Osnove kriptografije

Miladinović, Tena

Sveučilište J.J. Strossmayera u Osijeku
Odjel za matematiku
Sveučilišni preddiplomski studij Matematika

Tena Miladinović

Osnove kriptografije

Završni rad

Osijek, 2023.

Sveučilište J.J. Strossmayera u Osijeku
Odjel za matematiku
Sveučilišni preddiplomski studij Matematika

Tena Miladinović

Osnove kriptografije

Završni rad

Mentor: izv. prof. dr. sc. Ivan Soldo

Osijek, 2023.

Sažetak

Ovaj rad opisuje neke od poznatijih kriptosustava. Mnoge povijesne ličnosti poput kraljice Marije Stuart koristili su šifre, što je opisano u uvodnom dijelu. Također, opisana je i definicija kriptosustava te osnovni pojmovi koji su korišteni u cijelom radu. U glavnom dijelu opisane su monoalfabetske Cezarova i afina šifra te polialfabetska Vigenèreova šifra. Također, opisana je i blokovna Playfairova te poligramska Hillova šifra. Pojam savršene sigurnosti uveden je kroz jednokratnu bilježnicu. Stupčana transpozicija i šifriranje rešetkom opisani su u posljednjem poglavlju.

Ključne riječi

kriptografija, kriptosustav, šifre, otvoreni tekst, ključ, šifrat

Basics of cryptography

Summary

In this paper, we describe some of the better known cryptosystems. Many historical figures such as Queen Mary Stuart used ciphers, which is described in the introduction. Also, the definition of a cryptosystem and the basic terms used throughout the paper are described. In the main part, the monoalphabetic Caesar and Affine ciphers and the polyalphabetic Vigenère cipher are described. Also, the block Playfair cipher and the polygram Hill cipher are described. The concept of perfect security was introduced through a One-Time Pad. Columnar transposition and rail fence cipher are described in the last chapter.

Keywords

cryptography, cryptosystem, ciphers, plaintext, key, ciphertext

Sadržaj

Uvod

Znanstvena disciplina koja proučava metode slanja poruka tako da ih se pretvori u oblik u kojemu će ih samo određene osobe moći pročitati naziva se kriptografija. Grčke riječi *kryptos* (skriven), *logos* (riječ ili razlog) te *grafo* (pisati) osnova su riječi kriptografija. To bi se doslovno moglo prevesti kao tajnopis.

Korištenje šifri u svrhu tajnosti prenošenja poruke poznato je od davnina. Primjerice, u 5. stoljeću prije Krista, Grci su bili upozoreni na napad Perzijanaca tako što je Demarat urezao poruku upozorenja u drvene pločice i prekrio ih voskom te ju dostavio Grcima. Grci su također koristili i drveni štap (skital) na koji su namatali vrpcu od pergamenta te okomito upisivali poruku. Na odmotanoj vrpci ostali bi izmiješani znakovi koji bi se mogli pročitati samo ukoliko se vrpca namota na skital istog promjera. Prikaz skitala može se pronaći u [2, str. 1]

Još jedan primjer skrivanja poruke bilježi priča o Histajeju koji je poslao upute Aristagoru Miletskom za bunu protiv perzijskog kralja. Naime, on je odlučio glasniku obrijati glavu, na nju napisati poruku te pričekati da mu kosa naraste. Kada je glasniku kosa narasla, on je otputovao primatelju te je tamo, obrijavši glavu, prenio Histajejovu poruku. Ovo je klasičan primjer *steganografije*. To je način tajnog komuniciranja pri kojemu se skriva i samo postojanje poruke.

Također, u 16. stoljeću kraljici Mariji Stuart sudilo se zbog veleizdaje jer se vjerovalo da je bila predvodnik pokušaja ubojstva kraljice Elizabete, budući da su joj naizgled besmislena pisma upućena urotnicima bila uhvaćena.

Svrha je kriptografije omogućiti pošiljatelju i primatelju (Alice i Bob) komunikaciju putem nekog nesigurnog kanala tako da treća osoba (Eva ili Oskar) ne može shvatiti značenje poruke unatoč tome što može nadzirati komunikacijski kanal. *Otvorenim tekstom* zovemo poruku koju pošiljatelj želi poslati primatelju. Ta poruka može biti zapis na nekom jeziku, brojčani podatci i slično. Postupak transformiranja otvorenog teksta koristeći se unaprijed određenim *ključem* naziva se *šifriranje*, a tekst dobiven tim postupkom *šifrat* ili *kriptogram*. Pošiljatelj zatim komunikacijskim kanalom šalje šifrat primatelju. Osoba kojoj poruka nije namjenjena može vidjeti šifrat ukoliko prisluškuje komunikacijski kanal, ali ne može odgonetnuti otvoreni tekst ukoliko ne zna kojim ključem je šifrirana poruka. Primatelj kojemu je poznat ključ korišten za šifriranje može *dešifrirati* šifrat te saznati otvoreni tekst.

Kriptografski algoritam ili *šifra* matematička je funkcija koju koristimo za šifriranje i dešifriranje. Zapravo govorimo o dvije funkcije: prva je za šifriranje, dok druga služi za dešifriranje. One preslikavaju osnovne elemente otvorenog teksta (primjerice slova abecede, grupe slova, nule i jedinice i slično) u osnovne elemente šifrata i obratno. Te dvije funkcije biramo u ovisnosti o ključu. Definicija kriptosustava je sljedeća:

Definicija 1. *Uređena petorka* $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ *čini jedan kriptosustav pri čemu vrijedi sljedeće:*

- $\mathcal{P}$ *je konačan skup svih mogućih osnovnih elemenata otvorenog teksta*

- $\mathcal{C}$ *je konačan skup svih mogućih osnovnih elemenata šifrata*
- $\mathcal{K}$ *je konačan skup svih mogućih ključeva*
- $\mathcal{E}$ *je skup svih funkcija šifriranja*
- $\mathcal{D}$ *je skup svih funkcija dešifriranja.*

Za svaki $K \in \mathcal{K}$ *postoji funkcija šifriranja* $e_K \in \mathcal{E}$ *te pripadajuća funkcija dešifriranja* $d_K \in \mathcal{D}$. *Funkcije* $e_K \colon \mathcal{P} \to \mathcal{C}$ *i* $d_K \colon \mathcal{C} \to \mathcal{P}$ *imaju svojstvo da je* $d_K(e_K(x)) = x$ *za svaki* $x \in \mathcal{P}$.

