# Monoalfabetske supstitucijske šifre

**Božić, Lea**

Sveučilište J.J. Strossmayera u Osijeku
Odjel za matematiku
Sveučilišni diplomski studij matematike - financijska matematika i statistika

**Lea Božić**

# Monoalfabetske supstitucijske šifre

Diplomski rad

Osijek, 2017.

Sveučilište J.J. Strossmayera u Osijeku
Odjel za matematiku
Sveučilišni diplomski studij matematike - financijska matematika i statistika

**Lea Božić**

# Monoalfabetske supstitucijske šifre

Diplomski rad

Mentor: doc. dr. sc. Ivan Soldo

Osijek, 2017.

# Sadržaj

# Uvod

Cilj ovog diplomskog rada je opisati kriptoanalizu nekih monoalfabetskih supstitucijskih šifri. Najprije navodimo neke definicije i rezultate koji su potrebni kako bi se uspješno pratio sadržaj rada. Nakon toga, definirat ćemo monoalfabetske supstitucijske šifre te na primjerima pokazati šifriranje i dešifriranje ovih šifri. Isto ćemo napraviti za neke inačice monoalfabetskih šifri. Osim hebrejske, Cezarove i afine šifre gdje se slova zamijenjuju slovima, objasnit ćemo pigpen šifru u kojoj se slova zamijenjuju simbolima te šifriranje Polybiusovim kvadratom gdje se slovo šifrira s dva broja. Na kraju objašnjavamo homofone supstitucijske šifre u kojima se slovo zamijenjuje s više različitih znakova. Jedan primjer ovakve šifre je šifra kojom se koristio serijski ubojica Zodiac u svojim pismima. Neki dijelovi njegovih šifrata do danas nisu dekriptirani.

*Kriptologija* je znanost koja se bavi izučavanjem i definiranjem metoda za zaštitu informacija (šifriranjem) i izučavanjem i pronalaženjem metoda za otkrivanje šifriranih informacija (dekriptiranjem). U tu svrhu koristi znanja iz matematike, statistike i lingvistike. Rezultate kriptologije prvenstveno koriste oružane snage i diplomatska služba, a razvojem telekomunikacija i mnoge druge službe. Kriptologija obuhvaća kriptografiju i kriptoanalizu.

*Kriptografija* je znanstvena disciplina koja se bavi proučavanjem metoda koje omogućuju komunikacijsku sigurnost između dvije osobe - pošiljatelja i primatelja poruke (u kriptografskoj literaturi često nazvani Alice i Bob). Za razliku od steganografije u kojoj se skriva sama postojanost poruke, kod kriptografije je cilj da ako poruka dođe u ruke protivnika (u kriptografskoj literaturi često nazvanog Oscar ili Eve), on tu poruku ne bi trebao razumjeti. Riječ kriptografija dolazi iz grčkog jezika i znači tajnopis.

Otvoreni tekst (*engl. plaintext*) je poruka koju pošiljatelj želi poslati primatelju. On tu poruku šifrira kako bi zaštitio poruku od potencijalnog protivnika, što podrazumijeva transformacije po unaprijed dogovorenom pravilu ili ključu. Taj postupak se zove šifriranje ili kriptiranje. Šifriranjem se dobiva šifrat (*engl. chipertext*) ili kriptogram. Primatelj, kako je upoznat s pravilom šifriranja poruke, lako otkrije otvoreni tekst, odnosno, dešifrira poruku, dok protivnik s time ima poteškoće. Matematička funkcija koja se koristi za šifriranje ili dešifriranje se naziva kriptografski algoritam ili šifra. Ovdje se radi o dvije funkcije koje preslikavaju elemente otvorenog teksta u elemente šifrata i obrnuto. Biraju se iz određene familije funkcija,

ovisno o ključu. Prostor ključeva je skup svih mogućih vrijednosti ključeva.

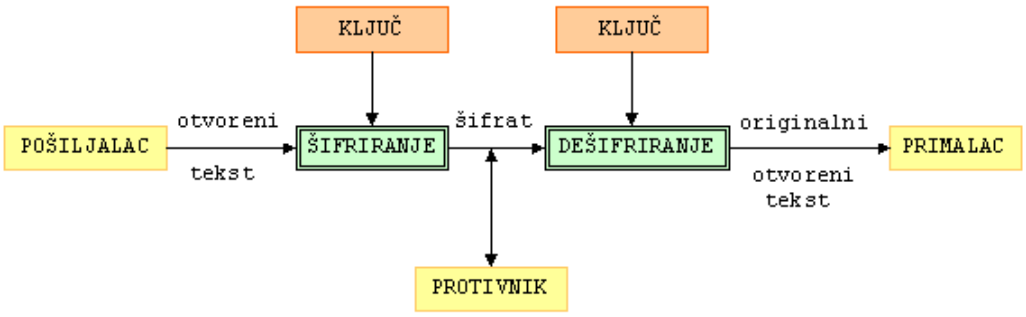
**Definicija 0.1.** *Kriptosustav je uređena petorka* $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ *za koju vrijedi:*

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 $y$, tj.

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

primaoc poruke neće znati treba li $y$ dešifrirati u $x_1$ ili $x_2$.




Slika 1: Primjena kriptografskog algoritma

Pošiljatelj i primatelj najprije biraju ključ $K \in \mathcal{K}$. Pošiljatelj sada šalje poruku $x = x_1x_2...x_n$ za neki cijeli broj $n > 0$, $x_i \in \mathcal{P}$, $0 < i < n + 1$. Svaki $x_i$ je šifriran

funkcijom $e_k$ s unaprijed dogovorenim ključem $K$. Pošiljatelj pomoću $y_i = e_K(x_i)$, $0 < i < n + 1$ dobiva šifrat $y = y_1y_2...y_n$ te ga šalje nesigurnim komunikacijskim kanalom primatelju. Kad primatelj dobije poruku takvog oblika, dešifrira ju funkcijom $d_K$ te dobiva otvoreni tekst.

Kriptografija se stoljećima primjenjivala kako bi se osigurala tajnost vojne i diplomatske komunikacije. Danas se poruke razmjenuju globalnim računalnim i komunikacijskim mrežama pa se kriptografija bavi podatcima u digitalnom obliku, a postupci kriptiranja i dekriptiranja provode se uz pomoć računala. Samim time, suvremena kriptografija se uglavnom oslanja na računarstvo.

*Kriptoanaliza* ili dekriptiranje je znanstvena disciplina koja proučava postupke za čitanje skrivenih poruka bez poznavanja pravila šifriranja i ključa pri čemu koristi znanja iz matematike, statistike i lingvistike. Kriptoanaliza se može provesti nagađanjem ključa ili korištenjem informacija o sustavu koji se napada. 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 točka početka kriptoanalize je 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.
Napadom zovemo svaku usmjerenu radnju kriptoanalitičara. Razlikujemo pet osnovnih napada na kriptosustave:

1. Napad poznatim šifratom (*engl. Ciphertext-only*): Kriptoanalitičar ima pristup samo šifratu od nekoliko poruka šifriranih istim algoritmom, a želi otkriti otvoreni tekst i ključ;

2. Napad poznatim otvorenim tekstom (*engl. Known-plaintext*): Kriptoanalitičar poznaje šifrat ($y$) i njemu odgovarajući otvoreni tekst ($x$), a cilj mu je otkriti ključ ili neki algoritam za dešifriranje poruka tim ključem;

3. Napad odabranim otvorenim tekstom (*engl. Chosen-plaintext*): Kriptoanalitičar može odabrati otvoreni tekst koji će biti šifriran te može dobiti njegov šifrat;

4. Napad odabranim šifratom (*engl. Chosen-ciphertext*): Kriptoanalitičar je dobio pristup alatu za dešifriranje pa može odabrati šifrat te dobiti odgovarajući otvoreni tekst, a cilj mu je otkriti ključ za dešifriranje;

5. Potkupljivanje, ucjena, krađa i slično.

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 otvorenog teksta se permutiraju (premještaju). Na primjer, ako riječ MAJKA šifriramo u AAJMK, načinili smo transpoziciju. Kod supstitucijskih šifri se svaki element otvorenog teksta (bit, slovo, grupa bitova ili slova) zamjenjuje nekim drugim slovom, bitom ili znakom prema unaprijed utvrđenoj transformaciji. Kod ovakve vrste šifri poredak ostaje isti, ali se za svako slovo koristi neki drugi simbol. Postoji nekoliko podjela supstitucijskih šifri. Jedna od njih je na monoalfabetske i polialfabetske šifre.
Kod monoalfabetskih supstitucijskih šifri više slova ne mogu biti zamijenjena istim znakom. Uobičajeno je da se svako slovo zamijenjuje točno jednim znakom. Ako je šifra za slovo A slovo B, to znači da svaki puta kada se u šifri pojavi slovo B, ono znači slovo A. Ovdje pripadaju i homofone supstitucijske šifre u kojima se slovo šifrira s više različitih znakova. Za razliku od monoalfabetskih, kod polialfabetskih šifri slovo je šifrirano s više slova te više slova može biti šifrirano istim slovom, ovisno o poziciji u tekstu.
Razlikujemo još i monogramske i poligramske supstitucijske šifre. Kod monogramskih šifara slovo je zamijenjeno točno jednim slovom ili znakom za razliku od poligramskih gdje je više slova zamjenjeno s nekoliko simbola. Kod bigramskih šifri dva znaka se zamijenjuju s neka dva druga.

U svakodnevnom životu susrećemo zamjene slova i riječi simbolima. To su na primjer znakovni jezik, točke i povlake u Morseovoj abecedi.

# 1 Osnovni pojmovi

U ovom poglavlju navest ćemo neke definicije i rezultate iz algebre i teorije brojeva koji su potrebni kako bi se uspješno pratio sadržaj ovog diplomskog rada - kriptografija i kriptoanaliza monoalfabetskih supstitucijskih šifri.

