



دانشگاه صنعتی اصفهان
دانشکده مهندسی برق و کامپیوتر

عنوان: تکلیف اول درس مبانی هوش محاسباتی

نام و نام خانوادگی: علیرضا ابره فروش

شماره دانشجویی: ۹۸۱۶۶۰۳

نیم سال تحصیلی: بهار ۱۴۰۲/۱۴۰۱

مدرس: دکتر مهران صفایانی

دستیاران آموزشی: فاطمه پیری-علیرضا حبیبی-علیرضا صالحی

۱.۱ نتیجه (خروجی)

A linear regression model relies on a continuous dependent variable. This implies that the dependent variable takes up numeric values instead of being classified under categories or groups. In contrast, logistic regression models rely on binary dependent variables. The dependent (or response) variable can take up only two values – 0 or 1. Also, linear regression output has a continuous value (it gives a range of values). For example,

- Length of the roof (25 inches, 19 inches, 5 ft)
- Height (5 ft 8 inches, 6 ft 2 inches, 5 ft 10 inches)
- Escape velocity (26000 mph, 21500 mph, 29500 mph)

On the other hand, the logistic regression model is revealed via probabilities. For example,

- 84.3% chance of losing a tennis match
- 23.1% chance of passing a bill in Congress
- 65.1% chance of imposing a curfew during a COVID-19 outbreak

Moreover, linear regression observes a normal or gaussian distribution, and logistic regression reveals a binomial distribution.

۲.۱ ارتباط بین متغیرها

Understanding the relationship between variables is crucial when deciding the type of regression model to be used for different purposes.

Linear regression describes a linear relationship between variables by plotting a straight line on a graph. It enables professionals to check on these linear relationships and track their movement over a period. On the contrary, logistic regression is known to study and examine the probability of an event occurrence. Since it does not denote a linear structure of a variable relationship, tracking logistic regression using linear structures is not required.

۱.۲ 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

۱.۱.۲ 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

۲.۱.۲ 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

۳.۱.۲ 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

\times	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

۴.۱.۲ 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.

۲.۲ سوال ۸.۱

\times	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.

۳.۲ سوال ۹.۱

۱.۳.۲ سوال ۱.۹.۱

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

۲.۳.۲ سوال ۲.۹.۱

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

۳.۳.۲ سوال ۳.۹.۱

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

۴.۳.۲ سوال ۴.۹.۱

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

۵.۳.۲ سوال ۵.۹.۱

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

$$\Rightarrow x = 5$$

۴.۲ سوال ۱۰.۱

$$m = 4 \quad ۱.۴.۲$$

$$(4, 1) = 1$$

$$(4, 3) = 1$$

$$m = 5 \quad ۲.۴.۲$$

$$(5, 1) = 1$$

$$(5, 2) = 1$$

$$(5, 3) = 1$$

$$(5, 4) = 1$$

$$m = 9 \quad ۳.۴.۲$$

$$(9, 1) = 1$$

$$(9, 2) = 1$$

$$(9, 4) = 1$$

$$(9, 5) = 1$$

$$(9, 7) = 1$$

$$(9, 8) = 1$$

$$m = 26 \quad ۴.۴.۲$$

$$(26, 1) = 1$$

$$(26, 3) = 1$$

$$(26, 5) = 1$$

$$(26, 7) = 1$$

$$(26, 9) = 1$$

$$(26, 11) = 1$$

$$(26, 15) = 1$$

$$(26, 17) = 1$$

$$(26, 19) = 1$$

$$(26, 21) = 1$$

$$(26, 23) = 1$$

$$(26, 25) = 1$$

Euler's phi function ۵.۴.۲

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

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

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

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

سوال ۱۳.۱ ۵.۲

$$(x_1, y_1)$$

$$(x_2, y_2)$$

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

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

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

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

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:

