Vigenéreova šifra

Kod supstitucijske šifre svakom slovu otvorenog teksta odgovara jedinstveno slovo šifrata (monoalfabetske šifre). Sada ćemo pokazati Vigenéreovu šifru koja spada u polialfabetske šifre. Kod nje se svako slovo otvorenog teksta može preslikati u jedno od m mogućih slova, gdje je m duljina ključa, u ovisnosti o svom položaju unutar otvorenog teksta.

Šifra je nazvana po francuskom diplomatu Blaise de Vigenéreu i definirana je na sljedeći način:

Definicija 1.1 *Neka je m fiksan prirodan broj. Definiramo $\mathcal{P} = \mathcal{C} = \mathcal{K} = \mathbb{Z}_{26}^m$. Za ključ $K = (k_1, k_2, \ldots, k_m)$, definiramo*

$$\begin{aligned} e_K(x_1, x_2, \ldots, x_m) &= (x_1 + k_1, x_2 + k_2, \ldots, x_m + k_m), \\ d_K(y_1, y_2, \ldots, y_m) &= (y_1 - k_1, y_2 - k_2, \ldots, y_m - k_m). \end{aligned}$$

(*Imajmo na umu zbrajanje i oduzimanje modulo* 26)!

Dakle, slova otvorenog teksta pomičemo za $k_1, k_2, \ldots$ ili k_m mjesta, u ovisnosti o tome na kojem se mjestu u otvorenom tekstu nalaze (preciznije, pomak ovisi o ostatku koji dobijemo kada poziciju slova podijelimo s duljinom ključa m). Kod ove su šifre osnovni elementi otvorenog teksta i šifrata "blokovi" od po m slova. No, šifriranje se zapravo provodi "slovo po slovo", pa ovdje nije nužno nadopuniti zadnji blok ako broj slova u otvorenom tekstu nije djeljiv s m.

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

.

Primjer 1.2 *Neka je $m = 4$, ključna riječ STOL, a otvoreni tekst*

$$BLAISEDEVIGENERE.$$

Numerički ekvivalent ključa je $K = (18, 19, 14, 11)$, a otvorenog teksta $(1, 11, 0, 8, 18, 4, 3, 4, 21, 8, 6, 4, 13, 4, 17, 4)$. *Šifriranje se provodi na sljedeći način:*

$$\begin{array}{rcccccccccccccccc} & 1 & 11 & 0 & 8 & 18 & 4 & 3 & 4 & 21 & 8 & 6 & 4 & 13 & 4 & 17 & 4 \\ + & 18 & 19 & 14 & 11 & 18 & 19 & 14 & 11 & 18 & 19 & 14 & 11 & 18 & 19 & 14 & 11 \\ \hline & 19 & 4 & 14 & 19 & 10 & 23 & 17 & 15 & 13 & 1 & 20 & 15 & 5 & 23 & 5 & 15 \end{array}.$$

Sada svakom broju pridružimo odgovarajuće slovo šifrata. Dobivamo šifrat

$$TEOTKXRPNBUPFXFP.$$

Možemo primjetiti da se prvo slovo I preslikalo u T, a drugo u B.

U prethodnom primjeru ključ se ponavljao unedogled pa ovu šifru možemo shvatiti kao primjer blokovne šifre.

Druga varijanta Vigenéreove šifre, koja je i sigurnija od originalne, je šifra s autoključem, u kojoj otvoreni tekst generira ključ. Originalni ključ koristi se samo za šifriranje prvog bloka od m slova, a za šifriranje daljnjih blokova koristi se prethodni blok otvorenog teksta. Time ova šifra spada u protočne šifre (tj. elementi otvorenog teksta obrađuju se jedan po jedan koristeći niz ključeva koji se paralelno generira).