**Definicija 1.1.** *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.
Nešto više o algebarskim strukturama može se vidjeti i proučiti iz [6].

**Definicija 1.2.** *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 1.1.** *Broj 20 je djeljiv s 5, odnosno 5 dijeli 20 jer je $20 = 5 \cdot 4$. To zapisujemo s $5|20$. 5 je djelitelj broja 20, a 20 je višekratnik broja 5.*
*Broj 20 nije djeljiv sa 7, odnosno 7 ne dijeli 20 jer ne postoji cijeli broj $x$ takav da je $20 = 5 \cdot x$. To zapisujemo $7 \nmid 20$.*

**Definicija 1.3.** *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 $(b,c)$.*

**Primjer 1.2.** *Zajednički djelitelji brojeva 20 i 30 su 2,5 i 10. $(20, 30) = 10$.*

**Teorem 1.1** (vidi [2, Teorem 1.1])**.** *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 1.2** (vidi [2, Teorem 1.5])**.** *Neka su $b$ i $c > 0$ cijeli brojevi. Pretpostavimo da je uzastopnom primjenom 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.*

**Primjer 1.3.** *Odredimo $d = (1005, 820)$ primjenom Euklidovog algoritma.*
*Rješenje:*
*Imamo*

$$\begin{aligned} 1005 &= 1 \cdot 820 + 185 \\ 820 &= 4 \cdot 185 + 80 \\ 185 &= 2 \cdot 80 + 25 \\ 80 &= 3 \cdot 25 + 5 \\ 25 &= 5 \cdot 5. \end{aligned}$$

*Dakle, $d = (1005, 820) = 5$.*
*Prikažimo $d = 5$ kao linearnu kombinaciju brojeva 252 i 198:*

$$\begin{aligned} 5 &= 80 - 3 \cdot 25 = 80 - 3(185 - 2 \cdot 80) = 7 \cdot 80 - 3 \cdot 185 \\ &= 7(820 - 4 \cdot 185) - 3 \cdot 185 = 7 \cdot 820 - 31 \cdot 185 \\ &= 7 \cdot 820 - 31(1005 - 820) = 38 \cdot 820 - 31 \cdot 1005. \end{aligned}$$

Rješenja jednadžbe $bx + cy = (b, c)$ dobit ćemo na sljedeći način.
Ako je:

$$\begin{aligned} r_{-1} = b, r_0 = c; r_i = r_{i-2} - q_i r_{i-1}; \\ x_{-1} = 1, x_0 = 0; x_i = x_{i-2} - q_i x_{i-1}; \\ y_{-1} = 0, y_0 = 1; y_i = y_{i-2} - q_i y_{i-1}, \end{aligned}$$

tada je

$$bx_i + cy_i = r_i, \text{ za } i = -1, 0, 1, \ldots, j + 1.$$

Vrijedi:

$$bx_j + cy_j = (b, c).$$

**Primjer 1.4.** *Nađimo cijele brojeve $x$ i $y$ takve da je $1005x + 820y = d$, gdje je $d = (1005, 820)$.*
*Rješenje:*
*U prethodnom primjeru smo, pomoću Euklidovog algoritma, odredili $d = (1005, 820) = 5$. U Tablici 1 dan je postupak računanja brojeva $x$ i $y$.*

| i | -1 | 0 | 1 | 2 | 3 | 4 |
|---|---|---|---|---|---|---|
| $q_i$ | | | 1 | 4 | 2 | 3 |
| $x_i$ | 1 | 0 | 1 | -4 | 9 | -31 |
| $y_i$ | 0 | 1 | -1 | 5 | -11 | 38 |

Tablica 1: *Postupak računanja brojeva $x$ i $y$*

*Dakle,* $1005 \cdot (-31) + 820 \cdot 38 = 5$.

**Definicija 1.4.** *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 1.5.** *Kažemo da su cijeli brojevi $a$ i $b$ relativno prosti ako je $(a, b) = 1$.*

**Primjer 1.5.** *Brojevi 20 i 7 su relativno prosti jer je $(20, 7) = 1$. Brojevi 20 i 30 nisu relativno prosti jer je $(20, 30) = 10 \neq 1$.*

**Definicija 1.6.** *Ako cijeli broj $m \neq 0$ dijeli razliku $a-b$, kažemo da je $a$ kongruentan $b$ modulo $m$ i pišemo*

$$a \equiv b \pmod{m}.$$

*U protivnom, kažemo da $a$ nije kongruentan $b$ modulo $m$ i pišemo*

$$a \not\equiv b \pmod{m}.$$

Kako je $a - b$ djeljivo s $m$ onda i samo onda ako je djeljivo s $-m$, usredotočit ćemo se samo na pozitivne module $m > 0$.

**Primjer 1.6.** *Ako bi izračunali 55 modulo 13, pisali bi $55 = 4 \cdot 13 + 3$. Kako je $0 \leq 3 < 13$, slijedi da je $55 \equiv 3 \pmod{13}$.*
*Da bismo izračunali 9 modulo 6, pišemo $9 = 1 \cdot 6 + 3$. Kako je $0 \leq 3 < 6$, slijedi da je $9 \equiv 3 \pmod{6}$.*
*Da bi izračunali $-55$ modulo 13, imamo $-55 = -4 \cdot (13) + 1$. Kako je $0 \leq 1 < 13$, slijedi da je $55 \equiv 1 \pmod{13}$.*

Navedimo sada neka osnovna svojstva kongruencija.

**Propozicija 1.1** (vidi [2, Propozicija 2.1.]). *Relacija "biti kongruentan modulo $m$" je relacija ekvivalencije na skupu $\mathbb{Z}$.*

**Propozicija 1.2** (vidi [2, Propozicija 2.2.]). *Neka su $a$, $b$, $c$, $d$ cijeli brojevi.*

1. *Ako je $a \equiv b \pmod{m}$ i $c \equiv d \pmod{m}$, onda je*

$$a + c \equiv b + d \pmod{m},$$
$$a - c \equiv b - d \pmod{m},$$
$$ac \equiv bd \pmod{m}.$$

2. *Ako je $a \equiv b \pmod{m}$ i $d|m$, onda je $a \equiv b \pmod{d}$.*

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

**Propozicija 1.3** (vidi [2, Propozicija 2.3.]). *Neka je $f$ polinom s cjelobrojnim koeficijentima. Ako je $a \equiv b \pmod{m}$, onda je $f(a) \equiv f(b) \pmod{m}$.*

**Teorem 1.3** (vidi [2, Teorem 2.4.]). *Vrijedi: $ax \equiv ay \pmod{m}$ ako i samo ako $x \equiv y \pmod{\frac{m}{(a,m)}}$. Specijalno, ako je $ax \equiv ay \pmod{m}$ i $(a, m) = 1$, onda je $x \equiv y \pmod{m}$.*

**Definicija 1.7.** *Skup $\{x_1, \ldots, x_m\}$ se zove potpuni sustav ostataka modulo $m$ ako za svaki $y \in \mathbb{Z}$ postoji jedinstveni $x_j \in \mathbb{Z}$ sa svojstvom $y \equiv x_j \pmod{m}$.*

Postoji beskonačno mnogo potpunih ostataka modulo $m$. Jedan od njih je sustav najmanjih nenegatinih ostataka:

$$\{0, 1, \ldots, m - 1\}.$$

**Primjer 1.7.** *Potpuni sustav ostataka modulo 12 je $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$. Ovo je sustav najmanjih negativnih ostataka. Još neki potpuni sustavi ostataka modulo 12 su:*

$$\{0, 7, 14, 21, 28, 35, 42, 49, 56, 63, 70, 77\},$$
$$\{0, 5, 10, 15, 20, 25, 30, 35, 40, 45, 50, 55\},$$
$$\{12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 35\}.$$

**Definicija 1.8.** *Klasa ostataka modulo $m$ je skup svih cijelih brojeva koji su kongruentni broju $x$ pri dijeljenju s $m$. Označavamo ju s $[x]$ i pišemo:*

$$[x] = \{x + k \cdot m : k \in \mathbb{Z}\}.$$

**Primjer 1.8.** *Klase ostataka modulo 5 su:*

$$\begin{aligned}
[0] &= \{\ldots, -10, -5, 0, 5, 10, 15, 20, 25, \ldots\}, \\
[1] &= \{\ldots, -9, -4, 1, 6, 11, 16, 21, 26, \ldots\}, \\
[2] &= \{\ldots, -8, -3, 2, 7, 12, 17, 22, 27, \ldots\}, \\
[3] &= \{\ldots, -7, -2, 3, 8, 13, 18, 23, 28, \ldots\}, \\
[4] &= \{\ldots, -6, -1, 4, 9, 14, 19, 24, 29, \ldots\}.
\end{aligned}$$

**Definicija 1.9.** *Promotrimo potpun sustav ostataka* $\{x_1, ..., x_m\}$ *modulo* $m$. *Na skupu klasa ostataka* $[x_1], ..., [x_m]$ *definiramo*

1. $[x_i] + [x_j] = [x_i + x_j]$,
2. $[x_i] \cdot [x_j] = [x_i \cdot x_j]$, $i, j = 1, ..., m$.

**Teorem 1.4** (vidi [1, Theorem 5.2.7.])**.** *Za pozitivan cijeli broj* $m$, *skup klasa ostataka modulo* $m$

$$\{[0], \ldots, [n-1]\}$$

*tvori komutativni prsten s jedinicom s operacijama iz prethodne definicije. Njega nazivamo prsten cijelih brojeva modulo* $m$ *i označavamo sa* $\mathbb{Z}_m$. *Neutralni element je* $[0]$, *a jedinica je* $[1]$.

