Kriptografija i sigurnost mreža 2023.

3. domaća zadaća

Doris Đivanović

Zadatak 1

Dekriptirajte šifrat

INEIJ	TCEUT	IEJOS	EIKTK	OJRAV	RNAIM
APGDE	KTSSI	ORLUF	MUOET	THDIO	

ako je poznato da je dobiven stupčanom transpozicijom iz otvorenog teksta na hrvatskom jeziku, te da je broj stupaca veći od 4, a manji od 16.

Rješenje

U zadanom šifratu ima $55 = 11 \cdot 5$ slova, pa ću ga zapisati u pravokutnik tih dimenzija, tj. u tablicu s 5 stupaca i 11 redaka. U svakom retku odredit ću odnos samoglasnika i suglasnika. Budući da je otvoreni tekst pisan na hrvatskom jeziku, odnos bi trebao biti približno 43% : 57% ili recimo 4 : 6, tj. 2 : 3.

I	E	R	D	F	2 : 3
N	J	A	E	M	2 : 3
E	O	V	K	U	2 : 3
I	S	R	T	O	2 : 3
J	E	N	S	E	2 : 3
T	I	A	S	T	2 : 3
C	K	I	I	T	2 : 3
E	T	M	O	H	2 : 3
U	K	A	R	D	2 : 3
T	O	P	L	I	2 : 3
I	J	G	U	O	3 : 2

Poznato je da su najfrekventniji bigrami u hrvatskom jeziku (frekvencija veća od $0,8\%$): AK, AN, AS, AT, AV, CI, DA, ED, EN, IC, IJ, IN, IS, JA, JE, KA, KO, LI, NA, NE, NI, NO, OD, OJ, OS, OV, PO, PR, RA, RE, RI, ST, TA, TI, VA, ZA.
Sada, za svaki od parova stupaca u gornjoj tablici gledam koliko se od 11 bigrama nalazi među najfrekventnijim. Podatke zapisujem u tablicu u kojoj se na mjestu (x, y) nalazi pripadni broj za stupce x i y redom.

	1	2	3	4	5
1		5	3	2	2
2	0		4	4	0
3	5	4		1	2
4	4	1	1		2
5	0	3	4	1	

Vidim da je najveći broj u tablici 5 i on se pojavljuje na mjestima $(1,2)$ i $(3,1)$. Iz toga bih mogla pretpostaviti da su stupci 1, 2 i 3 poredani redoslijedom 312. Sljedeći najveći broj u tablici je 4 i on se nalazi na pozicijama $(2,3)$, $(2,4)$, $(3,2)$, $(4,1)$ i $(5,3)$. Iz toga, ono što se uklapa u već donesenu pretpostavku jest da su stupci 3 i 5 poredani kao 53, a stupci 2 i 4 kao 24. Dakle, pretpostavljam da je poredak stupaca

53124.

Dobivam sljedeće:

F	R	I	E	D
M	A	N	J	E
U	V	E	O	K
O	R	I	S	T
E	N	J	E	S
T	A	T	I	S
T	I	C	K	I
H	M	E	T	O
D	A	U	K	R
I	P	T	O	L
O	G	I	J	U

Čitanjem ovog pravokutnika po stupcima dobivamo sljedeći, očito smisleni, otvoreni tekst:

FRIEDMAN JE UVEO KORISTENJE STATISTICKIH METODA U KRIPTOLOGIJU

Zadatak 2

Dekriptirajte sljedeća dva šifrata

UTOTRIK

IQQBBSY

ako je poznato da su dobiveni istim ključem po pravilu

$$y_i \equiv x_i + k_i \pmod{26}.$$

Također je poznato da su oba otvorena teksta riječi na hrvatskom jeziku koje počinju jednim od slova S, P, N, D.

Rješenje

Prvo slovo

Budući da je U - I = 12, te da su prva slova oba šifrata šifrirana istim ključem, promatrat ću moguća prva slova otvorenih tekstova x i y takva da vrijedi $x - y = 12$ i $x, y \in \{S, P, N, D\}$.

Najprije, neka je $x = \text{S} = 18$. Tada je $18 - y = 12$, tj. $y = 18 - 12 = 6 = \text{G}$. Kako $\text{G} \notin \{S, P, N, D\}$, ovaj slučaj otpada.

Neka je $x = \text{P} = 15$. Tada je $15 - y = 12$, tj. $y = 15 - 12 = 3 = \text{D}$. Dakle, **ovaj slučaj dolazi u obzir**.

Neka je x = N = 13. Tada je $13 - y = 12$, tj. $y = 13 - 12 = 1$ = B. Kako B $\notin \{S, P, N, D\}$, ovaj slučaj otpada.

Konačno, neka je x = D = 3. Tada je $3 - y = 12$, tj. $y = 3 - 12 = -9 \pmod{26} = 17$ = R. Kako R $\notin \{S, P, N, D\}$, i ovaj slučaj otpada.

