Osnove kriptografije

Zrno, Mia

Sveučilište J. J. Strossmayera u Osijeku
Odjel za matematiku
Preddiplomski studij matematike

Mia Zrno

Osnove kriptografije

Završni rad

Osijek, 2020.

Sveučilište J. J. Strossmayera u Osijeku
Odjel za matematiku
Preddiplomski studij matematike

Mia Zrno

Osnove kriptografije

Završni rad

Mentor: izv. prof. dr. sc. Ivan Matić

Osijek, 2020.

Sadržaj

1 Uvod i osnovni pojmovi

Kriptografija je znanstvena disciplina koja se bavi proučavanjem metoda za slanje poruka na način da se poruka pretvori u takav format da ta poruka ima smisla samo primatelju, a ne i nekome tko bi ju mogao presresti na putu do primatelja. Sama riječ dolazi od grčkog pridjeva *kriptos* ($\kappa\rho\upsilon\pi\tau o\zeta$) - "skriven" i glagola *grafo* ($\gamma\rho\alpha\phi\omega$) - "pisati".

Osnovni pojmovi u kriptografiji su: osnovni algoritam, šifriranje (kodiranje), dešifriranje (dekodiranje) te ključ.

Kriptografija je bila prisutna već u vrijeme starih Grka. Spartanci su u 5. stoljeću prije Krista koristili jednostavnu napravu za šifriranje - skital. To je bio drveni štap oko kojega se namatala vrpca od kože ili pergamenta. Pošiljatelj bi na namotanoj vrpci napisao poruku, a kad bi se ta vrpca odmotala, na njoj se nalazio samo niz naizgled besmislenih slova. Kada bi glasnik odnio odmotanu vrpcu primatelju, on bi pročitao tekst poruke tako što bi tu vrpcu omotao oko skitala jednakog promjera kao što je promjer skitala pošiljatelja. Dakle, ključ je bio skital određenog promjera.

To i jest osnovni zadatak kriptografije - omogućiti dvjema osobama (Alice i Bob) komuniciranje preko nekog nesigurnog kanala (u današnje vrijeme telefon, internet i sl.) na način da treća osoba, koja može nadzirati taj kanal, ne može razumjeti poruke.

Poruku koju pošiljatelj želi poslati primatelju nazivamo "otvoreni tekst". Taj tekst mogu biti nekakvi numerički podatci, tekst i sl. Njega pošiljatelj transformira pomoću unaprijed dogovorenog ključa. Taj postupak zovemo šifriranje, a rezultat nazivamo šifrat ili kriptogram. Dakle, ako protivnik nadzire komunikacijski kanal, on može saznati šifrat, ali ne i otvoreni tekst. Primatelj može pomoću ključa taj šifrat transformirati natrag u otvoreni tekst.

Kriptografski algoritam ili *šifra* je matematička funkcija koja se koristi za šifriranje i dešifriranje. Radi se o dvije funkcije: jednoj za šifriranje, a drugoj za dešifriranje. Te funkcije preslikavaju osnovne elemente otvorenog teksta u osnovne elemente šifrata, i obratno. Funkcije se biraju iz određene familije funkcija u ovisnosti o ključu. Skup svih mogućih vrijednosti ključeva nazivamo *prostor ključeva*. *Kriptosustav* se sastoji od kriptografskog algoritma te svih mogućih otvorenih tekstova, šifrata i ključeva.

Definicija 1.1. Kriptosustav je uređena petorka $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ za koju vrijedi:

1) $\mathcal{P}$ je konačan skup svih mogućih osnovnih elemenata otvorenog teksta,

2) $\mathcal{C}$ je konačan skup svih mogućih osnovnih elemenata šifrata,

3) $\mathcal{K}$ je konačan skup svih mogućih ključeva,

4) $\mathcal{E}$ je skup svih funkcija šifriranja,

5) $\mathcal{D}$ je skup svih funkcija dešifriranja,

6) za svaki $K \in \mathcal{K}$ postoji funkcija šifriranja $e_K \in \mathcal{E}$ i odgovarajuća funkcija dešifriranja $d_K \in \mathcal{D}$. Pritom su $e_K : \mathcal{P} \to \mathcal{C}$ i $d_K : \mathcal{C} \to \mathcal{P}$ funkcije sa svojstvom da je $d_K(e_K(x)) = x$, za svaki otvoreni tekst $x \in \mathcal{P}$.