Dakle, $\mathbb{Z}_m = \{0, 1, 2, \ldots, m-1\}$, s operacijama zbrajanja i množenja modulo $m$. Element $[x]$ u $\mathbb{Z}_m$ označavat ćemo s $x$.

**Primjer 1.9.** *Promotrimo zbrajanje i množenje u* $\mathbb{Z}_7$.
*Imamo* $13 \cdot 3 = 39 \equiv 4 \pmod 7$, *pa je u* $\mathbb{Z}_7$ $13 \cdot 3 = 4$.
*Analogno,* $13 + 3 = 16 \equiv 2 \pmod 7$, *pa je u* $\mathbb{Z}_7$ $13 + 3 = 2$.

**Teorem 1.5** (vidi [2, Teorem 2.6.])**.** *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 1.10.** *Kongruencija* $7x \equiv 11 (\mathrm{mod} 14)$ *nema rješenja jer* $d = nzd(7, 14) = 7$ *ne dijeli 11.*
*Kongruencija* $14x \equiv 4 \pmod{22}$ *ima rješenja jer* $d = nzd(14, 22) = 2$ *dijeli 4. Ova kongruencija ima točno dva rješenja.*
*Kongruencija* $21x \equiv 6 (\mathrm{mod}\ 33)$ *ima rješenja jer* $d = nzd(21, 33) = 3$ *i dijeli 6. Ova kongruencija ima točno tri rješenja.*

Ako je $p$ prost broj i $p$ ne dijeli $a$, kongruencija $ax \equiv b \pmod{p}$ ima jedinstveno rješenje. Pitamo se kako riješiti kongruenciju $a'x \equiv b' \pmod{m'}$, 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 $v$ se mogu naći pomoću Euklidovog algoritma. Dobijemo $a'u \equiv 1 \pmod{m'}$ pa je $x \equiv ub' \pmod{m'}$.

**Primjer 1.11.** *Riješimo kongruenciju* $820x \equiv 15 \pmod{1005}$.
*Rješenje:*
*Kako je* $(820, 1005) = 5$ *i* $5|15$*, ova kongruencija ima pet rješenja. Primjenjujući treće svojstvo Propozicije 1.2., treba riješiti kongruenciju* $164x \equiv 3 \pmod{201}$.
*Primijenimo Euklidov algoritam:*

$$\begin{aligned} 201 &= 164 \cdot 1 + 37 \\ 164 &= 37 \cdot 4 + 16 \\ 37 &= 16 \cdot 2 + 5 \\ 16 &= 5 \cdot 3 + 1 \\ 5 &= 1 \cdot 5. \end{aligned}$$

| i | -1 | 0 | 1 | 2 | 3 | 4 |
|---|---|---|---|---|---|---|
| $q_i$ | | | 1 | 4 | 2 | 3 |
| $y_i$ | 0 | 1 | -1 | 5 | -11 | 38 |

Tablica 2: *Postupak traženja rješenja kongruencije*

*Dakle, rješenje kongruencije* $164u \equiv 1 \pmod{201}$ *je* $u \equiv 38 \pmod{201}$ *pa je rješenje od* $164x \equiv 3 \pmod{201}$, $x \equiv 114 \pmod{201}$. *Rješenja polazne kongruencije su*

$$x \equiv 114, 315, 516, 717, 918 \pmod{1005}.$$

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

**Primjer 1.12.** *Pitamo se za koje vrijednosti a kongruencija* $ax \equiv b \pmod{26}$ *ima jedinstveno rješenje. Drugim riječima, tražimo brojeve a takve da je* $nzd(a, 26) = 1$.
*Vrijednosti parametra* $a \in \mathbb{Z}_{26}$ *su sljedeće:* $a = 1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25$.

**Definicija 1.10.** *Neka je $a \in \mathbb{Z}_m$. Multiplikativni inverz od a modulo m, u oznaci $a^{-1} \bmod m$, je element $a' \in \mathbb{Z}_m$ za koji vrijedi $aa' \equiv a'a \equiv 1 \pmod{m}$.*

Ako je $R$ komutativan prsten s jedinicom, tada je invertibilan element svaki koji posjeduje multiplikativni inverz. Element $a \in \mathbb{Z}_m$ je invertibilan ako je $nzd(a, m) = 1$. Ako multiplikativan inverz modulo $m$ postoji, on je jedinstven. Ako je $b = a^{-1}$, onda je $a = b^{-1}$. Ako je $p$ prost broj, svaki broj različit od nule na skupu $\mathbb{Z}_{26}$ ima multiplikativan inverz.

**Primjer 1.13.** *Pronađimo $7^{-1}$ u $\mathbb{Z}_{26}$.*
*Rješenje:*
*Kako je $7 \cdot 15 \equiv 1 \pmod{26}$, multiplikativni inverz od 7 modulo 26 jednak je 15. Dakle $7^{-1} = 15$ u $\mathbb{Z}_{26}$. Također, $15^{-1} = 7$ 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 1.11.** *Broj cijelih brojeva koji su relativno prosti s m na skupu $\mathbb{Z}_m$ označavamo s $\varphi(m)$, a funkciju $\varphi$ zovemo Eulerova funkcija.*

**Teorem 1.6** (vidi [2, Teorem 2.9])**.** *Ako je $(a, m) = 1$, onda je $a^{\varphi(m)} \equiv 1 \pmod{m}$.*

**Definicija 1.12.** *Funkciju $\vartheta : \mathbb{N} \to \mathbb{C}$ zovemo multiplikativna funkcija ako vrijedi:*

1. *$\vartheta(1) = 1$,*
2. *$\vartheta(mn) = \vartheta(m)\vartheta(n)$, $\forall m, n$ takve da je $(m, n) = 1$.*

**Teorem 1.7** (vidi [2, Teorem 2.11.])**.** *Eulerova funkcija je multiplikativna. Nadalje, za svaki prirodan broj $n > 1$ vrijedi*

$$\varphi(n) = n \prod_{p|n} (1 - \frac{1}{p}).$$

**Primjer 1.14.** *Izračunajmo koliko je brojeva relativno prosto s brojem 50 u sustavu $\mathbb{Z}_{50}$.*
*Rješenje:*
*Kako je $50 = 2^1 \cdot 5^2$, računamo $\varphi(50) = 50 \cdot (1 - \frac{1}{5}) \cdot (1 - \frac{1}{2}) = 20$. Dakle, 20 brojeva je relativno prosto s brojem 50 u sustavu modulo 50.*

# 2 Monoalfabetske supstitucijske šifre

Monoalfabetska supstitucijska šifra je najjednostavniji oblik kriptosustava sa supstitucijskim šiframa. Samim time taj kriptosustav nije siguran način komuniciranja preko nesigurnih kanala, odnosno, takve šifrate je vrlo lako razbiti i to u svega nekoliko minuta. Ovakve šifre nazivaju se jednostavnim supstitucijskim šiframa.

**Definicija 2.1.** *Neka je* $\mathcal{P} = \mathcal{C} = \mathbb{Z}_{26}$. *Skup* $\mathcal{K}$ *sastoji se od svih mogućih permutacija simbola* $0, 1, ..., 25$. *Za svaku permutaciju* $\pi \in \mathcal{K}$, *definiramo* $e_\pi(x) = \pi(x)$ *i* $d_\pi(y) = \pi^{-1}(y)$, *gdje je* $\pi^{-1}$ *permutacija inverzna* $\pi$.

Možemo pretpostaviti da $\mathcal{P}$ i $\mathcal{C}$ sadrže engleski alfabet od 26 slova. Funkciju šifriranja i dešifriranja promatramo kao permutaciju slova engleske abecede gdje je funkcija dešifriranja inverzna funkcija funkciji šifriranja. U tablicama 1 i 2 prikazan je primjer šifriranja i dešifriranja. 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 šifrirat ćemo 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, ako se u šifratu pojavi slovo A, njemu pripadno slovo otvorenog teksta je slovo i.

**Primjer 2.1.** *Poruku*

***close to the enemy,***

*koristeći Tablicu 3, zapisat ćemo u obliku* ***ZDTGI HT ICIRO.***
*Ako smo primili šifriranu poruku*

***HTQBO AG B JTTQ QBO,***

*koristeći Tablicu 4 dobijemo otvoreni tekst* ***today was a good day.***

Ne postoje stroga pravila šifriranja slova karakteristična za hrvatsku abecedu. Funkciju šifriranja i dešifriranja moguće je promatrati kao permutaciju slova hrvatske abecede. Primjer takvog šifriranja i dešifriranja dan je u sljedećoj tablici.

| 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 |

| 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 5: *Primjer šifriranja i dešifriranja supstitucijskom šifrom ako je otvoreni tekst pisan na hrvatskom jeziku*

**Primjer 2.2.** *Poruku*

***boj ne bije zlaćano oružje, već srce u junaka,***

*koristeći Tablicu 5, zapisat ćemo u obliku* ***ŠNE NJĐ ŠHEĐ VFČMČNJN NPIREĐ, LJĐM ZPLĐ I EINJČŽČ.***

Kod dešifriranja šifrata dobivenog na gore objašnjeni način primatelj poruke može imati problema. Ako se u šifratu pojavljuje NJ, to se može dešifrirati na dva načina $d_\pi(NJ) = n$ ili $d_\pi(N) = o$ i $d_\pi(J) = m$. Isto vrijedi ako se u šifratu pojave bigrami LJ i DŽ. Na primjer, šifrat **NJČPČLJNJN** može se dešifrirati

kao **omaracmomo**, **omaravomo**, **omaracmno**, **naracmomo**, **naracmno** ili **naravno**. Zbog toga je uobičajeno 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.

