Kryptoanaliza szyfru Vigenere'a
Test Kasiskiego

Pierwszym krokiem do złamania szyfru polialfabetycznego jest wyznaczenie długości klucza.
Pierwszą znaną metodą wyznaczenia długości klucza przy wykorzystaniu tylko kryptogramu był tzw. test Kasiskiego.
Załóżmy, że następujący tekst chcemy zaszyfrować za pomocą szyfru Vigenere'a z kluczem GAME

> Whether the object be to crush an army, to storm a city, or to assassinate an individual, it is always necessary to begin by finding out the names of the attendants,the aides-de-camp, and door-keepers and sentries of the general in command. Our spies must be commissioned to ascertain these. The enemy's spies who have come to spy on us must be sought out, tempted with bribes, led away and comfortably housed. Thus they will become converted spies and available for our service. Of old, the rise of the Yin dynasty was due to I Chih who had served under the Hsia (Sun Tzu on the Art of War)

Kryptoanaliza szyfru Vigenere'a
Test Kasiskiego

Usuwamy spacje i znaki przestankowe, dzielimy tekst na bloki o długości 4 (tak jak długość klucza).

Whet	hert	heob	ject	beto	crus	hana	rmyt	osto	rmac	ityo
rtoa	ssas	sina	tean	indi	vidu	alit	isal	ways	nece	ssar
ytob	egin	byfi	ndin	gout	then	ames	ofth	eatt	enda	ntst
heai	desd	ecam	pand	door	keep	ersa	ndse	ntri	esof	theg
ener	alin	comm	andO	ursp	iesm	ustb	ecom	miss	ione	dtoa
scer	tain	thes	eThe	enem	yssp	iesw	hoha	veco	meto	spyo
nusm	ustb	esou	ghto	utte	mpte	dwit	hbri	besl	edaw	ayan
dcom	fort	ably	hous	edTh	usth	eywi	llbe	come	conv	erte
dspi	esan	dava	ilab	lefo	rour	serv	iceO	fold	ther	iseo
fthe	Yind	ynas	tywa	sdue	toIC	hihw	hoha	dser	vedu	nder
theH	sia									

Kryptoanaliza szyfru Vigenere'a
Test Kasiskiego

Przykładowa grupa powtarzających się 3 liter:

Whet	hert	heob	ject	beto	crus	hana	rmyt	osto	rmac	ityo
rtoa	ssas	sina	tean	indi	vidu	alit	isal	ways	nece	ssar
ytob	egin	byfi	ndin	gout	then	ames	ofth	eatt	enda	ntst
heai	desd	ecam	pand	door	keep	ersa	ndse	ntri	esof	theg
ener	alin	comm	andO	ursp	iesm	ustb	ecom	miss	ione	dtoa
scer	tain	thes	eThe	enem	yssp	iesw	hoha	veco	meto	spyo
nusm	ustb	esou	ghto	utte	mpte	dwit	hbri	besl	edaw	ayan
dcom	fort	ably	hous	edTh	usth	eywi	llbe	come	conv	erte
dspi	esan	dava	ilab	lefo	rour	serv	iceO	fold	ther	iseo
fthe	Yind	ynas	tywa	sdue	toIC	hihw	hoha	dser	vedu	nder
theH	sia									

the $\rightarrow \alpha\beta\gamma$

The $\not\rightarrow \alpha\beta\gamma$

the $\not\rightarrow \alpha\beta\gamma$

Kryptoanaliza szyfru Vigenere'a
Test Kasiskiego

Ponumerujmy pozycje wszystkich liter.

Numery początków grup 3-literowych the różnią się o całkowitą wielokrotność długości klucza.

