Supstitucijske šifre

Božić, Maja

Master's thesis / Diplomski rad

2018

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **Josip Juraj Strossmayer University of Osijek, Department of Mathematics / Sveučilište Josipa Jurja Strossmayera u Osijeku, Odjel za matematiku**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:126:182770

Rights / Prava: In copyright / Zaštićeno autorskim pravom.

Download date / Datum preuzimanja: **2024-03-29**



Repository / Repozitorij:

Repository of School of Applied Mathematics and Computer Science







Sveučilište Josipa Jurja Strossmayera u Osijeku
Odjel za matematiku
Nastavnički studij matematike i informatike

Maja Božić

Supstitucijske šifre

Diplomski rad

Osijek, 2018.

Sveučilište Josipa Jurja Strossmayera u Osijeku
Odjel za matematiku
Nastavnički studij matematike i informatike

Maja Božić

Supstitucijske šifre

Diplomski rad

Mentor: izv. prof. dr. sc. Ivan Matić

Osijek, 2018.

Sadržaj

Uvod **i**

1 Osnovni pojmovi **1**

2 Supstitucijske šifre **7**
2.1 Šifriranje i dešifriranje supstitucijskih šifri 8
2.2 Cezarova šifra 14
2.3 Šifra s datumskim pomakom 17
2.4 Šifra s ključnom riječi 19
2.4.1 Cezarova šifra s ključnom riječi 19
2.5 Afina šifra 21

3 Nestandardne supstitucijske šifre **24**
3.1 Pigpen šifra 24
3.2 Polybiusov kvadrat 26
3.3 Nasumične supstitucijske šifre 28
3.4 Shadowljev kod 30

Literatura **32**

Sažetak **33**

Summary **34**

Životopis **35**

Uvod

Cilj je ovog diplomskog rada opisati kriptoanalizu supstitucijskih šifri, prvenstveno monoalfabetske supstitucijske šifre te ćemo navesti neke od nestandardnih supstitucijskih šifri. Na samom početku navest ćemo definicije, teoreme i rezultate koji su potrebni kako bi se uspješnije mogao pratio sadržaj ovog rada. Nakon toga, definirat ćemo supstitucijske šifre, prvenstveno monoalfabetske šifre te ćemo na različitim primjerima pokazati postupke šifriranja i dešifriranja istih. Također, isti ćemo postupak provesti i za nestandardne supstitucijske šifre poput pigpen šifre, Shadowljeva koda i drugih. Karakteristika monoalfabetskih supstitucijskih šifri, kao što su Cezarova i afina šifra, jest te da se slova zamijenjuju slovima. Međutim, u nestandardnim supstitucijskim šiframa, primjerice u pigpen šifri, slova se zamijenjuju simbolima, dok se šifriranje Polybiusovim kvadratom provodi tako da se slovo šifrira s dvama brojevima. Na kraju ćemo objasniti šifre u kojima se slovo zamijenjuje s više različitih znakova poput šifre Shadowljev kod, kojom se koristio serijski ubojica Zodiac u svojim pismima.

Kriptologija je znanost koja se bavi proučavanjem i definiranjem metoda za zaštitu informacija (šifriranjem) i proučavanjem i pronalaženjem metoda za otkrivanje šifriranih poruka (dešifriranje). Kriptologija obuhvaća dvije znanstvene discipline kao što su kriptografija i kriptoanaliza. Rezultate kriptologije prvenstveno koriste oružane snage i diplomatska služba, a razvojem telekomunikacija i mnoge druge službe.

Kriptografija je znanstvena disciplina koja se bavi proučavanjem metoda čiji je osnovni zadatak omogućiti komunikaciju između dviju osoba preko nesigurnog komunikacijskog kanala. Cilj je u komunikacijskom sustavu omogućiti komunikaciju pošiljatelju i primatelju poruke na način da treća osoba koja se zove protivnik ne može pročitati sadržaj poruke. Riječ kriptografija dolazi iz grčkog jezika i znači tajnopis.

Otvoreni tekst je poruka koju pošiljatelj šalje primatelju. Pošiljatelj otvoreni tekst transformira prema već unaprijed dogovorenom ključu ili pravilu. Taj postupak se zove *šifriranje* ili *kriptiranje*. Postupkom šifriranja dobiva se šifrat ili kriptogram. Nakon toga, pošiljatelj šalje poruku preko nesigurnog komunikacijskog kanala. Protivnik može prisluškujući doznati sadržaj šifri, ali ne i otvoreni tekst. Međutim, budući da primatelj zna ključ kojim je poruka šifrirana, lako može otkriti šifrat i otvoreni tekst. Matematička funkcija koja se koristi za šifriranje ili dešifriranje na-

ziva se kriptografski algoritam ili šifra. Ovdje se radi o dvjema funkcijama koje preslikavaju elemente otvorenog teksta u elemente šifrata i obratno. Te se funkcije biraju iz određene familije funkcija, ovisno o ključu. Prostor je ključeva skup svih mogućih vrijednosti ključeva.

Definicija 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 prostor ključeva, tj. 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 svojstva $d_K(e_K(x)) = x$ slijedi kako funkcije šifriranja $e_K(x)$ moraju biti injekcije. U suprotnom bi poruka mogla biti dvosmislena. Ako bi se dva različita slova otvorenog teksta x_1 i x_2 nekom funkcijom šifriranja šifrirala istim slovom y, odnosno

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

primatelj poruke može biti u nedoumici, tj. neće znati treba li y dešifrirati u x_1 ili x_2.

Kriptoanaliza ili dekriptiranje je znanstvena disciplina koja se bavi proučavanjem postupaka za čitanje skrivenih poruka bez poznavanja pravila za šifriranja ili ključa. Kriptoanaliza se može provesti nagađanjem ključa ili korištenjem informacija o sustavu koji se napada. Međutim, nije nužno da je smisao kriptoanalize narušavanje privatnosti. Naprotiv, kriptografija i kriptoanaliza se nadopunjuju jer je, uz prikupljanje informacija, svrha kriptoanalize i pronalaženje grešaka i propusta u kriptografskim algoritmima. Osnovna je točka početka kriptoanalize Kerckhoffov princip - „*Kriptosustav je siguran i u slučaju da kriptoanalitičar zna o kojemu se kriptosustavu radi*". Čak i da kriptoanalitičar ne zna o kojem sustavu se radi, to ne mijenja

bitno težinu dekriptiranja.
Svaka usmjerena radnja kriptoanalitičara naziva se napad. Razlikujemo pet osnovnih napada na kriptosustave:

1. napad poznatim šifratom: Kriptoanalitičar ima mogućnost pristupiti samo šifratu od nekoliko poruka šifriranih istim algoritmom. Njegov je cilj otkriti otvoreni tekst od što više poruka ili pak ključ kojim su šifrirane poruke;

2. napad poznatim otvorenim tekstom: Kriptoanalitičar poznaje šifrat (y), ali i u njemu odgovarajući otvoreni tekst (x). Njegov je cilj otkriti ključ ili algoritam za dešifriranje poruka tim ključem;

3. napad odabranim otvorenim tekstom: Kriptoanalitičar ima mogućnost odabrati otvoreni tekst koji će biti šifriran i može dobiti njegov šifrat;

4. napad odabranim šifratom: Kriptoanalitičar je dobio pristup alatu za dešifriranje pa u ovom slučaju može odabrati šifrat i dobiti odgovarajući otvoreni tekst. Zadatak je kriptoanalitičara otkriti ključ za dešifriranje. Ovaj je napad uobičajen kod kriptosustava s javnim ključem;

5. socijalni napad: Ovaj napad podrazumijeva ucjene, potkupljivanje, krađe i slične metode kako bi se došlo do rezultata.

Kriptosustave po tipu operacija koje se koriste pri šifriranju klasificiramo na transpozicijske šifre, supstitucijske šifre te kriptosustave koji kombiniraju ove dvije metode. Kod transpozicijskih šifri elementi se otvorenog teksta permutiraju (premještaju). Kod supstitucijskih se šifri svaki element otvorenog teksta zamjenjuje nekim drugim elementom. Ova je vrsta šifri specifična po tome jer poredak ostaje isti, ali se za svako slovo koristi drugi simbol. Postoji nekoliko podjela supstitucijskih šifri, a jedna je od njih je podjela na monoalfabetske i polialfabetske šifre.
Kod monoalfabetskih supstitucijskih šifri više slova ne mogu biti zamijenjena istim znakom. Drugim riječima, svako se slovo zamjenjuje točno jednim znakom. Primjerice, ukoliko je šifra za slovo M slovo A, to znači da svaki puta u šifratu kada se pojavi slovo A, ono upravo znači slovo M. Međutim, za razliku od monoalfabetskih, kod polialfabetskih šifri slovo je šifrirano s više slova te više slova može biti šifrirano istim slovom, a to ovisi o poziciji u tekstu.