**Primjer 2.3.** *Poruku*

***boj ne bije zlaćano oružje, već srce u junaka,***

*koristeći Tablicu 3, zapisat ćemo kao* ***ETP CI EAPI UDBZBCT TYXVPI, LIZ GYZI PXCBNB****.*
*Ako smo primili šifrat*

***SYTDPIZI,***

*koristeći Tablicu 4 dešifrirat ćemo ga u otvoreni tekst* ***proljece****. Očito je da umjesto c čitamo ć, odnosno, riječ otvorenog teksta je* ***proljeće****.*

Prostor ključeva sadrži sve moguće permutacije slova engleske abecede što znači da on sadrži 26! elemenata. Ispitivati ručno koji od ključeva je ispravan bilo bi jako zamorno i dugotrajno. Međutim, monoalfabetske supstitucijske šifre moguće je dekriptirati koristeći svojstva jezika na kojem je pisan otvoreni tekst. Osnovna metoda je analiza frekvencije slova. Smatra se da je upotreba takve analize počela u 14. stoljeću iako neki znanstvenici tvrde da je ta metoda poznata i pet stoljeća ranije. Ideja je da se broji ponavljanje svakog slova u šifratu te se njihova distribucija uspoređuje s poznatim podacima o distribuciji slova u jeziku na kojem je napisan otvoreni tekst. Velika je vjerojatnost da će najfrekventnije slovo u šifratu odgovarati najfrekventnijem slovu otvorenog teksta. Naravno, što je tekst dulji, vjerojatnije je da će to biti baš tako. U Tablici 6 navedene su frekvencije slova u engleskom jeziku.

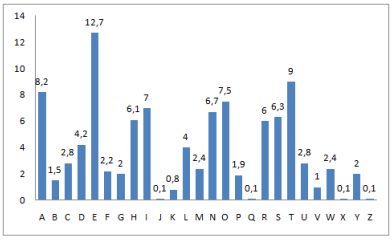
Kriptoanalitičaru može pomoći i poznavanje statističkih svojstava bigrama (skup od dva slova) te trigrama (skup od tri slova). Najčešći bigrami u engleskoj abecedi dani su u Tablici 7.

Najčešći trigrami u engleskoj abecedi su, u opadajućem redoslijedu:

THE (3.5%), ING(1.1%), AND(1.0%), HER, ERE, ENT, THA, NTH, WAS, ETH, FOR.

| Slovo | Postotak | Slovo | Postotak |
|---|---|---|---|
| A | 8.2 | N | 6.7 |
| B | 1.5 | O | 7.5 |
| C | 2.8 | P | 1.9 |
| D | 4.2 | Q | 0.1 |
| E | 12.7 | R | 6.0 |
| F | 2.2 | S | 6.3 |
| G | 2.0 | T | 9.0 |
| H | 6.1 | U | 2.8 |
| I | 7.0 | V | 1.0 |
| J | 0.1 | W | 2.4 |
| K | 0.8 | X | 0.1 |
| L | 4.0 | Y | 2.0 |
| M | 2.4 | Z | 0.1 |

Tablica 6: *Frekvencije slova engleskog jezika*




Slika 2: *Dijagram frekvencija slova engleskog jezika*

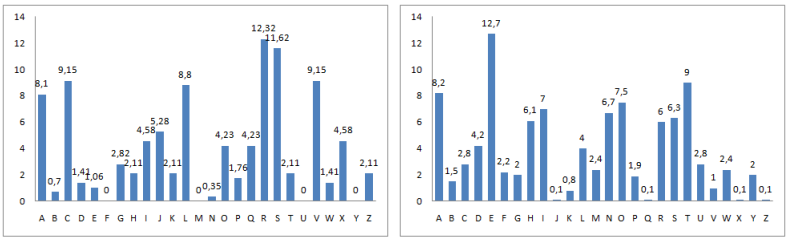
| Bigram | Postotak | Bigram | Postotak |
|---|---|---|---|
| TH | 3.15 | ON | 1.45 |
| HE | 2.51 | EA | 1.41 |
| AN | 1.72 | TI | 1.28 |
| IN | 1.69 | AT | 1.24 |
| ER | 1.54 | ST | 1.21 |
| RE | 1.48 | EN | 1.20 |
| ES | 1.45 | ND | 1.18 |

Tablica 7: Frekvencije bigrama u engleskom jeziku

Na temelju prethodnih analiza možemo uspješno dekriptirati šifrate dobivene monoalfabetskom supstitucijom teksta pisanog na engleskom jeziku što je objašnjeno

na sljedećem primjeru.

**Primjer 2.4.** *Dekriptirajmo šifrat:*
*CAR GLC L ZVVI IRLO HJQZASRXRI KP SAQC NRJP CDIIRX WALXZR, KDS CAR HROS SALS SARJR GLC XV SQTR SV KR OVCS, LC CAR GLC CAJQXBQXZ JLEQIOP ; CV CAR CRS SV GVJB LS VXWR SV RLS CVTR VH SAR VSARJ KQS. ARJ WAQX GLC EJRCCRI CV WOVCROP LZLQXCS ARJ HVVS, SALS SARJR GLC ALJIOP JVVT SV VERX ARJ TVDSA ; KDS CAR IQI QS LS OLCS, LXI TLXLZRI SV CGLOOVG L TVJCRO VH SAR ORHS-ALXI KQS.*
*Neka je poznato da je poruka šifrirana monoalfabetskom supstitucijskom šifrom te da je otvoreni tekst pisan na engleskom jeziku.*
*Rješenje:*
*Na dijagramima prikazanima na Slici 3 možemo vidjeti usporedbu frekvencije slova u zadanom šifratu s frekvencijom slova engleskog jezika.*




Slika 3: *Usporedba frekvencija slova u tekstu primjera s frekvencijama slova engleskog jezika*

*S dijagrama možemo naslutiti da* $e_\pi(e) = R$.
*Najčešći bigrami koji se pojavljuju pet puta su: AR, SA, GL, RO, SS.*
*Četiri puta pojavljuju se bigrami: RJ, VV, CA.*
*Kako su u engleskom jeziku najčešći bigrami TH i HE, možemo pretpostaviti kako je* $e_\pi(t) = S$ *i* $e_\pi(h) = A$. *Slovo S je drugo najfrekventnije slovo šifrata pa, kako je slovo t drugo najfrekventnije slovo engleskog alfabeta, ovo zaista ima smisla. Promotrimo sada simetrične bigrame. Najčešći u englesoj abecedi su ER i RE. U šifratu se četiri puta ponavlja bigram RJ i tri puta bigram JR. Kako smo već pretpostavili da je šifrat za slovo e slovo R, pretpostavimo da je* $e_\pi(r) = J$. *Provjerimo što samo do sad zaključili.*

*C**he** GLC L ZVVI I**e**LO HJQZ**hte**X**e**I KP **th**QC N**er**P CDII**e**X W**h**LXZ**e**, KD**t** C**he** He**O**t **th**L**t** **there** GLC XV **t**QT**e** **t**V K**e** OVC**t**, LC C**he** GLC C**hr**QXBQXZ **r**LEQIOP ; CV C**he** C**et** **t**V GV**r**B L**t** VXW**e** **t**V **e**L**t** CVT**e** VH **the** V**ther** KQ**t**. **her** W**h**QX GLC E**re**CC**e**I CV WOVC**e**OP LZLQXC**t** **her** HVVS, **th**L**t** **there** GLC **h**L**r**IOP **r**VVT **t**V VE**e**X **her** TVD**ht** ; KD**t** C**he** IQI Q**t** L**t** OLC**t**, LXI TLXLZ**e**I **nt**V CGLOOVG L TVJC**e**O VH **the** O**e**H**S**t-**h**LXI KQ**t**.*

*Vidimo da sve dosadašnje pretpostavke imaju smisla. Sada se naziru neke riječi:*

$$\textit{Che} \to \textit{the ili she (već imamo } d_\pi(S) = t) \to e_\pi(s) = C;$$
$$\textit{Slovo L se pojavljuje samo} \to d_\pi(l) = A \textit{ (član) ili } d_\pi(i) = I \textit{ (ja);}$$
$$\textit{thLt} \to d_\pi(L) = a \to e_\pi(a) = L.$$

*Našli smo šifrate za prva tri najfrekventnija slova engleskog jezika: E, T i A. Sljedeće najfrekventnije slovo je O. Pretpostavimo da je njegov šifrat slovo V (jer je to najfrekventnije slovo šifrata kojemu još nismo pridružili slovo otvorenog teksta)* $\to e_\pi(o) = V$*. Promotrimo što smo do sada zaključili.*

***she** G**as** **a** Z**oo**I I**ea**O H**r**QZ**hte**X**e**I KP **th**QC **er**JP **s**DII**e**X W**ha**XZ**e**, KD**t** **she** He**O**t **that** **there** G**as** X**o** **t**QT**e** **to** K**e** O**ost**, **as** **she** G**as** **shr**QXBQXZ **ra**EQIOP ; **so** **she** **set** **to** G**or**B **at** **o**XW**e** **to** **eat** **so**T**e** **o**H **the** **other** KQ**t**. **her** W**h**QX G**as** E**resse**I **so** WO**ose**OP **a**Z**a**QX**st** **her** H**oot**, **that** **there** G**as** **har**IOP **roo**T **to** **o**E**e**X **her** T**o**D**th** ; KD**t** **she** IQI Q**t** **at** O**ast**, **a**XI T**a**X**a**Z**e**I **to** **s**G**a**OO**o**G L T**orse**O **o**H **the** O**e**H**t-ha**XI KQ**t**.*

*Slično bismo nastavili dalje sve dok ne dobijemo otvoreni tekst. Na kraju dobijemo za funkciju šifriranja permutaciju prikazanu u Tablici 8.*

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

Tablica 8: *Supstitucija šifrata iz Primjera 12*

*Otvoreni tekst glasi:*

*She was a good deal frightened by this very sudden change, but she felt that there was no time to be lost, as she was shrinking rapidly ; so she set to work at once to eat some of the other bit. Her chin was pressed so closely against her foot, that there*

