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

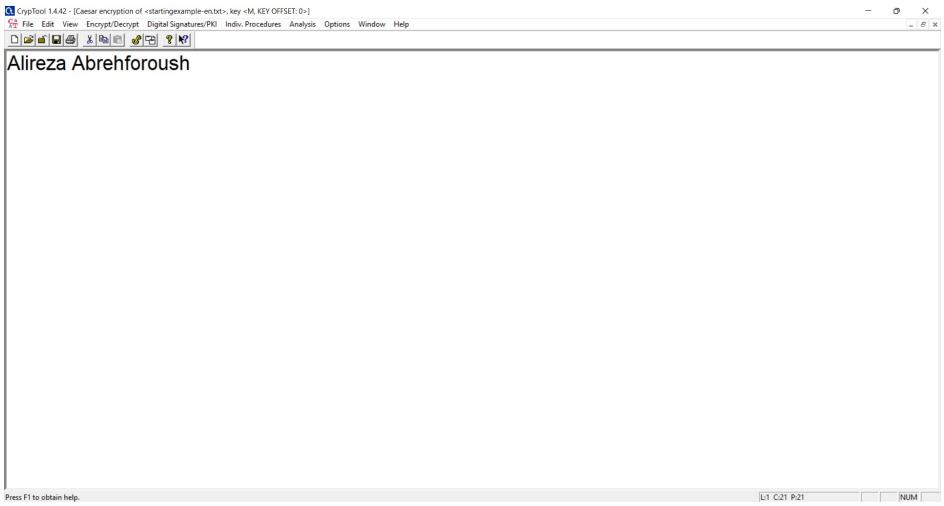
۱

a ۱.۱

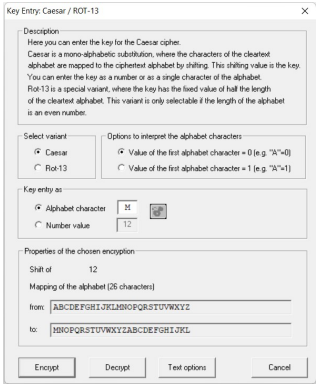
کلید Caesar cipher برابر M است که حرف ۱۳ام الفبای انگلیسی است. پس در واقع هر حرفِ الفبا به صورت حلقوی ۱۲ واحد شیفت می‌خورد. پس در نهایت به صورت زیر رمز می‌شود.

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

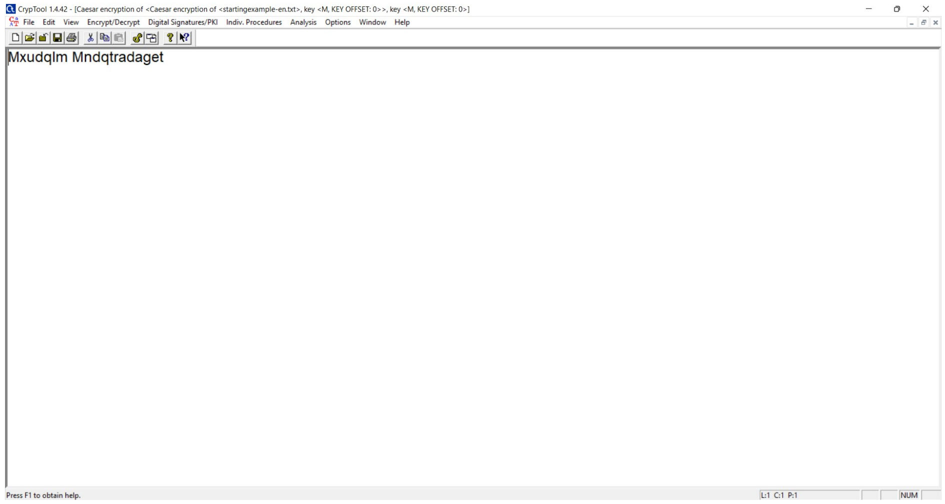
در نرم افزار CrypTool به صورت زیر رمز می‌کنیم.