W naszym przykładzie grupy the zaczynają się na pozycjach: 109, 173, 229, 389, 441

Wtedy:
$441 - 109 = 332 = 2 \cdot 2 \cdot 83$
$441 - 173 = 268 = 2 \cdot 2 \cdot 67$
$441 - 229 = 212 = 2 \cdot 2 \cdot 53$
$441 - 389 = 52 = 2 \cdot 2 \cdot 13$
$389 - 109 = 280 = 2 \cdot 2 \cdot 2 \cdot 5 \cdot 7$
$389 - 173 = 216 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 \cdot 3$
$389 - 229 = 160 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 5$
$229 - 109 = 120 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 5$
$229 - 173 = 56 = 2 \cdot 2 \cdot 2 \cdot 7$
NWD(332,268,212,52,280,216,160,120,56)=4

Kryptoanaliza szyfru Vigenere'a
Test Kasiskiego

Przykład ten sugeruje następującą metodę wyznaczenia długości klucza (test Kasiskiego):[1mm]

1. W kryptogramie odszukujemy powtarzającą się często grupę 3 liter.
2. Liczymy odległości pomiędzy pierwszymi znakami powtarzających się grup.
3. Długość klucza jest największym wspólnym dzielnikiem tych odległości.

Kryptoanaliza szyfru Vigenere'a
Indeks zgodności

Inną metodą wyznaczenia długości klucza jest wykorzystanie tzw. indeksu zgodności.

Indeks zgodności
Niech $x = x_1x_2x_3 \dots x_n$ będzie ciągiem n znaków alfabetu. Indeksem zgodności ciągu x nazywamy prawdopodobieństwo tego, że dwa losowo wybrane znaki z ciągu x będą identyczne. Indeks zgodności ciągu x oznaczać będziemy $I_c(x)$.

Oznaczmy:
n_0 – ilość wystąpień litery A w ciągu x
n_1 – ilość wystąpień litery B w ciągu x
$\vdots$
n_{25} – ilość wystąpień litery Z w ciągu x

Wtedy częstości występowania liter alfabetu:

A: $f_0 = \frac{n_0}{n}$, B: $f_1 = \frac{n_1}{n}$, C: $f_2 = \frac{n_2}{n}$, $\dots$, Z: $f_{25} = \frac{n_{25}}{n}$

Kryptoanaliza szyfru Vigenere'a
Indeks zgodności

Prawdopodobieństwo, że gdy wybierzemy z naszego ciągu x dwa znaki to będą to dwie litery A wynosi:

$$p_{A,A} \equiv p_{0,0} = \frac{N_{00}}{N_{XX}}$$

N_{00} – ilość par (A,A) w naszym ciągu
N_{XX} – ilość wszystkich par wybranych z naszego ciągu

$$N_{00} = \binom{n_0}{2} = \frac{n_0!}{2!(n_0-2)!} = \frac{n_0(n_0-1)}{2}$$
$$N_{XX} = \binom{n}{2} = \frac{n!}{2!(n-2)!} = \frac{n(n-1)}{2}.$$

Wtedy

$$I_c(x) = p_{0,0} + p_{1,1} + \cdots + p_{25,25}.$$

Zatem

$$I_c(x) = \frac{\sum_{i=0}^{25} n_i(n_i-1)}{n(n-1)} \approx \sum_{i=0}^{25} f_i^2.$$

Kryptoanaliza szyfru Vigenere'a
Indeks zgodności

Jeżeli x jest tekstem w języku angielskim, to wtedy

$$f_i = p_i,$$

gdzie p_i – częstość występowania i–tej litery w języku angielskim.

Częstości występowania poszczególnych liter

Litera	Język angielski	Język polski	Litera	Język angielski	Język polski
A	0,082	0,074	N	0,067	0,044
B	0,015	0,014	O	0,075	0,061
C	0,028	0,033	P	0,019	0,025
D	0,043	0,028	Q	0,001	0,001
E	0,127	0,065	R	0,060	0,035
F	0,022	0,002	S	0,063	0,035
G	0,020	0,013	T	0,091	0,030
H	0,061	0,009	U	0,028	0,018
I	0,070	0,072	V	0,010	0,001
J	0,002	0,018	W	0,023	0,035
K	0,008	0,026	X	0,001	0,001
L	0,040	0,019	Y	0,020	0,034
M	0,024	0,027	Z	0,001	0,049