*was hardly room to open her mouth ; but she did it at last, and managed to swallow a morsel of the left-hand bit.*
*(Tekst je preuzet iz knjige Alice's adventures in Wonderland autora Lewisa Carolla.)*

Pri napadu na šifrat čiji otvoreni tekst je pisan na engleskom jeziku uvelike nam pomažu neke važne činjenice o engleskom jeziku:

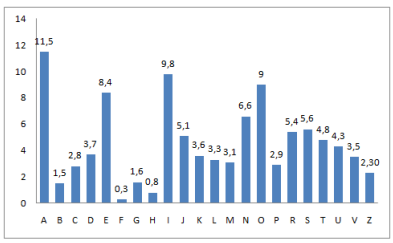
- Najčešća riječ od četiri slova je riječ THAT. Ova riječ počinje i završava istim slovom te u kriptoanalizi ima neprocijenjivu vrijednost. Ako se u šifratu pojavi riječ SJPS vrlo je vjerojatno da je to šifrat za riječ that.
- Najčešće korištene riječi od tri slova su THE i AND.
- Najčešći bigrami s dva jednaka slova su redom: LL, EE, SS, OO, TT, FF, RR, NN, PP, CC.
- Najčešće riječi od dva slova su redom OF, TO, IN.
- Najčešća slova koja se pojavljuju sama u rečenici su I i A.
- Slovo s kojim riječi najčešće počinju je slovo T. Slovo s kojim riječi najčešće završavaju je slovo E.
- Poslije Q gotovo uvijek dolazi U.
- Iza samoglasnika najčešće dolazi suglasnik N.

Ovo nam osobito pomaže ako želimo dekriptirati neki kraći šifrat na kojemu nema smisla analizirati frekvencije slova.

**Primjer 2.5.** *Dekriptirajmo šifrat:*
*OM OL FGM MIT LMKGFUTLM GY MIT LHTEOTL MINM LWKXOXTL, FGK MIT DGLM OFMTSSOUTFM MINM LWKXOXTL. OM OL MIT GFT MINM OL DGLM NRNHMNZST MG EINFUT.*
*Neka je poznato da je poruka šifrirana monoalfabetskom supstitucijskom šifrom te da je otvoreni tekst pisan na engleskom jeziku.*
*Rješenje:*
*Uočavamo da se tri puta pojavljuje riječ MINM. Prema prethodnim razmatranjima, razumno je pretpostaviti da je to šifra za riječ that, odnosno da je* $d_\pi(M) = t$, $d_\pi(I) = h$, $d_\pi(N) = a$. *Dobivamo sljedeće:*

*Ot OL FGt thT LtKGFUTLt GY thT LHTEOTL that LWKXOXTL, FGK thT DGLt OFtTSSOUTFt that LWKXOXTL. Ot OL thT GFT that OL DGLt aRNHtaZST tG EhNFUT.*
*Uočimo pojavljivanje riječi od tri slova koja počinje s th. Pretpostavimo da je to riječ the, odnosno da je $d_\pi(T) = e$. Također, u šifratu se pojavljuje bigram SS pa, kako je najčešći bigram od dva jednaka slova bigram ll, pretpostavimo da je $d_\pi(S) = l$. Promotrimo što smo do sad pretpostavili:*
*Ot OL FGt the LtKGFUeLt GY the LHeEOeL that LWKXOXeL, FGK the DGLt OFtellOUeFt that LWKXOXeL. Ot OL the GFe that OL DGLt aRNHtaZle tG EhNFUe.*
*Uočavamo riječ od dva slova koja počinje s T pa, kako je riječ to jedna od najčešćih riječi od dva slova koja se pojavljuje u engleskom jeziku, pretpostavimo da je $d_\pi(G) = o$. Promotrimo prvu riječ. Ovo je riječ od dva slova kojoj je drugo slovo slovo t. Moguće je da je to riječ at ili it. Ako u riječ OFtellOUeFt umjesto slova O pišemo slovo i, dobit ćemo riječ iFtelliUeFt pa možemo zaključiti kako je to riječ intelligent. Imamo $d_\pi(O) = i$, $d_\pi(F) = n$ te $d_\pi(U) = g$. Dobivamo sljedeće:*
*it iL nGt the LtKGngeLt GY the LHeEieL that LWKXiXeL, nGK the DGLt intelligent that LWKXiXeL. it iL the Gne that iL DGLt aRNHtaZle tG EhNnge.*
*Dalje bismo nastavili sličnim razmatranjima sve dok ne dobijemo citat engleskog znanstvenika Charlesa Darwina koji glasi: It is not the strongest of the species that survives, nor the most intelligent that survives. It is the one that is most adaptable to change.*

U Tablici 9 navedene su frekvencije slova u hrvatskom jeziku.




Slika 4: *Dijagram frekvencija slova hrvatskog jezika*

| Slovo | Postotak | Slovo | Postotak |
|---|---|---|---|
| A | 11.5 | L | 3.3 |
| B | 1.5 | M | 3.1 |
| C | 2.8 | N | 6.6 |
| D | 3.7 | O | 9 |
| E | 8.4 | P | 2.9 |
| F | 0.3 | R | 5.4 |
| G | 1.6 | S | 5.6 |
| H | 0.8 | T | 4.8 |
| I | 9.8 | U | 4.3 |
| J | 5,1 | V | 3.5 |
| K | 3.6 | Z | 2.3 |

Tablica 9: *Frekvencije slova hrvatskog jezika*

Najfrekventniji bigrami u hrvatskom jeziku su:

JE (2,7%), NA (1,5%), RA (1,5%), ST, AN, NI, KO, OS, TI, IJ, NO, EN, PR (1%),...

Iako J nije među najfrekventnijim slovima, JE je najfrekventniji bigram. Više od pola pojavljivanja slova J je uz slovo E. Najfrekventniji recipročni bigrami su NA i AN te NI i IN.
Najfrekventniji trigram u hrvatskom jeziku je IJE (0,6%). Slijede trigrami:

STA, OST, JED, KOJ, OJE, JEN,

s frekvencijama između 0.3% i 0.4%.
Kriptoanalizu teksta pisanog na hrvatskom jeziku analizom frekvencija slova pokazat ćemo kasnije.

Postoje razne inačice monoalfabetskih supstitucijskih šifri. To su primjerice Hebrejska, Cezarova i afina šifra. Također, otvoreni tekst ne moramo šifrirati slovima. To je možemo napraviti znakovima. Kao primjer takve šifre, opisat ćemo pigpen šifru. Puno različitih metoda za šifriranje i dešifriranje može se vidjeti i proučiti iz [[4], [5]].

## 2.1 Hebrejska šifra

Jedna od najstarijih i najjednostavnijih monoalfabetskih šifri je takozvani Atbash - princip obrnute abecede. Njega su koristili Hebrejski pisari oko 500.-600. g. pr. Kr. kod zapisivanja Knjige Jeremije i to tako da su umjesto prvog slova abecede pisali zadnje slovo, umjesto drugog slova abecede predposljednje, i tako dalje. Ovaj način šifriranja prikazan je u Tablici 10.

| 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 10: *Šifriranje Hebrejskom šifrom*

**Primjer 2.6.** *Poruka*

***close to the enemy***

*koristeći Tablicu 10, šifrirala bi se kao* ***XOLHV GL GSV VMVNB****.*
*Ako bismo primili šifriranu poruku*

***WZMZH QV GZQ WZM****,*

*koristeći Tablicu 10, dobijemo otvoreni tekst* ***danas je taj dan****.*

Umjesto korištenja slova, prilikom šifriranja moguće je koristiti i brojeve. Jedan od načina prikazan je u Tablici 11.

**Primjer 2.7.** *Ako bi poruku*

***close to the enemy***

*šifrirali korištenjem drugog dijela Tablice 11 (numeriranjem slova unatrag), dobili bismo šifrat* ***24 15 12 8 22 7 12 7 19 22 22 13 22 14 2****.*
*Ako smo primili poruku oblika*

***4 1 14 1 19 10 6 20 1 10 4 1 14***

*i znamo da je poruka nastala numeriranjem slova unaprijed, dešifrirali bismo ju korištenjem prvog dijela Tablice 11. Dobivamo otvoreni tekst* ***danas je taj dan****.*

Prethodno navedene metode vrlo su riskantne i potrebno je svega nekoliko minuta da neprijatelj otkrije sadržaj otvorenog teksta.

| | a | b | c | d | e | f | g | h | i | j | k | l | m | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | |
| n | o | p | q | r | s | t | u | v | w | x | y | z | | |
| 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | | |

| a | b | c | d | e | f | g | h | i | j | k | l | m |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 26 | 25 | 24 | 23 | 22 | 21 | 20 | 19 | 18 | 17 | 16 | 15 | 14 |
| n | o | p | q | r | s | t | u | v | w | x | y | z |
| 13 | 12 | 12 | 10 | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |

Tablica 11: *Šifriranje korištenjem brojeva*

## 2.2 Cezarova šifra

Cezarova šifra ili šifra s pomakom dobila je naziv po svom tvorcu Gaju Juliju Cezaru koji ih je koristio za slanje tajnih državnih poruka. Osnovna ideja ove šifre je zamijeniti slova otvorenog teksta slovima koja su pomaknuta od njih za određeni broj mjesta.