Vrlo važno svojstvo iz prethodne definicije je $d_K(e_K(x)) = x$ jer iz njega slijedi da funkcije šifriranja e_K moraju biti injekcije. Kada to ne bi bilo tako, odnosno kada bi za dva različita otvorena teksta x_1 i x_2 vrijedilo

$$e_K(x_1) = e_K(x_2) = y,$$

onda $d_K(y)$ ne bi bilo definirano budući da primatelj ne bi mogao odrediti s čime treba dešifrirati y. U skladu s time su, ukoliko je $\mathcal{P} = \mathcal{C}$, funkcije šifriranja e_K permutacije.

Klasifikacija kriptosustava određuje se prema sljedeća tri kriterija:

1. Tip operacija koje se koriste pri šifriranju

   Ovdje razlikujemo *supstitucijske* i *transpozicijske šifre*. U supstitucijskim šiframa svaki element otvorenog teksta zamjenjuje se nekim drugim elementom, dok se kod transpozicijskih šifri ti elementi permutiraju.

2. Način na koji se obrađuje otvoreni tekst

   Ovdje razlikujemo blokovne šifre kod kojih se svaki blok otvorenog teksta obrađuje pojedinačno pritom koristeći isti ključ, te protočne šifre kod kojih se elementi otvorenog teksta obrađuju jedan po jedan i to paralelno koristeći generirani niz ključeva.

3. Tajnost i javnost ključeva

   Ovdje razlikujemo simetrične kriptosustave te kriptosustave s javnim ključem. Kod simetričnih kriptosustava ključ za šifriranje moguće je izračunati poznavajući ključ za dešifriranje i obratno. Primjer simetričnog kriptosustava je DES (Data Encription Standard), a primjer kriptosustava s javnim ključem je RSA. Više o njima može se pročitati u [2].

1 Cezarova šifra

Poznato je da se rimski vojskovođa Julije Cezar toliko često koristio šiframa da je čak napisana i rasprava o tome koja nažalost nije očuvana. No, međutim, u Svetonijevom *Životu Cezara LVI* nalazi se detaljan opis jedne supstitucijske šifre kojom se Cezar koristio. U njoj se slova otvorenog teksta mijenjaju slovima koja se nalaze tri mjesta dalje u alfabetu (A se pretvara u D, B u E, itd.) uz pretpostavku da se alfabet ciklički nastavlja te da se koristi engleski alfabet. Ukoliko se koristi hrvatski alfabet, tada se slova Č, Ć, Đ, Dž, Lj, Nj, Š, Ž mijenjaju redom s C, C, DJ, DZ, LJ, NJ, S, Z. Danas se Cezarovom šifrom smatraju i one s pomakom različitim od tri. Kako bismo Cezarovu šifru definirali u okviru Definicije 1., uvodimo korespodenciju između slova alfabeta (A - Z) i cijelih brojeva (0 - 25). Sa $\mathbb{Z}_{26}$ označit ćemo skup brojeva $\{0,1,2,...,25\}$ uz pretpostavku da na njemu imamo definirane operacije množenja, zbrajanja i oduzimanja i na isti način kao na skupu $\mathbb{Z}$. Ukoliko rezultat nije iz toga skupa, on će se na kraju zamijeniti s njegovim ostatkom pri dijeljenju s 26. Dakle, za svako slovo alfabeta imamo njegov numerički ekvivalent (A je predstavljen 0, B brojem 1, itd.). Cezarovu šifru definiramo na sljedeći način:

Definicija 2. *Pretpostavimo da je* $\mathcal{P} = \mathcal{C} = \mathcal{K} = \mathbb{Z}_{26}$. *Tada za* $0 \leq K \leq 25$ *definiramo*

$$e_K(x) = (x + K) \ mod\ 26,\ d_K(y) = (y - K) \ mod\ 26.$$

Dakle, postoji 26 različitih ključeva, odnosno 26 je pozicija za koje možemo pomaknuti slova alfabeta šifrata. Za $K = 3$ dobivamo originalnu Cezarovu šifru. U 15. stoljeću arhitekt Leone Battista Alberti osmislio je napravu s dva diska pomoću koje se moglo šifrirati i dešifrirati bilo koju Cezarovu šifru. Prikaz naprave može se naći u [1, str. 5]. Upotreba Cezarove šifre može se vidjeti u sljedećem primjeru.

Primjer 1. *Neka je šifrat DFWDQRQYHUED dobiven Cezarovom šifrom. Dešifrirajmo ga.*

Rješenje:

D	*F*	*W*	*D*	*Q*	*R*	*Q*	*Y*	*H*	*U*	*E*	*D*
C	*E*	*V*	*C*	*P*	*Q*	*P*	*X*	*G*	*T*	*D*	*C*
B	*D*	*U*	*B*	*O*	*P*	*O*	*W*	*F*	*S*	*C*	*B*
A	*C*	*T*	*A*	*N*	*O*	*N*	*V*	*E*	*R*	*B*	*A*

Dakle, ključ $K = 3$ te je otvoreni tekst ACTA NON VERBA.

Budući da je broj ključeva Cezarove šifre malen, "grubom silom" moguće je isprobati sve potencijalne ključeve dok se ne dođe do smislenog teksta kao u prethodnom primjeru. Zbog toga se javlja afina šifra opisana u sljedećem poglavlju.

2 Afina šifra

Budući da je Cezarovu šifru lako razbiti, za funkcije šifriranja mogu se promatrati one funkcije koje uključuju više od jednog parametra. Najjednostavnija takva upravo je afina funkcija $e(x)=ax+b$. Budući da takva funkcija ne mora biti injekcija na $\mathbb{Z}_{26}$, parametar a biramo tako da bude relativno prost s modulom 26. Ime šifre dolazi od činjenice da su funkcije šifriranja i dešifriranja afine što je vidljivo u sljedećoj definiciji.

