



دانشگاه صنعتی اصفهان  
دانشکده مهندسی برق و کامپیوتر

عنوان: تکلیف دوم 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

”One-time pad is a cryptographic encryption technique that uses a random key that is as long as the message itself. The key is used only once, and both the sender and receiver must have a copy of the same key to encrypt and decrypt messages. Here are some pros and cons of one-time pad:

Pros:

1. Security: One-time pad encryption is considered to be unbreakable if used correctly, as it provides perfect secrecy. The encryption key used is completely random and cannot be guessed or predicted, making it virtually impossible for an attacker to break.
2. Simplicity: One-time pad encryption is simple to understand and implement, as it involves only the use of a random key and the XOR operation. It does not require complex algorithms or mathematical computations, making it a preferred choice for encrypting short messages.
3. Privacy: One-time pad encryption ensures complete privacy, as it does not reveal any information about the original message, even if an attacker intercepts the ciphertext.

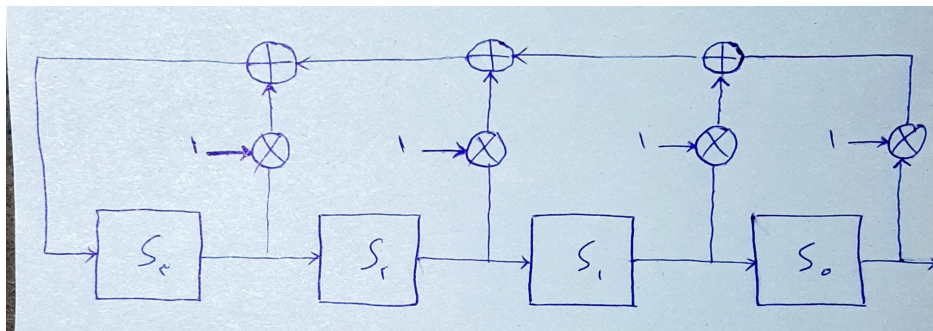
Cons:

1. Key distribution: One-time pad encryption requires both the sender and the receiver to have a copy of the same key. This can be challenging in practice, especially if the keys need to be distributed securely over long distances.
2. Key management: The one-time pad key can be used only once and must be discarded after use, making key management a challenge. Generating a truly random key that is as long as the message itself can also be difficult.
3. Size limitations: One-time pad encryption requires a key that is as long as the message, which can make it impractical for encrypting large amounts of data.
4. Vulnerable to certain attacks: One-time pad encryption is vulnerable to certain attacks, such as key reuse or guessing attacks, which can compromise the security of the encryption.”

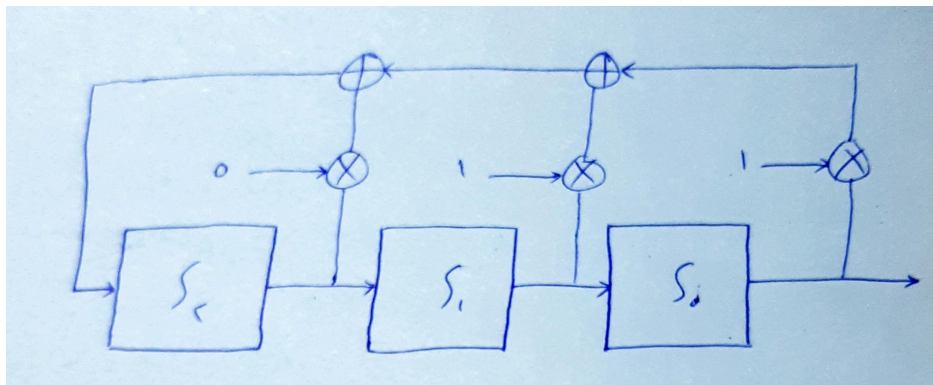
1. LFSRs which generate a maximum-length sequence. These LFSRs are based on primitive polynomials.
2. LFSRs which do not generate a maximum-length sequence but whose sequence length is independent of the initial value of the register. These LFSRs are based on irreducible polynomials that are not primitive. Note that all primitive polynomials are also irreducible.
3. LFSRs which do not generate a maximum-length sequence and whose sequence length depends on the initial values of the register. These LFSRs are based on reducible polynomials.