**Definicija 2.2.** *Neka je* $\mathcal{P} = \mathcal{C} = \mathcal{K} = \mathbb{Z}_{26}$. *Za* $0 \leq \mathcal{K} \leq 25$, *definiramo funkciju šifriranja* $e_K$ *i funkciju dešifriranja* $d_K$ *s:*

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

Kriptosustav je definiran na skupu $\mathbb{Z}_{26}$ jer engleska abeceda sadrži 26 slova. Ako bismo radili s hrvatskom abecedom, kriptosustav bismo definirali na skupu $\mathbb{Z}_{30}$. U Tablici 12 prikazane su zamjene slova engleske abecede odgovarajućim ostatcima modulo 26, odnosno njihovim numeričkim ekvivalentima.

| 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 12: *Numerički ekvivalenti slova engleskog jezika*

Dakle, osnovni elementi otvorenog teksta su slova, a ključ K određuje za koliko

mjesta udesno pomičemo slova pri šifriranju. Ovdje postoji 26 mogućih ključeva pa je moguće napraviti dekripciju za svega nekoliko minuta, čak i bez poznavanja ključa.

Rimski vojskovođa Gaj Julije Cezar koristio se šifrom u kojoj su se slova otvorenog teksta zamjenjivala slovima koja su za tri mjesta dalje u alfabetu. Drugim riječima, ključ ove šifre predstavlja pomak za 3. Definicija originalne Cezarove šifre glasi:

**Definicija 2.3.** *Neka je* $\mathcal{P} = \mathcal{C} = \mathbb{Z}_{26}$. *Za* $K = 3$, *definiramo funkciju šifriranja* $e_K$ *i funkciju dešifriranja* $d_K$ *s:*

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

*Odnosno imamo:*

$$e_3(x) = (x + 3) \bmod 26 \text{ i } d_3(y) = (y - 3) \bmod 26.$$

**Primjer 2.8.** *Šifrirajmo riječ* ***zima*** *originalnom Cezarovom šifrom.*
*Rješenje:*
*Numerički ekvivalenti slova riječi zima su* 25 8 12 0. *Koristeći funkciju šifriranja, šifriramo slovo po slovo:*

$$e_3(25) = 25 + 3 = 2 \bmod 26;$$
$$e_3(8) = 8 + 3 = 11 \bmod 26;$$
$$e_3(12) = 12 + 3 = 15 \bmod 26;$$
$$e_3(0) = 0 + 3 = 3 \bmod 26.$$

*Dobili smo numeričke ekvivalente slova šifrata* 2 11 15 3. *Njih pretvaramo u slova nakon čega dobivamo šifrat* ***CLPD***.

**Primjer 2.9.** *Dešifrirajmo poruku* ***OMHWR*** *ako znamo da je otvoreni tekst šifriran originalnom Cezarovom šifrom.*
*Rješenje:*
*Numerički ekvivalenti slova šifrata su* 14 12 7 22 17. *Koristeći funkciju dešifriranja, dešifriramo slovo po slovo:*

$$d_3(14) = 14 - 3 = 11 \bmod 26;$$
$$d_3(12) = 12 - 3 = 9 \bmod 26;$$
$$d_3(7) = 7 - 3 = 4 \bmod 26;$$
$$d_3(22) = 22 - 3 = 19 \bmod 26;$$
$$d_3(17) = 17 - 3 = 14 \bmod 26.$$

*Dobili smo numeričke ekvivalente slova šifrata* 11 9 4 19 14. *Njih pretvaramo u slova nakon čega dobivamo otvoreni tekst* ***ljeto***.

Tablica 13 prikazuje šifrate slova engleske abecede dobivene originalnom Cezarovom šifrom.

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

Tablica 13: *Originalna Cezarova šifra*

**Primjer 2.10.** *Poruku*

***close to the enemy***,

*šifrirat ćemo originalnom Cezarovom šifrom koristeći Tablicu 13 kao* ***FORVH WR HQHPB***.
*Dešifrirajmo poruku*

***GDQDV MH WDM GDQ***

*ako znamo da je šifrirana originalnom Cezarovom šifrom. Koristeći Tablicu 13 dobivamo otvoreni tekst* ***danas je taj dan***.

U sljedećim tablicama prikazan je postupak dobivanja tablice šifrata slova engleskog alfabeta Cezarovom šifrom s pomakom 21. Funkcija šifriranja je
$e_{21}(x_i) = (x_i + 21) \bmod 26$, za $i = 0, \ldots, 25$.
Nakon što numeričkim ekvivalentima slova alfabeta dodajemo broj 21, dobivamo numeričke ekvivalente slova šifrata. Nakon toga numeričkim ekvivalentima pridružimo odgovarajuća slova šifrata.

| | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $+_{26}21$ | 21 | 22 | 23 | 24 | 25 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |

| | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $+_{26}21$ | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 |

Tablica 14: *Cezarova šifra s pomakom 21*

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

Tablica 15: *Cezarova šifra s pomakom 21*

**Primjer 2.11.** *Šifrirajmo poruku*

***ovo je kraj***

*Cezarovom šifrom s pomakom 21.*
*Rješenje:*
*Koristeći tablicu 15 dobivamo šifrat* ***JQJ EZ FMVE****.*

Analogno bismo dobili tablicu dešifriranja šifrata dobivenog originalnom Cezarovom šifrom s pomakom 21 korištenjem funkcije dešifriranja
$d_{21}(y_i) = (y_i - 21) \bmod 26$, za $i = 0, \ldots, 25$.

U Šifri s pomakom prostor ključeva ima 26 elemenata pa nije teško dekriptirati šifrat.

**Primjer 2.12.** *Dekriptirajmo šifrat*

***BJ MFAJ KQJK KWTR TZW HTZSYWD***

*ako znamo da je poruka šifrirana Cezarovom šifrom.*
*Rješenje:*
*Zadatak ćemo riješiti tako da koristimo sve ključeve redom dok ne dođemo do smislenog teksta.*

*AI LEZI JPIJ JVSQ SYV GSYRXVC*
*ZH KDYH IOHI IURP RXU FRXQWUB*
*YG JCXG HNGH HTQO QWT EQWPVTA*
*XF IBWF GMFG GSPN PVS DPVOUSZ*
***WE HAVE FLEF FROM OUR COUNTRY***

*Očito je ključ* $K = 5$*. Dakle funkcije* $e_K$ *i* $d_K$ *su:*

$$e(x_i) = (x_i + 5) \bmod 26 \text{ i } d(y_i) = (y_i - 5) \bmod 26, \text{ za } i = 0, \ldots, 25.$$

## 2.3 Cezarova šifra s ključnom riječi

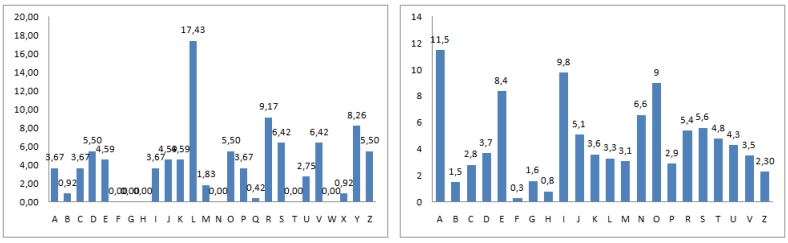
Cezarova šifra s ključnom riječi je monoalfabetska supstitucijska šifra. Kod ovakve vrste šifre funkcija šifriranja nije bilo koja permutacija, nego permutacija koja sadrži ključnu riječ. Ključ ovakve šifre je sama ta ključna riječ te broj koji označava poziciju mjesta u alfabetu otvorenog teksta od kojeg kreće ključna riječ. U Tablici 16 prikazan je primjer šifriranja Cezarovom šifrom s ključnom riječi u kojoj je ključ K=(FATAMORGANA, 6).

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

Tablica 16: *Cezarova šifra s ključnom riječi*

Dakle, od slova čiji numerički ekvivalent je broj koji je u ključu počinjemo pisati ključnu riječ nakon čega redom nastavljamo pisati slova abecede koja nisu iskorištena.

**Primjer 2.13.** *Dekriptirajmo šifrat*
*DIYVAOLRLUYJL ZS JRLRKAESRL QYKPYVUYRL DOZL KS MLEY VIOCPLELRZSB VOKACVLDL JL PYALRZS KDIYESRYX VOICDL MSJ VOJRLELRZL DUZCPL*
*dobiven Cezarovom šifrom s ključnom riječi ako je poznato da je tekst pisan na hrvatskom jeziku.*
*Rješenje:*
*Na dijagramima na Slici 5 prikazana je usporedba frekvencija slova u šifratu s frekvencijama slova u hrvatskom jeziku.*
*Kako je otvoreni tekst pisan na hrvatskom jeziku gdje je najfrekventnije slovo a, a u šifratu se slovo L pojavljuje najviše puta, pretpostavimo kako je $e(a) = L$. Najfrekventniji bigrami u šifratu su LR i RL. Kako su ovi bigrami simetrični, pretpostavimo da je riječ o najfrekventnijim simetričnim bigramima u hrvatskom jeziku, a to su bigrami an i na. Dakle, pretpostavimo da je $e(n) = R$. Sljedeće najfrekventnije slovo u šifratu je slovo Y. Kako je drugo najfrekventnije slovo u hrvatskom jeziku je slovo i, pretpostavimo da je $e(i) = Y$. Odredimo još čime je šifriran bigram je, najfrekventniji bigram u hrvatskom jeziku. Izuzev bigrama čijim slovima smo pretpostavili*




Slika 5: *Usporedba frekvencija slova u tekstu primjera s frekvencijama slova hrvatskog jezika*

*funkciju šifriranja, najfrekventniji bigrami u šifratu su bigrami ZS i VO koji se pojavljuju po tri puta. Kako je slovo e jedno od najfrekventnijih slova hrvatskog jezika, pretpostavimo da je ono šifrirano prvim neiskorištenim najfrekventnijim slovom u šifratu, slovom S ili V. Ako bi bilo* $e(e) = S$*, pretpostavimo kako je bigram je šifriran sa ZS, odnosno da je* $e(j) = Z$*. Pogledajmo što smo do sad pretpostavili:*

| a | b | c | d | e | f | g | h | i | j | k | l | m |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| L | | | | S | | | | Y | Z | | | |
| n | o | p | q | r | s | t | u | v | w | x | y | z |
| R | | | | | | | | | | | | |