Definicija 3. *Pretpostavimo da je* $\mathcal{P} = \mathcal{C} = \mathbb{Z}_{26}$, *te neka je*

$$K = \{(a, b) \in \mathbb{Z}_{26} \times \mathbb{Z}_{26} : (a, 26) = 1\}.$$

Za $K=(a,b) \in \mathcal{K}$ *definiramo*

$$e_K(x) = (ax + b) \ mod\ 26,\ d_K(y) = a^{-1}(y - b) \ mod\ 26.$$

Treba provjeriti je li uvjet $d_K(e_K(x)) = x$ zadovoljen:

$$d_K(e_K(x)) = d_K(ax + b) = a^{-1}(ax + b - b) = x.$$

Primjer 2. *Neka je* $K=(9,19)$ *i otvoreni tekst neka je KVANTNA FIZIKA. Treba šifrirati otvoreni tekst.*

Rješenje:
Ukoliko svako od slova poistovjetimo s njegovim numeričkim ekvivalentom, imamo:

$$\begin{aligned}
e_K(K) &= 10 \cdot 9 + 19 \equiv 5 \pmod{26} \rightarrow \text{F} \\
e_K(V) &= 21 \cdot 9 + 19 \equiv 0 \pmod{26} \rightarrow \text{A} \\
e_K(A) &= 0 \cdot 9 + 19 \equiv 19 \pmod{26} \rightarrow \text{T} \\
e_K(N) &= 13 \cdot 9 + 19 \equiv 6 \pmod{26} \rightarrow \text{G} \\
e_K(T) &= 19 \cdot 9 + 19 \equiv 8 \pmod{26} \rightarrow \text{I} \\
e_K(F) &= 5 \cdot 9 + 19 \equiv 12 \pmod{26} \rightarrow \text{M} \\
e_K(I) &= 8 \cdot 9 + 19 \equiv 13 \pmod{26} \rightarrow \text{N} \\
e_K(Z) &= 25 \cdot 9 + 19 \equiv 10 \pmod{26} \rightarrow \text{K}
\end{aligned}$$

pa time dobijemo šifrat FATGIGTMNKNFT.

Budući da parametar a treba birati u skladu s definicijom, postoji $12 \cdot 26 = 312$ mogućih ključeva što je više od broja mogućih ključeva kod Cezarove šifre. To je još uvijek premalo, jer se i ovdje pomoću računala može primjeniti "gruba sila" za dekriptiranje. Naime, postoji i drugačiji način ukoliko nam je poznato kojim jezikom je pisan otvoreni tekst. Supstitucijsku šifru puno je lakše dekriptirati ukoliko koristimo statistička svojstva jezika. Najčešće se to radi *analizom frekvencija slova*. Poznato je da postoje slova, pa i sami *bigrami* (parovi slova) i *trigrami* (nizovi od tri slova) koja se češće pojavljuju u tekstu od ostalih. Kako bi analizirali učestalost pojavljivanja nekog slova u šifratu, brojimo pojavljivanje svakog slova u njemu. Zatim se distribucija slova u šifratu uspoređuje s distribucijom slova u jeziku za koji pretpostavljamo da je jezik otvorenog teksta. Naravno, teže je ovakvu analizu raditi na

šifratima koji se sastoje od nekoliko riječi ili na tekstovima koji primjerice govore o nekoj temi u kojoj su određena slova puno učestalija nego što bi inače bila. Primjerice, članak iz polja matematike koji sadrži puno jednadžbi, koristi slova X, Y i Z pa su time ta slova učestalija nego što bi teoretski bila. Najfrekventnija slova hrvatskog jezika su A (11.5%), I (9.8%), O (9%), E (8.4%) te N (6.6%). Slijede ih S, R, J i T. Najmanje frekventno slovo je F (0.3%). U engleskom jeziku najfrekventnija su E (12.7%), T (9.1%), A (8.2%), O (7.5%) te I (7%), dok su najmanje frekventna Q, X i Z s 1%. U njemačkom jeziku najfrekventnija slova su E (17.5%), N (9.8%), I (7.7%), R (7.5%) te S (6.8%), dok je najmanje frekventno slovo Y (1%). Ukoliko promatramo bigrame, u hrvatskom jeziku nafrekventniji su JE (2.7%) te NA (1.5%). Najfrekventniji trigram je IJE (0.6%). Najfrekventniji bigrami engleskog jezika su TH (3.2%) te HE (2.5%), a najfrekventniji trigram je THE (3.5%). Najfrekventniji bigrami njemačkog jezika su ER (4.1%) te EN (4.0%), a trigrami EIN (1.2%) te ICH (1.1%). Više informacija o frekvencijama može se naći u [2, str. 10 i 11]. Dakle, pri analizi frekvencija promatramo koja slova šifrata su se najviše ili najmanje puta pojavila. Time ćemo lakše moći odrediti ključ kojim je otvoreni tekst šifriran. U sljedećem primjeru prikazano je korištenje ove metode.

Primjer 3. *Neka je dan šifrat*

$$EJQHGFUJQHTJYHEQHYSFWUFIFZIWFUF.$$

Dešifrirajmo ga imajući na umu da je dobiven afinom šifrom.

Rješenje:
Primjećujemo da se najviše pojavljuje slovo F, i to šest puta, a zatim H četiri puta te slova J, Q te U po tri puta. Također, uočavamo da se trigram JQH pojavio dva puta. Možemo pretpostaviti da je to upravo najfrekventniji trigram u hrvatskom jeziku IJE. To je također u skladu s time da su I i E jedna od najfrekventnijih slova. Ukoliko pretpostavimo da je

$$e_K(I) = J,\ e_K(J) = Q$$

imamo:

$$\begin{aligned} e_K(I) &= a \cdot 8 + b \\ e_K(J) &= a \cdot 9 + b, \end{aligned}$$

odnosno, budući da je numerički ekvivalent slova J upravo 9, a slova Q je 16:

$$\begin{aligned} 9 &= a \cdot 8 + b \\ 16 &= a \cdot 9 + b \\ 9 - 8 \cdot a &= 16 - 9 \cdot a \\ a = 16 - 9 \equiv 7 \pmod{26} &\implies b \equiv 5 \pmod{26}. \end{aligned}$$

Dakle, funkcije šifriranja i dešifriranja su:

$$e_K(x) = 7x + 5 \pmod{26},\ d_K(y) = 15(y - 5) \pmod{26}$$

budući da je broj 15 multiplikativan inverz na $\mathbb{Z}_{26}$ broju 7.
Primjenom funkcije dešifriranja na šifrat dobije se otvoreni tekst: LIJEPA RIJEČ I ŽELJEZNA VRATA OTVARA.

Afina i Cezarova šifra posebni su slučajevi *supstiticijske šifre*, čija definicija je dana u nastavku.

Definicija 4. *Pretpostavimo da je* $\mathcal{P} = \mathcal{C} = \mathbb{Z}_{26}$ *te neka se prostor ključeva* $\mathcal{K}$ *sastoji od svih permutacija skupa* $\{0, 1, 2, ..., 25\}$. *Za svaku permutaciju* $\pi \in \mathcal{K}$ *definiramo*

$$e_\pi(x) = \pi(x),\ d_\pi(y) = \pi^{-1}(y),$$

gdje je π^{-1} *inverzna permutacija od* π.