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

۳ CrypTool

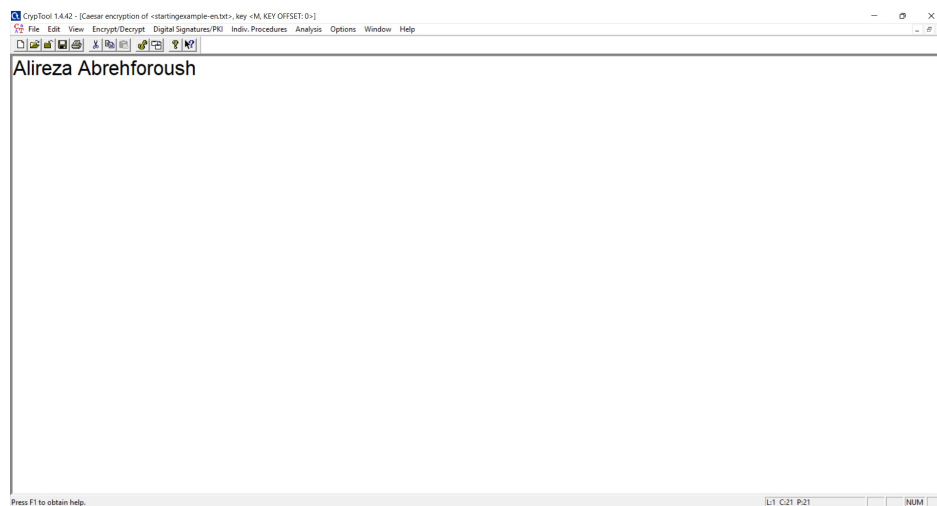
۱.۳

۱.۱.۳ a

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

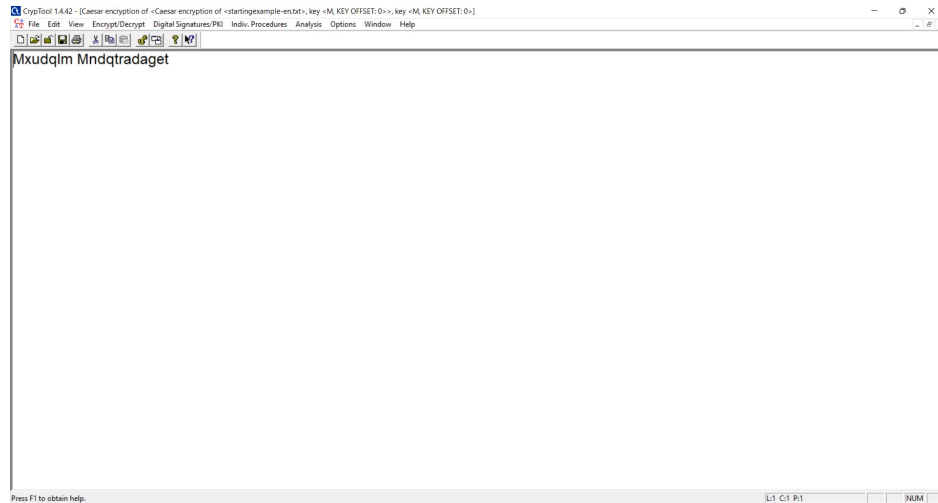
Options to interpret the alphabet characters
☒ Value of the first alphabet character = 0 (e.g. "A"=0)
☐ Value of the first alphabet character = 1 (e.g. "A"=1)