1 Osnovni pojmovi

U ovom ćemo poglavlju navesti neke osnovne definicije i rezultate iz algebre i teorije brojeva koji su potrebni kako bismo uspješno mogli pratiti sadržaj ovog diplomskog rada - kriptografija i kriptoanaliza supstitucijskih šifri.

Definicija 2. *Neprazan skup R na kojemu su definirane dvije binarne operacije, zbrajanje $(+)$ i množenje $(\cdot)$, tako da su zadovoljena sljedeća svojstva:*

1. *Zbrajanje je komutativno:*

$$x + y = y + x,\ \forall x, y \in R;$$

2. *Zbrajanje je asocijativno:*

$$x + (y + z) = (x + y) + z,\ \forall x, y, z \in R;$$

3. *Postoji element 0 takav da je $x + 0 = 0 + x = x$, $\forall x \in R$;*

4. *Za svaki $x \in R$ postoji aditivni inverz $-x$, takav da je $x + (-x) = -x + x = 0$;*

5. *Množenje je asocijativno:*

$$x \cdot (y \cdot z) = (x \cdot y) \cdot z, \forall x, y, z \in R;$$

6. *Množenje je distributivno s obzirom na zbrajanje:*

$$x \cdot (y + z) = x \cdot y + x \cdot z;$$
$$(x + y) \cdot z = x \cdot z + y \cdot z, \forall x, y, z \in R,$$

zove se prsten.
Ako u R postoji jedinični element ili kraće jedinica $1 \in R$ tako da je

$$1 \cdot x = x \cdot 1 = x,\ \forall x \in R,$$

onda kažemo da je R prsten s jedinicom.
Prsten R je komutativan prsten ako je

$$x \cdot y = y \cdot x,\ \forall x, y, z \in R;$$

inače govorimo o nekomutativnom prstenu.

Poznato je kako skup cijelih brojeva $\mathbb{Z}$ ima strukturu komutativnog prstena s jedinicom.

U ovom ćemo se radu baviti skupom $\mathbb{Z}_{26}$ za kojeg vrijede sva gore navedena svojstva. Dakle, skup $\mathbb{Z}_{26}$ je uz operacije $(a \pm b) \bmod 26$, $(a \cdot b) \bmod 26$, prsten (operacije $+_{26}$, $-_{26}$, $\cdot_{26}$ su zatvorene, komutativne, asocijativne, a vrijedi i distributivnost množenja prema zbrajanju).
Nadalje, broj 0 je neutralni element za zbrajanje u skupu $\mathbb{Z}_{26}$, a svaki element a ima svoj inverzni element. Broj 1 je neutralni element za množenje, no samo neki elementi imaju multiplikativni inverz u skupu $\mathbb{Z}_{26}$. To su oni elementi koju su relativno prosti s 26.

Definicija 3. *Neka su $a \neq 0$ i b cijeli brojevi. Kažemo da je b djeljiv s a, odnosno da a dijeli b ako postoji cijeli broj x takav da je $b = ax$. To zapisujemo s $a|b$ te kažemo da je a djelitelj od b, a da je b višekratnik od a. Ako b nije djeljiv s a, onda pišemo $a \nmid b$.*

Primjer 1. *Broj 35 je djeljiv s 5, tj. 5 dijeli 35 jer je $35 = 5 \cdot 7$. To zapisujemo na sljedeći način $5|35$. Odavde možemo zaključiti da je 5 djelitelj broja 35, a 35 je višekratnik broja 5.*
Broj 35 nije djeljiv s 2, tj. 2 ne dijeli 35 jer ne postoji cijeli broj x takav da je $35 = 5 \cdot x$. To zapisujemo kao $2 \nmid 35$.

Definicija 4. *Neka su b i c cijeli brojevi. Cijeli broj a zovemo zajednički djelitelj od b i c ako $a|b$ i $a|c$. Ako je barem jedan od brojeva b i c različit od nule, onda postoji konačno mnogo zajedničkih djelitelja od b i c. Najveći među njima zove se najveći zajednički djelitelj od b i c i označava se s (b,c).*

Teorem 1. *Za proizvoljan prirodan broj a i cijeli broj b postoje jedinstveni cijeli brojevi q i r takvi da je*

$$b = qa + r,\ 0 \leq r < a.$$

Teorem 2. *Neka su b i $c > 0$ cijeli brojevi. Pretpostavimo da je uzastopnom pri-*

mjenom prethodnog teorema dobiven niz jednakosti

$$\begin{aligned} b &= cq_1 + r_1, 0 < r_1 < c, \\ c &= r_1q_2 + r_2, 0 < r_2 < r_1, \\ r_1 &= r_2q_3 + r_3, 0 < r_3 < r_2, \\ &\vdots \\ r_{j-2} &= r_{j-1}q_j + r_j, 0 < r_j < r_{j-1}, \\ r_{j-1} &= r_jq_{j+1}. \end{aligned}$$

Tada je (b,c) jednak r_j, posljednjem ostatku različitom od nule. Vrijednosti od x_0 i y_0 u izrazu $(b, c) = bx_0 + cy_0$ mogu se dobiti izražavanjem svakog ostatka r_i kao linearne kombinacije od b i c.

Ovim teoremom iskazan je Euklidov algoritam koji ćemo moći vidjeti na sljedećem primjeru.

Primjer 2. *Odredimo $d = (41, 13)$ primjenom Euklidovog algoritma.*
Rješenje:
Imamo

$$\begin{aligned} 41 &= 13 \cdot 3 + 2 \\ 13 &= 6 \cdot 2 + 1 \\ 6 &= 1 \cdot 6 \end{aligned}$$

Dakle, $d = (41, 13) = 1$.

Definicija 5. *Kažemo da je prirodan broj $p > 1$ prost ako nema niti jednog djelitelja d takvog da je $1 < d < p$. Ako broj nije prost, kažemo da je složen.*

Definicija 6. *Kažemo da su cijeli brojevi a i b relativno prosti ako je $(a, b) = 1$.*

Primjer 3. *Brojevi 15 i 2 su relativno prosti jer je $(15, 2) = 1$. Brojevi 12 i 2 nisu relativno prosti jer je $(12, 2) \neq 1$.*

Definicija 7. *Neka su a, b i m cijeli brojevi, takvi da je $m > 0$. Ako m dijeli razliku $a - b$, kažemo da je a kongruentan b modulo m i pišemo*

$$a \equiv b \,(\mathrm{mod}\, m).$$

U suprotnom kažemo da a nije kongruentan b modulo m i pišemo

$$a \not\equiv b \,(\mathrm{mod}\, m).$$

Primjer 4. *Kako bismo izračunali 69 modulo 11, pišemo $69 = 6 \cdot 11 + 3$. Kako je $0 \leq 3 < 11$, slijedi da je $69 \equiv 3 \pmod{11}$.*

Važno je napomenuti da a modulo m gledamo kao nenegativan broj.

Primjer 5. *Kako bismo izračunali -47 modulo 11, pišemo $-47 = 4 \cdot (-11) + 3$. Kako je $0 \leq 3 < 11$, slijedi da je $47 \equiv 3 \pmod{11}$.*

Ako vrijedi $a \equiv b \pmod{m}$, onda se b zove ostatak od a modulo m. Za dani $a \in \mathbb{Z}$, skup cijelih brojeva $\{b \in \mathbb{Z}\colon\ a \equiv b \pmod{m}\}$ naziva se klasa ostataka od a modulo m u oznaci $[x]$.

Navedimo neka osnovna svojstva kongruencija.

Propozicija 1.1. *Relacija „biti kongruentan modulo m" relacija je ekvivalencije na skupu $\mathbb{Z}$.*

Propozicija 1.2. *Neka su a, b, c i d cijeli brojevi.*

1. *Ako je $a \equiv b \,(\mathrm{mod}\, m)$ i $c \equiv d \,(\mathrm{mod}\, m)$, onda je*

$$\begin{aligned} a + c &\equiv b + d \,(\mathrm{mod}\, m), \\ a - c &\equiv b - d \,(\mathrm{mod}\, m), \\ ac &\equiv bd \,(\mathrm{mod}\, m). \end{aligned}$$

2. *Ako je $a \equiv b \,(\mathrm{mod}\, m)$ i $d|m$, onda je $a \equiv b \,(\mathrm{mod}\, d)$.*

3. *Ako je $a \equiv b \,(\mathrm{mod}\, m)$, onda je $ac \equiv bc \,(\mathrm{mod}\, mc)$, $\forall c \neq 0$.*

Primjer 6. *Promotrimo zbrajanje i množenje u $\mathbb{Z}_{26}$.*
Imamo $9 \cdot 16 = 144 \equiv 5 \,(\mathrm{mod}\, 26)$, pa je u $\mathbb{Z}_{26}$ $9 \cdot 16 = 5$.
Analogno, $16 + 27 = 43 \equiv 1 \,(\mathrm{mod}\, 26)$, pa je u $\mathbb{Z}_{26}$ $16 + 27 = 1$.