Iz $d_K(e_K(x)) = x$ slijedi fa funkcije e_K moraju biti injekcije. Ako bi vrijedilo

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

za dva različita otvorena teksta x_1 i x_2, onda primalac ne bi mogao odrediti treba li y dešifrirati u x_1 ili x_2, tj. $d_K(y)$ ne bi bilo definirano. U skladu s tim vrijedi da ako je $\mathcal{P} = \mathcal{C}$, onda su funkcije e_K permutacije.

Kriptosustave dijelimo po tri kriterija:

1) Tip operacije koje se koriste pri šifriranju

   Ovdje razlikujemo supstitucijske šifre (svaki element otvorenog teksta zamjenjujemo nekim drugim elementom) i transpozicijske šifre (permutiramo elemente).

2) Način na koji se obrađuje otvoreni tekst

   Ovdje razlikujemo blokovne šifre (koristimo isti ključ) i protočne šifre (koristimo niz ključeva).

3) Tajnost i javnost ključeva

   Ovdje je osnovna podjela na simetrične kriptosustave (najčešće ključ za dešifriranje isti kao ključ za šifriranje, tajan) i kriptosustave s javnim ključem (ključ za dešifriranje se ne može izračunati iz ključa za šifriranje, bilo tko može šifrirati poruku pomoću njega, ali samo osoba koja ima odgovarajući ključ za dešifriranje (privatni ili tajni ključ) može dešifrirati tu poruku).

2 Cezarova šifra

Cezarova šifra jedan je od najjednostavnijih i najrasprostranjenijih načina šifriranja. To je tip šifre zamjene (supstitucije), u kome se svako slovo otvorenog teksta zamjenjuje odgovarajućim slovom abecede, pomaknutim za određeni broj mjesta. Na primjer, s pomakom 4, A se zamjenjuje slovom E, B slovom F itd. Ova je metoda dobila ime po Juliju Cezaru, koji ju je koristio za razmjenu poruka sa svojim generalima.

Primjer 1. *Otvoreni tekst VENI VIDI VICI s pomakom 5 glasio bi DJTN DNIN DNHN.*

Cezar je koristio pomak od 3 mjesta pa je abeceda (otvoreni tekst)

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

nakon šifriranja izgledala ovako:

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.

Cezarovu šifru formalno možemo definirati na sljedeći način:

Definicija 2.1. Neka je $\mathcal{P} = \mathcal{C} = \mathcal{K} = \mathbb{Z}_{26}$, gdje je $\mathbb{Z}_{26} = \{0, 1, \ldots, 25\}$. Za $0 \leq K \leq 25$ definiramo

$$e_K(x) = x + K \pmod{26}, \; d_K(y) = y - K \pmod{26}.$$

Primjer 2. *Dekriptirajmo šifrat ITOAITOEGT dobiven Cezarovom šifrom. Budući da je prostor ključeva mali (26 elemenata), možemo "ručno" dešifrirati, odnosno isprobavati ključeve. Brzo dolazimo do zaključka da je ključ $K = 4$ te da je otvoreni tekst MATEMATIKA.*

3 Afina šifra

Iz posljednjeg primjera prethodnog poglavlja možemo uočiti nedostatak Cezarove šifre, a to je da se primjenom "grube sile" lako može dešifrirati. Da bismo dobili malo sigurniju šifru, funkcija za šifriranje mogla bi uključivati više od jednog parametra. Najjednostavnija takva je afina funkcija $e(x) = ax+b$. Problem takvih funkcija je što na skupu $\mathbb{Z}_{26}$ ne mora imati inverz jer ne mora biti injekcija. Stoga parametar a ne može biti proizvoljan, već mora biti relativno prost s modulom 26. Afinu šifru definiramo formalno na sljedeći način:

Definicija 3.1. Neka je $\mathcal{P} = \mathcal{C} = \mathbb{Z}_{26}$ te neka je $\mathcal{K} = \{(a, b) \in \mathbb{Z}_{26} \times \mathbb{Z}_{26} : (a, 26) = 1\}$. Za $K = (a, b) \in \mathcal{K}$ definiramo

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

Provjerit ćemo je li uvjet $d_K(e_K(x)) = x$ zadovoljen:

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

Uočimo da ovdje a^{-1} označava multiplikativni inverz broja a u $\mathbb{Z}_{26}$. Budući da broj 26 nije prost, multiplikativni inverz imaju samo oni brojevi koji su relativno prosti s 26.