Vigenéreov kvadrat

Za šifriranje se može koristiti tablica alfabeta, tzv. Vigenéreov kvadrat. Sastoji se od alfabeta napisanog 26 puta u novom redu, svaki red rotiran ulijevo u odnosu na prethodni, odgovarajući svim mogućim kombinacijama Cezarove šifre. U pojedinoj točki procesa šifriranja, šifra koristi drugi alfabet iz jednog od redova. Koji će se red koristiti ovisi od ponavljajućeg ključa.

Primjer 1.3 *Neka je ključna riječ STOL, a otvoreni tekst*

$$BLAISEDEVIGENERE.$$

Šifrirat ćemo pomoću Vigenéreovog kvadrata. Ako slovo B treba šifrirati ključem S, gledamo stupac koji počinje sa B i redak koji počinje sa S. U presjeku dobijemo šifrat T.

ključ	*S*	*T*	*O*	*L*	*S*	*T*	*O*	*L*	*S*	*T*	*O*	*L*	*S*	*T*	*O*	*L*
otvoreni tekst	*B*	*L*	*A*	*I*	*S*	*E*	*D*	*E*	*V*	*I*	*G*	*E*	*N*	*E*	*R*	*E* .
šifrat	*T*	*E*	*O*	*T*	*K*	*X*	*R*	*P*	*N*	*B*	*U*	*P*	*F*	*X*	*F*	*P*

Ako bi proveli šifriranje s autoključem, dobili bi

ključ	*S*	*T*	*O*	*L*	*B*	*L*	*A*	*I*	*S*	*E*	*D*	*E*	*V*	*I*	*G*	*E*
otvoreni tekst	*B*	*L*	*A*	*I*	*S*	*E*	*D*	*E*	*V*	*I*	*G*	*E*	*N*	*E*	*R*	*E* .
šifrat	*T*	*E*	*O*	*T*	*T*	*P*	*D*	*M*	*N*	*M*	*J*	*I*	*I*	*M*	*X*	*I*

Kriptoanaliza Vigenéreove šifre

Prvi korak je određivanje duljine ključne riječi. Prikazat ćemo dvije metode. Prva metoda zove se *Kasiskijev test* i uveo ju je Friedrich Kasiski 1863. godine. Metoda se zasniva na činjenici da će dva identična segmenta otvorenog teksta biti šifrirana na isti način ukoliko se njihove početne pozicije razlikuju za neki višekratnik od m, gdje je m duljina ključa. Dakle, ako sa Sh označimo pomak i odgovarajuće pozicije istih blokova s P_1 i P_2 imamo: $Sh = P_1 \bmod m$, $Sh = P_2 \bmod m$, a to implicira $P_2 - P_1 = 0 \bmod m$. Dakle $P_2 - P_1$ je višekratnik od m.

U Primjeru 1.2 prvo i predzadnje slovo E šifrirani su na isti način, dakle, slovom X. Naime, njihove pozicije su 6 i 14, a to bi obzirom na duljinu ključa (=4) značilo da će biti šifrirani drugim slovom ključa. Razlika pozicija jednaka je 8, a to je $4 \cdot 2$, što nam ujedno znači šifriranje istim slovom.

Obratno, ako uočimo dva identična segmenta u šifratu, duljine barem 3, tada je vrlo vjerojatno da oni odgovaraju identičnim segmentima otvorenog teksta (podudarnost odsječaka duljine 2 lako može biti i slučajna, dok je kod odsječaka veće duljine to puno manje vjerojatno).

U Kasiskijevom testu u šifratu tražimo parove identičnih segmenata duljine barem 3, te (ako takvi postoje) zabilježimo udaljenosti između njihovih početnih položaja. Ako na takav način dobijemo udaljenosti $d_1, d_2, \ldots$, onda je razumna pretpostavka da duljina ključa m dijeli većinu d_i-ova. Nakon što odredimo m, nalazimo se u sličnoj situaciji kao kod Cezarove šifre. Naime, ako pogledamo samo ona slova koja su šifrirana pomakom za k_1 slova (a ako znamo m, onda znamo i koja su to slova), onda su ona šifrirana

običnom Cezarovom šifrom. Situacija je ipak nešto teža nego kod obične Cezarove šifre, zbog toga što to ovdje nisu uzastopna slova u otvorenom tekstu, pa njihovim dešifriranjem nećemo dobiti smisleni tekst. Zato ćemo opisati još jednu metodu za razbijanje Vigenéreove šifre.