Teorem 3. *Neka su a i m prirodni te b cijeli broj. Kongruencija $ax \equiv b \pmod{m}$ ima rješenja ako i samo ako $d = nzd(a, m)$ dijeli b. Ako je ovaj uvjet zadovoljen, onda gornja kongruencija ima točno d rješenja modulo m.*

Primjer 7. *Kongruencija $8x \equiv 13 \pmod{24}$ nema rješenja jer $d = nzd(8, 24) = 8$ ne dijeli 13.*
Kongruencija $2x \equiv 4 \pmod{26}$ ima rješenja jer $d = nzd(2, 26) = 2$ dijeli 4. Ova kongruencija ima točno dva rješenja.

Primjer 8. *Ako je p prost broj i p ne dijeli a, kongruencija $ax \equiv b \,(mod\, p)$ ima jedinstveno rješenje. Pitamo se kako riješiti kongruenciju $a'x \equiv b' \,(mod\, m')$, gdje je $(a', m') = 1$. Kako je $(a', m') = 1$, postoje cijeli brojevi u i v takvi da je $a'u + m'v = 1$. Brojevi u i v mogu se naći pomoću Euklidovog algoritma. Dobijemo $a'u \equiv 1 (mod m')$ pa je $x \equiv ub' (mod\ m')$.*

Primjer 9. *Riješimo kongruenciju $9x \equiv 12 \pmod{15}$.*
Rješenje:
Kako je $(9, 15) = 3$ i $3|12$, ova kongruencija ima tri rješenja. Primjenjujući treće svojstvo Propozicije 1.2., sada trebamo riješiti kongruenciju oblika $3x \equiv 4 \pmod{5}$. Primijenom Euklidova algoritma dobivamo:

$$5 = 3 \cdot 1 + 2$$
$$3 = 2 \cdot 1 + 1$$
$$2 = 1 \cdot 2.$$

i	-1	0	1	2
q_i			1	1
x_i	1	0	1	-1
y_i	0	1	-1	2

Tablica 1: *Postupak traženja rješenja kongruencije*

Dakle, rješenje kongruencije $3u \equiv 1 \pmod{5}$ je $u \equiv 2 \pmod{5}$. Rješenje od $3x \equiv 4 \pmod{5}$ je $x \equiv 3 \pmod{5}$. Konačno, rješenja su polazne kongruencije

$$x \equiv 3, 8, 13 \pmod{15}.$$

Iz prethodnog teorema možemo zaključiti da će kongruencija $ax \equiv b \pmod{m}$ imati jedinstveno rješenje ukoliko je $nzd(a, m) = 1$, odnosno ako su brojevi a i m relativno prosti brojevi.

Definicija 8. *Neka je $a \in \mathbb{Z}_m$. Multiplikativni inverz od a modulo m, u oznaci a^{-1} mod m, je element $a' \in \mathbb{Z}_m$ za koji vrijedi $aa' \equiv a'a \equiv 1 \pmod{m}$.*

Primjer 10. *Pronađimo 11^{-1} u $\mathbb{Z}_{26}$.*
Rješenje:
Kako je $11 \cdot 19 \equiv 1 \pmod{26}$, multiplikativni inverz od 11 modulo 26 jednak je 19. Dakle $11^{-1} = 19$ u $\mathbb{Z}_{26}$. Također, možemo vidjeti da je $19^{-1} = 11$ u $\mathbb{Z}_{26}$.

Ako je a invertibilan u $\mathbb{Z}_m$, onda linearna jednadžba $ax + b = c$ ima jedinstveno rješenje $x = a^{-1}(c - b)$. Primjerice, rješenje jednadžbe 15x+2=3 u $\mathbb{Z}_{26}$ ima jedinstveno rješenje $x = 7(3 - 2) = 7$.

Definicija 9. *Broj cijelih brojeva koji su relativno prosti s m na skupu $\mathbb{Z}_m$ označavamo s $\varphi(m)$, a funkciju φ zovemo Eulerova funkcija.*

Teorem 4. *Ako je $(a, m) = 1$, onda je $a^{\varphi(m)} \equiv 1 \pmod{m}$.*

Primjer 11. *Izračunajmo koliko je brojeva relativno prosto s brojem 26 u skupu $\mathbb{Z}_{26}$.*
Rješenje:
Budući da je $26 = 2 \cdot 13$, računamo $\varphi(26) = 26 \cdot (1 - \frac{1}{2}) \cdot (1 - \frac{1}{13}) = 12$. Dakle, 12 brojeva je relativno prosto s brojem 26 u $\mathbb{Z}_{26}$.

2 Supstitucijske šifre

Supstitucijske su šifre one šifre koje su karakteristične po tome što poredak slova uvijek ostaje isti, ali se za svako slovo koristi drugo slovo ili znak. Naziv *supstitucijske šifre* dolazi od toga što se nešto mijenja, odnosno, supstituira se svako slovo naše poruke. U radu ćemo prikazati neke od supstitucijskih šifri. U skupinu supstitucijskih šifri spadaju monoalfabetske i polialfabetske supstitucijske šifre. Monoalfabetske supstitucijske šifre poznate su po tome što svako slovo ili znak ima točno jedno i samo jedno supstitucijsko slovo ili znak. Drugim riječima, ukoliko je kod za slovo M jednako slovu L, onda u šifri slovo L uvijek znači slovo M. Riječ *kod* u ovom radu označavat će drugu riječ, slovo ili znak za pojam šifre. Međutim, kod polialfabetskih šifri slovo može biti šifrirano s više slova, ali isto tako više slova može biti šifrirano istim slovom. To zapravo ovisi o poziciji u tekstu. Dakako, postoje još i monogramske i poligramske supstitucijske šifre. Kod monogramskih šifri možemo uočiti kako je svako slovo šifrirano točno jednim slovom ili znakom, dok je kod poligramskih šifri više slova šifrirano je s nekoliko simbola.

U ovom radu uglavnom ćemo se baviti monoalfabetskim supstitucijskim šiframa. Supstitucijske šifre karakteristične su po tome što se postupak supstituiranja vrlo lako pamti. Ukoliko je ključ za dešifriranje jednostavan, protivnik vrlo lako može probiti šifru i pročitati poruku. Jedna od najstarijih i najjednostavnijih supstitucijskih šifri karakteristična je po tome što se u gornji redak slova zapisuju u abecednom poretku, dok u donjem retku poredak slova obrnut je abecednom poretku.

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

Tablica 2: *Primjer jednostavne supstitucijske šifre*

Na sljedećem primjeru možemo vidjeti kako izgleda postupak šifriranja poruka koristeći jednostavnu supstitucijsku šifru iz Tablice 2.

Primjer 12. *Poruku* ***upoznaj mog najboljeg prijatelja*** *zapisat ćemo* ***FKLAMZQ NLT MZQYLOQVT KIRQZGVOQZ*** *koristeći Tablicu 2.*

Nadalje, numerirajmo slova abecede unaprijed A=1, B=2, C=3 itd. odnosno unazad A=26, B=25, C=24 itd. U tom slučaju brojevi zamjenjuju slova. Kako bismo razlikovali jednoznamenkaste i dvoznamenkaste brojeve, koriste se crtice. Međutim, probijanje ovakve šifre vrlo je jednostavno pa nije preporučljivo za korištenje budući da bi protivnici vrlo lako mogli otkriti sadržaj poruke.

Primjer 13. *Napišite poruku*

upoznaj mog najboljeg prijatelja

pomoću jednostavne supstitucije.
Rješenje:
Prilikom rješavanja ovog primjera koristit ćemo numeriranje slova unaprijed kao što je prikazano u tablici te iščitavamo sljedeću poruku:

A	B	C	Č	Ć	D	DŽ	Đ	E	F	G	H	I	J	K
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

L	LJ	M	N	NJ	O	P	R	S	Š	T	U	V	Z	Ž
16	17	18	19	20	21	22	23	24	25	26	27	28	29	30

27 22 21 29 19 1 14 18 21 11 19 1 14 2 21 17 9 11 22 23 13 14 1 26 9 17 1

2.1 Šifriranje i dešifriranje supstitucijskih šifri

Definicija 10. *Neka je* $\mathcal{P} = \mathcal{C} = \mathbb{Z}_{26}$. $\mathcal{K}$ *se sastoji od svih mogućih permutacija 26 simbola:* $0, 1, ..., 25$. *Za svaku permutaciju* $\pi \in \mathcal{K}$, *definiramo*

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

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

Skup $\mathcal{P}$ je konačan skup svih mogućih osnovnih elemenata otvorenog teksta, a skup $\mathcal{C}$ je konačan skup svih mogućih osnovnih elemenata šifrata. Pretpostavimo da

$\mathcal{P}$ i $\mathcal{C}$ sadrže englesku abecedu od 26 slova. U hrvatskoj abecedi poistovijetit ćemo slova Č i Ć s C te Đ, DŽ, Š, Ž redom s D, S, Z. Funkciju šifriranja i dešifriranja promatramo kao permutaciju slova engleske abecede pri čemu je funkcija dešifriranja inverzna funkcija funkciji šifriranja. Primjer šifriranja i dešifriranja prikazat ćemo u sljedećim tablicama. Dakle, slova otvorenog teksta zapisana su malim slovima, a slova šifrata velikim tiskanim slovima.

a	b	c	d	e	f	g	h	i	j	k	l	m
B	E	Z	Q	I	K	J	W	A	P	N	D	R
n	o	p	q	r	s	t	u	v	w	x	y	z
C	T	S	F	Y	G	H	X	L	M	V	O	U

Tablica 3: *Primjer šifriranja supstitucijskom šifrom*

Vidimo da je $e_\pi(a) = B$, $e_\pi(b) = E$, $e_\pi(c) = Z$,... Drugim riječima, slovo a ćemo šifrirati slovom B, slovo b slovom E, slovo c slovom Z,...