Dakle, kod supstitucijske šifre za alfabet šifrata možemo odabrati bilo koju permutaciju slova alfabeta te time dobivamo čak $26! \approx 4 \cdot 10^{26}$ mogućih ključeva. Ispitati sve moguće ključeve postaje gotovo nemoguće. Ipak, supstitucijsku šifru lako je razbiti koristeći se ponovno analizom frekvencije slova. Dakle, monoalfabetske šifre (svakom slovu otvorenog teksta pripada jedinstveno slovo šifrata) kao što su Cezarova i afina ipak nisu toliko korisne budući da je za njihovo razbijanje potrebna samo "gruba sila" ili analiza frekvencije slova. Zbog toga se počela upotrebljavati *homofona šifra* u kojoj su najfrekventnija slova imala nekoliko različitih zamjena, što je povećavalo sigurnost šifre. No međutim, kriptoanalitičari i dalje se mogu osloniti na analizu bigrama i trigrama te razbiti šifru.

3 Vigenèreova šifra

Budući da Cezarova i afina šifra nisu bile dovoljno sigurne, kriptografi su trebali smisliti novu, jaču šifru koju kriptoanalitičari neće moći razbiti. Korijenje takve šifre seže do 16. stoljeća, točnije do Leona Battiste Albertija koji je osmislio novi način šifriranja tako da se koristi više od jednog šifriranog alfabeta. S njegovim spisima susreo se francuski diplomat Blaise de Vigenère te ideju takve šifre pretvorio u vrlo moćnu novu šifru koja se služi sa 26 šifriranih alfabeta. Šifru u kojoj svako slovo otvorenog teksta preslikavamo u jedno od m mogućih slova (m duljina ključa) naziva se *polialfabetska šifra*.

Definicija Vigenèreove šifre dana je na sljedeći način:

Definicija 5. *Pretpostavimo da je m fiksan prirodan broj te neka je $\mathcal{P} = \mathcal{C} = \mathcal{K} = \mathbb{Z}_{26}^m$. Za ključ $K = (k_1, k_2, ..., k_m)$, definiramo*

$$e_K(x_1, x_2, ..., x_m) = (x_1 +_{26} k_1, x_2 +_{26} k_2, ..., x_m +_{26} k_m),$$
$$d_K(y_1, y_2, ..., y_m) = (y_1 -_{26} k_1, y_2 -_{26} k_2, ..., y_m -_{26} k_m).$$

Dakle, prvi je korak u šifriranju crtanje Vigenèreova kvadrata. U prvom retku nalazi se alfabet otvorenog teksta, a iza njega slijedi još 25 redaka šifriranih alfabeta tako da se u drugom retku nalazi alfabet pomaknut jedno mjesto ulijevo, zatim u idućem retku za dva mjesta ulijevo, itd. Da bi primatelj znao odgonetnuti šifrat, mora znati dogovoreno pravilo kojim se izmjenjuju retci šifriranih alfabeta. To pravilo sadržano je u ključnoj riječi. Dakle, ključna riječ najprije se ispisuje iznad poruke koju želimo šifrirati tako da svako slovo poruke koju želimo šifrirati ima pripadajuće slovo odabrane ključne riječi. Da bismo šifrirali slovo otvorenog teksta, pogledamo koje slovo se nalazi iznad njega. Slovo ključne riječi određuje kojim ćemo se retkom Vigenèreovog kvadrata poslužiti, a slovo otvorenog teksta određuje kojim stupcem ćemo se poslužiti. Presjekom tog retka i stupca dobit ćemo slovo šifrata. Što je duža ključna riječ, to je šifra složenija. U sljedećem primjeru ilustrirano je šifriranje poruke Vigenèreovom šifrom.

Primjer 4. *Neka nam je dana duljina ključa m=6 i ključna riječ SKITAL. Numerički ekvivalent ključa je K=(18,10,8,19,0,11). Također, dan nam je otvoreni tekst SCIO ME NIHIL SCIRE, čiji je numerički ekvivalent (18,2,8,14,12,4,13,8,7,8,11,18,2,8,17,4). Šifrirajmo taj otvoreni tekst koristeći dani ključ.*

Rješenje:
Šifriranje se provodi na sljedeći način:

	18	10	8	19	0	11	18	10	8	19	0	11	18	10	8	19
$+_{26}$	18	2	8	14	12	4	13	8	7	8	11	18	2	8	17	4
	10	12	16	7	12	15	5	18	15	1	11	3	20	18	25	23

Dakle, šifrat je KMQHMPFSPBLDUSZX. Promotrimo li dobiveni šifrat, možemo primjetiti da se slovo I jednom preslikalo u S, a drugi puta u B.

Ukoliko umjesto pripadnih numeričkih ekvivalenata koristimo slova, taj primjer možemo prikazati i ovako:

ključ	S	K	I	T	A	L	S	K	I	T	A	L	S	K	I	T
otvoreni tekst	S	C	I	O	M	E	N	I	H	I	L	S	C	I	R	E
šifrat	K	M	Q	H	M	P	F	S	P	B	L	D	U	S	Z	X

Vigenèreova šifra neosjetljiva je na analizu frekvencije slova, ali također je moguć i velik broj ključeva. Za ključ možemo uzeti bilo koju riječ iz rječnika ili čak kombinirati nekoliko njih, što ne izostavlja korištenje neke izmišljene riječi. Vigenère je svoju šifru objavio 1586. u *Raspravi o tajnom pisanju*, a njezina primjena nastavila se širiti kroz sljedeća tri stoljeća. Budući da se smatralo da je šifru nemoguće razbiti, dobila je naziv *le chifre indechiffrable*. Međutim, ubrzo su se pojavili kriptoanalitičari koji su uspjeli pronaći način za razbijanje ove šifre. To su bili Friedrich Kasiski koji je uveo *Kasiskijev test* za određivanje duljine ključne riječi te William Friedman koji je uveo *Friedmanov test* u kojem se koristi indeks koincidencije za određivanje ključne riječi. Više o tome može se pročitati u [2].