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

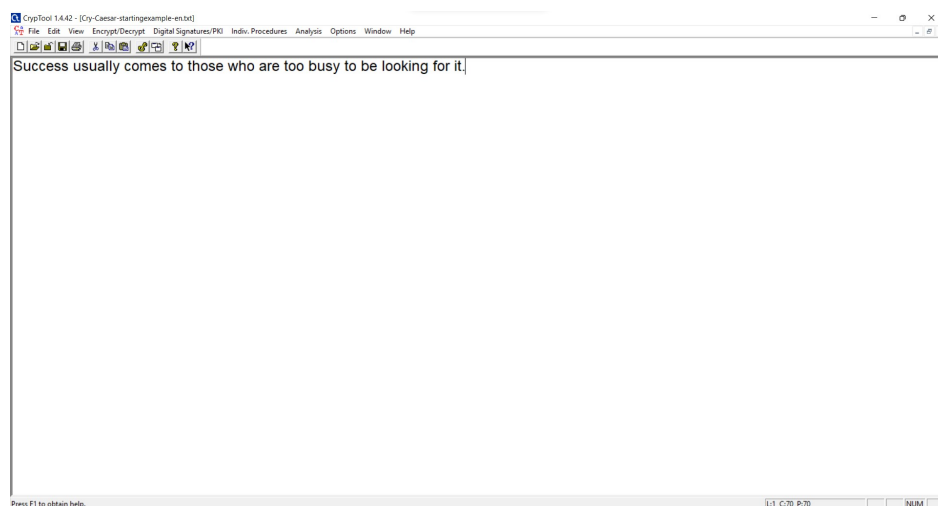
۲.۳

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

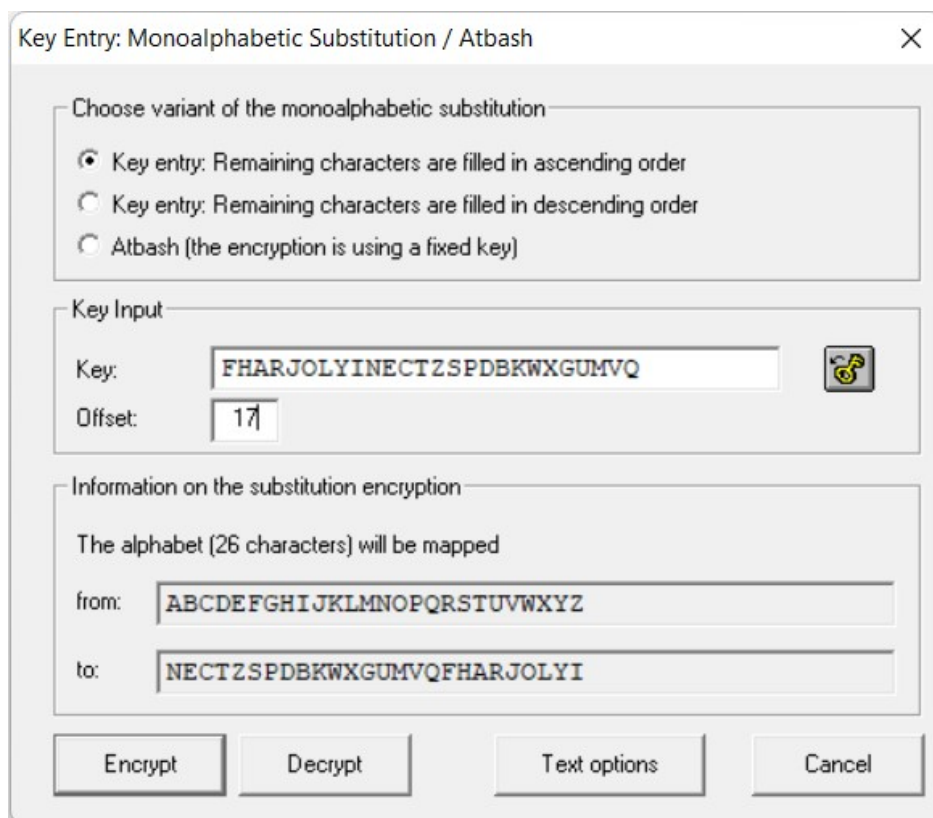
کلید Substitution cipher برابر fharjolyinectzspdbkwxgumvq و offset آن برابر ۱۷ است. در واقع الفبای انگلیسی به ترتیب به map NECTZSPDBKWXGUMVQFHARJOLYI می‌شود. پس در نهایت به صورت زیر رمز می‌شود.

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	.

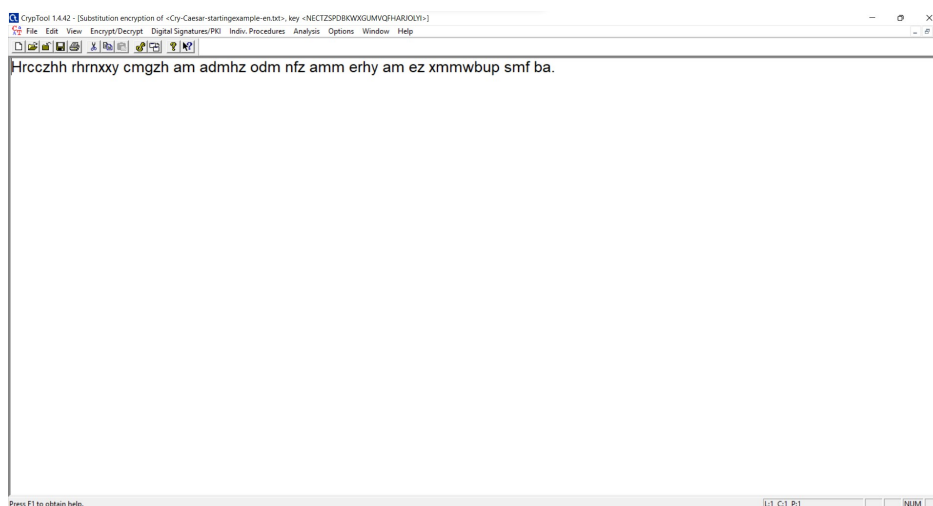
در نرم افزار CrypTool به صورت زیر رمز می‌کنیم.