A	B	C	D	E	F	G	H	I	J	K	L	M
i	a	n	l	b	q	s	t	e	g	f	v	w
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
k	y	j	d	m	p	o	z	x	h	u	r	c

Tablica 4: *Primjer dešifriranja supstitucijskom šifrom*

Vidimo da je $d_\pi(A) = i$, $d_\pi(B) = a$, $d_\pi(C) = n$,... Drugim riječima, ukoliko se u šifratu pojavi slovo A, u otvorenom tekstu slovu A pripada slovo i.

Primjer 14. *Šifrirajmo poruku:*

kocka je bačena.

Rješenje:
U ovom primjeru slovo Č poistovijetit ćemo sa slovom C. Dakle, koristeći Tablicu 3 poruku ćemo zapisati u obliku ***NTZNB PI EBZICB.***

Primjer 15. *Dešifrirajmo poruku* ***NB ULAPIUQBRB X LAGACI****.*
Rješenje:
Koristeći Tablicu 4, dobivamo poruku ***ka zvijezdama u visine****.*

U slučaju hrvatskog jezika ne postoje stroga pravila za šifriranje i dešifriranje slova, odnosno, sve ovisi između pošiljatelja i primatelja. Možemo reći da je funkciju šifriranja i dešifriranja moguće gledati kao permutaciju slova hrvatske abecede. Međutim, prilikom šifriranja i dešifriranja primatelj poruke može imati prilikom čitanja iste. Primjerice, ukoliko se u šifratu pojavi slovo NJ, njega možemo dešifrirati na dva načina $d_\pi(NJ) = n$ ili $d_\pi(N) = o$ i $d_\pi(J) = m$. Također, ukoliko se u šifratu pojave bigrami LJ i DŽ vrijedi prethodni postupak. Na primjer, šifrat **LJŠĐLJŠJ** može se dešifrirati kao npr. **vbevbm** ili **cmbecmbm**. Upravo zbog toga da ne dođe do problema prilikom čitanja, uobičajeno je da se koriste isključivo slova engleske abecede gdje se karakteristična slova hrvatske abecede zapisuju na sljedeći način: slova č i ć pišu se kao c, đ kao d, š kao s, ž kao z, dok se dž, lj i nj tretiraju kao parovi slova d i z, l i j te n i j. U Tablici 4 možemo vidjeti primjer šifriranja slova u slučaju kada je otvoreni tekst na hrvatskom jeziku.

a	b	c	č	ć	d	dž	đ	e	f	g	h	i	j	k
Č	Š	L	K	M	S	A	T	Đ	O	Ć	DŽ	H	E	Ž
l	lj	m	n	nj	o	p	r	s	š	t	u	v	z	ž
F	U	J	NJ	D	N	B	P	Z	G	C	I	LJ	V	R

Tablica 5: *Primjer šifriranja supstitucijskom šifrom ako je otvoreni tekst na hrvatskom jeziku*

U Tablici 5 možemo vidjeti primjer dešifriranje slova u slučaju kada je otvoreni tekst na hrvatskom jeziku.

A	B	C	Č	Ć	D	DŽ	Đ	E	F	G	H	I	J	K
dž	p	t	a	g	nj	h	e	j	l	š	i	u	m	č
L	LJ	M	N	NJ	O	P	R	S	Š	T	U	V	Z	Ž
c	v	ć	o	n	f	r	ž	d	b	đ	lj	z	s	k

Tablica 6: *Primjer dešifriranja supstitucijskom šifrom ako je otvoreni tekst na hrvatskom jeziku*

Primjer 16. *Šifrirajmo poruku:*

iskoristi dan, ne vjeruj sljedećem

ako nam je poznato da je otvoreni tekst na hrvatskom jeziku. Rješenje: Koristeći Tablicu 5 dobivamo poruku
***HZŽNPHZCH SČNJ, NJĐ LJEĐPIE ZUĐSĐMĐJ**.*

Primjer 17. *Dešifrirajmo poruku:*

ĆPHEĐGHCH EĐ UISZŽH

ako nam je poznato da je otvoreni tekst na hrvatskom jeziku. Rješenje: Koristeći Tablicu 6 dobivamo poruku

***griješiti je ljudski**.*

Nadalje, prostor ključeva engleske abecede poprilično je velik jer on sadrži 26! elemenata. Ukoliko bismo krenuli ručno ispitivati koji je od ključeva ispravan, taj bi nam posao oduzeo jako puno vremena. No, u rješavanju ovog problema mogu nam pomoći neka svojstva jezika na kojem je otvoreni tekst napisan. To je primjerice analiza frekvencije slova. Ideja analize frekvencije slova je ta da se broji koliko se puta neko slovo pojavilo u šifratu te se nakon toga uspoređuje njegova distribucija u šifratu s poznatim podacima o distribuciji slova jezika na kojem je otvoreni tekst pisan. Vrlo će vjerojatno najfrekventnije slovo šifrata odgovarati najfrekventnijem slovu otvorenog teksta.

Navest ćemo nekoliko važnih informacija o engleskom jeziku:

- najfrekventnija su slova u engleskom jeziku poredana od najfrekventnijeg do najmanje frekventnijeg:
  E(127), T(91), A(82), O(75), I(70), N(67), S(63), H(61), R(60), D(43), L(40), C(28), U(28), M(24), W(23), F(22), G(20), Y(20), P(19), B(15), V(10), K(8), J(2), Q(1), X(1), Z(1);
- Najfrekventniji bigrami su:
  TH (32), HE (25), AN, IN, ER, RE, ON, ES, TI, AT(12);

- najfrekventniji trigrami su:
  THE(35), ING(11), AND(10), ION, TIO, ENT, ERE, HER(7);
- slovo E je slovo koje se najčešće pojavljuje na kraju riječi;
- slovo T je slovo kojim najčešće riječi započinju;
- najčešće su riječi od dva slova su OF, TO, IN;
- najčešće su korištene riječi s trima slovima su THE i AND;
- poslije Q uvijek dolazi U;
- najčešća riječ od četiri slova je THAT;
- slovo N je suglasnik koji najčešće dolazi iza samoglasnika;
- najčešći bigrami s dvama jednakim slovima su: LL, EE, SS, OO, TT, FF, RR, NN, PP, CC;

Napomena:

- Najčešća je riječ od četiri slova THAT. Možemo uočiti da ova riječ započinje i završava istim slovom. Primjerice, ukoliko se u šifratu pojavi riječ MRSM vrlo je vjerojatno da je to šifrat za riječ that.
- Riječ XPP vrlo vjerojatno može odgovarati riječima kao što su ALL, TOO, SEE ili čak može odgovarati riječima kao što su ODD, ADD, ZOO.
- Riječ BDCKC vrlo vjerojatno odgovara riječima kao što su WHERE, THERE ili THESE. No, ta riječ može odgovarati i manje korištenim riječima kao što su NIECE, ROSES ili NOSES.
- Riječ ABCDB vrlo vjerojatno odgovara riječi WHICH.

Pogledajmo kako nam neka od gore navedenih svojstava engleskog jezika mogu pomoći u dešifriranju šifrata.