1.2.2

$$p_3 = p_2 = p_1 = p_0 = 1$$



شکل ۱

$$p_2 = 0, p_1 = p_0 = 1$$


شکل ۲

## ۳ CrypTool

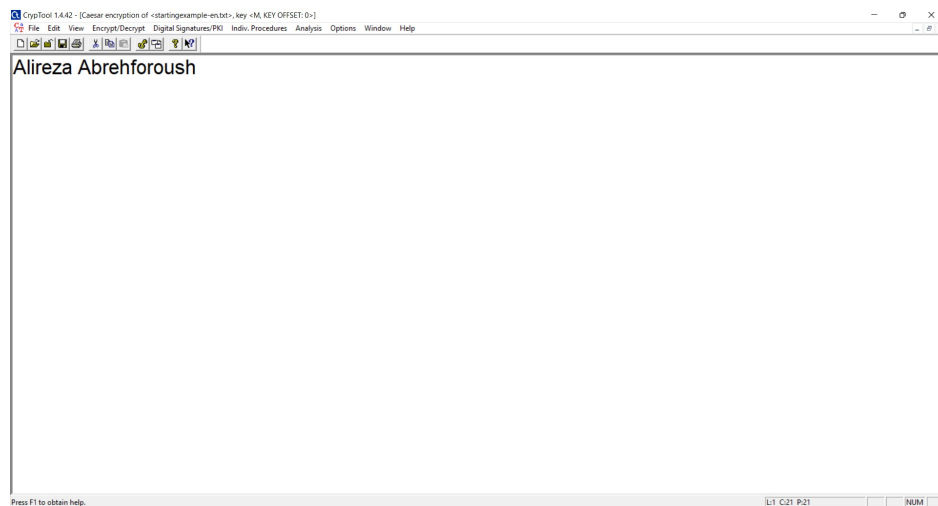
### ۱.۳

#### a ۱.۱.۳

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 ۳

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

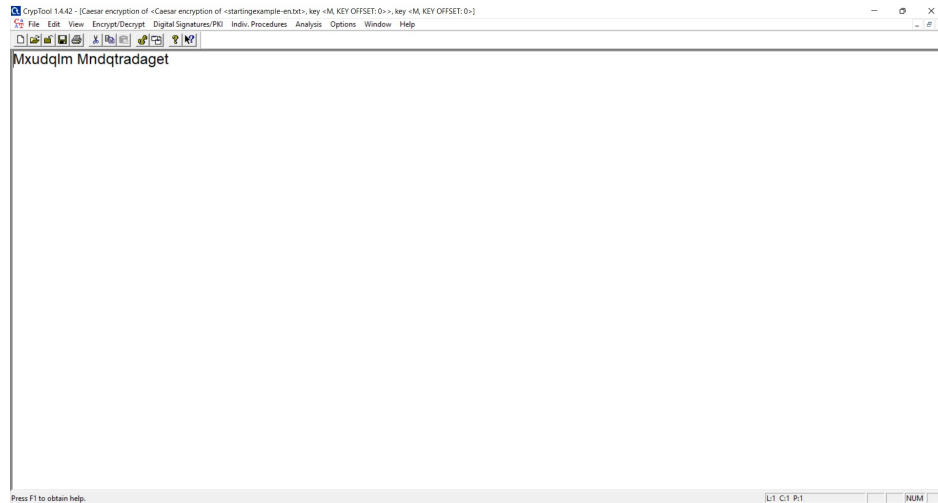
Mapping of the alphabet (26 characters)

from:

to:

Encrypt Decrypt Text options Cancel

شکل ۴



شکل ۵

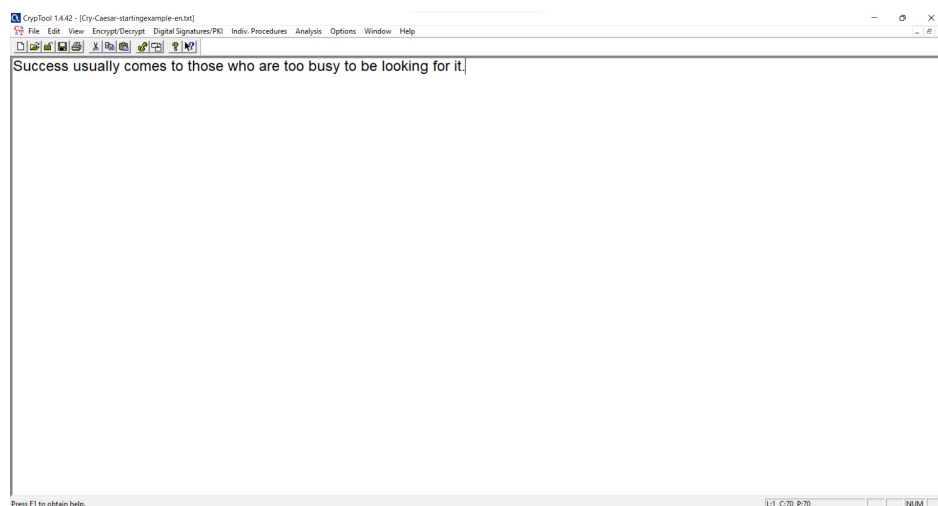
۲.۳

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

کلید Substitution cipher برابر fharjolyinectzspdbkwxgumvq 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 ۶

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

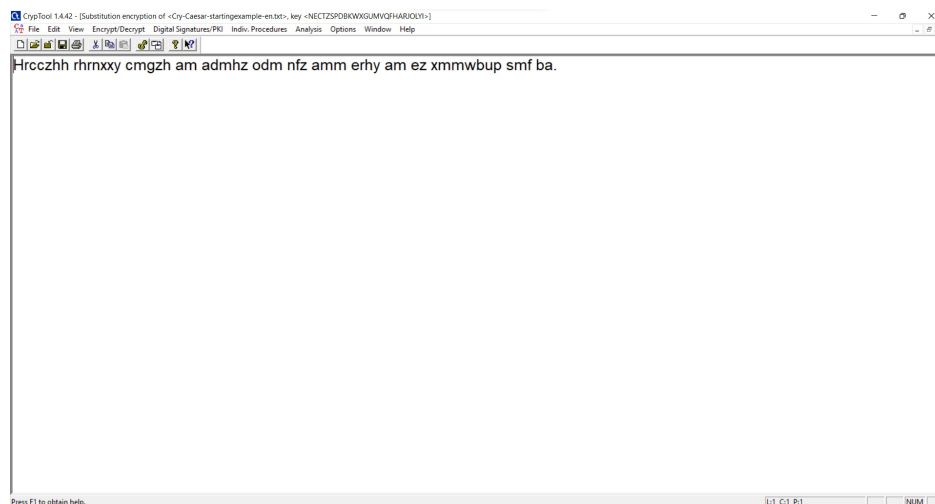
The alphabet (26 characters) will be mapped

from:

to:

Encrypt Decrypt Text options Cancel

شکل ۷



شکل ۸

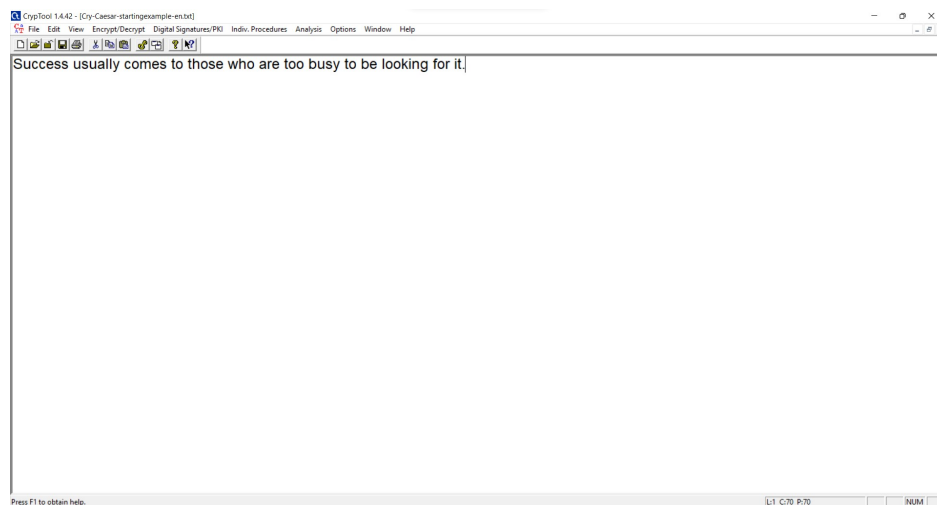
**a** 1.3.3

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

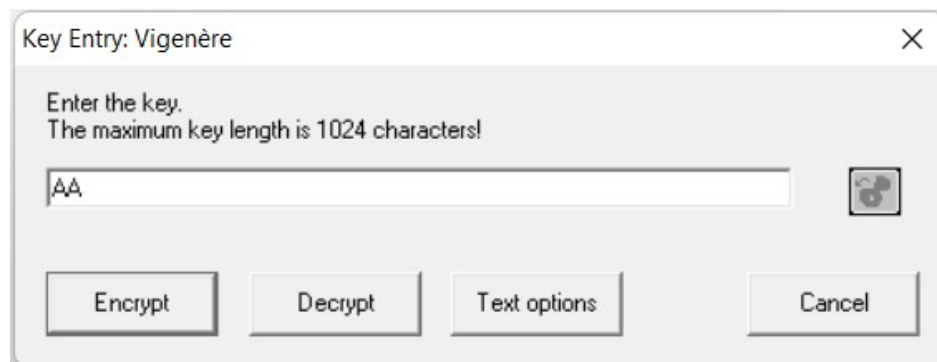
Key	A	a	a	a	a	a	a	a	a	a	a	a	a	a	a	a	a	a	a	a	a	a	a	a	a	a	a	a	a	a	a	a	.																												
$E(x)$	S	u	c	e	c	e	s	s	u	s	u	a	i	l	y	,	c	o	m	e	n	t	f	o	r	t	h	o	s	e	w	h	o	a	r	e	t	t	o	o	b	u	s	y	t	o	b	e	,	l	o	o	k	i	n	g	f	o	r	i	t



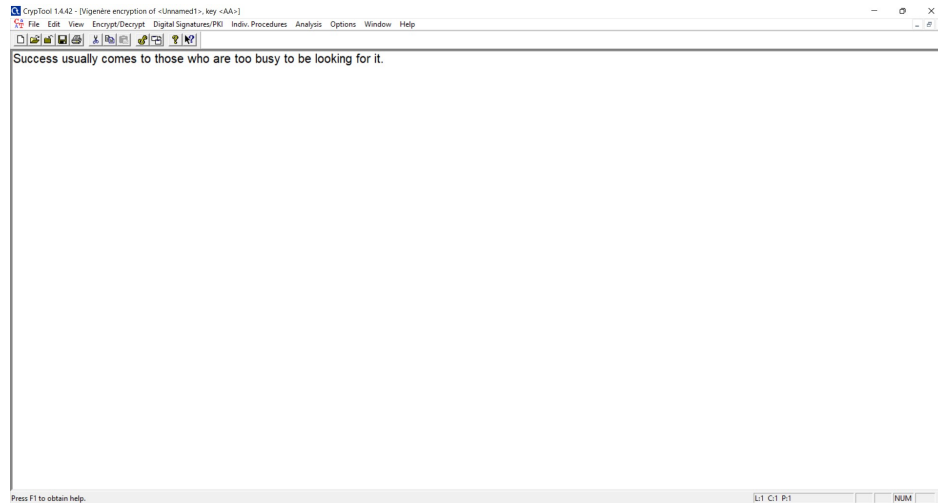
در نرم افزار CrypTool به صورت زیر رمز می کنیم.



شکل ۹



شکل ۱۰



شکل ۱۱

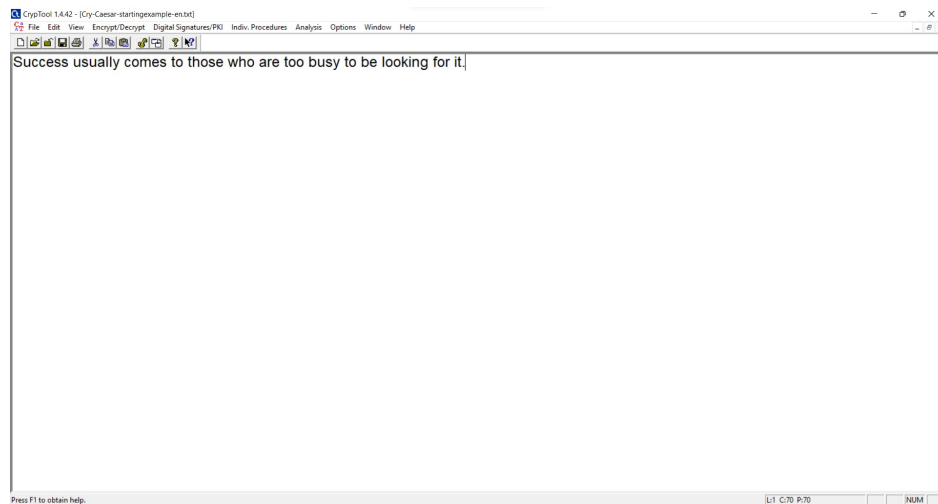
**b** ۲.۳.۳

مشابه قسمت قبل (صرفاً تغییر کلید) داریم:

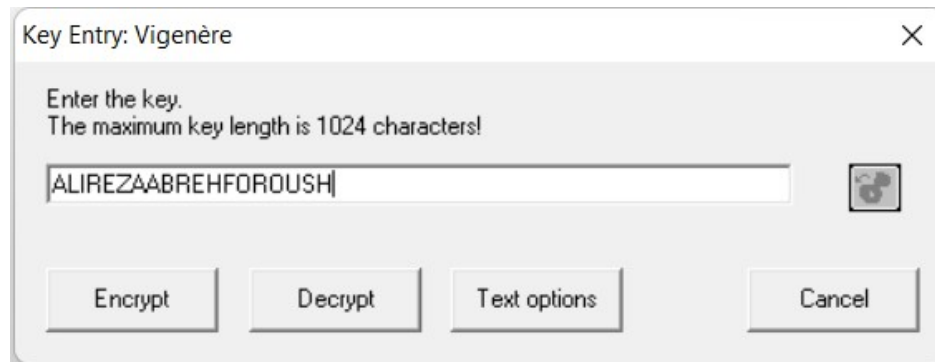
$$ALIREZA ABREHFORUSH \Rightarrow key = ALIREZAABREHFORUSH$$

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	.

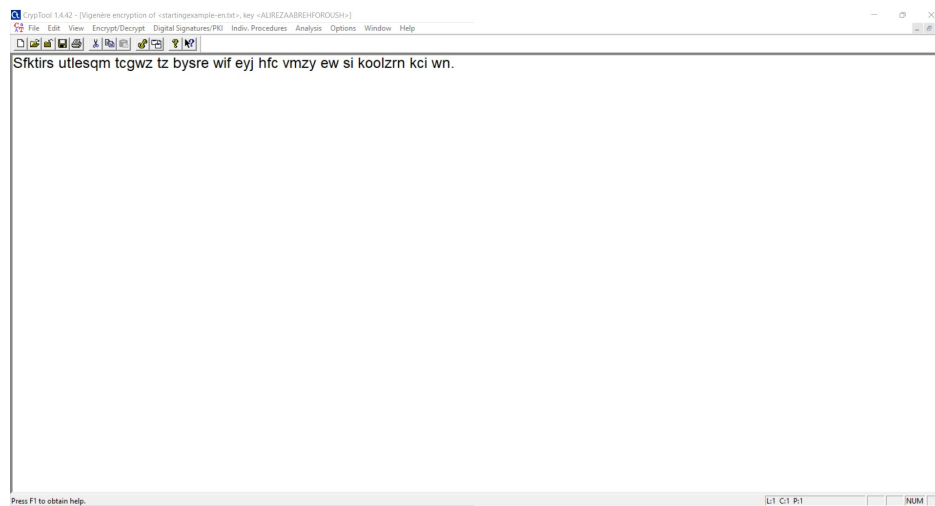
در نرم افزار CryTool به صورت زیر رمز می کنیم.