شکل ۴



شکل ۵



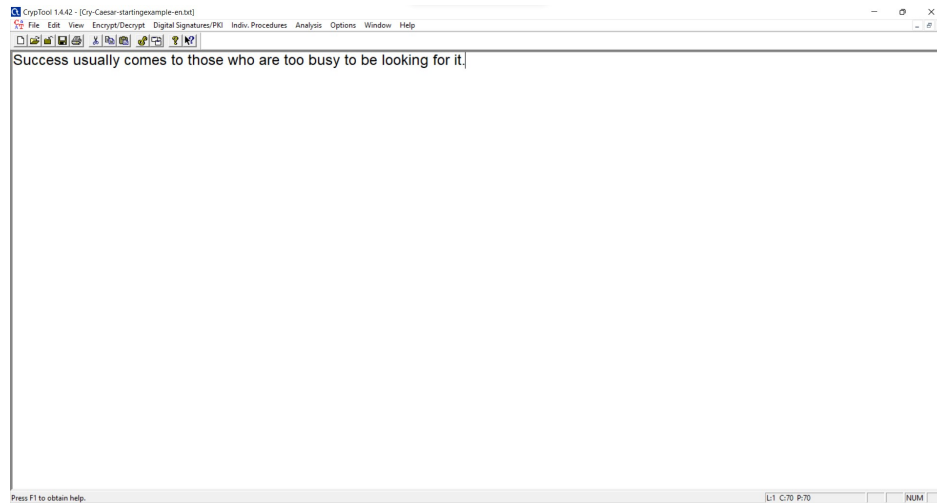
شکل ۶

a ۱.۳.۳

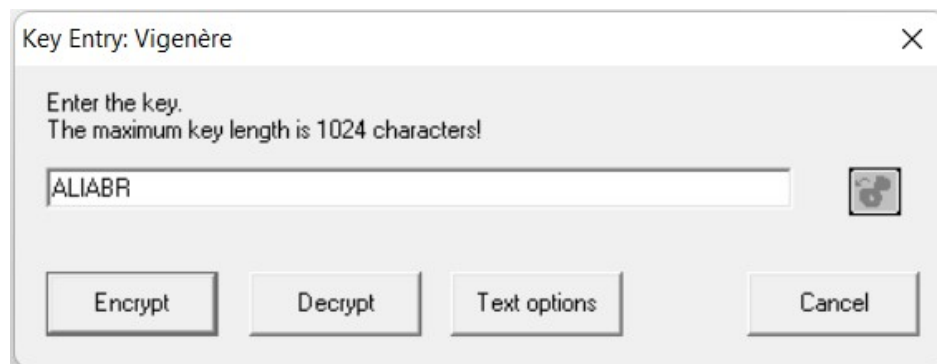
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y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

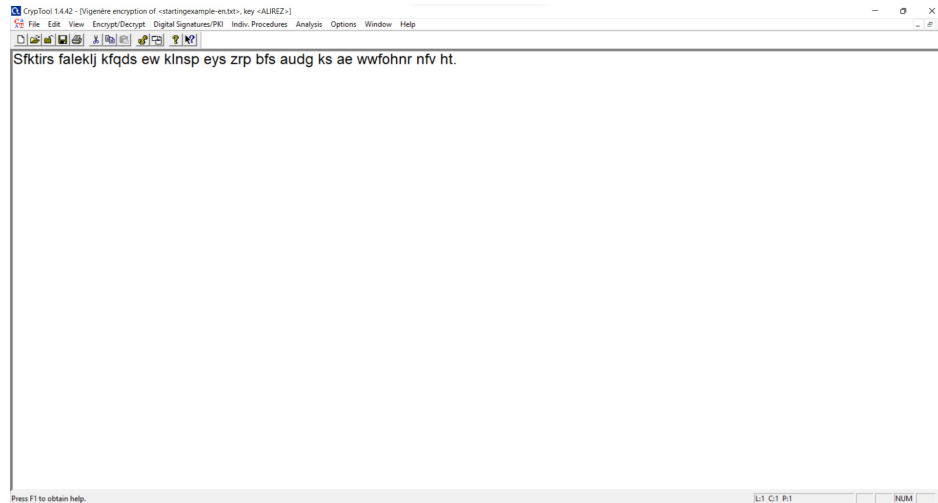
در نرم افزار CrypTool به صورت زیر رمز می کنیم.



