Е	F	G	Н
J	J	K	L	M	N	О	P	Q	R	S	T	U	V	W	X	Y	Z	A	В	С	D	Е	F	G	Н	I
K	K	L	M	N	О	P	Q	R	S	T	U	V	W	X	Y	Z	A	В	С	D	Е	F	G	Н	I	J
L	L	M	N	О	P	Q	R	S	T	U	V	W	X	Y	Z	A	В	С	D	Е	F	G	Н	I	J	K
M	M	N	О	P	Q	R	S	T	U	V	W	X	Y	Z	A	В	С	D	Е	F	G	Н	I	J	K	L
N	N	О	P	Q	R	S	T	U	V	W	X	Y	Z	A	В	С	D	Е	F	G	Н	I	J	K	L	M
o	О	P	Q	R	S	T	U	V	W	X	Y	Z	A	В	С	D	Е	F	G	Н	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	В	C	D	Е	F	G	Н	I	J	K	L	M	N	О
Q	Q	R	S	T	U	V	W	X	Y	Z	A	В	С	D	Е	F	G	Н	I	J	K	L	M	N	О	P
R	R	S	T	U	V	W	X	Y	Z	A	В	С	D	Е	F	G	Н	I	J	K	L	M	N	О	P	Q
S	S	T	U	V	W	X	Y	Z	A	В	C	D	Е	F	G	Н	I	J	K	L	M	N	О	P	Q	R
T	T	U	V	W	X	Y	Z	A	В	C	D	Е	F	G	Н	I	J	K	L	M	N	О	P	Q	R	S
U	U	V	W	X	Y	Z	A	В	С	D	Е	F	G	Н	I	J	K	L	M	N	О	P	Q	R	S	T
V	V	W	X	Y	Z	A	В	C	D	Е	F	G	Н	I	J	K	L	M	N	О	P	Q	R	S	T	U
W	W	X	Y	Z	A	В	C	D	Е	F	G	Н	I	J	K	L	M	N	О	P	Q	R	S	T	U	V
X	X	Y	Z	A	В	С	D	Е	F	G	Н	I	J	K	L	M	N	О	P	Q	R	S	T	U	V	W
Y	Y	Z	A	В	С	D	Е	F	G	Н	I	J	K	L	M	N	О	P	Q	R	S	T	U	V	W	X
Z	Z	A	В	С	D	Е	F	G	Н	I	J	K	L	M	N	О	P	Q	R	S	T	U	V	W	X	Y

همچنین کلید مورد استفاده در این الگوریتم به صورت زیر (حرف اول نام + حرف اول نام خانوادگی) ساخته میشود. $ALIREZA\ ABREHFOROUSH \Rightarrow key = AA$

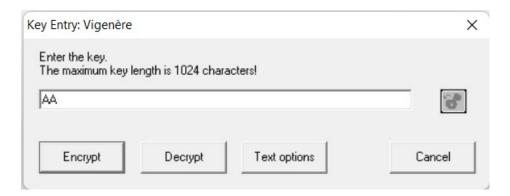
حال key را مکررا تکرار می کنیم تا طول آن برابر طول رشته ی که می خواهیم آن را رمز کنیم بشود (یا به عبارتی کاراکتر نظیر باقیمانده ی به پیمانه ی طول کلید (۶) را در کلید به دست آوریم). برای رمز کردن کاراکترِ iام در رشته، کاراکترِ اندیسِ باقیمانده ی باقیمانده ی طول کلید (۶) در کلید (key_i) به همراه خود کاراکترِ iام (x_i) به دست می آوریم. i بیمانه ی طول کلید (x_i) به همراه خود کاراکترِ (x_i) به دست می آوریم. (key_i) نظیر (x_i) باست.

key	A	а	a	а	а	a	a	а	a	a	a	a	a	a		a	a	a	a	a	T	a	a	a	a	a	a	а	T	а	a	a	а	а	a		a	а	а	а	ı a	a	a	а	a	2	a a	ı	а	a	a	а	а	a	а	T	a a	ıa	\Box	а	а	
x	S	u	с	с	e	s	s	u	s	u	a	1	1	у		с	о	m	e	s	Т	t	0	t	h	О	s	e		w	h	0	а	r	e	П	t	0	0	b) t	ı s	у	t	0	ŀ	5 0	:	1	o	o	k	i	n	g	. 1	f c) r		i	t	П
E(x)	S	u	с	с	e	s	s	u	s	u	a	1	1	у	П	с	o	m	e	s	Т	t	0	t	h	0	s	e	Т	w	h ·	0	a	r	e	П	t	0	0	ь) t	ıs	у	t	о	ŀ	5 0	-	1	o	o	k	i	n	g	Τ,	fι	г	П	i	t	П

در نرم افزار CrypTool به صورت زیر رمز می کنیم.