شکل ۱۲

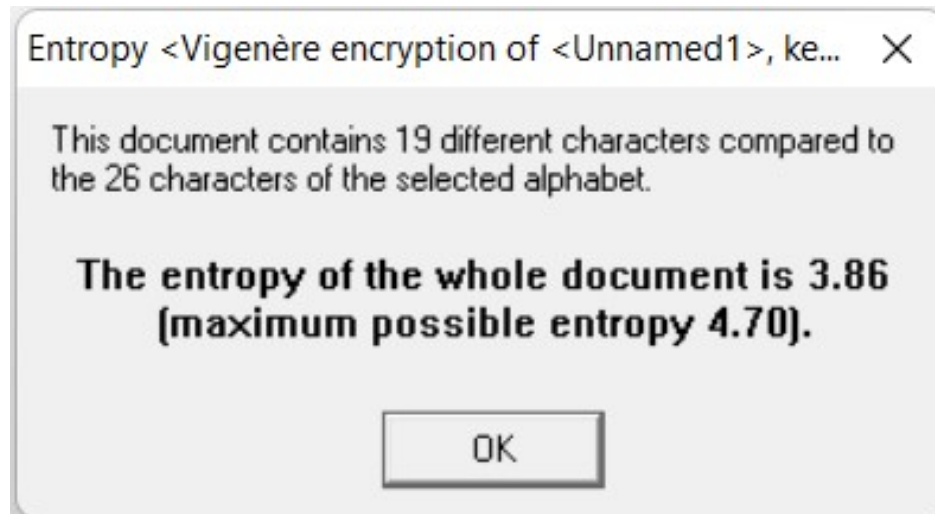


شکل ۱۳

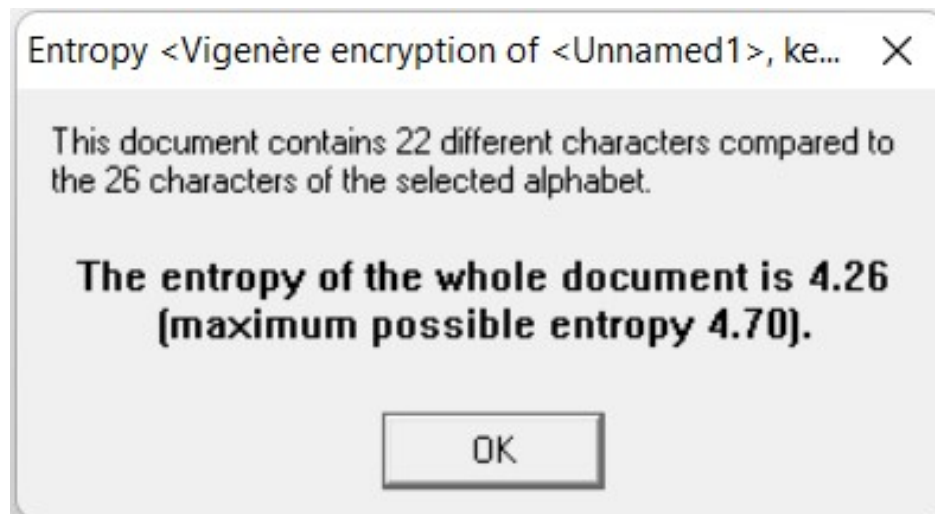


شکل ۱۴

c ۳.۳.۳



شکل ۱۵



شکل ۱۶

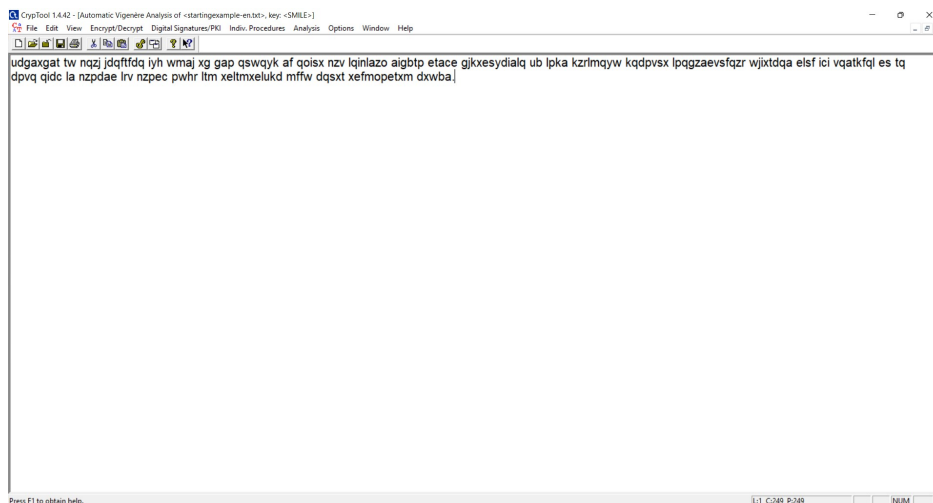
آنتروپی در حالت اول و دوم به ترتیب برابر ۸۶.۳ و ۲۶.۴ است.

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.

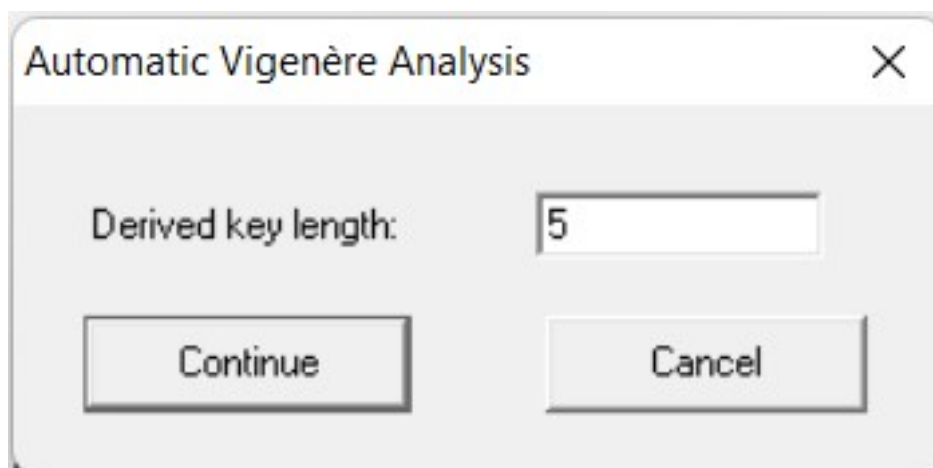
از آنجایی که در حالت دوم که طول کلید بیشتر است (کارکترهای متفاوت‌تری دارد) بی‌نظمی (randomness) بیشتری وجود دارد، رمز امن‌تر است. در حالی که در حالت اول چون دو کاراکتر یکسان بودند صرفاً از یک سطر (سطر اول که بدیهی هم هست) استفاده شده است و عبارت عملاً رمز نشده است.

## ۴.۳

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.