شکل ۷



شکل ۸



شکل ۹

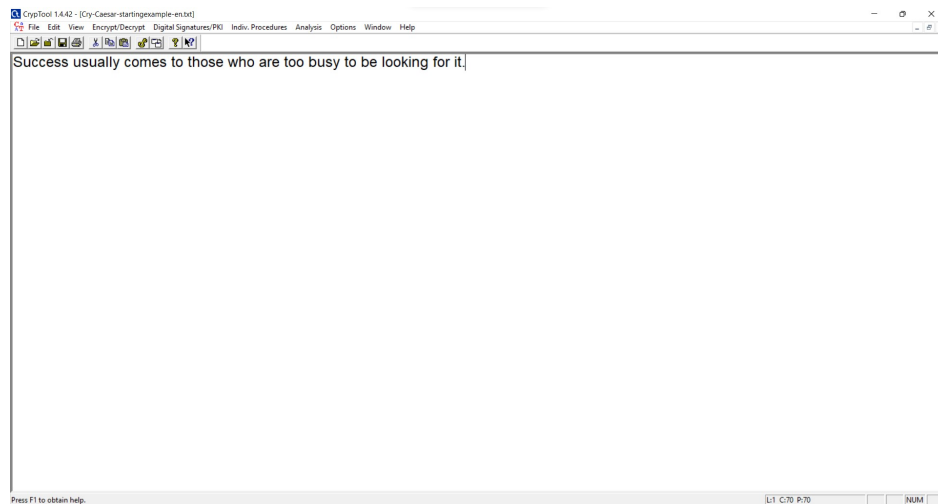
۲.۳.۳ b

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	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	l	o	k	i	n	g	f	o	r	i	t	.		
$E(x)$	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	e	w	s	i	k	o	o	l	i	z	i	n	g	k	c	i	w	n	.

در نرم افزار CrypTool به صورت زیر رمز می کنیم.