4 Playfairova šifra

Osnovni elementi otvorenog teksta ne moraju biti samo slova, već i blokovi od dva, tri ili više slova. Charles Wheatstone u drugoj je polovici 19. stoljeća realizirao jednu takvu ideju koristeći blokove od dva slova kao elemente otvorenog teksta. Ime šifre potječe od njegovog prijatelja baruna Playfaira od St. Andrewsa koji ju je popularizirao. *Playfairova šifra* zapravo je *bigramska šifra*. To znači da se šifriraju parovi slova te u konačnici rezultat ovisi o oba. Za šifriranje se koristi matrica 5×5 koju konstruiramo koristeći se ključnom riječi. Primjerice, neka je ključna riječ EUFEMIZAM. Matrica će tada izgledati ovako:

$$\begin{array}{ccccc} E & U & F & M & IJ \\ Z & A & B & C & D \\ G & H & K & L & N \\ O & P & Q & R & S \\ T & V & W & X & Y \end{array}$$

U matrici se nalazi 25 slova. Zbog toga ćemo poistovjećivati slova I i J, a ukoliko je otvoreni tekst na hrvatskom jeziku, poistovjetit ćemo slova W i V. Postupak šifriranja je sljedeći. Otvoreni tekst, odnosno poruku, podijelimo u blokove od po dva slova. Ono što je bitno je da ne postoji blok koji se sastoji od dva jednaka slova te da je broj slova od kojih je tekst sastavljen paran. Ukoliko jedan uvjet nije zadovoljen, dogovorno se umetne slovo X gdje je potrebno kako bi uvjeti bili zadovoljeni. Pri šifriranju mogu se dogoditi sljedeće tri situacije:

- Slova se nalaze u istom retku. Tada svako slovo zamijenimo sa slovom koje se nalazi za jedno mjesto udesno. Ukoliko je jedno od slova zadnje u retku, tada se ciklički vraćamo na početak retka. Primjerice, BC $\mapsto$ CD, RS $\mapsto$ SO.

- Slova se nalaze u istom stupcu. Tada, slično kao u prethodnom slučaju, zamijenimo svako od slova sa slovom koje se nalazi za jedno mjesto ispod. Ukoliko je jedno od slova zadnje u stupcu, vraćamo se ciklički na početak stupca. Primjerice, FB $\mapsto$ BK, RX $\mapsto$ XM.

- Zadnji, ali najopćenitiji slučaj je kada se slova nalaze nasumično u matrici. Tada pogledamo pravokutnik koji određuju ta dva slova te ih zamijenimo s druga dva vrha tako da u šifriranom bloku najprije dolazi ono slovo koje se nalazi u istom retku kao prvo slovo u bloku koji šifriramo. Primjerice, AR $\mapsto$ CP, YH $\mapsto$ VN.

Pokažimo na primjeru kako funkcionira šifriranje.

Primjer 5. *Šifrirajmo otvoreni tekst AVE IMPERATOR MORITURI TE SALUTANT pomoću Playfairove šifre koristeći ključ EUFEMIZAM.*

Rješenje:
Koristeći se matricom

$$\begin{array}{ccccc} E & U & F & M & IJ \\ Z & A & B & C & D \\ G & H & K & L & N \\ O & P & Q & R & S \\ T & V & W & X & Y \end{array}$$

dobivamo sljedeće:
AV EI MP ER AT OR MO RI TU RI TE SA LU TA NT $\mapsto$ HU UE UR MO ZV PS ER SM VE SM EZ PD HM VZ GY.

U sljedećem primjeru bit će ilustrirana dekripcija šifrata.

Primjer 6. *Neka nam je dan šifrat*

$$\begin{array}{cccccc} AJ & SB & QJ & IL & DU & PS \\ PS & DH & QJ & SF & PO & MZ \\ TA & XV & VM & BA & DC & TU \\ DI & SP & DI & ZL & BS & TP \\ BT & QJ & PT & FG & XM & VY \\ GF & AK & GF & SC & AK & GF \end{array}$$

dobiven Playfairovom šifrom. Dešifrirajmo ga imajući na umu da je otvoreni tekst na hrvatskom jeziku.

Rješenje:
Kako bismo dešifrirali ovaj šifrat, ne možemo koristiti samo analizu frekvencije bigrama budući da je šifrat prekratak. Metodu koju ćemo koristiti za dešifriranje zove se metoda vjerojatne riječi. Ona se koristi tako da napravimo listu mogućih fraza ili riječi koje se potencijalno nalaze u otvorenom tekstu te provjerimo postoji li u šifratu struktura koja se podudara s pretpostavljenom riječi ili frazom. Pretpostavit ćemo da otvoreni tekst sadrži riječ MAMA te frazu KOLIKO TOLIKO. Ukoliko pogledamo strukturu riječi MAMA, vidimo da se dva puta pojavljuje bigram MA zaredom. Ukoliko pogledamo šifrat, vidimo da se na kraju prvog i početku drugog retka pojavljuje upravo ta struktura, pa pretpostavimo da je PS šifrat od MA. Sada promatramo strukturu fraze KOLIKO TOLIKO. Bigram KO pojavljuje se tri puta i to na početku, na kraju i u sredini. Promotrimo li šifrat, vidimo da se takva struktura pojavljuje u zadnjem retku. GF se pojavljuje tri puta u šifratu što je u skladu s time da je jedan od najfrekventnijih bigrama u hrvatskom jeziku upravo KO. Dakle, imamo sljedeće: PS $\mapsto$ MA, GF $\mapsto$ KO, AK $\mapsto$ LI, SC $\mapsto$ TO. Pokušajmo sada popuniti kvadrat za šifriranje. Pretpostavimo da se slova bigrama ne nalaze u istom stupcu ili retku, pa dobivamo:

$$\begin{array}{ccccc} & & T & A & L \\ O & & & & \\ & & & I & K \\ M & & & & \end{array}$$

Sada možemo promatrati bigrame koji se pojavljuju više puta u šifratu te isprobavati kojem bi najfrekventnijem bigramu u hrvatskom jeziku pripadali, sukladno sa šifratom. Primjetimo da se pojavljuju bigrami TP i PT. Budući da su AN i NA najfrekventniji recipročni bigrami u hrvatskom jeziku, pretpostavimo sljedeće: PT $\mapsto$ NA, te TP $\mapsto$ AN. Također, ukoliko promotrimo kvadrat, jedina moguća opcija za slovo između I i K je J. Dopunimo kvadrat informacijama koje sada znamo:

$$\begin{array}{ccccc} & T & A & & L \\ O & & & & \\ & & I & J & K \\ M & N & P & & \end{array}$$