Druga metoda za odredivanje duljine ključa koristi tzv. *indeks koincidencije*. Taj je pojam uveo 1920. godine William Friedman u knjizi *Indeks koincidencije i njegove primjene u kriptografiji*.

Definicija 1.4 *Neka je $x = x_1, x_2, \ldots, x_n$ niz od n slova. Indeks koincidencije od x, u oznaci $I_c(x)$, definira se kao vjerojatnost da su dva slučajna elementa iz x jednaka.*

Neka su $f_0, f_1, \ldots, f_{25}$ redom frekvencije od A, B, C, ..., Z u x. Dva elementa iz x možemo odabrati na $\frac{n(n-1)}{2}$ načina, a za svaki $i = 0, 1, \ldots, 25$ postoji $\frac{f_i(f_i-1)}{2}$ načina odabira dvaput i-tog slova. Dakle, vrijedi sljedeća formula:

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

Pretpostavimo sada da x predstavlja neki tekst na hrvatskom jeziku. Označimo očekivane vjerojatnosti pojavljivanja slova A, B, ..., Z u hrvatskom jeziku redom s $p_0, p_1, \ldots, p_{25}$ (ovdje su to vrijednosti koje odgovaraju ranije navedenim frekvencijama slova u promilima). Ako je n dovoljno velik, za očekivati je da će vrijediti

$$I_c(x) \approx \sum_{i=0}^{25} p_i^2 \approx 0.064.$$

(vjerojatnost da su oba slova A je $p_0^2 \approx 0.115^2$, da su oba B je $p_1^2 \approx 0.015^2$, itd.)

Pretpostavimo sada da imamo šifrat $y = y_1 y_2 \ldots y_n$ koji je dobiven Vigenéreovom šifrom. Rastavimo y na m podnizova $z_1, z_2, \ldots, z_m$ tako da y napišemo, po stupcima, u matricu dimenzija $m \times \frac{n}{m}$. (Ako m ne dijeli n, možemo nadopuniti y na prozvoljan način ili promatrati "krnju matricu" s nepotpunim zadnjim retkom. Redci ove matrice su upravo traženi podnizovi $z_1, z_2, \ldots, z_m$. Ako je m jednak duljini ključne riječi, onda su elementi istog retka matrice šifrirani pomoću istog slova ključa. Na primjer, prvi redak sadrži prvo, $(m+1)$-vo, $(2m+1)$-vo, ... slovo šifrata, a sva su ta slova šifrirana pomoću k_1. Zato bi svi indeksi koincidencije $I_c(z_i), i = 1, \ldots, m$ trebali biti približno jednaki 0.064. S druge strane, ako m nije duljina ključne riječi, onda će z_i-ovi izgledati više-manje slučajni nizovi slova, budući su dobiveni pomacima pomoću različitih slova ključa.

Primijetimo da za potpuno slučajni niz r imamo

$$I_c(r) \approx \sum_{i=0}^{25} (\frac{1}{26})^2 = 26 \cdot (\frac{1}{26})^2 = \frac{1}{26} \approx 0.038.$$

Ove dvije vrijednosti $k_p = 0.064$ i $k_r = 0.038$ (p = plaintext, r = random) su dovoljno daleko jedna od druge, tako da ćemo najčešće na ovaj način moći odrediti točnu duljinu ključne riječi (ili potvrditi pretpostavku dobivenu pomoću Kasiskijeve metode). Napomenimo da je u engleskom jeziku $k_p = 0.065$, u njemačkom $k_p = 0.076$.
Pogledajmo sada kako bi to funkcioniralo na primjeru:

Primjer 1.5 *Dešifrirajmo šifrat dobiven Vigenéreovom šifrom:*

UCOOA VWVJO OVGVF KRVNB BPQQB FRYMJ MFGZZ RGZQG
WGBJO UAMXJ HUAVN EXKOF OFJXQ AXDSF VREFC QZZIK
CMZRY ZXOWG BJOUR VGVYU TZDFD UTZTC TGJVM JYOPJ
NJHGD RMVFG HCBTW ZMGHJ HAXBX QOOHI TUIQT ANTSB
IGHDC ICIBA SIQZE ZTXIQ T.

Najprije treba odrediti duljinu ključne riječi. Primijenimo najprije Kasiskijev test. Nakon analize frekvencije slova, uočavamo nekoliko trigrama koji se dva puta pojavljuju u šifratu. To su VGV na pozicijama 12 i 96 ($96-12 = 84 = 2^2 \cdot 3 \cdot 7$), WGB na pozicijama 41 i 89 ($89 - 41 = 48 = 2^4 \cdot 3$), GBJ na pozicijama 42 i 90 ($90 - 42 = 48 = 2^4 \cdot 3$), BJO na pozicijama 43 i 91 ($91 - 43 = 48 = 2^4 \cdot 3$), JOU na pozicijama 44 i 92 ($92 - 44 = 48 = 2^4 \cdot 3$), UTZ na pozicijama 100 i 106 ($106 - 100 = 6 = 2 \cdot 3$) i IQT na pozicijama 153 i 179 ($179 - 153 = 26 = 2 \cdot 13$). Vidimo da broj 6 dijeli sve osim jedne razlike, pa je razumno pretpostaviti da je duljina ključne riječi (ključa) jednaka $m = 6$. Pogledajmo hoćemo li i pomoću indeksa koincidencije doći do istog zaključka.

$$
\begin{aligned}
&m = 1 : 0.0418\\
&m = 2 : 0.0413, 0.0559\\
&m = 3 : 0.0519, 0.0508, 0.0475\\
&m = 4 : 0.0338, 0.0606, 0.0374, 0.0434\\
&m = 5 : 0.0360, 0.0444, 0.0508, 0.0286, 0.0349\\
&m = 6 : 0.0645, 0.0851, 0.0459, 0.0713, 0.0414, 0.0851.
\end{aligned}
$$

Sada već s prilično velikom sigurnošću možemo zaključiti da je duljina ključne riječi jednaka 6.

Sljedeće je pitanje kako odrediti ključnu riječ ukoliko znamo njezinu duljinu. Tu nam može pomoći medusobni indeks koincidencije dvaju nizova.

Definicija 1.6 *Neka su $x = x_1, x_2, \ldots, x_n$ i $y = y_1, y_2, \ldots, y_{n'}$ dva niza od n, odnosno n' slova. Međusobni indeks koincidencije od x i y, u oznaci $MI_c(x, y)$, definira se kao vjerojatnost da je slučajni element od x jednak slučajnom elementu od y. Ako frekvencije od $A, B, C, \ldots, Z$ u x i y označimo s $f_0, f_1, \ldots, f_{25}$, odnosno $f_0', f_1', \ldots, f_{25}'$, onda je*

$$MI_c(x, y) = \frac{\sum_{i=0}^{25} f_i f_i'}{nn'}.$$

Neka je m duljina ključne riječi, $K = (k_1, k_2, \ldots, k_m)$ ključna riječ i neka su podnizovi $z_1, z_2, \ldots, z_m$ dobiveni iz šifrata kao prije. Pokušajmo ocijeniti indeks $MI_c(z_i, z_j)$. Promotrimo proizvoljno slovo u z_i i proizvoljno slovo u z_j . Procijenimo vjerojatnost da su oba ta slova u tim dijelovima šifrata jednaka A. Prvo slovo A smo dobili pomakom za k_i, a drugo pomakom za k_j. Vjerojatnost da pomakom za k_i dobijemo slovo A približno je jednaka vjerojatnosti s kojom se u hrvatskom jeziku pojavljuje slovo čiji je numerički ekvivalent $-k_i \bmod 26$. Dakle, $i + k_i \equiv 0 (\bmod 26), j + k_j \equiv 0 (\bmod 26)$,

