

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

a \.\

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 می شود.

X	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>	- ø ×
Ref. File Edit View Encrypt/Decrypt Digital Signatures/PKI Indiv. Procedures Analysis Options Window Help	_ E ×
Alireza Abrehforoush	
/ till eZa / tibrellior oddin	
Press F1 to obtain help.	L1 C21 P21 NUM

شکل ۱

Here you can enter the key for the Caesar cipher. Caesar is a mon-orbihabelic subthinion, where the characters alphabet are mapped to the ciphertest alphabet by shifting. This You can enter the key as a number or as a single character of Roci-3 is a special variant, where the key has the finder value of the cleantest alphabet. This variant is only selectable if the le is an even number.	s shifting value is the key the alphabet.
alphabet are mapped to the ciphertext alphabet by shifting. Thi You can enter the key as a number or as a single character of Rot-13 is a special variant, where the key has the fixed value of the cleartext alphabet. This variant is only selectable if the le	s shifting value is the key the alphabet.
You can enter the key as a number or as a single character of it. Rot-13 is a special variant, where the key has the fixed value of the cleartest alphabet. This variant is only selectable if the le	the alphabet.
Rot-13 is a special variant, where the key has the fixed value of the cleartest alphabet. This variant is only selectable if the le	
of the cleartest alphabet. This variant is only selectable if the le	of half the length
is an even number.	ngth of the alphabet
Select variant Options to interpret the alphabet char	racters
	racter = 0 (e.g. "A"=0)
C Rot-13 C Value of the first alphabet cha	racter = 1 (e.g. "A"=1)
Key entry as	
Alphabet character	
(6)	
C Number value 12	
Properties of the chosen encryption	
Shift of 12	
Shift of 12	
Mapping of the alphabet (26 characters)	
from ABCDEFGHIJKLMNOPQRSTUVWXYZ	
to: MNOPORSTUVWXYZABCDEFGHIJKL	
O. PROPURSIONWAIZABCDEFGRIORE	

شکل ۲

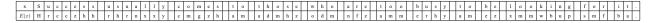


شکل ۳

۲

 $9816603 \equiv 17 \mod 26$

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



در نرم افزار CrypTool به صورت زیر رمز می کنیم.



شکل ۴



شکل ۵



شکل ۶

٣

a 1.7

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

	A	В	\mathbf{C}	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	\mathbf{S}	T	U	\mathbf{V}	\mathbf{W}	X	Y	Z
A	A	В	C	D	Е	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	Е	F	G	Н	I	J	K	L	M	N	О	P	Q	R	S	T	U	V	W	X	Y	Z	Α
C	C	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	С
E	Е	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
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	C	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	C	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	С	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	C	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 (سه حرف اول نام + سه حرف اول نام خانوادگی) ساخته می شود. $ALIREZA\ ABREHFOROUSH \Rightarrow key = ALIABR$

حال key را مکررا تکرار می کنیم تا طول آن برابر طول رشته ای که میخواهیم 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 دست می آوریم. i به دست می آوریم. i به بیمانه ی i به مراه خود کاراکترِ قرار گرفته در سطر i و ستون i است.

_	_	_		_				_	_	_	_	_	_	_		_								_	_	_	-	_	_	_				_	_	_					_		_		_	_	_	_		_	-	_	_		_	_		_	_	_		_	_	_
key	1	1	i	a	Ь	r	a		1	i	a	ь	r	a	1	i	a	b	r	a	Ш	1	i	- -	a i	b	r :	a i	1	i	a	b		r	a	1	i	a	b	Ш	r	a	1	i	а	b		r	a		1	i	a	ь	r	а	1	i	a	ь	11	r	a	.
x	5	i u	c	c	e	s	s		u	s	u	а	1	1	у	с	0	m	e	s	П	t	0	T	t i	h	0	s (e	w	h	0	П	a	r	e	t	0	o	П	b	u	s	у	t	0		b	e	T	1	0	o	k	i	n	g	f	0	r	П	i	t	٦
E(x)	5	f	k	c	f	i	s	П	f	a	u	ь	с	1	i	k	0	n	v	s	П	e	w	T	t	i	f	s I	р	е	h	р	П	r	r	р	ь	0	р	П	s	u	d	g	t	р		s	e	١,	ν ,	w	o	1	z	n	r	n	1 0	s	П	z	t	7

در نرم افزار CrypTool به صورت زیر رمز می کنیم.