Kryptoanaliza szyfru Vigenere'a
Indeks zgodności

Zatem dla tekstu w języku angielskim

$$I_c(x) = \sum_{i=0}^{25} p_i^2 = (0{,}082)^2 + (0{,}015)^2 + \cdots + (0{,}001)^2 = 0{,}065.$$

Dla losowego ciągu znaków

$$f_i = \frac{1}{26}.$$

Zatem dla losowego ciągu znaków alfabetu

$$I_c(x) = \sum_{i=0}^{25} \left(\frac{1}{26}\right)^2 = 26 \cdot \left(\frac{1}{26}\right)^2 = \frac{1}{26} = 0{,}038.$$

Kryptoanaliza szyfru Vigenere'a
Indeks zgodności

Po podstawieniu monoalfabetycznym zachowane zostają częstości występowania poszczególnych znaków (gdy np. E$\rightarrow$X to w szyfrogramie X występuje z taką samą częstością jak E w tekście jawnym).

Indeks zgodności jest sumą kwadratów występowania wszystkich znaków zatem nie zmienia się po podstawieniu monoalfabetycznym.

Kryptogram otrzymany za pomocą podstawienia monoalfabetycznego ma taki sam indeks zgodności jak tekst niezaszyfrowany.

Jeżeli mamy kryptogram otrzymany za pomocą szyfru Vigenere'a z kluczem o długości k_0, to podciągi liter kryptogramu wybrane w następujący sposób

$1, 1 + k_0, 1 + 2k_0, 1 + 3k_0, 1 + 4k_0, 1 + 5k_0, \ldots$
$2, 2 + k_0, 2 + 2k_0, 2 + 3k_0, 2 + 4k_0, 2 + 5k_0, \ldots$
$3, 3 + k_0, 3 + 2k_0, 3 + 3k_0, 3 + 4k_0, 3 + 5k_0, \ldots$

są zaszyfrowane za pomocą podstawień monoalfabetycznych.

Kryptoanaliza szyfru Vigenere'a
Indeks zgodności

Wobec tego, gdy mamy kryptogram otrzymany za pomocą szyfru Vigenere'a i chcemy wyznaczyć długość klucza, to tworzymy podciągi

$1, 1 + k, 1 + 2k, 1 + 3k, 1 + 4k, 1 + 5k, \ldots$

$2, 2 + k, 2 + 2k, 2 + 3k, 2 + 4k, 2 + 5k, \ldots$

$3, 3 + k, 3 + 2k, 3 + 3k, 3 + 4k, 3 + 5k, \ldots$

dla różnych wartości k i liczymy dla nich indeksy zgodności.

Dla jednej z wartości $k = k_0$ spodziewamy się otrzymać indeksy zgodności zbliżone do $0{,}065$, dla innych k zbliżone do $0{,}038$.

Wtedy k_0 jest szukaną długością klucza.

Kryptoanaliza szyfru Vigenere'a
Indeks zgodności

Tekst zaszyfrowany:

CHQXNEDXNEAFPEOXHEFSIRGWN
AZEXMKXUSFSXMMGOTKSXTAEYS
MWYIZEZEMRONPMBIPYGLUXOS

Podciągi dla k=2:

CHQXNEDXNEAFPEOXHEFSIRGWN
AZEXMKXUSFSXMMGOTKSXTAEYS
MWYIZEZEMRONPMBIPYGLUXOS

1+2i: CQNDNAPOHFIGNZXKUFXMOKXAYMYZZMOPBPGUO

2+2i: HXEXEFEXESRWAEMXSSMGTSTESWIEERNMIYLXS

Kryptoanaliza szyfru Vigenere'a
Indeks zgodności
Podciągi dla k=3:

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

1+3i: CXDEPXFRNEKSXGKTYWZEOMPLO

2+3i: HNXAEHSGAXXFMOSASYEMNBYUS

3+3i: QENFOEIWZMUSMTXEMIZRPIGX

Kryptoanaliza szyfru Vigenere'a
Załóżmy, że mamy następujący kryptogram, zaszyfrowany przy pomocy szyfru Vigenere'a:

```
CHREEVOAHMAERATBIAXXWTNXBEEOPHBSBQMQEQERBW
RVXUOAKXAOSXXWEAHBWGJMMQMNKGRFVGXWTRZXWIAK
LXFPSKAUTEMNDCMGTSXMXBTUIADNGMGPSRELXNJELX
VRVPRTULHDNQWTWDTYGBPHXTFALJHASVBFXNGLLCHR
ZBWELEKMSJIKNBHWRJGNMGJSGLXFEYPHAGNRBIEQJT
AMRVLCRREMNDGLXRRIMGNSNRWCHRQHAEYEVTAQEBBI
PEEWEVKAKOEWADREMXMTBHHCHRTKDNVRZCHRCLQOHP
WQAIIWXNRMGWOIIFKEE
```

Spróbujmy najpierw wyznaczyć długość klucza.

Kryptoanaliza szyfru Vigenere'a
Test Kasiskiego
Zastosujmy test Kasiskiego:

```
CHREEVOAHMAERATBIAXXWTNXBEEOPHBSBQMQEQERBW
RVXUOAKXAOSXXWEAHBWGJMMQMNKGRFVGXWTRZXWIAK
LXFPSKAUTEMNDCMGTSXMXBTUIADNGMGPSRELXNJELX
VRVPRTULHDNQWTWDTYGBPHXTFALJHASVBFXNGLLCHR
ZBWELEKMSJIKNBHWRJGNMGJSGLXFEYPHAGNRBIEQJT
AMRVLCRREMNDGLXRRIMGNSNRWCHRQHAEYEVTAQEBBI
PEEWEVKAKOEWADREMXMTBHHCHRTKDNVRZCHRCLQOHP
WQAIIWXNRMGWOIIFKEE
```

Jak widać grupa liter CHR występuje pięciokrotnie.

Kryptoanaliza szyfru Vigenere'a
Test Kasiskiego
Pierwsza litera grupy CRH znajduje się odpowiednio na pozycjach:

1, 166, 236, 276, 286

Odległości od pierwszego wystąpienia do pozostałych czterech są równe odpowiednio:

165, 235, 275, 285

$165 = 3 \cdot 5 \cdot 11$,
$235 = 5 \cdot 47$,
$275 = 5 \cdot 5 \cdot 11$,
$285 = 3 \cdot 5 \cdot 19$.

Zatem: NWD(165,235,275,285)=5

Test Kasiskiego sugeruje, że długość klucza wynosi 5.

Kryptoanaliza szyfru Vigenere'a
Indeks zgodności

Policzmy teraz indeks zgodności dla podciągów wybranych z kryptogramu zakładając różne długości klucza.

Dla $k = 1$ mamy jeden podciąg – cały tekst.

Liczba znaków całego tekstu: $n = 313$.

Ilości poszczególnych znaków: {A, 19}, {B, 15}, {C, 8}, {D, 7}, {E, 26}, {F, 6}, {G, 15}, {H, 17}, {I, 11}, {J, 7}, {K, 10}, {L, 12}, {M, 17}, {N, 15}, {O, 7}, {P, 8}, {Q, 10}, {R, 24}, {S, 9}, {T, 14}, {U, 4}, {V, 10}, {W, 16}, {X, 20}, {Y, 3}, {Z, 3}

Zatem indeks zgodności dla całego tekstu wynosi:

$$\begin{aligned} I_C(x) &= \frac{\sum_{i=0}^{25} n_i(n_i - 1)}{n(n-1)} \\ &= \frac{19(19-1) + 15(15-1) + \cdots + 3(3-1)}{313(313-1)} = 0{,}0450. \end{aligned}$$

Zauważmy, że stosując przybliżenie $I_C(x) = \sum_{i=0}^{25} f_i^2$ otrzymalibyśmy w tym przypadku wynik $0{,}0480$.