Primjer 3. *Neka je $K = (5, 2)$. Šifrirajmo otvoreni tekst FIZIKA.*

Slova otvorenog teksta poistovjećujemo s njihovim numeričkim ekvivalentima u $\mathbb{Z}_{26}$.

$$\begin{aligned} e_K(F) &= (5 \cdot 7 + 2) \bmod 26 = 11 \\ e_K(I) &= (8 \cdot 7 + 2) \bmod 26 = 6 \\ e_K(Z) &= (25 \cdot 7 + 2) \bmod 26 = 21 \\ e_K(K) &= (10 \cdot 7 + 2) \bmod 26 = 20 \\ e_K(A) &= (0 \cdot 7 + 2) \bmod 26 = 2. \end{aligned}$$

Dakle, šifrat je LGVGUB.

Promotrimo sada primjer kako dešifrirati poruku kriptiranu Afinom šifrom.

Primjer 4. *Dekriptirati šifrat MEVYMEVSCESSRDWLMEVSCE.*

Broj mogućih ključeva je $\varphi(26) = 12 \cdot 26 = 312$. Tehnički je moguće provesti "grubu silu", no postoji elegantniji način. Pretpostavit ćemo da je otvoreni tekst pisan hrvatskim jezikom. Sada se možemo poslužiti frekvencijom slova u hrvatskom jeziku. Najfrekventnija slova su A, I, O, E i N, točno u tom redoslijedu. Stoga možemo promatrati najfrekventnija slova u šifratu, tj. E i S. Slovo E pojavljuje se 5 puta, dok se slovo S pojavljuje 4 puta. Sada možemo pretpostaviti da je $e_K(A) = E$ i $e_K(I) = S$. Važno je napomenuti kako ova metoda nije u potpunosti pouzdana te

da je moguće da prvi pokušaj neće biti uspješan.

Imamo $e_K(A) = a \cdot 0 + b = 4 (mod\ 26)$ *te* $e_K(I) = a \cdot 8 + b = 8a + b = 18 (mod\ 26)$. *Očito je* $b = 4$, *a rješavanjem linearne kongruencije* $8a \equiv 14 (mod\ 26)$ *dobivamo* $a = 5$. *Kako je multiplikativni inverz od* 5 *u* $\mathbb{Z}_{26}$ *jednak* 21, *dobivamo da je* $d_K(y) = 21(y - 4)\ mod\ 26$. *Primjenom funkcije* d_K *na šifrat, dobivamo otvoreni tekst*

MATEMATIKA I INFORMATIKA.

Cezarova i Afina šifra specijalni su slučajevi supstitucijske šifre koju možemo definirati na sljedeći način:

Definicija 3.2. Neka je $\mathcal{P} = \mathcal{C} = \mathbb{Z}_{26}$. Prostor ključeva $\mathcal{K}$ sastoji se od svih permutacija skupa $\{0, 1, \ldots, 25\}$. 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.

Broj mogućih ključeva je 26!, što je približno $4 \cdot 10^{26}$ pa bi ispitivanje svih mogućih ključeva bilo nemoguće. Upravo iz tog razloga važno je koristiti analizu frekvencija slova. Svakom slovu šifrata brojimo frekvenciju te uspoređujemo dobivene frekvencije s poznatim najčešćim frekvencijama unutar jezika kojim je pisan otvoreni tekst. Što je dulji tekst, to je veća vjerojatnost da se najčešća slova u šifratu podudaraju s najčešćim slovima u jeziku. Dodatno, često se koriste informacije o bigramima i trigramima, tj. nizovima od dva ili tri slova.

4 Vigenereova šifra

Prethodno obrađene šifre - Cezarova i Afina - nazivaju se monoalfabetske. To je zato što kod njih svakom slovu otvorenog teksta odgovara jedinstveno slovo šifrata. Odmah je jasno da je takve šifre lakše dešifrirati nego onih koje bi jednom slovu otvorenog teksta mogle pridružiti različita slova šifrata. Takve šifre nazivaju se polialfabetske, a primjer je Vigenereova šifra. Dobila je ime po francuskom diplomatu Blaise de Viegenereu. Jedna je od najpopularnijih kriptosustava u povijesti - bila je u uporabi u vrijeme Američke revolucije te u Američkom građanskom ratu. Definira se na sljedeći način:

Definicija 4.1. Neka je m fiksan prirodan broj te $\mathcal{P} = \mathcal{C} = \mathcal{K} = \mathbb{Z}_{26}^m$. Za ključ $K = (k_1, k_2, \ldots, k_m)$ definiramo

$$e_K(x_1, x_2, \ldots, x_m) = (x_1 + k_1, x_2 + k_2, \ldots, x_m + k_m)$$
$$d_K(y_1, y_2, \ldots, y_m) = (y_1 - k_1, y_2 - k_2, \ldots, y_m - k_m).$$

U prethodnoj definiciji treba pripaziti na činjenicu da zbrajanje i oduzimanje radimo modulo 26.