شکل ۷



شکل ۸



شکل ۹

b 7.7

مشابه قسمت قبل (صرفا تغییر کلید) داریم:

 $ALIREZA\ ABREHFOROUSH \Rightarrow key = ALIREZAABREHFOROUSH$

k	ey	Α	1	Ī	i	r	e	z	а		а	b	r		e	h	f	0	Τ	r	0	Ī	1	s	h		a	1	I	i	r	e	z	1	ı	a	. 1	,	r		e li	1	ì	0	r	0	Τ	u	s	ŀ	n	a	1	T	i	r	e	T	z	a	а	b	Ţ	r	e	h	1		5 :	r	T	0	u	
-	х	s	u		с	с	e	s	s	П	u	s	u	8	а	1	1	у	Т	c	0	-	n	e	s	П	t	o		t	h	о	s		:	W	- 1	1 4	0	8	1 1		: [t	o	0	Т	ь	u	ı s	8	у	t	Т	,	ь	e	Т	1	0	0	k	Т	i	n	g	1			r	Т	i	t	7
E	(x)	s	f	1	k	t	i	r	s	П	u	t	1		e	s	q	m	Т	t	c		3	w	z	П	t	z		ь	у	s	r		:	W			f		. ,	j	T	h	f	с	Т	v	n	1 2		у	e	,	v	s	i	Т	k	0	0	1	Т	z	r	n	k	: (2	i	,	N	n	٦

در نرم افزار CrypTool به صورت زیر رمز می کنیم.



شکل ۱۰

The maximum key length is 1024 characters! [ALIREZAABREHFOROUSH]		Enter the key.		
ALIREZAABREHFOROUSH 8	ALIREZAABREHFOROUSH		-	
		ALIBEZAARBEHI	OROUSH	68

شکل ۱۱

CrypTool 1.4.42 - [Vigenère encryption of «startingexample-en.tst», key «ALIREZAABREHFOROUSH»] The Edit View Encrypt/Decrypt Digital Signature/PRI Indiv. Procedures Analysis Options Window Help	- Ø ×
Sfktirs utlesqm tcgwz tz bysre wif eyj hfc vmzy ew si koolzrn kci wn.	
Press F1 to obtain help.	L:1 C:1 P:1 NUM

شکل ۱۲

۳.۳

۴

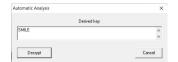
در نرم افزار CrypTool به صورت زیر رمزگشایی می کنیم. طول کلید (به طور پیشفرض) ۵ است و کلید در Vigenère cipher برابر SMILE به دست می آید.



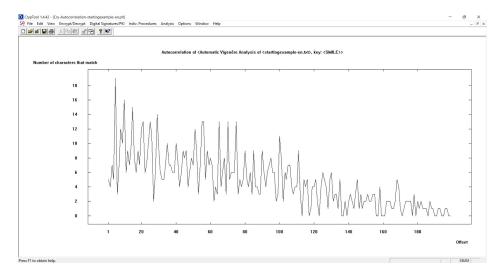
شکل ۱۳



شکل ۱۴



شکل ۱۵



شکل ۱۶

شکل ۱۷

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 match می شوند واحد شده است. توجه شود که فقط حروف الفبای انتخاب شده (انگلیسی یا آلمانی برای مثال) تجزیه و تحلیل می شوند. همچنین تعداد جابه جایی ها 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.



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

منابع