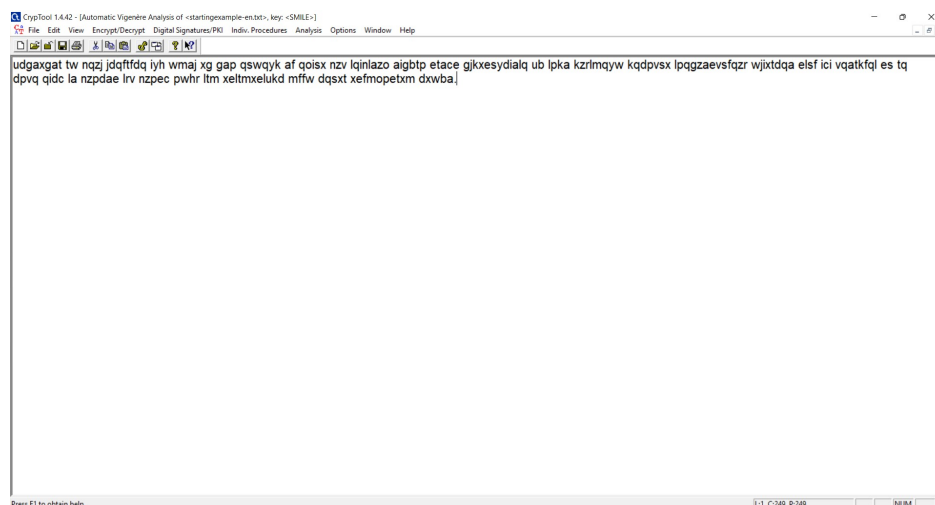
شکل ۱۰



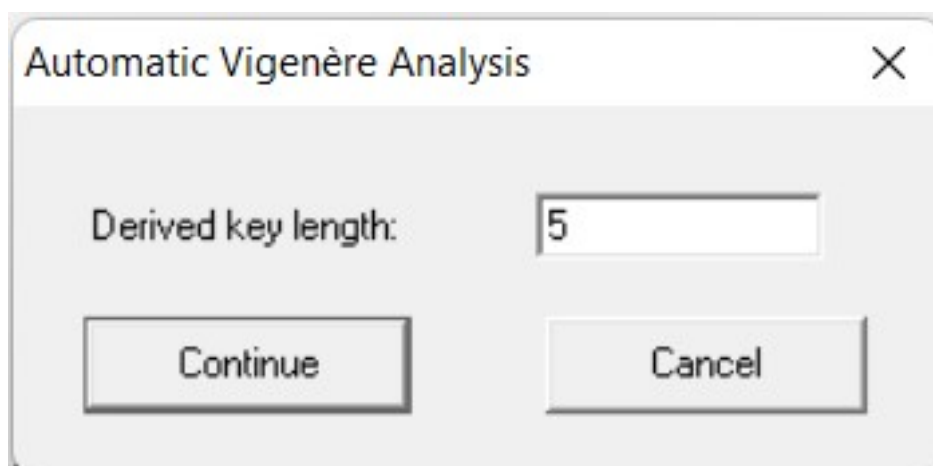
~~~~~

۴.۳

98166.3



شکل ۱۳

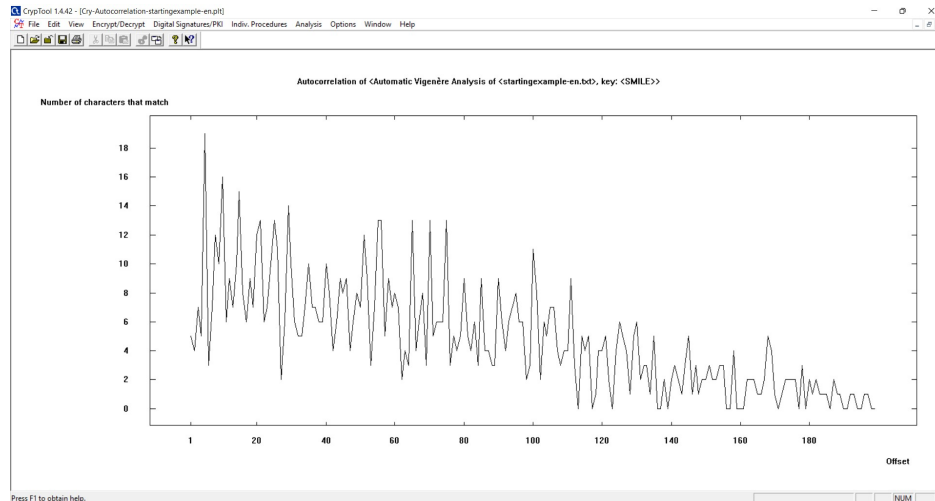


شکل ۱۴

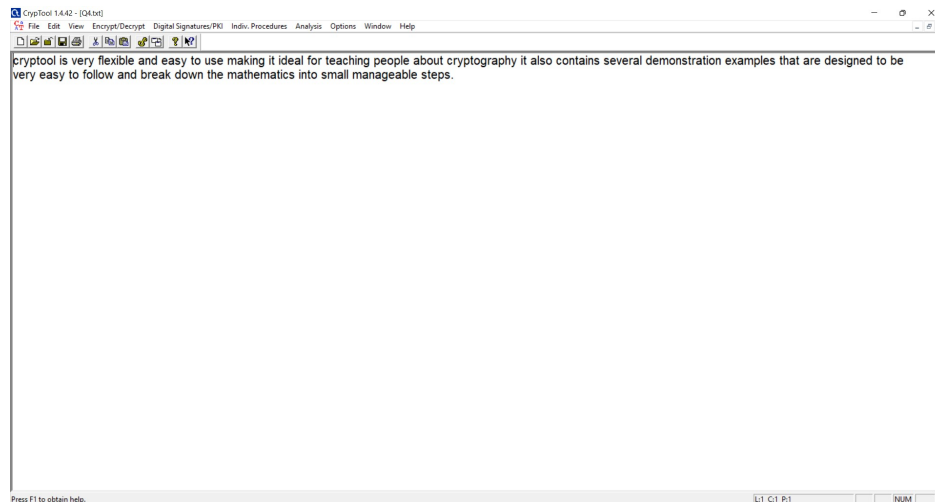


شکل ۱۵





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.

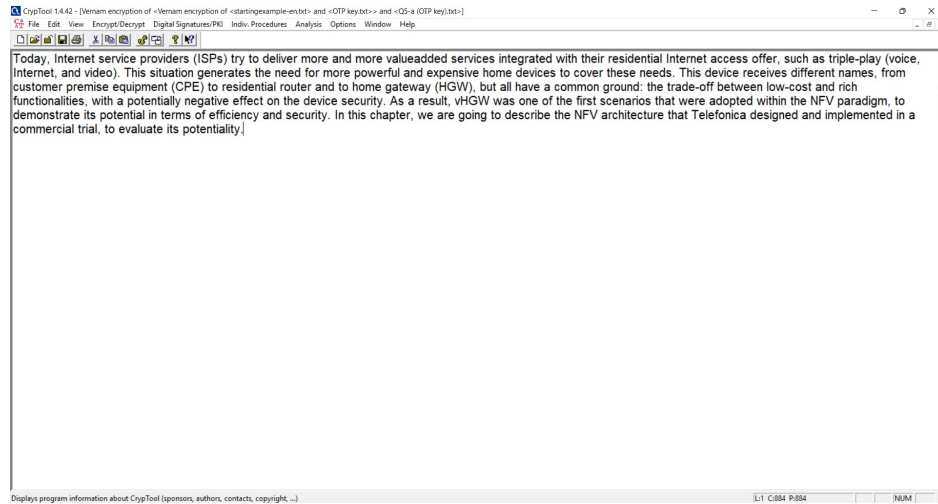