Budući da se bigram QJ pojavljuje tri puta u šifratu, pretpostavimo da on odgovara najfrekventnijem bigramu JE, dakle, QJ $\mapsto$ JE. Imamo:

$$\begin{array}{ccccc} & T & A & & L \\ O & & & E & \\ & & I & J & K \\ M & N & P & Q & \end{array}$$

Bigram DI pojavljuje se dva puta u šifratu. U kvadratu za šifriranje već imamo slovo I te, ukoliko promotrimo položaj slova, jedina smislena pozicija za slovo D bila bi između A i I, odnosno:

$$\begin{array}{ccccc} & T & A & & L \\ O & & D & E & \\ & & I & J & K \\ M & N & P & Q & \end{array}$$

Kvadrat za šifriranje sada je dovoljno popunjen da možemo pretpostaviti pozicije određenih slova, pa slijedi:

$$\begin{array}{ccccc} & T & A & & L \\ O & C & D & E & F \\ G & H & I & J & K \\ M & N & P & Q & \end{array}$$

Sada je već vidljvo da je ključna riječ STABLO, pa popunimo i preostala prazna mjesta čime dobivamo kvadrat za šifriranje:

$$\begin{array}{ccccc} S & T & A & B & L \\ O & C & D & E & F \\ G & H & I & J & K \\ M & N & P & Q & R \\ U & V & X & Y & Z \end{array}$$

Dešifriranjem dobivamo:

BI	LA	JE	KA	OX	MA
MA	CI	JE	LO	MD	RU
ST	VU	UN	AT	OC	SV
AD	AM	AD	RZ	AL	AN
AS	JE	NA	OK	UP	UX
KO	LI	KO	TO	LI	KO

Kada maknemo dodana slova X, dobivamo otvoreni tekst:
Bila je kao mama cijelom društvu-unatoč svađama držala nas je na okupu koliko toliko.

Budući da je Playfairova šifra bigramska, puno je teže iskoristiti analizu frekvencije slova budući da se u šifratu gube jednoslovne riječi. Također, broj bigrama puno je veći od broja individualnih slova (26 slova što čini 676 bigrama). Također, frekvencije bigrama puno su ujednačenije od frekvencije slova. Zbog toga se ova šifra koristila tijekom 1. i 2. svjetskog rata. No ipak, kod dugih tekstova postaje nesigurna jer postoji mogućnost analize frekvencije bigrama, ali i samih slova. Time se čak može i odrediti o kojoj vrsti šifre se radi.

5 Hillova šifra

Poligramska šifra koju je izumio Lester Hill početkom 20. stoljeća definirana je na sljedeći način:

Definicija 6. *Pretpostavimo da je m fiksan prirodan broj te neka vrijedi da je $\mathcal{P} = \mathcal{C} = \mathbb{Z}_{26}^m$, i neka je*

$$\mathcal{K} = \{m \times m \text{ invertibilne matrice nad } \mathbb{Z}_{26}\}.$$

Za $K \in \mathcal{K}$ definiramo

$$e_K(x) = xK,\ d_K(y) = yK^{-1},$$

gdje su sve operacije u prstenu $\mathbb{Z}_{26}$.

Kod ove šifre blok od m slova otvorenog teksta zamjenjuje se s blokom m slova u šifratu. U situacijama kada broj slova otvorenog teksta nije djeljiv s m, poruku ćemo dopuniti tako da ju možemo podijeliti u blokove od po m slova. Preporuka je da se koriste involutorne matrice, odnosno one kod kojih je $K^{-1} = K$. Iako to smanjuje broj mogućih ključeva, olakšava postupak šifriranja i dešifriranja.

Primjer 7. *Neka je ključ*

$$K = \begin{bmatrix} 2 & 7 & 16 \\ 24 & 1 & 19 \\ 11 & 21 & 4 \end{bmatrix}$$

te neka nam je dan otvoreni tekst OLOVKA čiji je numerički ekvivalent (14,11,14,21,10,0). Šifrirajmo ga koristeći Hillovu šifru.

Rješenje:
Računamo:

$$\begin{bmatrix} 14 & 11 & 14 \end{bmatrix} \begin{bmatrix} 2 & 7 & 16 \\ 24 & 1 & 19 \\ 11 & 21 & 4 \end{bmatrix} = \begin{bmatrix} 446 & 403 & 489 \end{bmatrix} \bmod 26 = \begin{bmatrix} 4 & 13 & 21 \end{bmatrix} = \text{ENV},$$

$$\begin{bmatrix} 21 & 10 & 0 \end{bmatrix} \begin{bmatrix} 2 & 7 & 16 \\ 24 & 1 & 19 \\ 11 & 21 & 4 \end{bmatrix} = \begin{bmatrix} 282 & 157 & 526 \end{bmatrix} \bmod 26 = \begin{bmatrix} 22 & 1 & 6 \end{bmatrix} = \text{WBG}.$$

Dakle, šifrat je ENVWBG.

Dakle, Hillova šifra kod kojih je matrica 3×3 ne daje nikakve informacije o frekvencijama slova i bigrama. Zbog toga za matrice čije su dimenzije 5×5 (ili veće), ova šifra može se smatrati gotovo potpuno sigurnom od napada "samo šifrat". Međutim, šifru je lako razbiti pomoću ostalih vrsta napada pa zbog toga nije bila toliko u uporabi. Sljedećim primjerom ilustrirano je kako razbiti Hillovu šifru.

Primjer 8. *Koristeći se Hillovom šifrom u kojoj je $m = 2$ iz otvorenog teksta INDEKS dobiven je šifrat LBURIU. Kako izgleda ključ K?*

Rješenje:
Dakle, imamo:

$$e_K(8,13) = (11,1),$$
$$e_K(3,4) = (20,17),$$
$$e_K(10,18) = (8,20).$$

Koristeći prve dvije jednakosti dobivamo:

$$\begin{bmatrix} 8 & 13 \\ 3 & 4 \end{bmatrix} K = \begin{bmatrix} 11 & 1 \\ 20 & 17 \end{bmatrix}.$$