شکل ۱



شکل ۲



شکل ۳

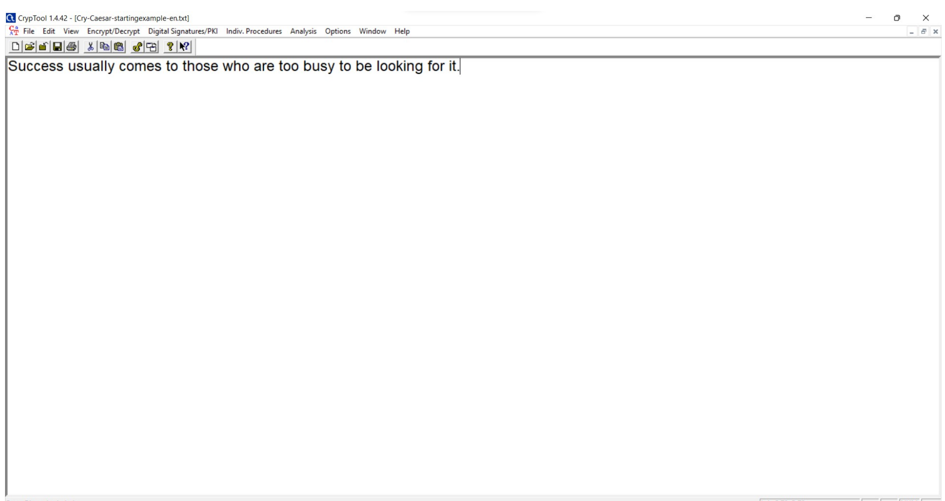
۲

$9816603 \equiv 17 \quad mod\ 26$

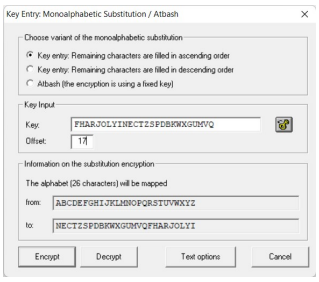
کلید Substitution cipher برابر fharjolyinectzspdbkwxgumvq و offset آن برابر ۱۷ است. در واقع الفبای اگلیسی به ترتیب به NECTZSPDBKWXGUMVQFHARJOLYI map می‌شود. پس در نهایت به صورت زیر رمز می‌شود.

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	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		e	r	h	y		a	m		e	z		x	m	m	w	b	u	p		s	m	f		b	a	.

در نرم افزار CrypTool به صورت زیر رمز می‌کنیم.



شکل ۴



شکل ۵

شکل ۶

۳

a ۱.۳

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

	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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

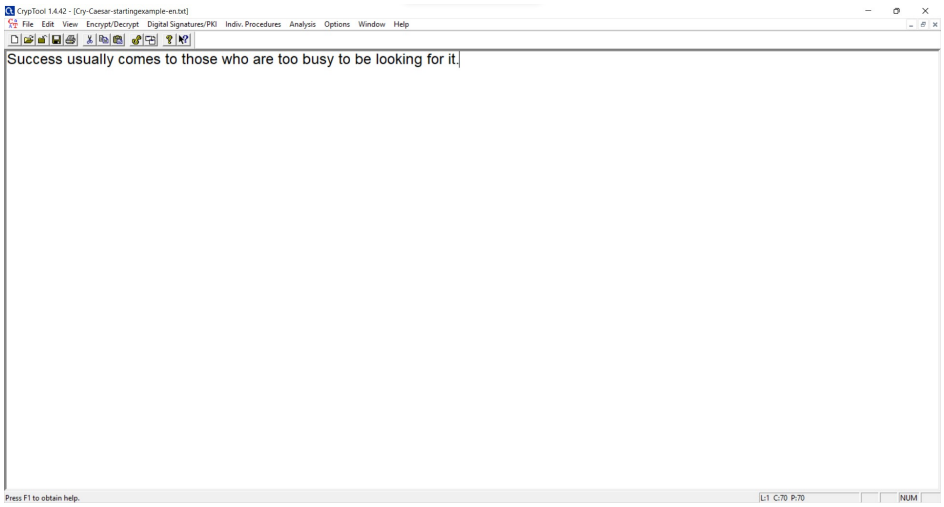
همچنین کلید مورد استفاده در این الگوریتم به صورت زیر (سه حرف اول نام + سه حرف اول نام خانوادگی) ساخته می‌شود.

$ALIREZA\ ABREHFOROUSH \Rightarrow key = ALIABR$

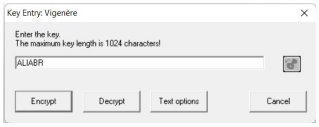
حال key را مکررا تکرار می‌کنیم تا طول آن برابر طول رشته‌ای که می‌خواهیم آن را رمز کنیم بشود (یا به عبارتی کاراکتر نظیر باقیمانده‌ی i به پیمانه‌ی طول کلید (۶) را در کلید به دست آوریم). برای رمز کردن کاراکترِ iام در رشته، کاراکترِ اندیسِ باقیمانده‌ی i به پیمانه‌ی طول کلید (۶) در کلید (key_i) به همراه خود کاراکترِ iام (x_i) به دست می‌آوریم. $cipher_i$ نظیر x_i برابر کاراکتر قرار گرفته در سطرِ key_i و ستون x_i است.

key	A	l	i	a	b	r	a		l	i	a	b	r	a	l		i	a	b	r	a		l	i		a	b	r	a	l		i	a	b		r	a	l		i	a	b		r	a	l	i		a	b		r	a		l	i	a	b	r	a	l		i	a	b		r	a	.
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	o	o	k	i	n	g		f	o	r		i	t	.
$E(x)$	S	f	k	c	f	j	s		f	a	u	b	c	l	j		k	o	n	v	s		e	w		t	i	f	s	p		e	h	p		r	r	p		b	o	p		s	u	d	g		t	p		s	e		w	w	o	l	z	n	r		n	o	s		z	t	.