Kryptoanaliza szyfru Vigenere'a
Indeks zgodności

Dla $k = 2$ mamy dwa podciągi:

x_1 =CREOHARTIXWNBEPBBMEEBRXOKASXEHWJMMK RVXTZWALFSATMDMTXXTIDGGSEXJLVVRUHNW WTGPXFLHSBXGLHZWLKSINHRGMJGXEPANBEJA RLRENGXRMNNWHQAYVAEBPEEKKEARMMBHHT DVZHCQHWA GFGWRXIKXPKUENCGSMBUANMPRLNEXRPTLDQT DYBHTAJAVFNLCRBEEMJKBWJNGSLFYHGRIQTMVC RMDLRIGSRCRHEETQBIEWVAOWDEXTHCRK NRCRLOPQIWNMWIFE

Kryptoanaliza szyfru Vigenere'a
Indeks zgodności

Długości tych podciągów, ilości znaków oraz indeksy zgodności wynoszą odpowiednio:

dla x_1: $n(x_1) = 157$[1mm] {A, 10}, {B, 8}, {C, 2}, {D, 3}, {E, 14}, {F, 2}, {G, 8}, {H, 11}, {I, 5}, {J, 4}, {K, 6}, {L, 6}, {M, 9}, {N, 7}, {O, 3}, {P, 4}, {Q, 2}, {R, 11}, {S, 5}, {T, 7}, {U, 1}, {V, 5}, {W, 8}, {X, 12}, {Y, 1}, {Z, 3}[1mm]

$$I_C(x_1) = \frac{10(10-1) + 8(8-1) + \cdots + 3(3-1)}{157(157-1)} = 0{,}0456.$$

dla x_2: $n = 156$[1mm] {A, 9}, {B, 7}, {C, 6}, {D, 4}, {E, 12}, {F, 4}, {G, 7}, {H, 6}, {I, 6}, {J, 3}, {K, 4}, {L, 6}, {M, 8}, {N, 8}, {O, 4}, {P, 4}, {Q, 8}, {R, 13}, {S, 4}, {T, 7}, {U, 3}, {V, 5}, {W, 8}, {X, 8}, {Y, 2}, {Z, 0}[1mm]

$$I_C(x_2) = \frac{9(9-1) + 7(7-1) + \cdots + 0}{156(156-1)} = 0{,}0410.$$

Kryptoanaliza szyfru Vigenere'a
Indeks zgodności
Analogicznie liczymy indeksy zgodności dla podciągów wybranych z kryptogramu zakładając długości klucza $k = 3, 4, 5, \ldots$ [2mm]

Długość klucza	indeksy zgodności podciągów
1	0,045
2	0,046; 0,041
3	0,043; 0,050; 0,047
4	0,042; 0,039; 0,046; 0,040
5	0,063; 0,068; 0,069; 0,061; 0,072

Analiza indeksów zgodności sugeruje, że długość klucza wynosi 5.

Kryptoanaliza szyfru Vigenere'a
Wzajemny indeks zgodności

Wzajemny indeks zgodności
Niech $x = x_1x_2x_3 \ldots x_n$ i $y = y_1y_2 \ldots y_{n'}$ będą ciągami n i n' znaków alfabetu. Wzajemnym indeksem zgodności ciągów x i y nazywamy prawdopodobieństwo tego, że losowo wybrany znak ciągu x i losowo wybrany znak ciągu y są jednakowe. Wzajemny indeks zgodności (ang. *mutual index of coincidence*)oznaczamy $MI_c(x, y)$.