Primjer 18. *Dešifrirajmo šifrat:*
ESTIT DR ALESDAN TDESTI NLLM LI POM PHE ESDAUDAN COUTR DE RL.
ako nam je poznato da je otvoreni tekst na engleskom jeziku. Rješenje:

Možemo uočiti da u našem šifratu imamo riječ ESTIT. To bi nam moglo ukazivati na to da za riječ ESTIT možemo pretpostaviti da je to riječ THERE. Sada primijenimo supstituciju otkrivenu kroz tu riječ na ostatak teksta:

T	H	E	R	E		-	-		-	-	T	-	-	-	-	
E	S	T	I	T		D	R		A	L	E	S	D	A	N	
E	-	T	H	E	R		-	-	-	-		-	R	-	-	-
T	D	E	S	T	I		N	L	L	M		L	I	P	O	M
		-	-	T		T	H	-	-	-	-	-	-			
		P	H	E		E	S	D	A	U	D	A	N			
		-	-	-	E	-	-	T		-	-					
		C	O	U	T	R		D	E		R	L				

Tablica 7: *Tablica s riječi THERE u tekstu*

Pretpostavimo da je $d_\pi(D) = i$ jer bi tada dobili riječ EITHER, potom bismo mogli pretpostaviti da je $d_\pi(R) = s$ jer u tom slučaju dobivamo za drugu riječ riječ IS.
Dobivamo sljedeće:

T	H	E	R	E		I	S		-	-	T	-	I	-	-	
E	S	T	I	T		D	R		A	L	E	S	D	A	N	
E	I	T	H	E	R		-	-	-	-		-	R	-	-	-
T	D	E	S	T	I		N	L	L	M		L	I	P	O	M
		-	-	T		T	H	I	-	-	I	-	-			
		P	H	E		E	S	D	A	U	D	A	N			
		-	-	-	E	S		I	T		S	-				
		C	O	U	T	R		D	E		R	L				

Tablica 8: *Tablica s riječi THERE u tekstu*

Sada bismo mogli prepostaviti da je $d_\pi(L) = o$, $d_\pi(N) = g$ i $d_\pi(M) = d$ jer bismo tad dobili riječ GOOD. Postupak nastavljamo sve dok nam se ne otkriju sva slova. Naposljetku, konačno rješenje izgleda ovako:

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

Tablica 9: *Otkriveni dio šifre*

Poslije tablice dobivamo citat engleskog književnika, glumca i redatelja Williama Shakespearea koji glasi: "There is nothing either good or bad, but thinking makes it so".

2.2 Cezarova šifra

Cezarova šifra poznata je kao šifra pomaka, a dobila naziv po tvorcu šifre Gaju Juliju Cezaru (100.pr.Kr. - 44.pr.Kr.), poznatom rimskom vojskovođi, piscu i političaru. Cezarova šifra jedna je od najjednostavnijih i najrasprostranjenijih načina šifriranja. To je tip šifre u kojem se svako slovo otvorenog teksta zamjenjuje odgovarajućim slovom abecede pomaknutim za određeni broj mjesta. Dakle, Gaj Julije Cezar u komunikaciji sa svojim prijateljima koristio se šifrom u kojoj su se slova otvorenog teksta zamjenjivala slovima koja su se nalazila za 3 mjesta udaljena od njih u abecedi. Ukoliko se u otvorenom tekstu našlo slovo Z, njega se zamijenilo sa slovom C koji je udaljen od slova Z za tri mjesta. Odnosno, pretpostavljamo da se abeceda ciklički nastavlja. Međutim, danas se Cezarovom šifrom nazivaju šifre s pomakom različitim od 3. Dakle, Cezarovu šifru definirat ćemo na sljedeći način:

Definicija 11. *Neka je* $\mathcal{P} = \mathcal{C} = \mathcal{K} = \mathbb{Z}_{26}$. *Za* $0 \leq \mathcal{K} \leq 25$, *definiramo*

$$e_K(x) \equiv x + K \pmod{26}$$
$$d_K(y) \equiv y - K \pmod{26},\ x, y \in \mathbb{Z}_{26}.$$

Budući da engleska abeceda ima 26 slova, kriptosustav je definiran na skupu $\mathbb{Z}_{26}$. Ukoliko radimo s hrvatskom abecedom koja ima 30 slova, kriptosustav je definiran na skupu $\mathbb{Z}_{30}$. Također, kao i što je gore navedeno, slova poput dž, lj, nj koja

imamo u hrvatskom jeziku nije jasno kako šifrirati i čitati. Drugim riječima, postoji više načina za šifriranje i dešifriranje, a ovise o odabiru pošiljatelja i primatelja. Upravo zbog toga, slova č i ć pišu se kao c, đ kao d, š kao s, ž kao z, dok se dž, lj i nj tretiraju kao parovi slova d i z, l i j te n i j.

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Tablica 10: *Numerički ekvivalenti slova engleske abecede*

Elementi su otvorenog teksta slova, dok ključ K određuje za koliko mjesta udesno pomičemo slova prilikom šifriranja. U ovom slučaju imamo 26 mogućih ključeva. Očito je $(d_K(e_K(x))) = x$, što se i zahtijeva u definiciji kriptosustava. U slučaju kada nam je $K = 3$, dobivamo originalnu Cezarovu šifru.

Ključ je u sljedećem primjeru jednak 5. Drugim riječima, ključ ove šifre predstavlja pomak koji je u ovom slučaju uvijek 5.

Definicija 12. *Neka je* $\mathcal{P} = \mathcal{C} = \mathbb{Z}_{26}$. *Za* $K = 5$, *definiramo funkciju šifriranja* e_K *i funkciju dešifriranja* d_K *kao:*

$$e_K(x) = (x + K) \bmod 26$$
$$d_K(y) = (y - K) \bmod 26,\ x, y \in \mathbb{Z}_{26}.$$

Odnosno imamo:

$$e_5(x) = (x + 5) \bmod 26$$
$$d_5(y) = (y - 5) \bmod 26.$$

Primjer 19. *Šifrirajmo riječ* ***sladoled*** *Cezarovom šifrom.*
Rješenje:
Numerički su ekvivalenti slova riječi SLADOLED 18 11 0 3 14 11 4 3. *Koristeći funkciju šifriranja, šifriramo slovo po slovo:*

$$e_5(18) = 18 + 5 = 23 \bmod 26;$$
$$e_5(11) = 11 + 5 = 16 \bmod 26;$$
$$e_5(0) = 0 + 5 = 5 \bmod 26;$$
$$e_5(3) = 3 + 5 = 8 \bmod 26;$$
$$e_5(14) = 14 + 5 = 19 \bmod 26;$$
$$e_5(4) = 4 + 5 = 9 \bmod 26.$$

Sada iz Tablice 10 iščitamo numeričke ekvivalente slova šifrata: 23 16 5 8 19 16 9 8*, a nakon toga numerički ekvivalent pretvorimo u slova nakon čega dobivamo šifrat* ***XQFITQJI****.*

Primjer 20. *Dešifrirajmo poruku* ***UWTQOJHJ*** *ako znamo da je otvoreni tekst šifriran Cezarovom šifrom ključem* 5*.*
Rješenje:
Numerički su ekvivalenti slova šifrata 20 22 19 16 14 9 7*. Koristeći funkciju dešifriranja, dešifriramo slovo po slovo:*

$$d_5(20) = 20 - 5 = 15 \bmod 26;$$
$$d_5(22) = 22 - 5 = 17 \bmod 26;$$
$$d_5(19) = 19 - 5 = 14 \bmod 26;$$
$$d_5(16) = 16 - 5 = 11 \bmod 26;$$
$$d_5(14) = 14 - 5 = 9 \bmod 26;$$
$$d_5(9) = 9 - 5 = 4 \bmod 26;$$
$$d_5(7) = 7 - 5 = 2 \bmod 26.$$

Numerički su ekvivalent slova šifrata 15 17 14 11 9 4 2 4*. Nakon što numerički ekvivalent pretvarimo u slova, dobivamo otvoreni tekst* ***proljeće****.*

U nastavku možemo vidjeti Tablicu 11 u kojoj je prikazan postupak dobivanja tablice šifrata slova engleske abecede Cezarovom šifrom s pomakom 18. Funkcija šifriranja jest

$$e_{18}(x_i) = (x_i + 18) \bmod 26, \text{ za } i = 0, \ldots, 25.$$

Nakon što numeričkim ekvivalentima slova alfabeta dodamo 18, dobivamo numeričke ekvivalente slova šifrata. Zatim, numeričkim ekvivalentima pridružimo odgovarajuća slova šifrata kao što je prikazano u Tablici 12.

	0	1	2	3	4	5	6	7	8	9	10	11	12
$+_{26}18$	18	19	20	21	22	23	24	25	0	1	2	3	4
	13	14	15	16	17	18	19	20	21	22	23	24	25
$+_{26}18$	5	6	7	8	9	10	11	12	13	14	15	16	17

Tablica 11: *Numerički ekvivalent slova Cezarove šifre s pomakom* 18

a	b	c	d	e	f	g	h	i	j	k	l	m
S	T	U	V	W	X	Y	Z	A	B	C	D	E
n	o	p	q	r	s	t	u	v	w	x	y	z
F	G	H	I	J	K	L	M	N	O	P	Q	R

Tablica 12: *Cezarova šifra s pomakom* 18

Primjer 21. *Šifrirajmo poruku*

ovo je moj dan

Cezarovom šifrom s pomakom 18.
Rješenje:
Koristeći Tablicu 12, dobivamo šifrat ***GNG BW EGB VSF****.*

Primjer 22. *Dešifrirajmo šifrat*

SZITRQKI MVOTMASM

ako znamo da je poruka šifrirana Cezarovom šifrom s pomakom 18.
Rješenje:
Koristeći Tablicu 12, dobivamo šifrat ***kraljica Engleske****.*

2.3 Šifra s datumskim pomakom

Budući da se neke šifrirane poruke vrlo lako dešifriraju bez ključa, došlo je do ideje da je moguće mijenjati broj pomaka za svako slovo. Jedan od poznatih načina takvog dešifriranja i šifriranja poruka jest korištenje datuma. Primjerice, ukoliko želimo koristiti datum 11. veljače 1995. godine, to zapisujemo na sljedeći način: Veljača predstavlja 2. mjesec u godini te prema američkom sustavu to zapisujemo

kao $02-11-95$. Kada uklonimo crtice dobivamo 021195. Sada dobiveni broj pišemo iznad svakog slova u našoj poruci.
Na sljedećem primjeru možemo vidjeti kako izgleda postupak šifriranja poruke s datumskim pomakom.