Dakle, zaključujem da je **prvo slovo gornjeg otvorenog teksta P, a prvo slovo donjeg otvoreng teksta D**.

Drugo slovo

Budući da je T - Q = 19 − 16 = 3, razlika između drugih slova otvorenih tekstova x i y trebala bi biti $x - y = 3$. Kandidate za druga slova promatrat ću među najčešćim drugim slovima u hrvatskom jeziku: $\{A, E, O, R, I, U\}$. Vidim da se među slovima A, E, O, R, I, U, samo parovi U i R, te R i O razlikuju za 3. Dakle, x = U i y = R ili x = R i y = O, tj. **prva dva slova otvorenih tekstova su**

PU i DR ili PR i DO.

Treće slovo

Kako je O - Q = 24, treća slova otvorenih tekstova x i y trebala bi se razlikovati za 24, tj. $x - y = 24$.

Prvo ću promatrati slučaj da otvoreni tekstovi počinju s PU i DR. Kako su otvoreni tekstovi na hrvatskom jeziku, pretpostavljam da bi u nekoj riječi nakon DR vjerojatno trebao dolaziti samoglasnik, dakle neki $\in \{A, E, O, I, U\}$. Iz znanja hrvatskog jezika, najvjerojatnije mi se čini da riječ od 7 slova počinje s DRA ili DRU, pa ću provjeriti te slučajeve.

Neka je y = A = 0. Tada je $x - 0 = 24$, tj. $x = 24$ = Y. Slovo Y ne postoji u hrvatskoj abecedi, dakle ovaj slučaj ne dolazi u obzir.

Neka je y = U = 20. Tada je $x - 20 = 24$, tj. $x = 24 + 20 = 44 \pmod{26} = 18$ = S. Dakle, kandidati za prva tri slova otvorenih tekstova su

PUS i DRU.

Iz ovakvih početaka riječi trenutno ne mogu intuitivno zaključiti o kojim bi se hrvatskim riječima moglo raditi. Iz liste najčešćih bigrama u hrvatskom jeziku u kojoj se nalazi bigram ST, mogla bih pretpostaviti da je četvrto slovo prve riječi T, tj. da prva riječ počinje s PUST. Kako je T - B = 18, četvrta slova otvorenih tekstova x i y trebala bi se razlikovati za 18, tj. $x - y = 18$. Ako je x = T = 19, onda $19 - y = 18$, tj, $y = 1$ = B. Dakle, ako prva riječ počinje s PUST, druga riječ počinje s DRUB, ali ne poznajem ni jednu hrvatsku riječ koja počinje s DRUB, pa **ovo razmatranje zasad otpada**.

Sada ću promatrati slučaj da otvoreni tekstovi počinju s PR i DO. Kako su otvoreni tekstovi na hrvatskom jeziku, pretpostavljam da bi u nekoj riječi nakon PR vjerojatno trebao dolaziti samoglasnik, dakle neki $\in \{A, E, O, I, U\}$. Iz znanja hrvatskog jezika, najvjerojatnije mi se čini da riječ od 7 slova počinje s PRA, PRE, PRI ili PRO, pa ću provjeriti te slučajeve.

Neka je x = A = 0. Tada je $0 - y = 24$, tj. $y = -24 \pmod{26} = 2$ = C . Dakle, kandidati za prva tri slova otvorenih tekstova su

PRA i DOC.

Budući da ne poznajem puno riječi na hrvatskom eziku koje počinju s DOC, **ovo razmatranje zasad otpada**.

Neka je $x = \text{I} = 8$. Tada je $8 - y = 24$, tj. $y = 8 - 24 = -16 \pmod{26} = 10 = \text{K}$. Dakle, kandidati za prva tri slova otvorenih tekstova su

PRI i DOK.

Sada, iz poznavanja hrvatskog jezika, mogla bih pretpostaviti da je druga riječ DOKUMENT, no ona ima 8 slova. Također, druga riječ bi mogla biti i npr. DOKAZI, ali ona ima 6 slova. **Ovaj ću slučaj zasad ostaviti po strani**.

Neka je $x = \text{O} = 14$. Tada je $14 - y = 24$, tj. $y = 14 - 24 = -10 \pmod{26} = 16 = \text{Q}$. Slovo Q ne postoji u hrvatskoj abecedi, dakle ovaj slučaj ne dolazi u obzir.

Neka je $x = \text{E} = 4$. Tada je $4 - y = 24$, tj. $y = 4 - 24 = -20 \pmod{26} = 6 = \text{G}$. Dakle, kandidati za prva tri slova otvorenih tekstova su

PRE i DOG.

Sada, iz poznavanja hrvatskog jezika, mogla bih pretpostaviti da je druga riječ DOGAĐAJ, tj. DOGADAJ, pa ću provjeriti taj slučaj.