Tablica 17: *Cezarova šifra s ključnom riječi*

*DI**i**VAO**ana**Ui**Ja** **je** J**nan**KAE**ena** Q**i**KP**i**VU**ina** DO**ja** K**e** M**a**E**i** VIOCP**a**E**anje**B VOKACV**a**D**a** J**a** P**i**A**anje** KDI**i**E**eni**X VOICD**a** M**e**J VOJ**na**E**anja** DUjCP**a**. Možemo uočiti riječ J**nan**KAE**ena** koja je vjerojatno šifrat za riječ znanstvena. Dakle, pretpostavimo da je* $e(z) = J$*,* $e(s) = K$*,* $e(t) = A$ *te* $e(v) = E$*.*

| a | b | c | d | e | f | g | h | i | j | k | l | m |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| L | | | | S | | | | Y | Z | | | |
| n | o | p | q | r | s | t | u | v | w | x | y | z |
| R | | | | | K | A | | E | | | | J |

Tablica 18: *Cezarova šifra s ključnom riječi*

*DI**i**V**t**O**ana**Ui**Ja** **je** **znanstvena** Q**si**P**i**VU**ina** DO**ja** **se** M**avi** VIOCP**avanje**B*

*VO**st**CV**a**D**a** **za** P**itanje** **s**DI**iveni**X VOICD**a** M**ez** VO**znavanja** DU**j**CP**a**.*
*Uočavmo riječi M**avi** i M**ez**. To su vrlo vjerojatno riječi bavi i bez a je e(b)=M. Riječ **s**DI**iveni**X je vrlo vjerojatno riječ skrivenih pa je $e(k) = D$, $e(r) = I$ te $e(h) = X$. Uočavamo riječ DO**ja** koja, uvrštavanjem $e(k) = D$, postaje **k**O**ja** te je vrlo vjerojatno $e(o) = O$.*

| a | b | c | d | e | f | g | h | i | j | k | l | m |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| L | M | | | S | | | X | Y | Z | D | | |
| n | o | p | q | r | s | t | u | v | w | x | y | z |
| R | O | | | I | K | A | | E | | | | J |

Tablica 19: *Cezarova šifra s ključnom riječi*

*U tablici uočavamo pojavljivanje slova XYZ nakon čega slijedi slovo D. Kako je malo vjerojatno da ključna riječ počinje s ZD, pretpostavimo kako počinje s D i to na desetoj poziciji. Na 18. poziciji pojavljuje se slovo A. U slučaju da ne sadrži slovo A, ključna riječ je oblika: D - - R O - - I K. Pretpostavimo da je to riječ DUBROVNIK. Imamo sljedeću tablicu šifriranja:*

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

Tablica 20: *Cezarova šifra s ključnom riječi*

*Nakon dešifriranja korištenjem Tablice 18, dobivamo sljedeći otvoreni tekst:*
*Kriptoanaliza je znanstvena disciplina koja se bavi proučavanjem postupaka za čitanje skrivenih poruka bez poznavanja ključa.*
*Dakle, ključ $K = (DUBROVNIK, 10)$ je dobar ključ.*

## 2.4 Afina šifra

Afina šifra poseban je slučaj supstitucijske šifre gdje je funkcija šifriranja oblika $e(x) = (ax + b) \bmod 26$, gdje $a$ i $b$ poprimaju cjelobrojne vrijednosti ne veće od 26. Samim time što je uključeno više od jednog parametra, ova šifra je sigurnija od prethodno navedenih. Da bi bilo moguće pravilno dešifriranje, gornja funkcija mora biti injekcija, odnosno, mora imati inverz na skupu $\mathbb{Z}_{26}$. Upravo zbog toga parametar $a$ nije proizvoljan, nego mora biti relativno prost s modulom 26.
Afina šifra definira se na sljedeći način:

**Definicija 2.4.** *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:*

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

Ova šifra naziva se afinom jer su funkcije šifriranja afine funkcije. Broj $a^{-1}$ označava multiplikativni inverz broja a u prstenu $\mathbb{Z}_{26}$. Kako broj 26 nije prost, nemaju svi elementi iz $\mathbb{Z}_{26}$ multiplikatvni inverz, nego samo oni koji su relativno prosti s 26. U Tablici 13 su prikazani takvi brojevi zajedno 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 21: *Multiplikativni inverzi brojeva koji su relativno prosti s 26 modulo 26*

**Primjer 2.14.** *Ako je ključ $K = (5, 3)$, funkcija šifriranja je*

$$e_K(x) = (5x + 3) \bmod 26,$$

*a funkcija dešifriranja*

$$d_K(y) = 21(y - 3) \bmod 26 = (21y - 63) \bmod 26 = (21y - 11) \bmod 26.$$

*Ispitajmo je li funkcija šifriranja injekcija:*
$d_K(e_K(x)) = d_K(5x + 3) = 21(5x + 3) - 11 = 105x + 63 - 11 = x$

**Primjer 2.15.** *Pretpostavimo da je $K = (5, 3)$. Šifrirajmo otvoreni tekst **slika**.*
*Rješenje:*
*Najprije slova otvorenog teksta poistovjećujemo s njihovim numeričkim ekvivalentima:*

$$slika \rightarrow 18\ 11\ 8\ 10\ 0$$

*Sada računamo šifrat za svako slovo. Imamo:*

$$\begin{aligned} e_K(18) &= 5 \cdot 18 + 3 = 15 \bmod 26, \\ e_K(11) &= 5 \cdot 11 + 3 = 6 \bmod 26, \\ e_K(8) &= 5 \cdot 8 + 3 = 17 \bmod 26, \\ e_K(10) &= 5 \cdot 10 + 3 = 1 \bmod 26, \\ e_K(0) &= 5 \cdot 0 + 3 = 3 \bmod 26, \end{aligned}$$

*pa je numerički ekvivalent šifrata 15 6 17 1 3, odnosno, šifrat je **PGRBD**.*

**Primjer 2.16.** *Dešifrirajmo riječ **SDQ** ako je poznato da je dobivena afinom šifrom s ključem $K = (5, 3)$.*
*Rješenje:*
*Najprije slova šifrata poistovjećujemo s njihovim numeričkim ekvivalentima:*

$$SDQ \rightarrow 18\ 3\ 16$$

*Pomoću funkcije dešifriranja računamo numerički ekvivalent slova otvorenog teksta:*

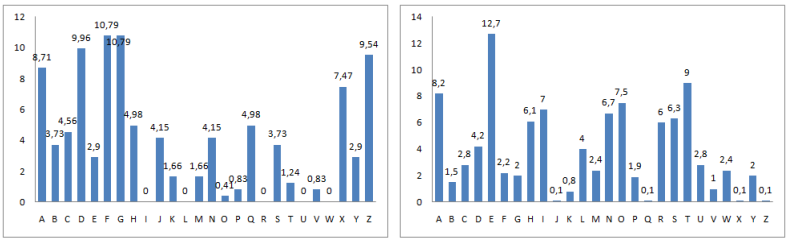
$$\begin{aligned} d_K(19) &= 21(18 - 3) = 3 \bmod 26, \\ d_K(4) &= 21(3 - 3) = 0 \bmod 26, \\ d_K(17) &= 21(16 - 3) = 13 \bmod 26. \end{aligned}$$

*Pridružujući dobivenim numeričkim ekvivalentima pripadna slova, dobivamo otvoreni tekst **dan**.*

Kako $a$ mora biti relativno prost s 26, postoji $\varphi(26) \cdot 26 = 12 \cdot 26 = 312$ mogućih ključeva. Čak i da ne znamo elegantniji način za dekriptirati šifrat, to možemo učiniti upotrijebljujući grubu silu. Općenito, broj ključeva u afinoj šifri u skupu $\mathbb{Z}_n$ jednak je $n \cdot \varphi(n)$. Ključ ćemo odrediti analizom frekvencije slova u šifratu. Pretpostavimo da znamo na kojem je jeziku pisan otvoreni tekst. Čak i da nam ta informacija nije poznata, to ne mijenja bitno složenost kriptoanalize. Frekvencijskom analizom doći ćemo do vjerojatnih supstitucija slova. Ako nam je

pretpostavka za šifrat barem dva slova ispravna, nakon rješavanja sustava dviju jednadžbi s dvjema nepoznanicama lako dolazimo do ključa, odnosno do vrijednosti $(a, b)$.