Częstości występowania kolejnych liter alfabetu w ciągu x oznaczmy:

$$A\colon f_0 = \frac{n_0}{n}, \quad B\colon f_1 = \frac{n_1}{n}, \ldots, Z\colon f_{25} = \frac{n_{25}}{n},$$

w ciągu y:

$$A\colon f'_0 = \frac{n'_0}{n'}, \quad B\colon f'_1 = \frac{n'_1}{n'}, \ldots, Z\colon f'_{25} = \frac{n'_{25}}{n'}.$$

Kryptoanaliza szyfru Vigenere'a
Wzajemny indeks zgodności
Literę A z ciągu x i literę A z ciągu y możemy wybrać na $n_0n'_0$ sposobów.

Literę B na $n_1n'_1$ sposobów.

$\vdots$

Zatem takie same znaki w x i y możemy wybrać na

$$\sum_{i=0}^{25} n_in'_i$$

sposobów.

Dowolną parę znaków, jeden z x, drugi z y, możemy wybrać na nn' sposobów.[2mm]Zatem

$$MI_c(x, y) = \frac{\sum\limits_{i=0}^{25} n_in'_i}{nn'} = \sum_{i=0}^{25} f_if'_i.$$

Kryptoanaliza szyfru Vigenere'a
Wzajemny indeks zgodności
Zauważmy, że gdy $x = y$ to wzajemny indeks zgodności jest równy indeksowi zgodności ciągu x

$$MI_c(x, x) = I_c(x).$$

Kryptoanaliza szyfru Vigenere'a
Wzajemny indeks zgodności
Załóżmy, że ciąg x jest tekstem jawnym w języku angielskim a ciąg y powstał z ciągu x w wyniku zastosowania szyfru Cezara z kluczem o wartości k.

Wtedy litera A występuje w ciągu y z taką częstością jak litera $0 - k = 26 - k \mod 26$ w ciągu x.

Zatem ogólnie litera o numerze i występuje w ciągu y z taką częstością jak litera $i - k \mod 26$ w ciągu x.

Zatem

$$f'_i = f_{i-k}$$

Wobec tego dla takich ciągów x i y wzajemny indeks zgodności wynosi

$$MI_c(x, y) = \sum_{i=0}^{25} f_i f_{i-26}.$$

Wzajemny indeks zgodności dla języka angielskiego
Zachodzi równość:

$$\sum_{i}^{25} f_i f_{i-k} = \sum_{i}^{25} f_i f_{i+k}$$

Rzeczywiście, ... [2mm]Zatem:

$$MI_c(x, x^k) = MI_c(x, x^{26-k})$$

Rzeczywiście, ...

$MI_c(x, x^{14}) = MI_c(x, x^{12})$,
$MI_c(x, x^{15}) = MI_c(x, x^{11})$,
...

Przesunięcie k	$MI_c(x, x^k)$
0	0.065
1	0.039
2	0.032
3	0.034
4	0.044
5	0.033
6	0.036
7	0.039
8	0.034
9	0.034
10	0.038
11	0.045
12	0.039
13	0.043

Kryptoanaliza szyfru Vigenere'a
Wzajemny indeks zgodności

Niech x będzie tekstem w języku angielskim a x^{k_1}, x^{k_2} będą kryptogramami otrzymanymi x za pomocą szyfru Cezara z kluczami k_1 and k_2, odpowiednio.

Wzajemny indeks zgodności ciągów x^{k_1} i x^{k_2} wynosi:

$$MI_c(x^{k_1}, x^{k_2}) = \sum_{i=0}^{25} f'_i f''_i = \sum_{i=0}^{25} f_{i-k_1} f_{i-k_2} = \sum_{i=0}^{25} f_i f_{i+k_1-k_2} = MI_c(x, x^{k_1-k_2}).$$

Zauważmy, że wartość tego wzajemnego indeksu zgodności zależy tylko od różnicy $k_1 - k_2 \mod 26$, którą nazywać będziemy względnym przesunięciem x^{k_1} i x^{k_2}.