در نرم افزار CrypTool به صورت زیر رمز می‌کنیم.



شکل ۷



شکل ۸

شکل ۹

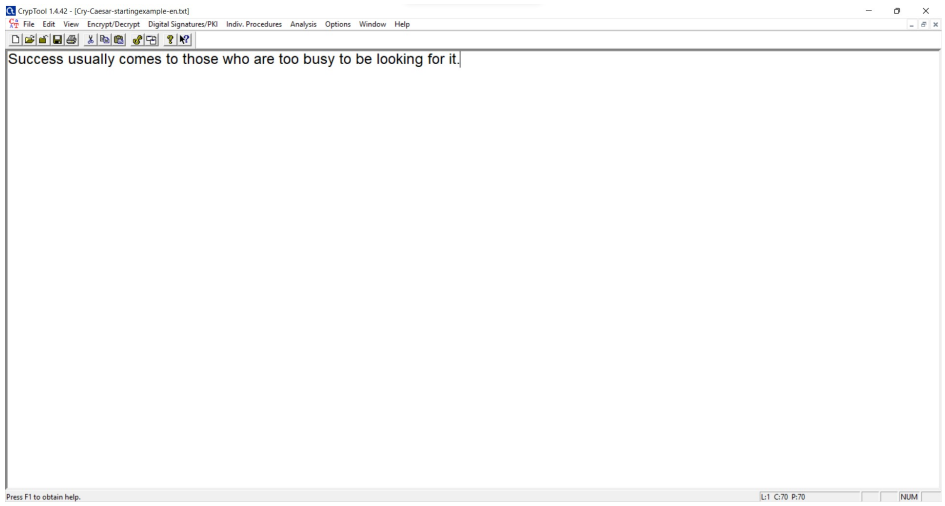
۲.۳ b

مشابه قسمت قبل (صرفا تغییر کلید) داریم:

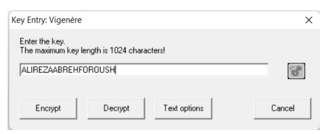
$$ALIREZA\ ABREHFOROUSH \Rightarrow key = ALIREZAABREHFOROUSH$$

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

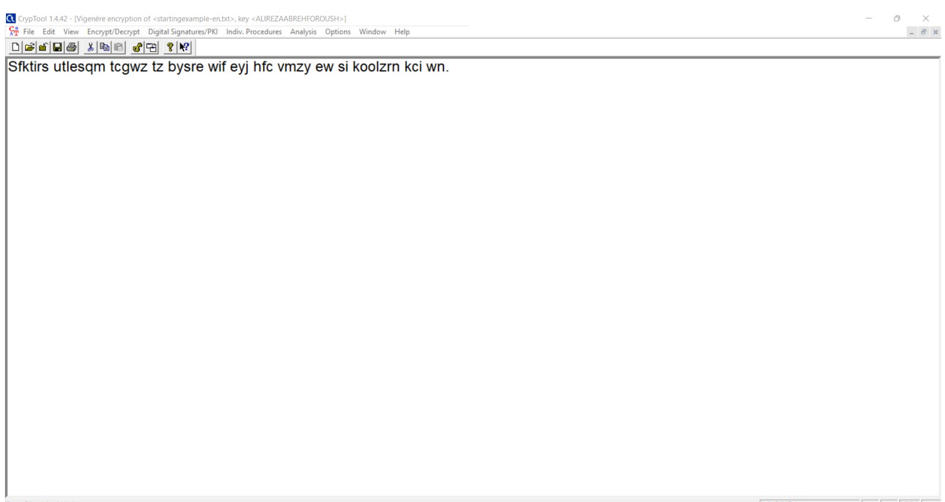
در نرم افزار CrypTool به صورت زیر رمز می‌کنیم.