Primjer 23. *Šifrirajmo poruku*

ljubav sve pobjeđuje

s datumom 11. *veljače* 1995. *godine.*
Rješenje:
Najprije zapišemo broj 021195 *iznad svakog slova naše poruke.*

0	2	1	1	9	5		0	2	1		1	9	5	0	2	1	1	9	5
L	J	U	B	A	V		S	V	E		P	O	B	J	E	D	U	J	E

Kako bismo šifrirali ovu poruku, npr. slovo L ne pomičemo zbog 0; slovo J potrebno je pomaknuti za 2 *slova udesno i ono tad postane L; slovo U je potrebno pomaknuti za* 1 *slovo udesno te ono postaje slovo V i tako dalje za preostala slova naše poruke. Konačna poruka korištenjem ključa* 021195 *i grupiranjem slova od po* 5 *slova u grupi postaje šifrat:*

LLVCJA SXF QXGJGEVSJ

Prilikom dešifriranja poruke, potrebno je napisati ključ iznad poruke te postupak uraditi unatrag, tj. pomak abecede uraditi unatrag. Ukoliko se dogodi da pomak ide dalje od slova A, u tom se slučaju vraćamo na kraj abecede i nastavljamo postupak unatrag. Drugim riječima, postupak se provodi ciklički.
U sljedećem primjeru možemo vidjeti postupak dešifiranja poruke s datumskim pomakom.

Primjer 24. *Dešifrirajmo poruku*

PXTXKXA WBLHSLSPL SEMR

s datumom 12. *rujna* 1964. *godine.*
Rješenje:
Najprije zapišemo broj 091264 *iznad svakog slova naše poruke.*

			0	9	1	2	6	4	0					
			P	X	T	X	K	X	A					
9	1	2	6	4	0	9	1	2		6	4	0	9	
W	B	L	H	S	L	S	P	L		S	E	M	R	

Pomičući svako slovo abecede unatrag onoliko mjesta koliki je broj iznad slova, dobivamo poruku:

POSVETA NAJBOLJOJ MAMI

2.4 Šifra s ključnom riječi

Jedan od jednostavnijih načina za kreiranje abecede za šifriranje je korištenje ključne riječi ili fraze. Ukoliko za primjer uzmemo ključnu riječ „SLADOLED" postupak je sljedeći: Ispod svakog slova abecede ispišemo zadanu ključnu riječ, u ovom slučaju „SLADOLED", i onda nadopisujemo preostala slova abecede.

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

Tablica 13: *Tablica jednostavne supstitucijske šifre s ključnom riječi „SLADOLED"*

Ključne riječi vrlo su lako pamtljive te svaka ključna riječ kreira drugačiju tablicu supstitucijske šifre i samu supstitucijsku šifru. Postupak šifriranja i dešifriranja provodi se jednako kao i dosad opisanim metodama.

2.4.1 Cezarova šifra s ključnom riječi

Cezarova šifra s ključnom riječi poznata je monoalfabetska supstitucijska šifra. Ova šifra karakteristična je po tome što je funkcija šifriranja permutacija s ključnom

riječi. Ključ šifre čine ključna riječ i broj koji označava poziciju mjesta u abecedi otvorenog teksta od koje kreće ključna riječ, a preostala slova nadopisujemo u abecedenom poretku.
Sljedeći nam primjer pokazuje postupak šifriranja Cezarovom šifrom s ključnom riječi u kojoj je ključ K=(DUBROVNIK, 11).

Primjer 25.

a	b	c	d	e	f	g	h	i	j	k	l	m
J	L	M	P	Q	S	T	W	X	Y	Z	D	U

n	o	p	q	r	s	t	u	v	w	x	y	z
B	R	O	V	N	I	K	A	C	E	F	G	H

Tablica 14: *Cezarova šifra s ključnom riječi*

Možemo uočiti da od broja koji se nalazi u ključu, u našem slučaju 11, započinjemo pisati ključnu riječ nakon čega redom zapisujemo preostala slova alfabeta koja nisu dotad iskorištena.

Primjer 26. *Dešifrirajmo šifrat:*

KMGT STGLG GB RHGLVBLT

dobiven Cezarovom šifrom s ključnom riječi. Poznato je da je otvoreni tekst na hrvatskom jeziku, a ključ je K=(TAJNA, 1). Rješenje:
Šifrirana abeceda nastaje tako da na početak abecede stavi ključ. Slova, koja se ponavljaju u ključnoj riječi, ne zapisujemo više, a ostatak se popuni slovima koja se ne nalaze u ključu i to redom od početka abecede. Pogledajmo što dosad imamo:

a	b	c	d	e	f	g	h	i	j	k	l	m
T	A	J	N	B	C	D	E	F	G	H	I	K

n	o	p	q	r	s	t	u	v	w	x	y	z
L	M	O	P	Q	R	S	U	V	W	X	Y	Z

Tablica 15: *Cezarova šifra s ključnom riječi*

Nakon dešifriranja dobivamo otvoreni tekst:

moja tajna je skrivena.

Dakle, ključ $K = (TAJNA, 1)$ *je uistinu dobar ključ.*

2.5 Afina šifra

Afina je šifra jedan specifičan slučaj supstitucijske šifre kojoj je funkcija šifriranja oblika $e(x) = (ax + b) \pmod{26}$, pri čemu a i b poprimaju cjelobrojne vrijednosti, ali ne veće od 26. Ova je šifra sigurnija od prethodnih upravo zbog toga što je uključeno više od jednog parametra. Kako bismo mogli pravilno provesti postupak dešifriranja, gore navedena funkcija mora biti injekcija. Drugim riječima, funkcija mora imati inverz na skupu $\mathbb{Z}_{26}$. Iz toga razloga, parametar a nije proizvoljan, već mora biti relativno prost s modulom 26.
Afina šifra definira se na sljedeći način:

Definicija 13. *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* $\mathcal{K} = (a, b) \in K$ *definirmo:*

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

Naziv ove funkcije dolazi zbog toga jer su funkcije šifriranja afine. Parametar a^{-1} označava multiplikativni inverz broja a u prstenu $\mathbb{Z}_{26}$. Budući da broj 26 nije prost, to znači da nemaju svi elementi iz $\mathbb{Z}_{26}$ multiplikatvni inverz, nego samo oni koji su relativno prosti s 26. U Tablici 16 možemo vidjeti brojeve skupa s njihovim multiplikativnim inverzima.

a	1	3	5	7	9	11	15	17	19	21	23	25
a^{-1}	1	9	21	15	3	19	7	23	11	5	17	25

Tablica 16: Multiplikativni inverzi brojeva relativno prostih s 26 modulo 26

Ako je ključ $K = (11, 4)$, funkcija šifriranja jest

$$e_K(x) = (11x + 4) \bmod 26,$$

a funkcija dešifriranja

$$d_K(y) = 19(y-4) \bmod 26 = (19y - 76) \bmod 26 = (19y - 24) \bmod 26.$$

Ispitajmo je li funkcija šifriranja injekcija:
$d_K(e_K(x)) = d_K(11x + 4) = 19(11x + 4) - 24 = 209x + 76 - 24 = x$

Primjer 27. *Pretpostavimo da je* $K = (11, 4)$. *Šifrirajmo otvoreni tekst* ***more****. Najprije slova otvorenog teksta poistovjećujemo s njihovim numeričkim ekvivalentima.* more $\rightarrow$ 12 14 17 4. *Sada kada smo odredili numerički ekvivalent slova računamo šifrat za svako slovo. Dobivamo:*

$$\begin{aligned} e_K(12) &= 11 \cdot 12 + 4 \equiv 6 \pmod{26}, \\ e_K(14) &= 11 \cdot 14 + 4 \equiv 2 \pmod{26}, \\ e_K(17) &= 11 \cdot 17 + 4 \equiv 9 \pmod{26}, \\ e_K(4) &= 11 \cdot 4 + 4 \equiv 22 \pmod{26}, \end{aligned}$$

odakle iščitavamo numerički ekvivalent šifrata 6 2 9 22, *odnosno, šifrat je* ***GCJW****.*

Budući da a mora biti relativno prost s 26, postoji $\varphi(26) \cdot 26 = 12 \cdot 26 = 312$ mogućih ključeva. Ukoliko ne znamo elegantniji način za dešifrirati šifrat, postupak dešifriranja možemo provesti upotrijebljujući „grubu silu". Općenito, broj ključeva u afinoj šifri na skupu $\mathbb{Z}_n$ jednak je $n \cdot \varphi(n)$. Ključ ćemo lako odrediti analizom frekvencija slova u šifratu. Pretpostavimo da znamo na kojem je jeziku pisan otvoreni tekst. Međutim, ukoliko i ne znamo na kojem je jeziku napisan otvoreni tekst, ne mijenja se složenost kriptoanalize. Ukoliko nam je pretpostavka za šifre barem dva slova ispravna, nakon što riješimo sustav dviju jednadžbi, lako možemo doći do ključa. Drugim riječima, lako možemo doći do vrijednosti (a, b).