Četvrto slovo

Kako je, iz šifrata, T - B = 18, četvrta slova otvorenih tekstova x i y trebala bi se razlikovati za 18, tj. $x - y = 18$.

Ako pretpostavim da je $y = \text{A} = 0$, onda $x - 0 = 18$, tj, $x = 18 = \text{S}$. Dakle, kandidati za prva četiri slova otvorenih tekstova su

PRES i DOGA.

Početak riječi PRES možda ima smisla, pa ću nastaviti s pretpostavkom da je druga riječ DOGADAJ.

Kako je, iz šifrata, R - B = 16, peta slova otvorenih tekstova x i y trebala bi se razlikovati za 16, tj. $x - y = 16$.

Ako je $y = \text{D} = 3$, onda $x - 3 = 16$, tj, $x = 16 + 3 = 19 = \text{T}$. Dakle, ako druga riječ počinje s DOGAD, prva riječ počinje s PREST, ali, na prvu, ne poznajem ni jednu hrvatsku riječ od 7 slova koja počinje s PREST, pa **ovo razmatranje zasad otpada**.

Sada, iz poznavanja hrvatskog jezika, pretpostavit ću da je druga riječ DOGOVOR, i provjeriti taj slučaj.

Neka je četvrto slovo druge riječi $y = \text{O} = 14$. Tada je $x - 14 = 18$, tj. $x = 18 + 14 = 32 \pmod{26} = 6 = \text{G}$. Dakle, kandidati za prva četiri slova otvorenih tekstova su

PREG i DOGO.

Početak riječi PREG možda ima smisla, pa ću nastaviti s pretpostavkom da je druga riječ DOGOVOR, a naslućujem da bi prva riječ mogla biti PREGLED.

Ostatak riječi

Neka je peto slovo druge riječi $y = \text{V} = 21$. Tada je $x - 21 = 16$, tj. $x = 16 + 21 = 37 \pmod{26} = 11 = \text{L}$. Dakle, ako druga riječ počinje s DOGOV, prva riječ počinje s PREGL.

Sada ću s velikom sigurnošću pretpostaviti da su otvoreni tekstovi uistinu PREGLED i DOGOVOR, a to ću i provjeriti.

Kako je, iz šifrata, I - S $= 8 - 18 = -10 \pmod{26} = 16$, šesta slova otvorenih tekstova x i y trebala bi se razlikovati za 16, tj. $x - y = 16$. Ako pretpostavim da je $x = \text{E} = 4$ i $y = \text{O} = 14$, tada je $x - y = 4 - 14 = -10 \pmod{26} = 16$, **pa je zasad sve u redu**.

Kako je, iz šifrata, K - Y $= 10 - 24 = -14 \pmod{26} = 12$, sedma slova otvorenih tekstova x i y trebala bi se razlikovati za 12, tj. $x - y = 12$. Ako pretpostavim da je $x = \text{D} = 3$ i $y = \text{R} = 17$, tada je $x - y = 3 - 17 = -14 \pmod{26} = 12$, pa zaključujem da su **otvoreni tekstovi za dane šifrate** uistinu

PREGLED i DOGOVOR.

Zadatak 3

Odredite skupove $test_1(E_1, E_1^*, C_1')$ i $test_2(E_2, E_2^*, C_2')$ ako je

$$E_1 = 000101, \quad E_1^* = 110001, \quad C_1' = 0010,$$
$$E_2 = 000010, \quad E_2^* = 110110, \quad C_2' = 1011.$$

Rješenje

Najprije računam

$$E_1' = E_1 \oplus E_1^* = 110100$$

($\oplus$ je bitovna operacija isključivo ili).

Sada koristim tablicu priloženu u materijalima s predavanja kako bih utvrdila skup $IN_1(E_1', C_1') = IN_1(110100, 0010)$, tj. skup mogućih inputa za output XOR = 0010.
Imam sljedeći skup:

$$\begin{aligned} IN_1(110100, 0010) = \{&000100, 000101, 001110, 010001, 010010,\\ &010100, 011010, 011011, 100000, 100101,\\ &100110, 101110, 101111, 110000, 110001, 111010\}. \end{aligned}$$

Sada, budući da je $test_1(E_1, E_1^*, C_1') = \{B_1 \oplus E_1 : B_1 \in IN_1(E_1', C_1')\}$, provođenjem potrebnih operacija, dobivam:

$$\begin{aligned} test_1(E_1, E_1^*, C_1') = \{&000001, 000000, 001011, 010100, 010111,\\ &010001, 011111, 011110, 100101, 100000,\\ &100011, 101011, 101010, 110101, 110100, 111111\}. \end{aligned}$$

Analogno,

$$E_2' = E_2 \oplus E_2^* = 110100,$$
$$IN_2(E_2', C_2') = IN_2(110100, 1011) = \emptyset,$$

pa zaključujem da je

$$test_2(E_2, E_2^*, C_2') = \emptyset.$$