|               |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
|---------------|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 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.

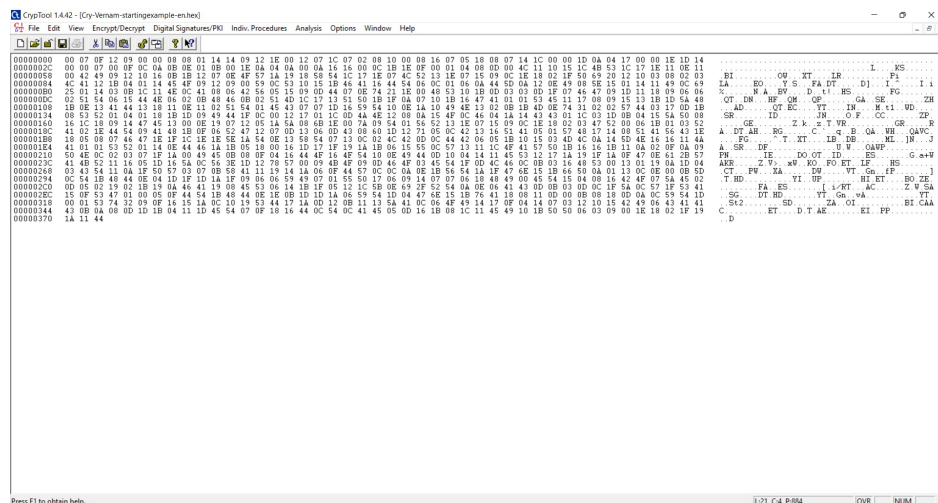
۵.۳

a ۱.۵.۳

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



شکل ۱۸



شکل ۱۹

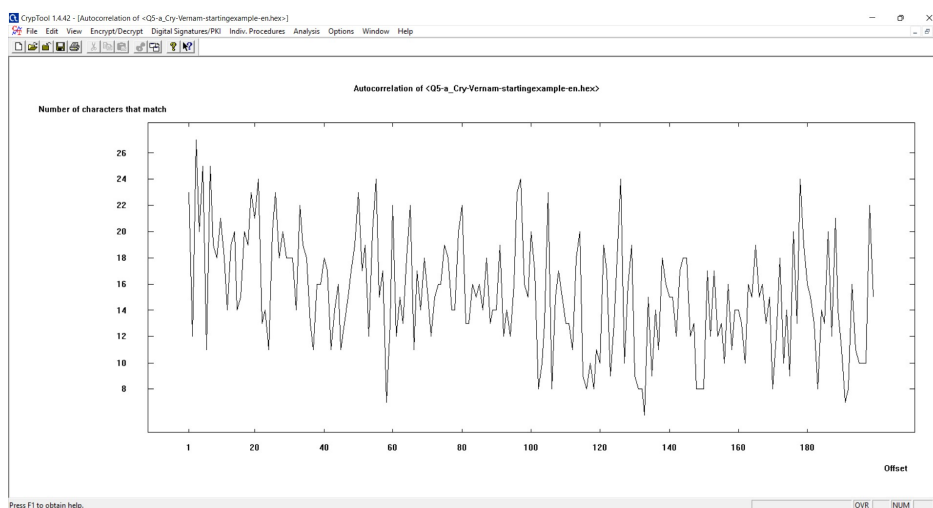