Dakle, kod Vigenereove šifre slova otvorenog teksta pomičemo za k_1, $k_2, \ldots$ ili k_m mjesta ovisno o tome na kojem mjestu se u otvorenom tekstu nalaze. Osnovni elementi otvorenog teksta i šifrata su ovdje "blokovi" od po m slova, a šifriranje se provodi "slovo po slovo" pa ne moramo dopuniti zadnji blok ako broj slova u otvorenom tekstu nije djeljiv s m.

Primjer 5. *Neka je $m = 4$, ključna riječ KIST, a otvoreni tekst KRIPTOANALIZA.*

Numerički ekvivalent ključa je $K = (10, 8, 18, 19)$, a otvorenog teksta $(10, 17, 8, 15, 19, 14, 0, 13, 0, 11, 8, 25, 0)$. *Šifriranje provodimo na sljedeći način*

	10	17	8	15	19	14	0	13	0	11	8	25	0
+	10	8	18	19	10	8	18	19	10	8	18	19	10
	20	25	0	8	3	22	18	6	10	19	0	18	10

Svakom broju sada pridružujemo odgovarajuće slovo. Dobivamo šifrat

UZAIDWSGKTASK.

Ključ ponavljamo unedogled te stoga ovu šifru možemo shvatiti kao primjer blokovne šifre. No, postoji i druga varijanta Vigenereove šifre koja je sigurnija od originalne. Radi se o šifri kod koje se originalni ključ koristi samo za šifriranje prvog bloka otvorenog teksta od m slova, a za šifriranje daljnjih blokova korist se prethodni blok otvorenog teksta. Dakle, elementi otvorenog teksta šifriraju se jedan po jedan korištenjem niza ključeva koji se paralelno generira pa ova šifra spada u tzv. protočne šifre.

Za šifriranje se može koristiti tzv. Vigenereov kvadrat, tj. tablica alfabeta koja se sastoji od alfabeta napisanog 26 puta u novom redu, pri čemu je svaki red rotiran ulijevo u odnosu na prethodni. Tako dobivena tablica odgovara svim mogućim kombinacijama Cezarove šifre. Ovakav tip Vigenereove šifre promotrit ćemo u sljedećem primjeru.

Primjer 6. *Neka je ključna riječ KIST, a otvoreni tekst KRIPTOANALIZA. Za razliku od Primjera 5., ovdje ćemo radi preglednosti šifriranje provoditi baš na slovima otvorenog teksta, a ne njihovim numeričkim ekvivalentima.*

otvoreni tekst	*K*	*R*	*I*	*P*	*T*	*O*	*A*	*N*	*A*	*L*	*I*	*Z*	*A*
ključ	*S*	*T*	*O*	*L*	*K*	*R*	*I*	*P*	*T*	*O*	*A*	*N*	*A*
šifrat	*U*	*Z*	*A*	*I*	*D*	*F*	*I*	*C*	*T*	*Z*	*I*	*M*	*A*

Možemo primijetiti da je početak šifrata, točnije prvi blok duljine 4*, isti kao i kod šifrata iz Primjera 5. Također, peto slovo šifrata se podudara u danim primjerima, no to je samo posljedica činjenice da u ovom primjeru ključna riječ i otvoreni tekst počinju istim početnim slovom.*

5 Playfairova šifra

Playfairovu šifru smislio je britanski znanstvenik Charles Wheatstone u 19. stoljeću, no ime je dobila po barunu Playfairu od St. Andrewsa, njegovom prijatelju koji ju je popularizirao. Ona predstavlja poboljšanje u odnosu na polialfabetske šifre jer je u pitanju bigramska šifra, tj. šifriraju se parovi slova tako da rezultat ovisi o oba slova. Algoritam šifriranja baziran je na 5×5 matrici slova. Kako imamo 26 slova, u slučaju da je otvoreni tekst pisan na engleskom, dogovorno se poistovjećuju slova I i J, dok u hrvatskom poistovjećujemo slova V i W. Nadalje, otvoreni tekst dijeli se na blokove od dva slova pa se u slučaju da je duljina teksta neparna umeće slovo X na kraj. Također, blok se ne smije sastojati od dva ista slova te se taj problem isto rješava umetanjem slova X između ponovljenih slova. Playfairova šifra ima dvije varijante - bez upotrebe ključa i s upotrebom. Ako ne koristimo ključ, onda bi matrica slova za hrvatski jezik bila