jer 0 je numerički ekvivalent slova A. Prema tome, vjerojatnost da su oba promatrana slova jednaka A približno je jednaka $p_{-k_i}p_{-k_j}$, da su oba slova B približno je jednaka $p_{1-k_i}p_{1-k_j}$, itd. (operacije u indeksima su modulo 26). Dakle, imamo ocjenu

$$MI_c(z_i, z_j) \approx \sum_{h=0}^{25} p_{h-k_i}p_{h-k_j} = \sum_{h=0}^{25} p_h p_{h+k_i-k_j},$$

tj. pomakom indeksa suma se ne mijenja. Uočimo da ova ocjena ovisi samo o razlici $k_i - k_j \bmod 26$, koju ćemo zvati *relativni pomak* od z_i i z_j i označiti s $q = k_i - k_j$. Tada vrijedi

$$\sum_{h=0}^{25} p_h p_{h+q} = \sum_{h=0}^{25} p_h p_{h-q}$$

To znači da za pomak q dobivamo istu ocjenu kao i za pomak $26 - q$ (jer za pomak $q = 0, 1, \ldots, 25$ sve gledano modulo 26 iznosi $26 - q = -q \bmod 26$, a to su pomaci $0, -1, \ldots, -25 \bmod 26$, tj. pomaci $0, \ldots, 25$). Stoga je dovoljno promatrati pomake između 0 i 13. Za hrvatski jezik, ako je relativni pomak $q = 0$, onda je $MI_c = 0.064$. Za ostale $q \in \{1, \ldots, 13\}$ vrijednost od MI_c je između 0.031 i 0.044.

Pretpostavimo da smo fiksirali niz z_i, pa promotrimo efekt šifriranja z_j sa slovima $A, B, C, \ldots, Z$, tj. pomakom za 0, 1, 2, ..., 25 mjesta. Tako dobivene nizove označimo sa $z_j^0, z_j^1, \ldots, z_j^{25}$. Za $g = 0, 1, \ldots, 25$ izračunamo indeks $MI_c(z_i, z_j^g)$ po formuli

$$MI_c(z_i, z_j^g) = \frac{\sum_{i=0}^{25} f_i f'_{i-g}}{nn'}.$$

Ako je $g \equiv q (\bmod 26)$, onda bi MI_c trebao biti blizu 0.064, a za $g \not\equiv q (\bmod 26)$ trebao bi varirati uglavnom između 0.031 i 0.044.

Mi ćemo sada pretpostaviti da nam je poznato da je otvoreni tekst pisan na hrvatskom jeziku. Dakle, naš niz $z_i = x$ je otvoreni tekst hrvatskog jezika. To znači da su relativne frekvencije f_i/n približno jednake vjerojatnosti p_i, pa je

$$MI_c(x, z_j^g) = \frac{\sum_{i=0}^{25} p_i f'_{i-g}}{n'}.$$

Očekujemo da je $MI_c(x, z_j^g) \approx 0.064$ ako je $g \equiv -k_j (\bmod 26)$, a u protivnom da je $MI_c(x, z_j^g) < 0.045$.

Da bi odredili j-to slovo k_j ključne riječi, postupamo na sljedeći način. Za $0 \leq g \leq 25$ računamo

$$M_g = \frac{\sum_{i=0}^{25} p_i f'_{i-g}}{n'}.$$

(operacije u indeksu su modulo 26). Zatim odredimo l takav da je $M_l = \max\{M_g : 0 \leq g \leq 25\}$, te stavimo $l \equiv -k_j \pmod{26}$, tj. $k_j \equiv -l \pmod{26}$.