b ۲.۵.۳

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؛ کلید OTP را برابر تکرار رشته‌ی Alireza Abrehforoush قرار می‌دهیم).

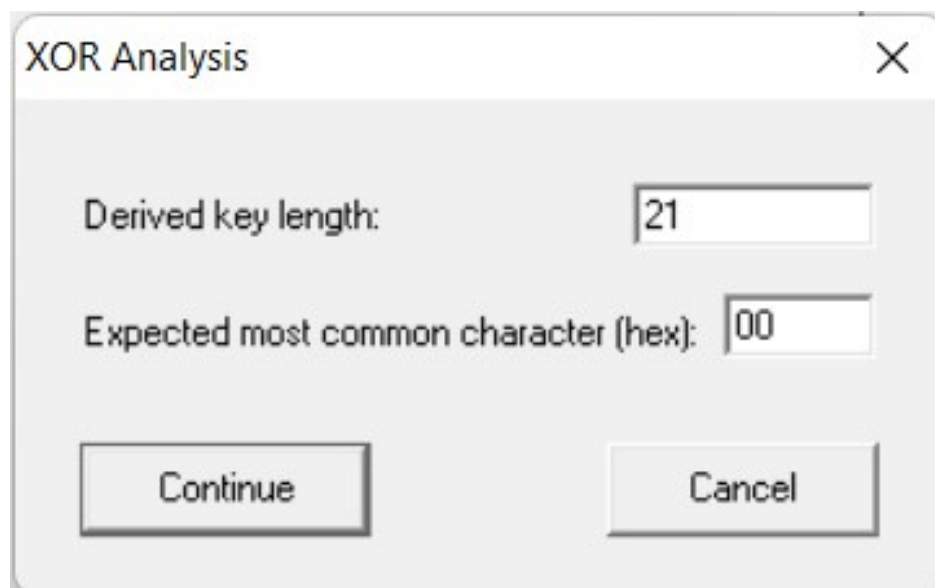




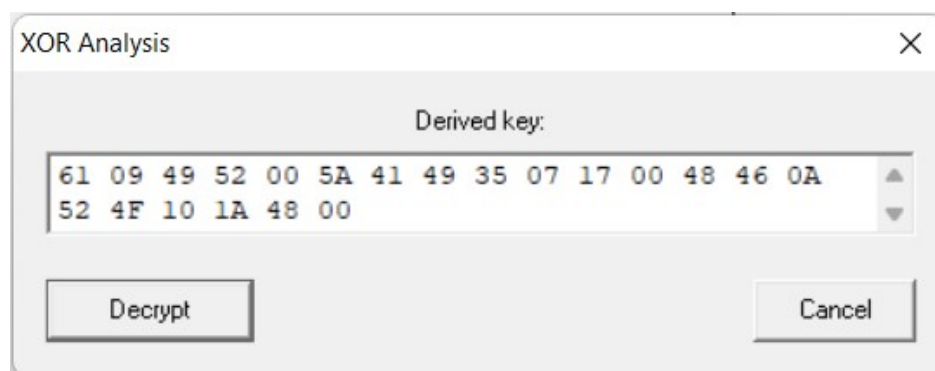
شکل ۲۲



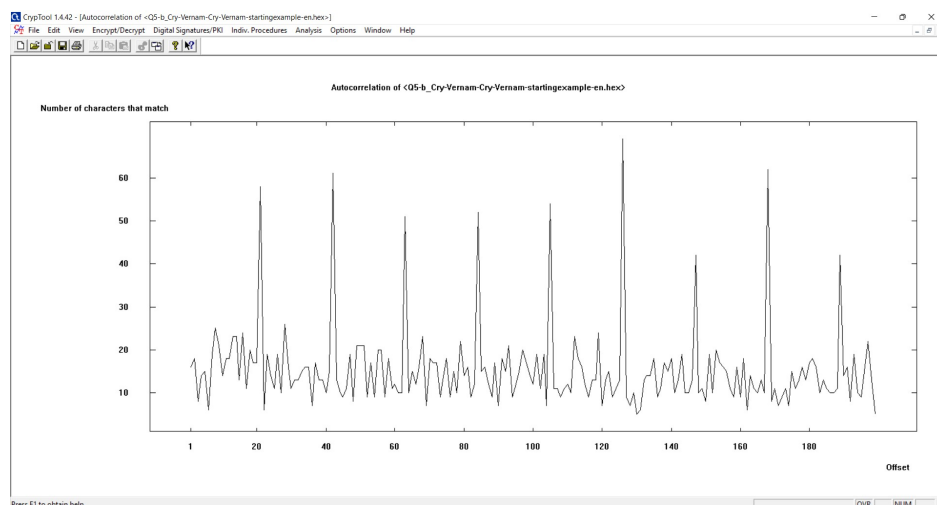
شکل ۲۳



شکل ۲۴



شکل ۲۵



شکل ۲۶

منابع

□□□□□□□□□□