شکل ۱۰



شکل ۱۱



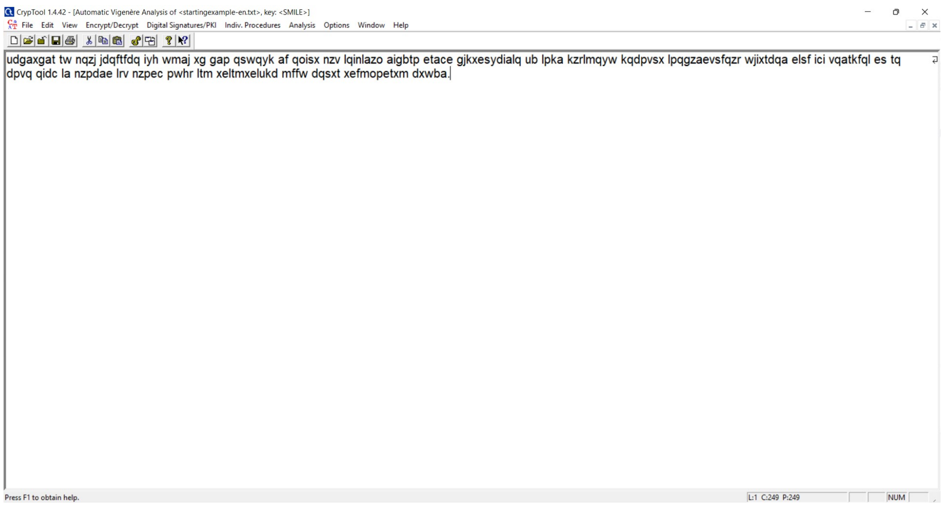
شکل ۱۲

۳.۳

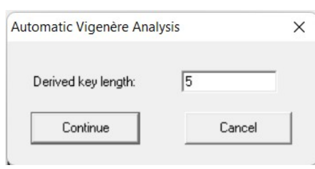
؟؟

۴

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

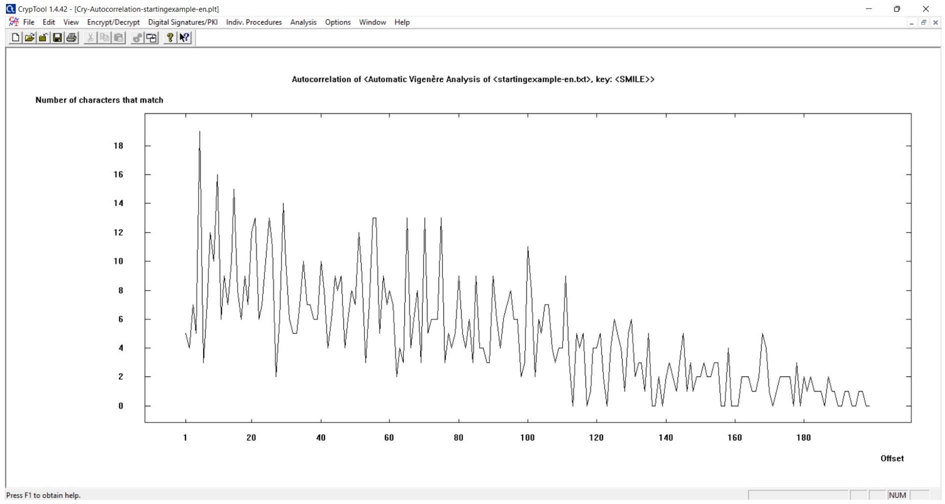


شکل ۱۳

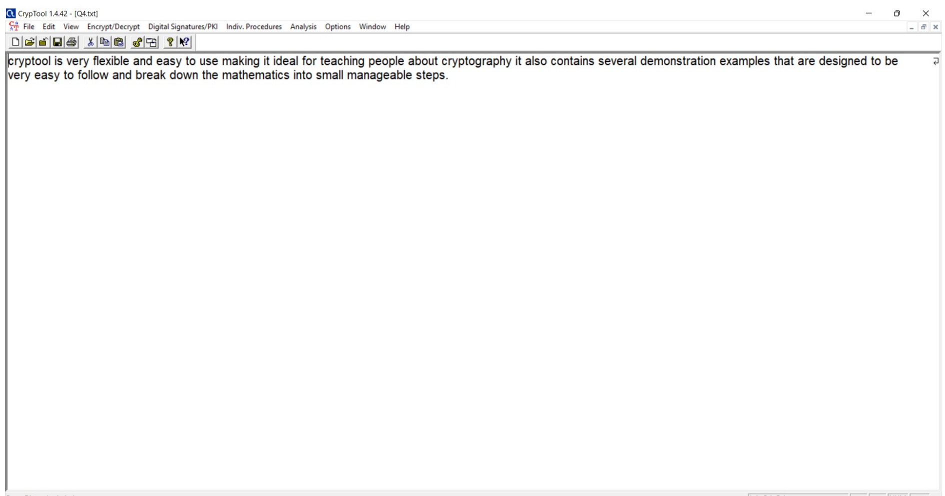


شکل ۱۴

شکل ۱۵



شکل ۱۶



شکل ۱۷

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 matchشده 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 جابه‌جایی‌ها 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.

Orginal 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	.							

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

منابع