شکل ۷



شکل ۸

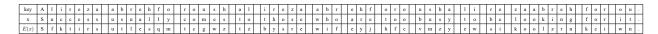


شکل ۹

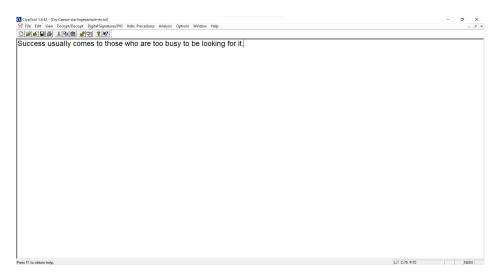
b 7.7.7

مشابه قسمت قبل (صرفا تغییر کلید) داریم:

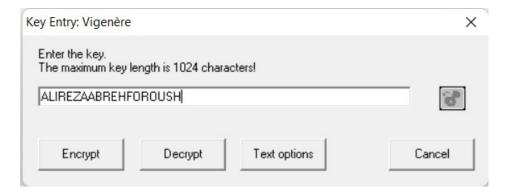
$ALIREZA\ ABREHFOROUSH \Rightarrow key = ALIREZAABREHFOROUSH$



در نرم افزار CrypTool به صورت زیر رمز می کنیم.



شکل ۱۰



شکل ۱۱

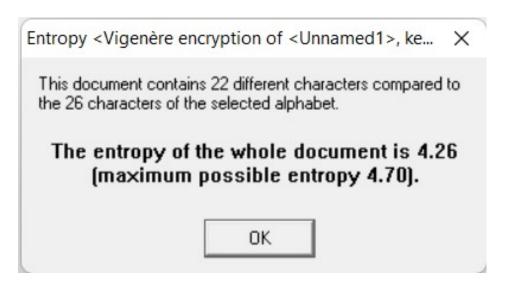


شکل ۱۲

c 7.7.7

Entropy <vigenère <unnamed1="" encryption="" of="">, ke</vigenère>	×
This document contains 19 different characters compared the 26 characters of the selected alphabet.	to
The entropy of the whole document is 3.8 (maximum possible entropy 4.70).	6
OK	

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.

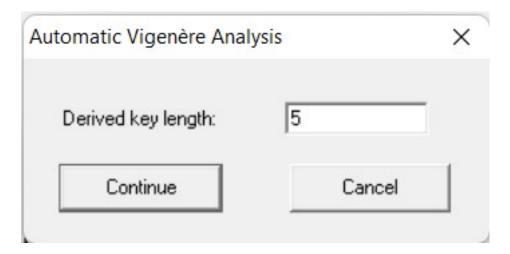
از آنجایی که در حالت دوم که طول کلید بیشتر است (کارکترهای متفاوتتری دارد) بینظمی (randomness) بیشتری وجود دارد، رمز امن تر است. در حالی که در حالت اول چون دو کاراکتر یکسان بودند صرفا از یک سطر (سطر اول که بدیهی هم هست) استفاده شده است و عبارت عملا رمز نشده است.

4.7

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

CrypTool 1.4.42 - [Automatic Vigenère Analysis of <startingexample-en.txt>, key: <smile>]</smile></startingexample-en.txt>	- ø ×
\$\frac{\chi}{c^4}\$ File Edit View Encrypt/Decrypt Digital Signatures/PKI Indiv. Procedures Analysis Options Window Help	_ E >
udgaxgat tw nqzj jdqftfdq iyh wmaj xg gap qswqyk af qoisx nzv lqinlazo aigbtp etace gjkxesydialq ub lpka kzrlmqyw kqdpvsx lpqgz. dpvq qidc la nzpdae irv nzpec pwhr ltm xeltmxelukd mffw dqsxt xefmopetxm dxwba.	aevsfqzr wjixtdqa elsf ici vqatkfql es tq
Dave 51 to admin hole	Ld. C240, D240