Nastavak primjera 1.5: Već smo zaključili da je $m = 6$. Stoga imamo sljedeće

podnizove:

$$\begin{aligned} z_1 &= UWGNBMGBXNOXEIYBGDTMNMBHXTNHBET \\ z_2 &= CVVBFFZJJEFDFKZJVFCJJVTJQUTDAZ \\ z_3 &= OJFBRGQOHXJSCCXOYDTYHFWHOISCST \\ z_4 &= OOKPYZGUUKXFQMOUUUGOGGZAOQBIIX \\ z_5 &= AORQMZWAAOQVZZVRTTJPDHMXHTICQI \\ z_6 &= VVVQJRGMVFARZRGVZZVJRCGBIAGIZQ. \end{aligned}$$

Sada za $j = 1, \ldots, 6$ računamo vrijednosti $M_0, \ldots M_{25}$. Npr. za $j = 1$ je

$$\begin{aligned} M_0 &= \frac{\sum_{i=0}^{25} p_i f_i^{'}}{31} = \frac{p_0 f_0^{'} + p_1 f_1^{'} + \cdots + p_{25} f_{25}^{'}}{31} \\ &= \frac{0.115 \cdot 0 + 0.015 \cdot 5 + \cdots + 0.023 \cdot 0}{31} \approx 0.0347, \\ M_1 &= \frac{\sum_{i=0}^{25} p_i f_{i-1}^{'}}{31} = \frac{p_0 f_{25}^{'} + p_1 f_0^{'} + p_2 f_1^{'} \cdots + p_{25} f_{24}^{'}}{31} \\ &= \frac{0.115 \cdot 0 + 0.015 \cdot 0 + \cdots + 0.023 \cdot 1}{31} \approx 0.0411. \end{aligned}$$

Sve vrijednosti prikazane su u sljedećoj tablici:

j	vrijednosti od M_g za $g = 0, 1, 2, \ldots, 25$						
1	0.0347	0.0411	0.0428	0.0398	0.0285	0.0355	0.0415
	0.0646	0.0364	0.0248	0.0293	0.0405	0.0382	0.0521
	0.0397	0.0319	0.0396	0.0443	0.033	0.0275	0.0407
	0.0394	0.0438	0.033	0.0354	0.0408		
2	0.0349	0.0379	0.0232	0.0347	0.0407	0.0600	0.0309
	0.0309	0.0419	0.0620	0.0422	0.0352	0.0332	0.037
	0.0374	0.0399	0.0369	0.0423	0.0333	0.0358	0.0339
	0.0504	0.0227	0.0293	0.0363	0.0560		
3	0.0353	0.0394	0.0413	0.0418	0.0321	0.0318	0.0428
	0.0455	0.0376	0.0277	0.036	0.0465	0.0616	0.0304
	0.0251	0.0318	0.0495	0.0381	0.0320	0.0335	0.0416
	0.0481	0.0363	0.0381	0.0349	0.0404		
4	0.0412	0.0335	0.0349	0.0458	0.0357	0.0387	0.0469
	0.0356	0.0303	0.0333	0.0395	0.0347	0.0464	0.0294
	0.0506	0.0370	0.0421	0.0215	0.0359	0.0342	0.0708
	0.0349	0.0303	0.0323	0.0470	0.0368		
5	0.0433	0.0479	0.0349	0.0332	0.0403	0.0392	0.0319
	0.0365	0.0295	0.0411	0.0393	0.0419	0.0398	0.0381
	0.0451	0.0374	0.0273	0.0364	0.0559	0.0407	0.0377
	0.0399	0.04	0.0367	0.0345	0.0305		
6	0.0396	0.0392	0.0389	0.0333	0.0336	0.0553	0.023
	0.0266	0.0402	0.0678	0.0295	0.0308	0.0345	0.0571
	0.0431	0.0319	0.0199	0.0373	0.0519	0.0455	0.044
	0.0286	0.0396	0.0372	0.0393	0.0278		