Primjer 28. *Dešifrirajmo šifrat dobiven afinom šifrom iz otvorenog teksta na hrvatskom jeziku.*

UNAW TOPEW JEXAW JIBNI XAPAQ NUZAW RUFAP EXZAW IAQEQ PRAVI TUFRQ GAXZO HINAA
QVIJA OWUWQ YUXUN VIZOA JANUP OBNIX INIWW FQRGI.

Rješenje:

Slova I i A imaju najveću frekvenciju, tj. slovo I se pojavljuje 14 *puta, a slovo A se pojavljuje* 11 *puta. Budući da su slova A i I najfrekventnija slova u hrvatskom jeziku, možemo pretpostaviti da je* $e_K(a) = I$ *i* $e_K(i) = A$.

Sada imamo $e_K(0) = 8$ *i* $e_K(8) = 0$ *pa riješimo sustav:*

$$0 \cdot a + b = 8 \bmod 26,$$
$$8 \cdot a + b = 0 \bmod 26.$$

Nakon što riješimo sustav dobivamo jedinstveno rješenje $a = 25$ *i* $b = 8$*. Kako je* $(a, 26) = (25, 26) = 1$*, dobili smo ključ. Izračunajmo funkciju dešifriranja* $d_K(y) = 25(y - 8)$ *za svaki* y *iz šifrata.*

Dolazimo do supstitucije prikazane u Tablici 17.

a	b	c	d	e	f	g	h	i	j	k	l	m
I	H	G	F	E	D	C	B	A	Z	Y	X	W
n	o	p	q	r	s	t	u	v	w	x	y	z
V	U	T	S	R	Q	P	O	N	M	L	K	J

Tablica 17: *Supstitucija afinom šifrom*

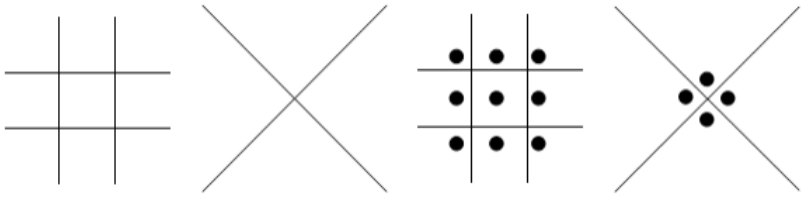
Dobili smo sljedeći tekst: ***Ovim putem želim zahvaliti svojim roditeljima i sestri na podršci, ljubavi i snazi u mom školovanju i životu. Hvala vam od srca!***

*Odavde možemo zaključiti da je K(*25,8*) dobar ključ.*

3 Nestandardne supstitucijske šifre

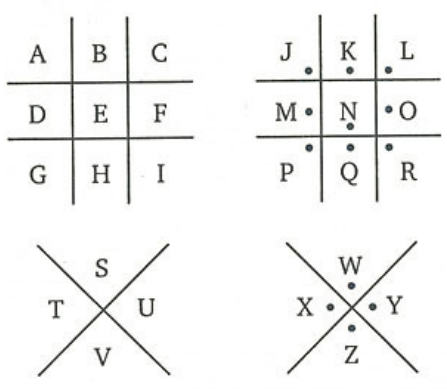
3.1 Pigpen šifra

Pigpen (engl. svinjac) šifra je jedna od monoalfabetskih supstitucijskih šifri u kojoj se slova zamjenjuju simbolima koji su dijelovi rešetke. Ova šifra dobila je ime po načinu na koji se slova odvajaju linijama, baš poput svinja u svinjcu. Pigpen šifra još je poznata kao masonska šifra koju je koristilo masonsko društvo otprilike početkom 18. stoljeća. Masonsko društvo ovu je šifru uglavnom koristilo kako bi se zaštitili neki od povijesnih zapisa i zapisi o obredima. Na Slici 1 možemo vidjeti osnovni oblik pigpen šifre.



Slika 1: *Osnovni oblik pigpen šifre*

Dakle, prvo nacrtamo polje kao kad bismo crtali polja za igru „križić-kružić" i veliko slovo X, a potom ponovno nacrtamo ta ista polja, ali tako da u svakom odjeljku stavimo točku, baš kao što je prikazano na Slici 1.
Abecedna slova ispišemo u sva polja na crtežima. Slova ispisujemo proizvoljnim poretkom. Primjerice, na Slici 2 možemo vidjeti da su abecedna slova poredana prema desno u svakom retku križić-kružić tablice, od prvog prema zadnjem. Međutim, u X uzorku slova idu od gornjeg nalijevo, pa desno i završava s donjim elementom.



Slika 2: *Osnovni oblik pigpen šifre s rasporedom slova po vlastitoj želji*

Poruku šifriramo na način da se svako slovo zamjenjuje crtežom polja u kojem se nalazi.

Primjer 29. *Šifrirajmo poruku*

Djela, ne riječi

pigpen šifrom. Šifrat je prikazan na Slici 3.



Slika 3: *Šifrat dobiven pigpen šifrom*

Primjer 30. *Neka je šifrat prikazan na Slici 4.*



Slika 4: *Šifrat dobiven pigpen šifrom*

Pomoću Slike 2 dešifriramo poruku i dobivamo otvoreni tekst

danas je prvi dan proljeća.

3.2 Polybiusov kvadrat

Polybiusov kvadrat izmislio je grčki povjesničar i znanstvenik Polybius. Polybius (200.pr.Kr.-118.pr.Kr.) je poznati grčki povjesničar i znanstvenik. Izmislio je kvadrat u svrhu smanjivanja broja znakova u tekstu. U Tablici 18 možemo vidjeti osnovni oblik Polybiusovog kvadrata s engleskom abecedom. Dakle, slova engleske abecede zapisujemo u 5×5 matricu. Redovi i stupci se numeriraju od 1 do 5 tako da svako slovo predstavlja odgovarajući par retka i stupca.

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I/J	K
3	L	M	N	O	P
4	Q	R	S	T	V
5	V	W	X	Y	Z

Tablica 18: *Polybiusov kvadrat s engleskom abecedom*

Možemo primijetiti da slova I i J dijele istu ćeliju. Također, može se dogoditi da slova V i W dijele istu ćeliju, ovisno o kojoj se vrsti abecede radi. No, problem određivanja koje ćemo slovo uzeti, možemo iščitati iz samoga konteksta poruke. Dakle, slova zamjenjujemo brojevima retka i stupca u kojem se to slovo nalazi. Primjerice, riječ **MORE** zapisali bismo kao 32344215. Međutim, slova u tablici možemo zapisati s nekom ključnom riječi.
Primjerice, kvadrat s ključnom riječi **sladoled** možemo zapisati na sljedeći način kao što je prikazano u Tablici 19:

	1	2	3	4	5
1	S	L	A	D	O
2	E	B	C	F	G
3	H	I	J	K	M
4	N	P	Q	R	T
5	U	V/W	X	Y	Z

Tablica 19: *Polybiusov kvadrat s engleskom abecedom s ključnom riječi SLADOLED*

Primjer 31. *Šifrirajmo otvoreni tekst:*

pomoću Polybiusovog kvadrata s ključnom riječi MJESEC.
Rješenje:
Najprije formirajmo Polybiusov kvadrat. Kako se radi o otvorenom tekstu na hrvatskom jeziku, možemo poistovijetiti slova V i W.

	1	2	3	4	5
1	M	J	E	S	C
2	A	B	D	F	G
3	H	I	K	L	N
4	O	P	Q	R	T
5	U	V/W	X	Y	Z

Tablica 20: *Polybiusov kvadrat s ključnom riječi MJESEC*

Sada šifrirajmo svako slovo posebno pomoću brojeva retka i stupca u kojima se to slovo nalazi. Slovo P šifrirat ćemo s 42 *jer se nalazi u četvrtom retku i drugom stupcu. Slovo O šifrirat ćemo s* 4 *jer se nalazi u četvrtom retku i prvom stupcu. Slovo D šifrirat ćemo s* 23 *jer se nalazi u drugom retku i trećem stupcu. Postupak nastavljamo sve dok ne dobijemo sljedeći šifrat:*
42 41 23 32 12 13 34 32 42 21 52 34 21 23 21 12**.**

Primjer 32. *Dešifrirajmo šifrat*
31 23 43 23 51 11 21 44 24 41 23 25 43 44 52 23 43 14 *ukoliko je poznato da je otvoreni tekst šifriran Polybiusovim kvadratom s ključnom riječi JUPITER.*
Rješenje:
Formirajmo Polybiusov kvadrat s ključnom riječi JUPITER kao što je prikazano u Tablici 21.