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

U slučaju da koristimo ključnu riječ, npr. TELEFON, matrica bi se dobila pisanjem ključne riječi te dopunjavanjem preostalim neiskorištenim slovima u abecednom poretku:

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

Kod šifriranja blokova od dva slova razlikujemo tri moguća slučaja, koji ovise o položaju slova u matrici. Primjeri koji su navedeni odnose se na matricu za ključnu riječ TELEFON.

1) Slova se nalaze u istom retku. Slova tada mijenjamo sa slovima koja se nalaze za jedno mjesto udesno, pri čemu krajnje desno slovo mijenjamo s krajnje lijevim slovom u istom retku, tj. pomičemo se ciklički unutar reda. Npr. TF $\leftarrow$ EO, IJ $\leftarrow$ JK, PS $\leftarrow$ QM.

2) Slova se nalaze u istom stupcu. Slova tada mijenjamo sa slovima koja se nalaze za jedno mjesto ispod, pri čemu krajnje donje slovo mijenjamo s krajnje gornjim slovom u istom stupcu, tj. pomičemo se ciklički unutar stupca. Npr. BQ $\leftarrow$ IX, DK $\leftarrow$ KS, GU $\leftarrow$ MT.

3) U suprotnom, promatramo pravokutnik koji je određen tim dvama slovima te ih zamijenimo s preostalim vrhovima tog pravokutnika, pri čemu prvo dolazi ono slovo koje se nalati u istom retku kao prvo slovo polaznog bloka. Npr. TI $\leftarrow$ LG, HO $\leftarrow$ KE, AZ $\leftarrow$ DV.

Primjer 7. *Šifrirajmo otvoreni tekst INFORMATIKA pomoću Playfairove šifre s ključem TELEFON.*

Otvoreni tekst podijelimo na blokove od dva slova: IN FO RM AT IK AX.

Šifrat sada glasi: GB OT SP NE JG BV.

Dešifriranje se vrši na sličan način kao šifriranje.

1) Slova se nalaze u istom retku. Tada ih mijenjamo sa slovima koja se nalaze jedno mjesto ulijevo - ciklički.

2) Slova se nalaze u istom stupcu. Tada ih mijenjamo sa slovima koja se nalaze jedno mjesto prema gore - ciklički.

3) Slova tvore pravokutnik - postupamo kao kod šifriranja.

Primjer 8. *Dešifrirajmo šifrat EZCHE LSZLU FMLAB NOPJL QJPCLG dobiven pomoću Playfairove šifre s ključnom riječi TELEFON ako je poznato da je otvoreni tekst pisan hrvatskim jezikom.*

Šifrat podijelimo na blokove od dva slova:

EZ CH EL SZ LU FM LA BN OP JL QJ PC LG.

Dešifriranjem dobivamo blokove:

OV AJ TE KS TX TR EB AD ES IF RI RA TI.

Budući da se u otvorenom tekstu pojavljuje slovo X, a njega ubacujemo kako bi izbjegli blokove od jednakih slova prilikom šifriranja, njega uklanjamo. Dakle, otvoreni tekst je OVAJ TEKST TREBA DEŠIFRIRATI.

6 Hillova šifra

Hillova šifra dobila je ime po Lesteru Hillu, koji ju je izumio 1929. godine. Kod ove šifre se m uzastopnih slova otvorenog teksta mijenja s m slova u šifratu, tj. radi se o poligramskoj šifri. Ako broj slova u otvorenom tekstu nije djeljiv s m, onda poruku treba nadopuniti kako bi ju mogli podijeliti u blokove od po m slova. Sam kriptosustav definiran je na sljedeći način:

Definicija 6.1. Neka je $m \in \mathbb{N}$ fiksan te $\mathcal{P} = \mathcal{C} = \mathbb{Z}_{26}$ te $\mathcal{K} = GL(m, \mathbb{Z}_{26})$. Za $K \in \mathcal{K}$ definiramo

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

gdje su $x, y \in \mathcal{M}_{1,m}(\mathbb{Z}_{26})$ i sve su operacije u prstenu $\mathbb{Z}_{26}$.