Iz tablice iščitavamo redom:

- Za $j = 1$ imamo $l = 7$ pa je $k_1 = -7 \pmod{26} = 26 - 7 = 19$.
- Za $j = 2$ imamo $l = 9$ pa je $k_2 = -9 \pmod{26} = 26 - 9 = 17$.
- Za $j = 3$ imamo $l = 12$ pa je $k_3 = -12 \pmod{26} = 26 - 12 = 14$.
- Za $j = 4$ imamo $l = 20$ pa je $k_4 = -20 \pmod{26} = 26 - 20 = 6$.
- Za $j = 5$ imamo $l = 18$ pa je $k_5 = -18 \pmod{26} = 26 - 18 = 8$.
- Za $j = 6$ imamo $l = 9$ pa je $k_6 = -9 \pmod{26} = 26 - 9 = 17$.

Prema tome, ključna riječ je TROGIR. Otvoreni tekst možemo dobiti pomoću Vigenéreovog kvadrata (redak iznad "—" nam odgovara slovima ključne riječi, stupac lijevo od "|" nam odgovara slovima otvorenog teksta, a u tablici su slova šifrata), samo primjenom postupka dešifriranja. U tablici ispod slova T pronađemo slovo šifrata U i onda u stupcu lijevo od "|" pročitamo o kojem se slovu otvorenog teksta radi. Dobijemo slovo B. Na potpuno analogan način slijedi nam otvoreni tekst:

BLAIS EDEVI GENER EJEUK NJIZI ODSES TOSTR ANICA
OPISA OSVES TOSEU NJEGO VOVRI JEMEZ NALOO KRIPT
OGRAF IJIOP ISAOJ ENEKO LIKOP OLIAL FABET SKIHS
USTAV ATERA ZLICI TEPOS TUPKE ZAIZR ADUKL JUCEV
APOMO CURIJ ECIIL IFRAZ A.

Otvoreni tekst s umetnutim "kvačicama", razmacima i interpunkcijskim znakovima:

Blaise de Vigenére je u knjizi od šesto stranica opisao sve što se u njegovo vrijeme znalo o kriptografiji. Opisao je nekoliko polialfabetskih sustava, te različite postupke za izradu ključeva pomoću riječi ili izraza.

Primjer 1.7 *Pomoću Vigenéreove šifre s ključnom riječi BROJ kriptirati otvoreni tekst:*

Matematika je znanost mladih. Drukčije ne može ni biti. Bavljenje matematikom predstavlja takvu gimnastiku uma, da je za nju potrebna sva gipkost i izdržljivost mladosti.

Šifriranje provodimo tako da prvo slovo otvorenog teksta M šifriramo slovom B, drugo slovo A šifriramo slovom R, itd. Ključ ponavljamo onoliko puta koliko je potrebno. Dobivamo šifrat:

NRHNN RHRLR XNAEO WPJIV MRRRI UFDLT WSFES VPQSW
JSWCJ SOEMC SWKVA JUVAJ UZYXN GFNEJ HJWCX JURYE
VXWVO RGCJB IDNRR JKVNJ OAIYP KFNCE OBWRU RQBCB
UZWIE INUKZ JXTKA UBUCB UZ.