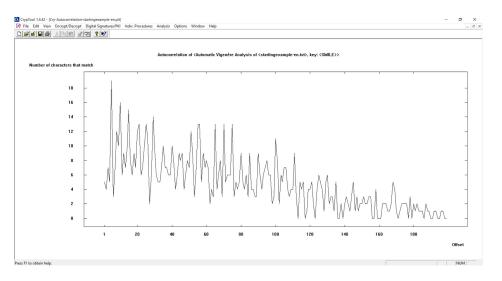
شکل ۱۵



شکل ۱۶



شکل ۱۷



شکل ۱۸

CypTool 1.4.42 - [Q4.txt] —	0 >	
😤 File Edit View Encrypt/Decrypt Digital Signatures/PKI Indiv. Procedures Analysis Options Window Help	_ 6	×
cryptool is very flexible and easy to use making it ideal for teaching people about cryptography it also contains several demonstration examples that are designed to very easy to follow and break down the mathematics into small manageable steps.	be	ą

شکل ۱۹

نمودار رسم شده autocorrelation را نشان می دهد. autocorrelation یک متن را با نسخههای مختلف شیفت یافته ی آن (به طول یکسان) مقایسه می کند. در هر حالت کاراکترهایی که باهم match می شوند (یکساناند) را تعیین می کنیم. در نمودار رسم شده تعداد کاراکترهای مقاست 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 می شوند. همچنین تعداد جابه جاییها به طول متن بستگی دارد (شما می توانید متنی متشکل از n کاراکتر را حداکثر n واحد جابجا کنید، سپس آنها به نوعی زیر یکدیگر قرار می گیرند). به مثال زیر توجه کنید.

Orginal text	S	u	c	c	e	s	s	T	u	s	u	а	1	1	у		c	o	m	e	5	T	Τ	t	o		t	h	0	s	e		w	h	c	1			е	1	 0		T	ы	ш	s	у		t	0		ь	e		1	0	0	k	i	n	g	f	0	r	T	i	t	_
Modified	S	u	c	с	e	s	s	u	s	u	a	1	1	у	с	0	m	e	s	t	() 1		h	o	s	e	w	h	0	a	r	e	t	c	1	,	1	s y	1	b	, (à	1 0	0	o	k	i	n	g	f	0	r	i	t										T		I	_
Shifted by 6	5						s	u	с	с	e	s	ŝ	u	s	u	a	1	1	у			, 1	m	e	s	t	0	t	h	0	s	e	w	ŀ	. [e 1		b	1	a :	s !	у	t	0	Ь	e	1	o	0	k	î	n	g	f	0	r	i	t	П			Т	П	Т	٦

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

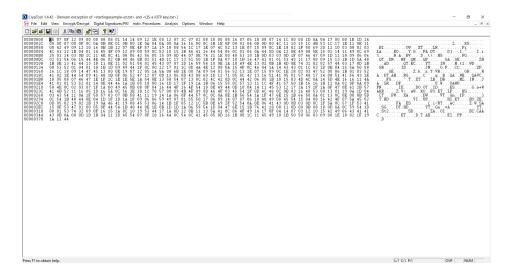
۵.۲

a 1.Δ.Υ

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

CrypTool 1.4.42 - [startingerample-en.txt]	- 0	×
🔀 File Edit View Encrypt/Decrypt Digital Signatures/PKI Indiv. Procedures Analysis Options Window Help	-	8 X
Today, Internet service providers (ISPs) try to deliver more and more valueadded services integrated with their residential Internet access offe triple-play (voice, Internet, and video). This situation generates the need for more powerful and expensive home devices to cover these needs, receives different names, from customer premise equipment (CPE) to residential router and to home gateway (HSW), but all have a common gibetween low-cost and rich functionalities, with a potentially negative effect on the device security. As a result, vHGW was one of the first scen adopted within the NFV paradigm, to demonstrate its potential in terms of efficiency and security. In this chapter, we are going to describe the that Telefonica designed and implemented in a commercial trial, to evaluate its potentiality.	This device round: the trade-of arios that were	ਹ ਜ਼ ਜ਼ਿਲ੍ਹਾ ਹ ਹ
Pres F1 to obtain help. L1 C884 P884	NUM	