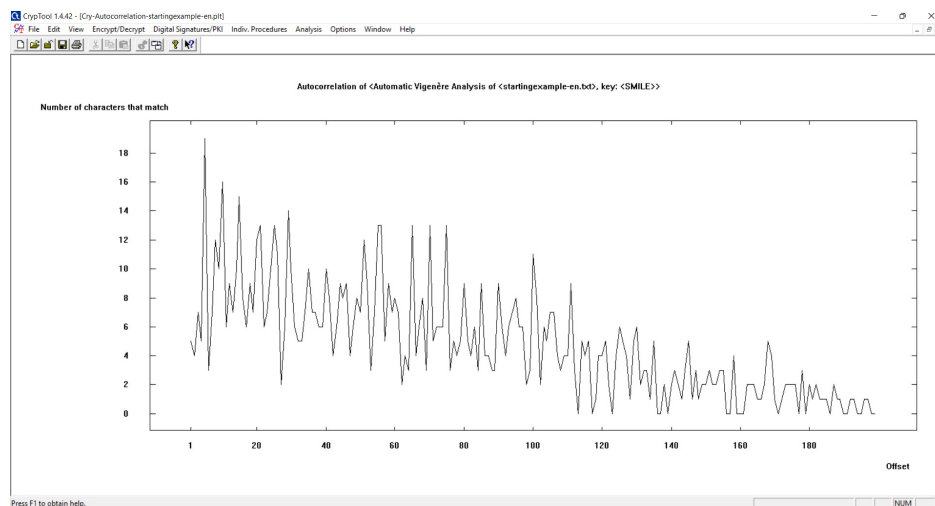
شکل ۱۷



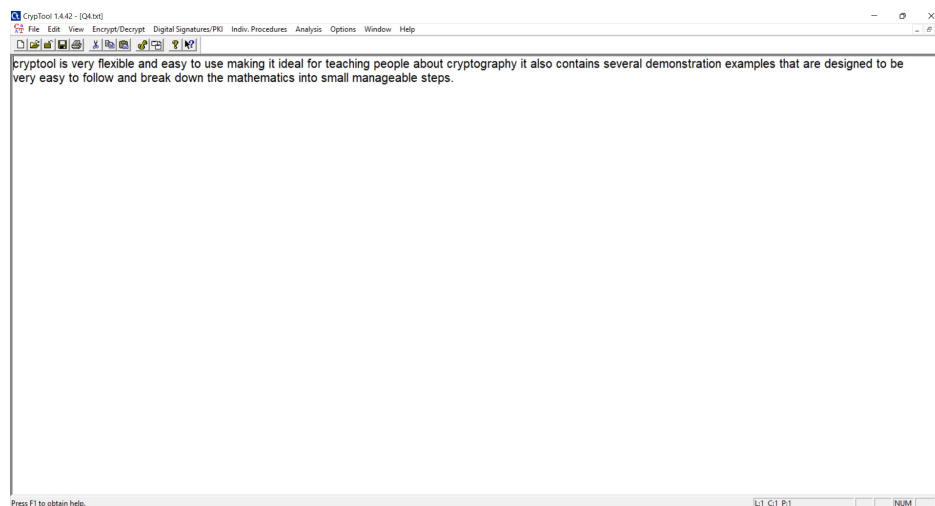
شکل ۱۸



شکل ۱۹



شکل ۲۰



شکل ۲۱

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	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	.

**a** 1.5.3

CrypTool 1.4A2 - [startingexample-encrypted]

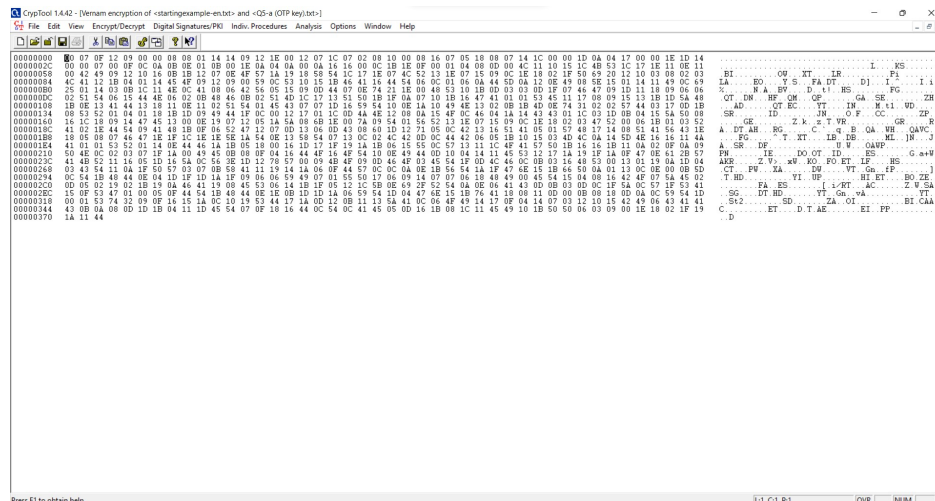
File Edit View Encrypt/Decrypt Digital Signatures (PKI) Indiv. Procedures Analysis Options Window Help

Today, Internet service providers (ISPs) try to deliver more and more value-added services integrated with their residential Internet access offer, such as triple-play (voice, Internet, and video). This situation generates the need for more powerful and expensive home devices to cover these needs. This device receives different names, from customer premise equipment (CPE) to residential router and to home gateway (HGW), but all have a common ground: the trade-off between low-cost and rich functionalities, with a potentially negative effect on the device security. As a result, vHGW was one of the first scenarios that were adopted within the NFV paradigm, to demonstrate its potential in terms of efficiency and security. In this chapter, we are going to describe the NFV architecture that Telefonica designed and implemented in a commercial trial, to evaluate its potentiality.

Page 1 | to obtain data

3-1 C:\SRL-0-004

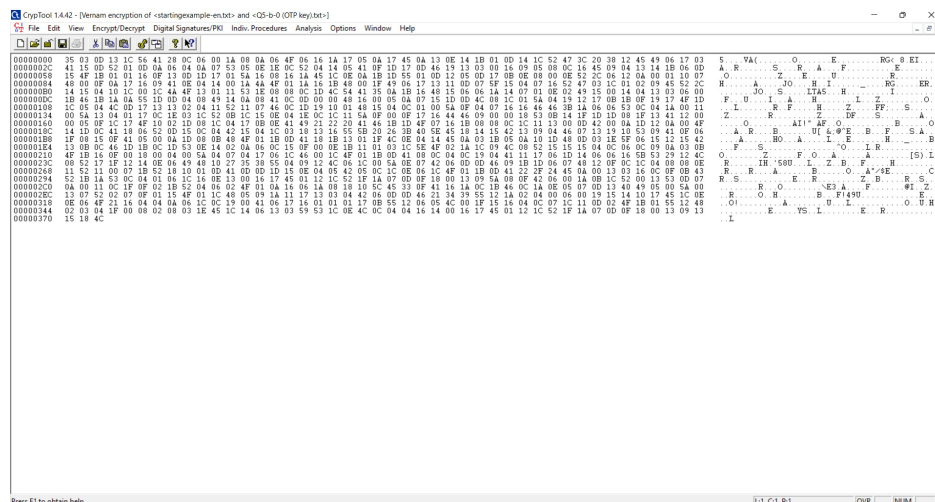
علیرضا ابره فروش



شکل ۲۳

b ۲.۵.۳

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؛ به سه روش کلید OTP را انتخاب می‌کنیم. 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 بودن plain text انتخاب می‌کنیم) و بار دیگر صرفاً تکرار مکرر "Alireza Abrehforoush". هر سه حالت کلیدهای مذکور به پاسخ تکلیف پیوست شده است. (در اینجا فقط حالت اول آورده شده است)