Provedimo sada postupak dešifriranja za tako dobiveni šifrat. Najprije treba pronaći duljinu ključne riječi. U šifratu se nalazi nekoliko trigrama koji se dva puta pojavljuju: NRH na pozicijama 1 i 5 (5 - 1 = 4), VAJ na pozicijama 54 i 58 (58 - 54 = 4), AJU na

pozicijama 55 i 59 (59 - 55 = 4), CBU na pozicijama 119 i 139 (139 - 119 = 20), BUZ na pozicijama 120 i 140 (140 - 120 = 20). Najveći broj kojim su djeljive sve razlike je 4 pa možemo pretpostaviti da je duljina ključne riječi $m = 4$. Provjerimo to i pomoću indeksa koincidencije:

$$\begin{aligned} m &= 1 : 0.0447 \\ m &= 2 : 0.0402, 0.0624 \\ m &= 3 : 0.0425, 0.0426, 0.0379 \\ m &= 4 : 0.0476, 0.0730, 0.0487, 0.0655. \end{aligned}$$

Prilično smo sigurni da je duljina ključne riječi jednaka 4, pa imamo podnizove:

$$\begin{aligned} z_1 &= NNLAPMILFPJJMKUUNEWUVOJNKOPCWQUEKTBU \\ z_2 &= RRREJRUTEQSSCVVZGJCRXRBRVAKERBZIZKUZ \\ z_3 &= HHXOIRFWSSWOSAAYFHXYWGIRNIFOUCWNJAC \\ z_4 &= NRNWVRDSVWCEWJJXNJJEVCDJJYNBRBIUXUB. \end{aligned}$$

Sada za $j = 1, 2, 3, 4$ računamo $M_0, \ldots M_{25}$. Npr. za $j = 1$ i $g = 0$ dobivamo

$$M_0 = \frac{\sum_{i=0}^{25} p_i f_i'}{36} = \frac{0.115 \cdot 1 + 0.015 \cdot 1 + \cdots + 0.023 \cdot 0}{36} \approx 0.0457.$$

Ostale vrijednosti nalaze se u sljedećoj tablici:

j	vrijednosti od M_g za $g = 0, 1, 2, \ldots, 25$						
1	0.0467	0.0345	0.0305	0.0319	0.0439	0.0428	0.0462
	0.0327	0.0355	0.0353	0.0381	0.0282	0.0273	0.0373
	0.0417	0.0403	0.0389	0.0416	0.0336	0.0418	0.0423
	0.0407	0.0333	0.0348	0.0471	0.0521		
2	0.0449	0.0423	0.034	0.0334	0.0375	0.0369	0.0239
	0.0286	0.0363	0.0670	0.0386	0.0351	0.0346	0.0486
	0.0443	0.0336	0.0363	0.0508	0.0387	0.0398	0.0399
	0.0311	0.0448	0.0373	0.0372	0.0311		
3	0.0433	0.0361	0.0351	0.0401	0.0646	0.0290	0.0447
	0.0354	0.0474	0.0317	0.0317	0.0345	0.0599	0.0431
	0.0314	0.0274	0.0385	0.0429	0.0399	0.0335	0.0359
	0.0516	0.0416	0.0367	0.0287	0.0324		
4	0.0396	0.0362	0.029	0.0293	0.0447	0.0463	0.0394
	0.0332	0.0425	0.0403	0.0355	0.0345	0.0444	0.0488
	0.0266	0.0262	0.0385	0.069	0.0377	0.0305	0.0263
	0.0449	0.0383	0.0395	0.0319	0.0457		

Iz tablice iščitavamo redom:

- Za $j = 1$ imamo $l = 25$, pa je $k_1 = -25 \pmod{26} = 26 - 25 = 1$.

- Za $j = 2$ imamo $l = 9$, pa je $k_2 = -9 \pmod{26} = 26 - 9 = 17$.
- Za $j = 3$ imamo $l = 12$, pa je $k_3 = -12 \pmod{26} = 26 - 12 = 14$.
- Za $j = 4$ imamo $l = 17$, pa je $k_4 = -17 \pmod{26} = 26 - 17 = 9$.

Dobili smo ključnu riječ BROJ. Sada dešifriramo na isti način kao u prethodnom primjeru te dobivamo zadani otvoreni tekst.