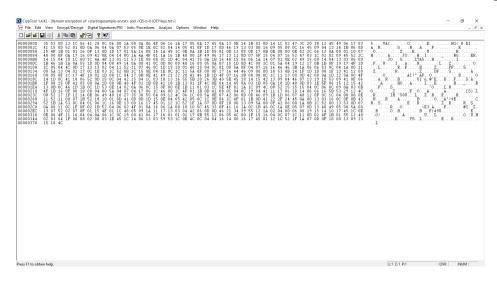
شکل ۲۰



شکل ۲۱

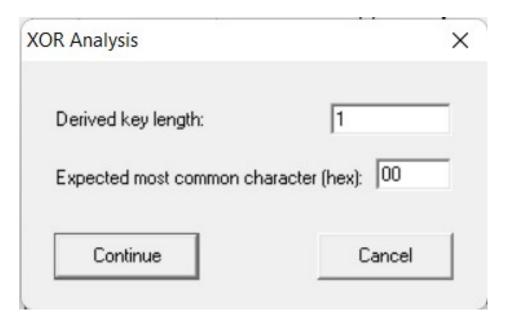
b Y.Δ.Y

plaintext مذکور را به شکل زیر با تکنیک one-time pad رمز می کنیم. از آنجایی که طول کلید OTP بایستی بزرگتر مساوی طول رشته plaintext (شته ای که می خواهیم رمز کنیم باشد؛ به سه روش کلید OTP را انتخاب می کنیم. یک بار کلید را برابر "ALIREZAABREHFOROUSH"، یک بار تکرار منظم حروف ALIREZAABREHFOROUSH (یعنی با حفظ ترتیب کاراکترها را مطابق با بزرگ یا کوچک بودن یا کاراکتر نمادی بودنِ plain text انتخاب می کنیم) و بار دیگر صرفا تکرار مکرر "Alireza Abrehforoush". هر سه حالت کلیدهای مذکور به پاسخ تکلیف پیوست شده است. (در اینجا فقط حالت اول آورده شده است)

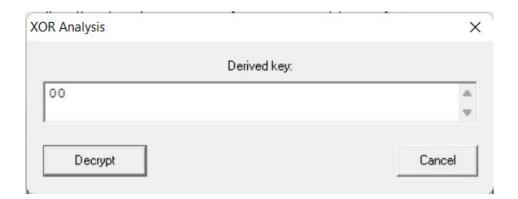


شکل ۲۲

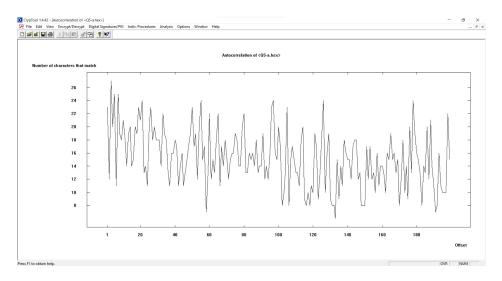
به شکل زیر تحلیل برای کشف کلید OTP به ترتیب برای قسمت a و b انجام می شود.



شکل ۲۳



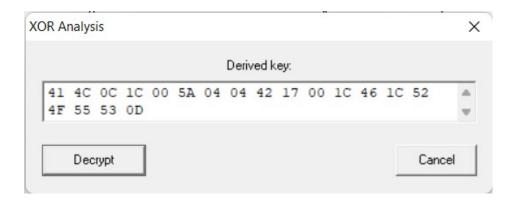
شکل ۲۴



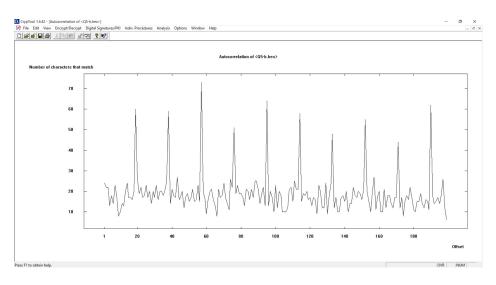
شکل ۲۵

XOR Analysis	×
Derived key length:	19
Expected most common ch	naracter (hex): 00
Continue	Cancel