Kryptoanaliza szyfru Vigenere'a
Wzajemny indeks zgodności

Z prezentowanej tabelki wynika, że gdy względne przesunięcie jest różne od 0 to wtedy oczekiwane wartości MI_c należą do przedziału 0.031-0.045. Natomiast gdy gdy względne przesunięcie wynosi 0 to oczekiwana wartość MI_c jest bliska 0.065.

Obserwację tę możemy wykorzystać do wyznaczenia oczekiwanej wartości względnego przesunięcia między x^{k_1} i x^{k_2}.

Załóżmy, że ustalamy x^{k_1} i następnie wyznaczmy ciągi otrzymane z x^{k_2} za pomocą szyfru Cezara z kluczami kolejno $e_0 = 0$, $e_1 = 1, \ldots$.

Oznaczmy te otrzymane ciągi przez $x_0^{k_2}$, $x_1^{k_2}$, itd.

Wzajemne indeksy zgodności $MI_c(x^{k_1}, x_g^{k_2})$, $0 \le g \le 25$ możemy policzyć ze wzoru

$$MI_c(x^{k_1}, x_g^{k_2}) = \sum_{i=0}^{25} f_i^{x^{k_1}} f_{i-g}^{x^{k_2}}.$$

Gdy $g = k_1 - k_2$, wtedy MI_c powinien być zbliżony do 0.065, ponieważ wtedy względne przesunięcie x^{k1} i $x_{k_1-k_2}^{k_2}$ wynosi 0. Dla wartości $g \neq k_1 - k_2$, MI_c powinny należeć do przedziału między 0.031 a 0.045.

Kryptoanaliza szyfru Vigenere'a
Wzajemny indeks zgodności

Zakładamy, że długość klucza wynosi 5.

CHREE|VOAHM|AERAT|BIAXX|WTNXB|EEOPH|BSBQM|QEQERBW
RVXUOAKXAOSXXWEAHBWGJMMQMNKGRFVGXWTRZXWIAK
LXFPSKAUTEMNDCMGTSXMXBTUIADNGMGPSRELXNJELX
VRVPRTULHDNQWTWDTYGBPHXTFALJHASVBFXNGLLCHR
ZBWELEKMSJIKNBHWRJGNMGJSGLXFEYPHAGNRBIEQJT
AMRVLCRREMNDGLXRRIMGNSNRWCHRQHAEYEVTAQEBBI
PEEWEVKAKOEWADREMXMTBHHCHRTKDNVRZCHRCLQOHP
WQAIIWXNRMGWOIIFKEE

x^1 =CVABWEB...

x^2 =HOEITES...

x^3 =RARANOB...

$x^4 = \ldots$ $\quad x^5 = \ldots.$

$x_0^2 = x^2$, $\quad x_1^2$ =IPFJUFT... $\quad x_2^2$ =JRGKVGU... [1mm]$MI_c(x^1, x_0^2) = \ldots$ $\quad MI_c(x^1, x_1^2) = \ldots$ $\quad MI_c(x^1, x_2^2) = \ldots$