Napomena: $GL(m, \mathbb{Z}_{26})$ je skup invertibilnih kvadratnih matrica reda m nad $\mathbb{Z}_{26}$. Takva matrica A je invertibilna ako je $(\det A, 26) = 1$.
Šifriranje Hillovom šifrom predstavit ćemo u sljedećem primjeru.

Primjer 9. *Neka je $m = 3$ i*

$$K = \begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix}$$

te neka je otvoreni tekst PAPIR. Kako duljina otvorenog teksta nije djeljiva s 3, nadopunimo ga do PAPIRX. Otvorenom tekstu odgovara vektor

$$x = [15\ 0\ 15\ 8\ 17\ 23].$$

Šifriranje obavljamo množenjem:

$$\begin{bmatrix} 15 & 0 & 15 \end{bmatrix} \cdot \begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix} = \begin{bmatrix} 390 & 615 & 240 \end{bmatrix} =_{26} \begin{bmatrix} 0 & 17 & 6 \end{bmatrix},$$

$$\begin{bmatrix} 8 & 17 & 23 \end{bmatrix} \cdot \begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix} = \begin{bmatrix} 729 & 855 & 523 \end{bmatrix} =_{26} \begin{bmatrix} 1 & 23 & 3 \end{bmatrix}.$$

Dobivamo šifrat ARGBXD.

Postupak dešifriranja vrlo je sličan postupku šifriranja, kao što se može vidjeti u sljedećem primjeru.

Primjer 10. *Korištenjem Hillove šifre s ključem*

$$K = \begin{bmatrix} 1 & 2 & 1 \\ 2 & 3 & 0 \\ 0 & 3 & 1 \end{bmatrix}$$

dobiven je šifrat XTSNXGKAINJF. Kako je $detK = 5$ *i* $(5, 26) = 1$, *postoji* K^{-1} *u* $\mathbb{Z}_{26}$ *i ona je*

$$K^{-1} = \begin{bmatrix} 11 & 21 & 15 \\ 10 & 21 & 16 \\ 22 & 15 & 5 \end{bmatrix}.$$

Šifratu pridružujemo njegov numerički ekvivalent te formiramo matricu

$$y = \begin{bmatrix} 23 & 19 & 18 \\ 13 & 23 & 6 \\ 10 & 0 & 8 \\ 13 & 9 & 5 \end{bmatrix}.$$

Otvoreni tekst dobivamo kao

$$x = yK^{-1} = \begin{bmatrix} 839 & 1152 & 739 \\ 505 & 846 & 593 \\ 286 & 330 & 190 \\ 343 & 537 & 364 \end{bmatrix} =_{26} \begin{bmatrix} 7 & 8 & 11 \\ 11 & 14 & 21 \\ 0 & 18 & 8 \\ 5 & 17 & 0 \end{bmatrix}.$$

Dakle, otvoreni tekst je HILLOVA SIFRA.

7 Literatura

[1] M. W. BALDONI, C. CILIBERTO, G. M. PIACENTINI CATTANEO, *Elementary Number Theory, Cryptography and Codes*, Springer, 2009.

[2] T. KOSHY, *Elementary Number Theory with Applications,* Academic Press, 2001.

[3] D. R. STINSON, *Cryptography, theory and practice,* Chapman and Hall, 2005.

[4] J. J. TATTERSALL, *Elementary Number Theory in Nine Chapters,* Cambridge University Press, 2005.

Sažetak

U ovom su radu predstavljene neke osnovne šifre u kriptografiji. U uvodnom dijelu definiran je kriptosustav. Glavni dio rada usmjeren je na definiciju Afine, Cezarove, Vigenereove, Playfairove te Hillove šifre. Uz svaku šifru prikazani su primjeri šifriranja i dešifriranja različitih poruka.

Ključne riječi: kriptografija, kriptosustav, šifra

Abstract

Some basic cryptography ciphers are presented in this paper. In the introductory part, the term cryptosystem is defined. The main part of the paper is focused on the definition of the Affine, Caesar's, Vigenere's, Playfair's and Hill's cipher. Examples of coding and decoding each cipher are also presented.

Keywords: cryptography, cryptosystem, cipher