Neka je

$$X = \begin{bmatrix} 8 & 13 \\ 3 & 4 \end{bmatrix}.$$

Ovdje je det X mod 26 = -7 mod 26 = 19, (19,26)=1, pa vrijedi da je $(\det X)^{-1} = 11$. Slijedi:

$$X^{-1} = 11 \begin{bmatrix} 4 & -13 \\ -3 & 8 \end{bmatrix} = \begin{bmatrix} 44 & -143 \\ -33 & 88 \end{bmatrix} =_{26} \begin{bmatrix} 18 & 13 \\ 19 & 10 \end{bmatrix}$$

pa je

$$\text{K}= \begin{bmatrix} 18 & 13 \\ 19 & 10 \end{bmatrix} \begin{bmatrix} 11 & 1 \\ 20 & 17 \end{bmatrix} = \begin{bmatrix} 458 & 239 \\ 409 & 189 \end{bmatrix} =_{26} \begin{bmatrix} 16 & 5 \\ 19 & 7 \end{bmatrix}.$$

Provjerimo ključ na trećem paru:

$$\begin{bmatrix} 10 & 18 \end{bmatrix} \begin{bmatrix} 16 & 5 \\ 19 & 7 \end{bmatrix} = \begin{bmatrix} 502 & 176 \end{bmatrix} \text{ mod } 26 = \begin{bmatrix} 8 & 20 \end{bmatrix}.$$

Dakle, ključ je

$$\text{K}= \begin{bmatrix} 16 & 5 \\ 19 & 7 \end{bmatrix}.$$

Ukoliko ne znamo m, tada trebamo isprobati $m = 2, 3, 4, ...$, dok ne pronađemo odgovarajući ključ.

6 Jednokratna bilježnica

Budući da su kriptoanalitičari uspješno razbijali svaku novu šifru, zanima nas postoji li šifra, odnosno kriptosustav, koji je *savršeno siguran*, i kako bi se to uopće postiglo. Taj pojam uveo je Claude Shannon sredinom 20. stoljeća. Savršeno siguran kriptosustav bio bi onaj u kojem nam šifrat ne bi davao nikakve informacije o otvorenom tekstu. To bi značilo da je vjerojatnost pojavljivanja otvorenog teksta x jednaka uvjetnoj vjerojatnosti da je x pripadni otvoreni tekst ukoliko je poznato da je y šifrat. U graničnom slučaju kada je $|\mathcal{K}| = |\mathcal{C}| = |\mathcal{P}|$, kriptosustav je savršeno siguran ako je svaki ključ korišten s istom vjerojatnošću i da za svaki $x \in \mathcal{P}$, $y \in \mathcal{C}$ postoji jedinstven ključ $K \in \mathcal{K}$ takav da je $e_K(x) = y$.

Jednokratna bilježnica primjer je realizacije ideje savršene sigurnosti koji su uveli Gilbert Vernam i Joseph Mauborgne početkom 20. stoljeća. Definicija jednokratne bilježnice je:

Definicija 7. *Pretpostavimo da je n prirodan broj, $\mathcal{P} = \mathcal{C} = \mathcal{K} = \mathbb{Z}_2^n$. Za $K = (k_1, k_2, ..., k_n)$ $\in \mathcal{K}$ definiramo*

$$e_K(x_1, x_2, ..., x_n) = (x_1 +_2 k_1, x_2 +_2 k_2, ..., x_n +_2 k_n),$$
$$d_K(y_1, y_2, ..., y_n) = (y_1 +_2 k_1, y_2 +_2 k_2, ..., y_n +_2 k_n).$$

Jednokratna bilježnica ne radi sa slovima, nego s binarnim podatcima, dakle jedinicama i nulama. To znači da su ključ, otvoreni tekst i šifrat nizovi nula i jedinica duljine n. Šifrat je rezultat primjene operacije "ekskluzivno ili" (XOR): $y_i = x_i \oplus k_i$ na bitovima otvorenog teksta. Postupak dešifriranja $x_i = y_i \oplus k_i$ identičan je postupku šifriranja jer su u $\mathbb{Z}_2$ operacije zbrajanja i oduzimanja identične.

Budući da se ovakav kriptosustav može s lakoćom razbiti pomoću napada "poznati otvoreni tekst", savršena sigurnost može se postići samo ukoliko svaki ključ koristimo samo jednom. Zbog toga se ovaj kriptosustav zove jednokratna bilježnica. Dakle, svaki list bilježnice koristio bi se kao jednokratni ključ. No, problem je u tome što duljina ključa, koji treba biti sigurno prenesen, treba biti jednaka kao i duljina poruke koju želimo poslati. Također, treba biti slučajno generiran, što se postizalo primjerice bacanjem novčića u zrak. Ovakav kriptosustav ima dvije velike mane: treba uložiti puno vremena i velike novčane resurse. Zbog toga nije bio puno u primjeni. Koristio se u komunikaciji tijekom hladnog rata te tijekom špijunaže. Također, korišten je u 2. svjetskom ratu kada su kriptoanalitičari htjeli obavijestiti ministarstvo o porukama njemačke ENIGME koje su uspjeli dešifrirati, ali tako da oni ne saznaju ništa o tome uspjehu.

U sljedećem primjeru prikazano je šifriranje koristeći se jednokratnom bilježnicom.

Primjer 9. *Koristeći zapis znakova s tipkovnice u binarnom obliku, šifrirajmo riječ PAS koristeći ključ K=(!, (, /) čiji je numerički ekvivalent u binarnom obliku K=(00100001, 00101000, 00101111).*

Rješenje:
Numerički ekvivalent u binarnom obliku riječi PAS je (01010000, 01000001, 01010011). Koristeći se operacijom zbrajanja u $\mathbb{Z}_2$, imamo sljedeće:

	0	1	0	1	0	0	0	0		0	1	0	0	0	0	0	1		0	1	0	1	0	0	1	1
$+_2$	0	0	1	0	0	0	0	1		0	0	1	0	1	0	0	0		0	0	1	0	1	1	1	1
	0	1	1	1	0	0	0	1		0	1	1	0	1	0	0	1		0	1	1	1	1	1	0	0

Dakle, šifrat je (01110001, 01101001, 01111100), odnosno qi|.