شکل ۲۶



شکل ۲۷

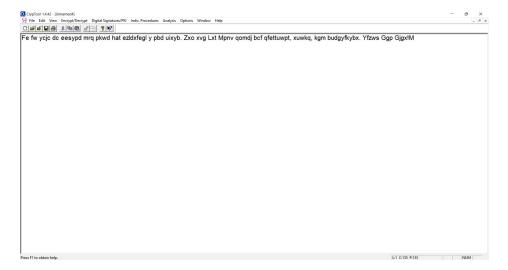


شکل ۲۸

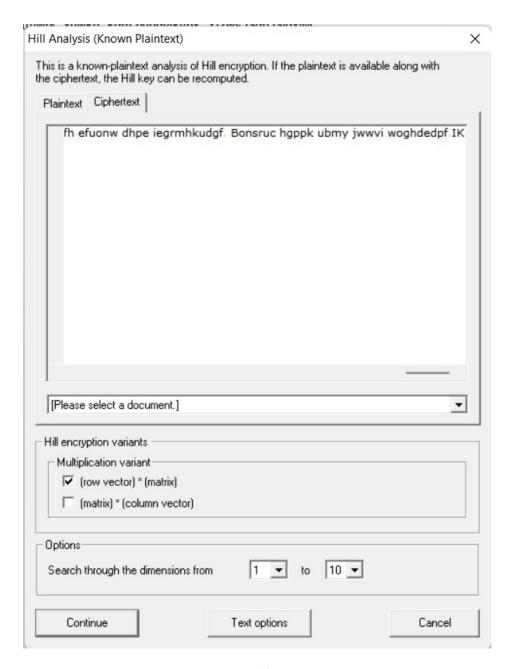
همانطور که مشاهده می کنیم در حالت دوم که کلید دارای عبارات و کاراکترهای تکراری است طول کلید به درستی حدس زده شده است. پس امنیت پایین تری دارد.

8.7

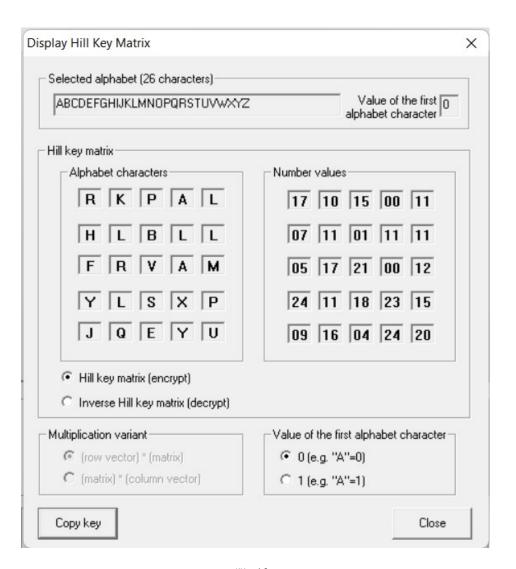
در نرم افزار CrypTool به صورت زیر رمزگشایی می کنیم.



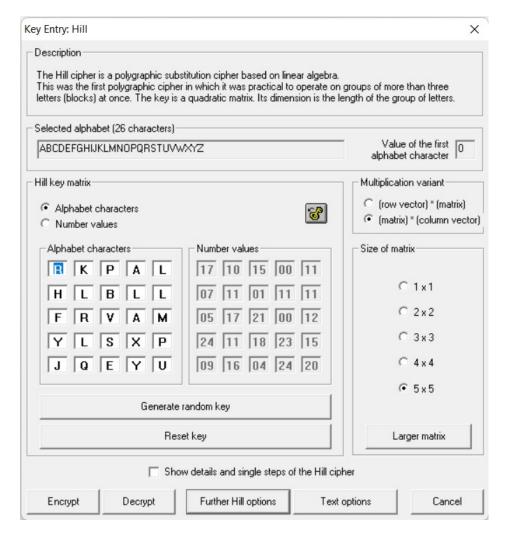
شکل ۲۹



شکل ۳۰



شکل ۳۱



شکل ۳۲

CrypTool 1.4.42 - [Hill decryption of CrypTool 1.4.42 - [Hill decryption of 	- o ×
$\frac{C_{1}^{2}}{C_{2}^{2}}$ File Edit View Encrypt/Decrypt Digital Signatures/PKI Indiv. Procedures Analysis Options Window Help	_ 8 ×
It is time to forget the past and celebrate a new start. May the New Year bring you happiness, peace, and prosperity. Happy New Year!A	
it is the to longer the past and detectate a new start. May the new Year bring you happiness, peace, and prosperty. Happy new Year bring you happiness, peace, and prosperty. Happy new Year bring you happiness,	

شکل ۳۳

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

منابع