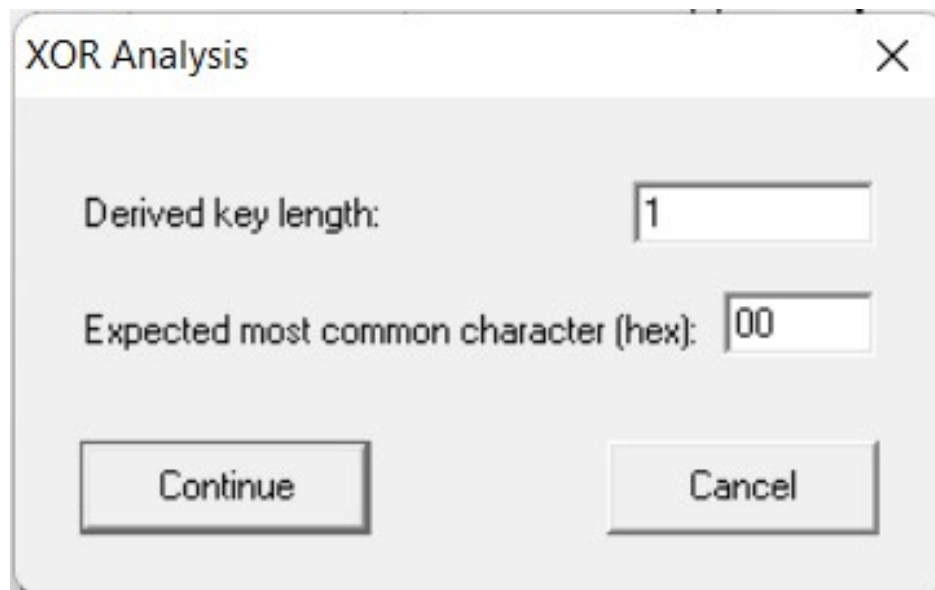


شکل ۲۴

c ۳.۵.۳

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

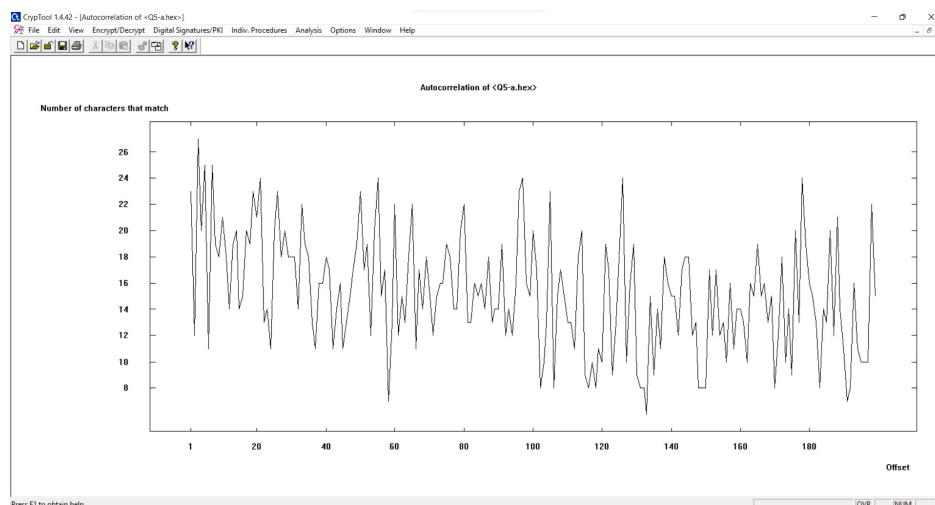




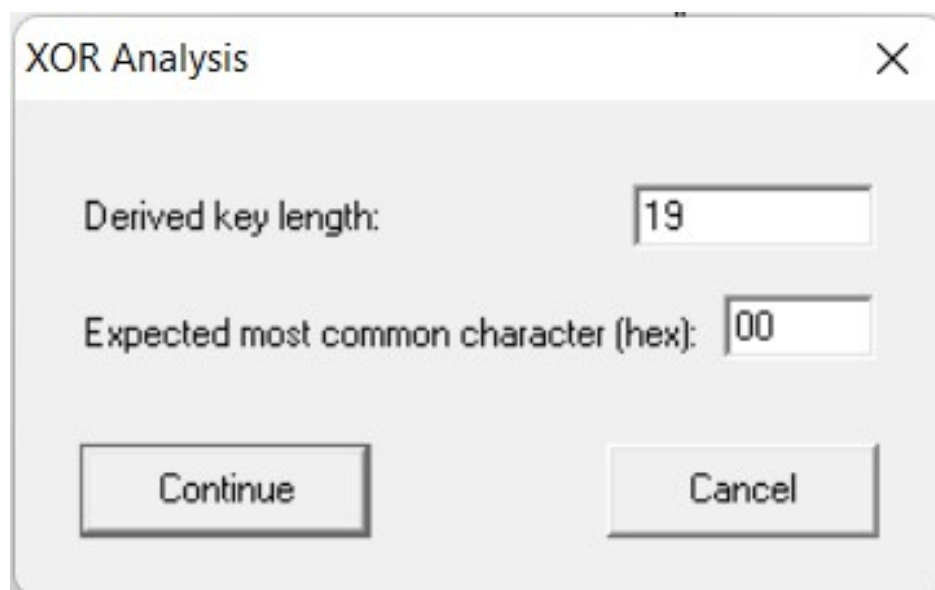
شکل ۲۵



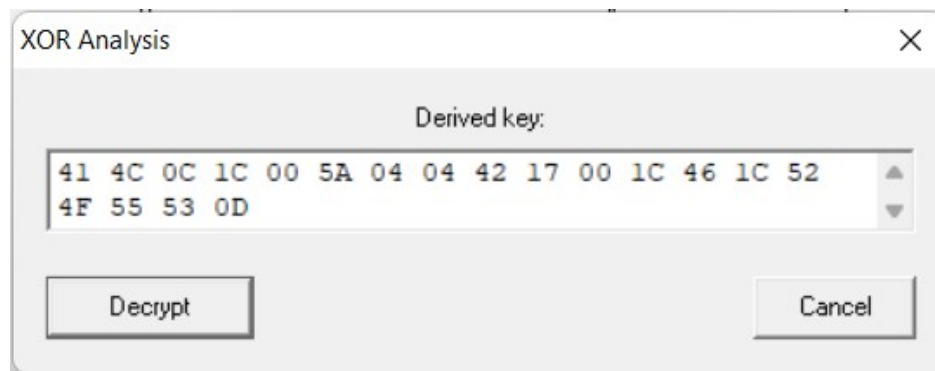
شکل ۲۶



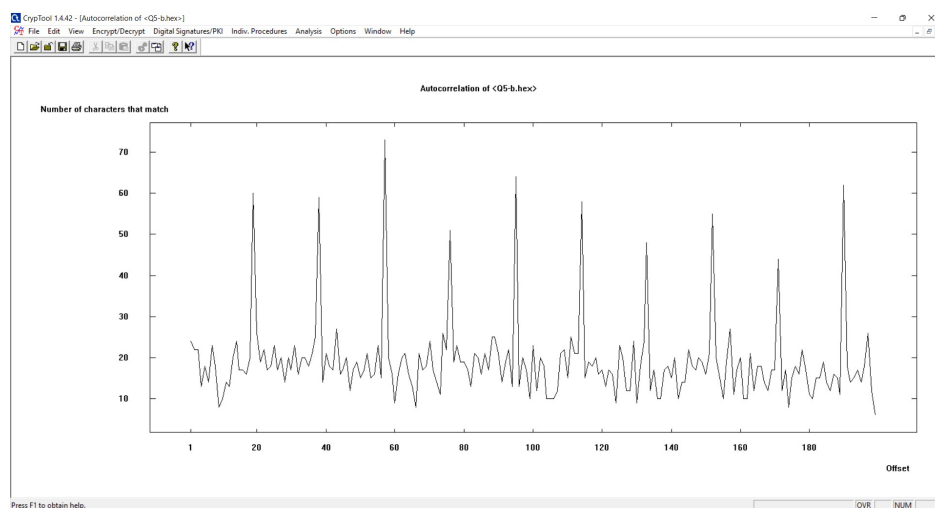
شکل ۲۷



شکل ۲۸



شکل ۲۹

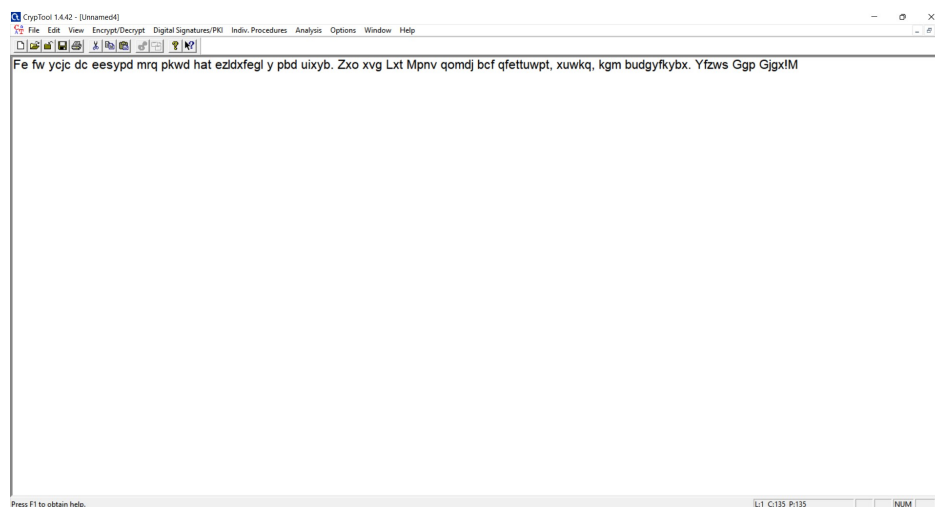


شکل ۳۰

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.

### ۶.۳

در نرم افزار CrypTool به صورت زیر رمزگشایی می‌کنیم.