Kryptoanaliza szyfru Vigenere'a
Wzajemny indeks zgodności

i	j	Wartości $MI_c(\mathbf{y}_i\mathbf{y}_j^g)$								
1	2	0,028	0,027	0,028	0,034	0,039	0,037	0,026	0,025	0,052
		$\boxed{0{,}068}$	0,044	0,026	0,037	0,043	0,037	0,043	0,037	0,028
		0,041	0,041	0,034	0,037	0,051	0,045	0,042	0,036	
1	3	0,039	0,033	0,040	0,034	0,028	0,053	0,048	0,033	0,029
		0,056	0,050	0,045	0,039	0,040	0,036	0,037	0,032	0,027
		0,037	0,036	0,031	0,037	0,055	0,029	0,024	0,037	
1	4	0,034	0,043	0,025	0,027	0,038	0,049	0,040	0,032	0,029
		0,034	0,039	0,044	0,044	0,034	0,039	0,045	0,044	0,037
		0,055	0,047	0,032	0,027	0,039	0,037	0,039	0,035	
1	5	0,043	0,033	0,028	0,046	0,043	0,044	0,039	0,031	0,026
		0,030	0,036	0,040	0,041	0,024	0,019	0,048	$\boxed{0{,}070}$	0,044
		0,028	0,038	0,044	0,043	0,047	0,033	0,026	0,046	
2	3	0,046	0,048	0,041	0,032	0,036	0,035	0,036	0,030	0,024
		0,039	0,034	0,029	0,040	$\boxed{0{,}067}$	0,041	0,033	0,037	0,045
		0,033	0,033	0,027	0,033	0,045	0,052	0,042	0,030	
2	4	0,046	0,034	0,043	0,044	0,034	0,031	0,040	0,045	0,040
		0,048	0,044	0,033	0,024	0,028	0,042	0,039	0,026	0,034
		0,050	0,035	0,032	0,040	0,056	0,043	0,028	0,028	
2	5	0,033	0,033	0,036	0,046	0,026	0,018	0,043	$\boxed{0{,}080}$	0,050
		0,029	0,031	0,045	0,039	0,037	0,027	0,026	0,031	0,039
		0,040	0,037	0,041	0,046	0,045	0,043	0,035	0,030	
3	4	0,038	0,036	0,040	0,033	0,036	0,060	0,035	0,041	0,029
		0,058	0,035	0,035	0,034	0,053	0,030	0,032	0,035	0,036
		0,036	0,028	0,046	0,032	0,051	0,032	0,034	0,030	
3	5	0,035	0,034	0,034	0,036	0,030	0,043	0,043	0,050	0,025
		0,041	0,051	0,050	0,035	0,032	0,033	0,033	0,052	0,031
		0,027	0,030	$\boxed{0{,}072}$	0,035	0,034	0,032	0,043	0,027	
4	5	0,052	0,038	0,033	0,038	0,041	0,043	0,037	0,048	0,028
		0,028	0,036	$\boxed{0{,}061}$	0,033	0,033	0,032	0,052	0,034	0,027
		0,039	0,043	0,033	0,027	0,030	0,039	0,048	0,035	

Wzajemne indeksy zgodności dla omawianego kryptogramu przy założeniu długości klucza 5.

Kryptoanaliza szyfru Vigenere'a
Wzajemny indeks zgodności

Otrzymujemy układ równań:

$$
\begin{aligned}
k_1 - k_2 &= 9 \\
k_1 - k_5 &= 16 \\
k_2 - k_3 &= 13 \\
k_2 - k_5 &= 7 \\
k_3 - k_5 &= 20 \\
k_4 - k_5 &= 11
\end{aligned}
$$

Stąd otrzymujemy:

$$
\begin{aligned}
k_2 &= k_1 + 17 \\
k_3 &= k_1 + 4 \\
k_4 &= k_1 + 21 \\
k_5 &= k_1 + 10
\end{aligned}
$$

Kryptoanaliza szyfru Vigenere'a
Wzajemny indeks zgodności

Zatem możemy założyć, że klucz ma postać:[2mm] $(k_1, k_1 + 17, k_1 + 4, k_1 + 21, k_1 + 10)$

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Zatem przypuszczamy, że klucz ma jedną z postaci:[2mm] AREVK, BQFWL, CSGXM, ...

Pozostaje znaleźć właściwy klucz przeszukując wszystkie 26 mozliwości. Po sprawdzeniu znajdujemy właściwy klucz:

JANET

Kryptoanaliza szyfru Vigenere'a

Tekst po rozszyfrowaniu:

> The almond tree was in tentative blossom. The days were longer, often ending with magnificent evenings of corrugated pink skies. The hunting season was over, with hounds and guns put away for six months. The vineyards were busy again as the well-organized farmers treated their vines and the more lackadaisical neighbors hurried to do the pruning they should have done in November.