7 Transpozicijske šifre

Kod *transpozicijskih šifri* ne mijenjamo elemente otvorenog teksta kao što je to slučaj kod monoalfabetskih i polialfabetskih šifri. Odlika ovakvih šifri zapravo je mijenjanje položaja elemenata otvorenog teksta. Definicija je sljedeća:

Definicija 8. *Pretpostavimo da je m fiksan prirodan broj. Neka je $\mathcal{P} = \mathcal{C} = \mathbb{Z}_{26}^m$, te neka se u $\mathcal{K}$ nalaze sve permutacije skupa $\{1, 2, ..., m\}$. Za $\pi \in \mathcal{K}$ definiramo*

$$e_\pi(x_1, x_2, ..., x_m) = (x_{\pi(1)}, x_{\pi(2)}, ..., x_{\pi(m)}),$$
$$d_\pi(y_1, y_2, ..., y_m) = (y_{\pi^{-1}(1)}, y_{\pi^{-1}(2)}, ..., y_{\pi^{-1}(m)}).$$

U praksi se najviše upotrebljavala *stupčana transpozicija*. Postupak je sljedeći-otvoreni tekst upišemo u pravokutnik po redcima, a onda ga čitamo po stupcima, ali s promijenjenim poretkom. Ključ može biti niz brojeva koje ćemo razmjestiti ili primjerice riječ. Tada svakom slovu dodijelimo broj i promijenimo poredak na željeni način. Ukoliko se posljednji redak ne popuni do kraja, tada ga dopunimo proizvoljnim slovom. Mogu se koristiti i nepotpuni pravokutnici. U sljedećem primjeru ilustrirano je šifriranje stupčanom transpozicijom.

Primjer 10. *Šifrirajmo otvoreni tekst*

SJEDIO JE NA TRIJEMU RAZMIŠLJAJUĆI O SVEMU.

koristeći stupčanu transpoziciju s ključem 6 3 5 2 1 4.

Rješenje:

ključ	6	3	5	2	1	4
otvoreni tekst	S	J	E	D	I	O
	J	E	N	A	T	R
	I	J	E	M	U	R
	A	Z	M	I	S	L
	J	A	J	U	C	I
	O	S	V	E	M	U

Dakle, šifrat je ITUSCMDAMIUEJEJZASORRLIUENEMJVSJIAJO.

Transpozicijsku šifru lako je prepoznati budući da su joj frekvencije slova jednake kao kod otvorenog teksta. U sljedećem primjeru ilustrirano je kako dešifrirati šifrat nastao stupčanom transpozicijom.

Primjer 11. *Dešifrirajmo šifrat*

OEBGSGLAALDALNOANSBJORAEZTP

dobiven stupčanom transpozicijom.

Rješenje:
Budući da je u šifratu 27 slova, postoje dvije moguće dimenzije: 3×9 i 9×3. Ukoliko upišemo šifrat u pravokutnike, dobivamo:

O	L	B	1 : 2
E	D	J	1 : 2
B	A	O	2 : 1
G	L	R	0 : 3
S	N	A	1 : 2
G	O	E	2 : 1
L	A	Z	1 : 2
A	N	T	1 : 2
A	S	P	1 : 2

O	G	L	L	L	A	B	R	Z	2 : 7
E	S	A	D	N	N	J	A	T	3 : 6
B	G	A	A	O	S	O	E	P	5 : 4

Sada provjeravamo odnos samoglasnika i suglasnika u oba pravokutnika. On bi trebao biti sličan njihovom odnosu u jeziku kojim je otvoren tekst pisan. Za hrvatski jezik to je omjer 43% : 57%. Vidimo da je prva mogućnost realističnija obzirom na odnos samoglasnika i suglasnika. Budući da je broj stupaca malen, lako je premetanjem doći do smislene poruke. Ukoliko nije takav slučaj, tada se koristi analiza frekvencije bigrama čime se dolazi do ključa koji je korišten. Dakle, isprobavanjem kombinacija stupaca, dobije se ključ 3 1 2, te poruka glasi: BOLJE DOBAR GLAS NEGO ZLATAN PAS.

Transpozicijska šifra može se realizirati i na drugi način, uz pomoć rešetki. Ukoliko se otvori na rešetkama odaberu na prikladan način, rešetka se može popuniti slovima otvorenog teksta u izmiješanom redoslijedu. Primjer je *Cardanova rotirajuća rešetka*. Dakle, odaberemo kvadrat čija je duljina stranice paran broj te ga podijelimo na četiri manja kvadrata. Neka to bude kvadrat dimenzija 6×6. U svaki od četiri kvadrata upišemo brojeve od 1 do 9 tako da nakon što upišemo brojeve u prvi od njih, zakrenemo kvadrat za 90° u smjeru kazaljke na satu te nastavimo s upisivanjem dok ne popunimo svaki od njih na isti način. Zatim u velikom kvadratu odaberemo svaki od brojeva točno po jednom. Sada otvoreni tekst podijelimo u blokove od 36 slova. Svaki blok šifriramo tako da upisujemo po devet slova u otvore u rešetkama, zatim okrećemo za 90° u smjeru kazaljke na satu i popunjavamo na isti način sve dok ne popunimo kvadrat. U sljedećem primjeru ilustriran je proces šifriranja Cardanovom rotirajućom rešetkom.

Primjer 12. *Šifrirati otvoreni tekst*

HEBERNOV ELEKTRIČNI STROJ ZA KODIRANJE

pomoću sljedeće Cardanove rotirajuće rešetke:

1	2	**3**	7	4	1
4	5	6	8	**5**	**2**
7	**8**	9	9	6	3
3	**6**	**9**	9	8	**7**
2	5	8	6	5	4
1	**4**	7	3	2	**1**

gdje naglašeni brojevi predstavljaju otvore u rešetki.

Rješenje:
Koraci šifriranja prikazani su u sljedećim tablicama:

			H		**E**
	B				
		E			**R**
	N			**O**	
V					**E**

			H		E
L	B			**E**	
	K	E	**T**		R
	N			O	**R**
V		**I**			E
	C		**N**		**I**

	S		H		E
L	B	**T**		E	**R**
	K	E	T	**O**	R
J	N		**Z**	O	R
V		I		**A**	E
K	C	**O**	N		I

D	S	**I**	H	**R**	E
L	B	T	**A**	E	R
N	K	E	T	O	R
J	N	**J**	Z	O	R
V	**E**	I	**X**	A	E
K	C	O	N	**X**	I

Budući da se poruka sastojala od 34 slova, na poruku se nadodaju dva slova X kako bi ju dopunili do 36 slova.

Literatura

[1] A. Beutelspacher, *Cryptology*, The Mathematical Association of America, Washington, 1994.

[2] A. Dujella, M. Maretić, *Kriptografija*, Element, Zagreb, 2007.

[3] J. S. Kraft, L. C. Washington, *An Introduction to Number Theory with Cryptography*, CRC Press, Suite, 2018.

[4] S. Singh, *Šifre: kratka povijest kriptografije*, Mozaik knjiga, Zagreb, 2003.

[5] W. Trappe, L. C. Washington, *Introduction to Cryptography with Coding Theory*, Pearson Education International, New York, 2006.