شکل ۳۱

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  to

Continue Text options Cancel

شکل ۳۲

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 ۳۳

**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

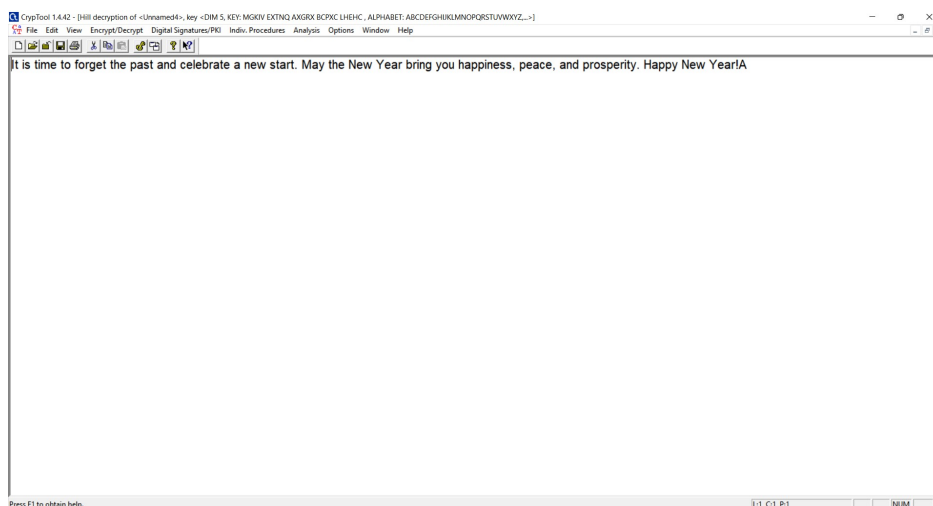
☒ 5 x 5

Larger matrix

☐ Show details and single steps of the Hill cipher

Encrypt Decrypt Further Hill options Text options Cancel

شکل ۳۴



شکل ۳۵

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

□□□□□□□□□□