	1	2	3	4	5
1	J	U	P	I	T
2	E	R	A	B	C
3	D	F	G	H	K
4	L	M	N	O	Q
5	S	V/W	X	Y	Z

Tablica 21: *Polybiusov kvadrat s ključnom riječi JUPITER*

Dakle, prvo dešifrirajmo prvu riječ. Razdvojimo znamenke na grupe od po dvije. Imamo 31 23 43 23 51. *Slovo otvorenog teksta kojem odgovara šifrat* 31 *pronaći ćemo tako da pogledamo koje se slovo nalazi u trećem retku i prvom stupcu tablice. Šifrat* 31 *odgovara slovu D. Slovo otvorenog teksta kojem odgovara šifrat* 23 *iščitamo iz Tablice 21 tako da nađemo slovo koje se nalazi u drugom retku i trećem stupcu. Šifrat* 23 *odgovara slovu A. Postupak nastavljamo analogno dalje sve dok ne dobijemo otvoreni tekst koji glasi:*

danas je oblačno vani.

3.3 Nasumične supstitucijske šifre

Sve supstitucijske šifre obrađene u ovom radu karakteristične su po tome što su koristile abecedu ispisanu prema pravilima karakterističnim za šifru koju koristimo. Prednost takvih šifri je ta što za njihovo dešifriranje nije potrebno nositi ključ.
Međutim, nasumična supstitucijska šifra jest šifra koje je konstruirana bez ikakvih pravila, odnosno, uz svako slovo abecede stavimo bilo koji znak ili slovo. Nasumične su šifre specifične po tome što je njihovo probijanje izrazito teško, odnosno, puno teže od probijanja šifri temeljenih na jednostavnim sustavima. Jedan primjer iz svakodnevnog života korištenja nasumičnih supstitucijskih šifri su detektivske priče i romani koji su temeljili svoje glavne dijelove radnje upravo na tim šiframa. Jedna od poznatih priča je priča Edgara Allana Poea, „The Gold Bug", u kojoj šifra koristi brojeve i simbole. Također, poznat je članak Davida Kahna nazvan „The Encyclopedia Americana" u kojem je opisan jednostavan jednostruki sustav, odnosno šifra koju su koristili komunistički agenti u Drugom svjetskom ratu. Ta je šifra doista neprobojna te njena kompliciranost i potreba za generiranjem ključa za svaku šifru nije praktična za svakodnevnu upotrebu.

Na Slici 5 možemo vidjeti abecedu kodiranu simbolima nasumične supstitucijske šifre.

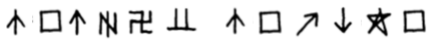


Slika 5: *Nasumična supstitucijska šifra*

Primjer 33. *Šifrirajmo poruku:*

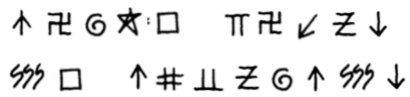
požuri polako

nasumičnom supstitucijskom šifrom.
Rješenje možemo vidjeti na Slici 6.



Slika 6: *Šifrirana poruka nasumičnom supstitucijskom šifrom*

Primjer 34. *Dešifrirajmo poruku:*



Slika 7: *Šifrirana poruka nasumičnom supstitucijskom šifrom*

nasumičnom supstitucijskom šifrom.
Rješenje:

preko trnja do zvijezda.

3.4 Shadowljev kod

Poznati misteriozni borac protiv zločina Shadow u 30-im godinama prošlog stoljeća bio je junak popularnog časopisa i popularne radijske emisije Street & Smith. Obučen u crno, Shadow se neprimjetno kretao kroz tamu kako bi se borio protiv zla. Maxwell Grant (1897. - 1985.) je poznati američki pisac koji je pisao priče o Shadowu te je često u priče uključivao vrlo čudne šifrirane poruke. Na Slici 8 možemo vidjeti jednu od najboljih šifri iz gore navedene priče koja se nalazi u noveli „The Chain of Death".

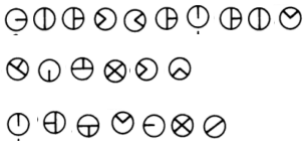


Slika 8: *Shadowljev kod*

Na dnu Slike 8 možemo vidjeti četiri simbola koja se mogu ubaciti na bilo koje mjesto u šifratu. Svaki od tih simbola prikazuje kako se stranica, na kojoj se nalazi šifrat, mora okrenuti za nastavak dešifriranja. Stranica, na kojoj se nalazi šifrat, mora biti tako okrenuta sve dok ne dođemo do jednog od tih četiriju simbola koji

će nam ukazati kako okrenuti stranicu u tom trenutku. Crta u svakom od ta četiri simbola ukazuje koja od stranica papira treba biti gornja stranica. Dakle, ukoliko se u tekstu pojavi simbol označen s brojem 1, kao na Slici 8, to znači da papir treba ostati kako je dotad bio, tj. u normalnom položaju. Nadalje, ukoliko se u tekstu pojavi simbol označen s brojem 4, kao na Slici 8, to znači da je potrebno okrenuti papir udesno tako da lijevi rub papira postane gornji rub i tako dalje. Pogledajmo na sljedećem primjeru kako poruka može izgledati šifrirana Shadowljevim kodom.

Primjer 35. *Poruka* ***hrabroga sreća prati*** *može izgledati ovako:*



Slika 9: *Poruka šifrirana Shadowljevim kodom*

Primjer 36. *Dešifirajmo poruku:*



Slika 10: *Poruka šifrirana Shadowljevim kodom*

Rješenje:

izgled vara

Literatura

[1] G. Baumslag, B. Fine, M. Kreuzer, G. Rosenberger, *A Course in Mathematical Cryptography*, De Gruyter, Boston, 2015.

[2] A. Dujella, *Uvod u teoriju brojeva*, PMF-Matematički odjel, Sveučilište u Zagrebu, skripta, 2003.

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

[4] M. Gardner, *Codes, ciphers and secret writing*, Dover Publications, New York, 1972.

[5] I. Matić, *Uvod u teoriju brojeva*, Odjel za matematiku, Sveučilište u Osijeku, 2015.

Sažetak

U ovom radu bavili smo se supstitucijskim šiframa kao što su monoalfabetske supstitucijske šifre i nekima od nestandardnih supsticijskih šifri. Na samom početku rada naveli smo definicije, teoreme i rezultate iz područja algebre i teorije brojeva koji su nužni za praćenje daljnih rezultata u radu. Definirali smo supstitucijske šifre i na različitim primjerima proveli smo postupak šifriranja i dešifriranja istih. Prikazali smo šifre poput Cezarove i afine šifre, pigpen šifre i Polybiusovog kvadrata. Za svaku od ovih šifri naveli smo različite primjere na kojima smo pokazali postupke šifriranja i dešifriranja po pravilu za svaku navedenu šifru. Na kraju smo rada prikazali šifru koju je koristio serijski ubojica Zodiac, čiji šifrati već nekoliko godina nisu dekriptirani.

Ključne riječi:

Supstitucijske šifre, Cezarova šifra, Cezarova šifra s ključnom riječi, afina šifra, pigpen šifra, Polybiusov kvadrat, nasumične supstitucijske šifre Shadowljev kod

Summary

This paper elaborates on substitution ciphers such as monoalphabetic ciphers and some non-standard substitution ciphers. The paper starts with the definitions, theorems and results in the field of algebra and number theory all of which are essential for the paper scope and results. Upon defining the substitution ciphers, the procedures of ciphering and deciphering are exemplified, namely the Caesar, affine, pigpen and Polybius square ciphers are elaborate on. Each of the ciphers are exemplified and the procedures of ciphering and deciphering illustrated. Finally, the cipher used by the serial murderer Zodiac, whose ciphers have not been deciphered yet, is described.

Keywords:

Substitution ciphers, Caesar cipher, Caesar key word cipher, affine cipher, pigpen cipher, Polybius square, random substitution ciphers, Shadow cipher

Životopis

Rođena sam 11. veljače 1995. u Osijeku. Osnovnu školu „Vladimir Nazor" završila sam 2009. godine. Tijekom osnovne škole, točnije 2003., upisala sam Osnovnu glazbenu školu „Ivan Goran Kovačić" u Đakovu te ju završila 2009. godine s odličnim uspjehom. Iste sam godine upisala Gimnaziju A. G. Matoša (opći smjer) u Đakovu. Srednju sam školu završila 2013. s odličnim uspjehom i položila državnu maturu. Iste sam godine upisala Preddiplomski studij matematike na Odjelu za matematiku Sveučilišta u Osijeku. 2014. godine prebacila sam se na Sveučilišni nastavnički studij matematike i informatike na Odjelu za matematiku.