**Primjer 2.17.** *Dekriptirajmo šifrat:*
*ONZG GAFQ ZAF AFDSY ZXJFGAHQT ZECDZAHQT DKXNG HQ GAF EXXC D CHGGCF BDP XMM, DQY ZAF ZBDJ QFDSFS GX JDVF XNG BADG HG BDZ : DG MHSZG ZAF GAXNTAG HG JNZG KF D BDCSNZ XS AHEEXEXG-DJNZ, KNG GAFQ ZAF SFJFJKFSFY AXB ZJDCC ZAF BDZ QXB, DQY ZAF ZXXQ JDYF XNG GADG HG BDZ XQCP D JXNZF, GADG ADY ZCHEEFY HQ CHVF AFSZFCM.*
*Neka je poznato da je otvoreni tekst pisan engleskim alfabetom i šifriran je afinom šifrom.*
*Rješenje:*
*Na dijagramima na Slici 6 prikazana je usporedba pojavljivanja slova u šifratu i frekvencije slova engleskog alfabeta.*




Slika 6: *Usporedba frekvencija slova iz šifrata i frekvencija slova engleskog jezika*

*Slova F i G imaju najveću frekvenciju, pa, kako slova e i t imaju najveću frekvenciju u engleskom alfabetu, pretpostavimo da je* $e_K(e) = F$ *i* $e_K(t) = G$.
*Imamo* $e_K(4) = 5$ *i* $e_K(19) = 6$ *pa riješimo sustav:*

$$4a + b = 5 \bmod 26,$$
$$19a + b = 6 \bmod 26.$$

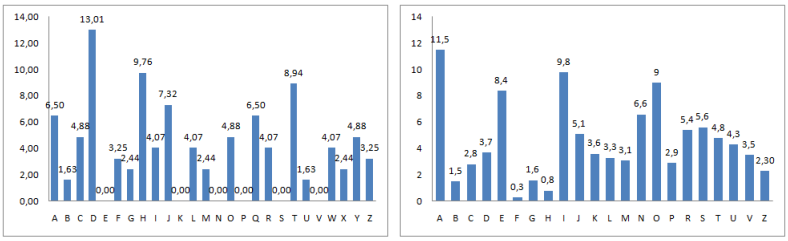
*Dobijemo jedinstveno rješenje* $a = 7$ *i* $b = 3$. *Kako je* $nzd(a, 26) = nzd(7, 26) = 1$, *dobili smo ključ. Izračunajmo funkciju dešifriranja. Dobivamo* $d_K(y) = 15(y - 3)$, *za svaki y iz šifrata. Odgovarajući alfabet šifrata prikazan je u Tablici 22.*

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

Tablica 22: *Alfabet šifrata*

*Dobili smo sljedeći otvoreni tekst:*
*Just then she heard something splashing about in the pool a little way off, and she swam nearer to make out what it was : at first she thought it must be a walrus or hippopotamus, but then she remembered how small she was now, and she soon made out that it was only a mouse, that had slipped in like herself.*
*(Tekst je preuzet iz knjige Alice's adventures in Wonderland autora Lewisa Carolla.)*
*Zaključujemo da je ključ K=(7,3) dobar ključ.*

**Primjer 2.18.** *Dekriptirajmo šifrat:*
*LTOWGOD YIDQTOD AT YGJYDCDID ATCQHZ YHXIHWQHZ LHWATRF - UJMQJXZTQF. ODA LHWATR AT UJH ODRH MDFMTO, CD LDR QJ BIDWF QJAT YHCJBDH RDC AT CHXDH ZDIJ YGJQL.*
*Neka je poznato da je otvoreni tekst pisan na hrvatskom jeziku i da je šifriran afinom šifrom.*
*Rješenje:*
*Na sljedećim dijagramima prikazana je usporedba frekvencija slova u danom šifratu s frekvencijama slova hrvatskog jezika.*




Slika 7: *Usporedba frekvencija slova iz šifrata i frekvencija slova hrvatskog jezika*

*Kako je u hrvatskom jeziku najfrekventnije slovo a, a u šifratu se najviše puta pojavljuje slovo D, pretpostavimo da je $e_K(a) = D$. Drugo najfrekventnije slovo hrvatskog jezika je slovo i pa, kako je u šifratu drugo najfrekventnije slovo slovo H, pretposta-*

*vimo da je* $e_K(i) = H$*. Imamo* $e_K(0) = 3$ *i* $e_K(8) = 7$ *pa rješavamo sustav:*

$$b = 3 \bmod 26;$$
$$8a + b = 7 \bmod 26.$$

*Ovaj sustav ima dva rješenja:* $a_1 = 7$*,* $b_1 = 3$ *i* $a_2 = 20$*,* $b_2 = 3$*. Kako* $a_2 = 20$ *nije relativno prost s 26, drugo rješenje ne uzimamo u obzir. Broj 7 je relativno prost s 26 pa uzmimo u obzir* $K = (7, 3)$ *kao mogući ključ. Izračunajmo funkciju dešifriranja. Dobivamo* $d_K(y) = 15(y - 3)$*, za svaki y iz šifrata. Odgovarajući alfabet šifrata prikazan je u Tablici 23.*

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

Tablica 23: *Alfabet šifrata*

*Dešifriranjem bismo dobili tekst koji nema smisla, što znači da smo pogriješili u pretpostavci. Neka i dalje pretpostavljamo kako je slovo a otvorenog teksta šifrirano slovom D. Kako je slovo o treće slovo po frekvencijama u hrvatskom jeziku, pretpostavimo da je* $e_K(o) = H$*. Sada imamo* $e_K(0) = 3$ *i* $e_K(14) = 7$ *pa rješavamo sustav:*

$$b = 3 \bmod 26;$$
$$14a + b = 7 \bmod 26.$$

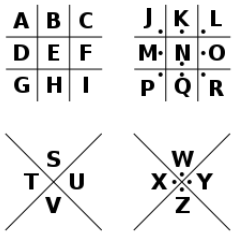
*Ponovno imamo dva rješenja* $a_1 = 4$*,* $b_1 = 3$ *te* $a_1 = 17$*,* $b_1 = 3$*. Slično ranijim zaključcima, odbacujemo prvo rješenje. Pretpostavimo da je ključ* $K = (17, 3)$*. Izračunajmo funkciju dešifriranja. Dobivamo* $d_K(y) = 23(y-3)$*, za svaki y iz šifrata. Odgovarajući alfabet šifrata prikazan je u Tablici 24.*
*Dobivamo sljedeći tekst:*
*Cetvrta planeta je pripadala jednom poslovnom covjeku - biznismenu. Taj covjek je bio tako zauzet, da cak ni glavu nije podigao kad je došao mali princ.*
*Zaključujemo kako je* $K = (17, 3)$ *dobar ključ.*

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

Tablica 24: *Alfabet šifrata*

## 2.5 Pigpen šifra

Pigpen (*engl. svinjac*) šifra, poznata kao masonska šifra, monoalfabetska je supstitucijska šifra gdje se slova zamjenjuju simbolima koji su dijelovi rešetke. Ime je dobila po načinu na koji se slova odvajaju linijama, kao svinje u svinjcu. Nije točno poznato kada se ova šifra počinje upotrijebljavati, no postoje zapisi o njenoj uporabi početkom 18. stoljeća. Ovakvu vrstu šifre koristili su masoni više od stotinu godina kako bi zaštitili povijesne zapise i zapise o obredima. Na Slici 8 prikazan je osnovni oblik pigpen šifre.




Slika 8: *Osnovni oblik pigpen šifre*

Rešetke ispunjavamo slovima proizvoljnim redoslijedom. Tekst se šifrira tako da se svako slovo zamijenjuje crtežom odjeljka u kojem se slovo nalazi.

**Primjer 2.19.** *Šifriranje poruke* ***close to the enemy*** *pigpen supstitucijom prikazano je na Slici 9.*

Slika 9: *Šifrat dobiven pigpen šifrom*

**Primjer 2.20.** *Neka je šifrat prikazan na Slici 10.*

Slika 10: *Šifrat dobiven pigpen šifrom*

*Pomoću Slike 8 dešifriramo te dobivamo otvoreni tekst* ***danas je taj dan****.*

Kriptoanaliza se izvodi frekvencijskom analizom, kao i ranije.

## 2.6 Polybiusov kvadrat

Polybiusov kvadrat izmislio je grčki povjesničar i znanstvenik Polybius kako bi se smanjio broj znakova u tekstu. U Tablici 25 prikazan je osnovni oblik Polybiusovog kvadrata s engleskim alfabetom.

| | 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 25: *Polybiusov kvadrat*

Slova su zamijenjena brojevima retka i stupca u kojem se nalaze. Tako bismo, na primjer, riječ **rak** zapisali **421125**. Kako engleski alfabet sadrži 26 slova, poistovjećujemo slova I i J. U hrvatskom jeziku uobičajeno je poistovijetiti slova V i W. Polybius nije imao ovakvih problema jer se grčki alfabet sastoji od 24 slova. Također, moguće je slova u tablicu pisati proizvoljnim redoslijedom ili s nekom ključnom riječi. Primjer kvadrata s ključnom riječi ENEMY dan je u Tablici 26.
U tablicu najprije pišemo slova ključne s time da izostavljamo slova koja se ponavljaju. Nakon što smo napisali ključnu riječ, tablicu popunjavamo redom slovima alfabeta koja se ne pojavljuju u ključnoj riječi.
U ovom slučaju, riječ **rak** šifrirali bismo kao **431533**.

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

Tablica 26: *Polybiusov kvadrat s ključnom riječi ENEMY*

**Primjer 2.21.** *Šifrirajmo otvoreni tekst:*

***Za one koji putuju, zvijezde su vodiči.***
***Za druge su samo male svijetle točke.***

*pomoću Polybiusovog kvadrata s ključnom riječi ZVIJEZDA.*
*Rješenje:*
*Formirajmo najprije Polybiusov kvadrat. Kako se radi o otvorenom tekstu na hrvatskom jeziku, poistovijetit ćemo slova V i W.*

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

Tablica 27: *Polybiusov kvadrat s ključnom riječi ZVIJEZDA*

*Šifrirajmo slovo po slovo pomoću brojeva retka i stupca u kojima se nalaze. Slovo z šifrirat ćemo s 11 jer se nalazi u prvom retku i prvom stupcu. Slovo a šifrirat ćemo s 22 jer se nalazi u drugom retku i drugom stupcu. Slovo o šifrirat ćemo s 42 jer se nalazi u četvrtom retku i drugom stupcu. Nastavljamo dalje dok ne dobijemo šifrat:*
***1122 424115 33421413 435352531453, 1112131415112115 5153 124221132413. 1122 2145533115 5153 51223542 35223415 51121314155234 15 52422433 15.***

**Primjer 2.22.** *Dešifrirajmo šifrat*
***442144 131444 2232 2415142144, 444112 2232 213252153142221552 44,***

*ako je poznato da je otvoreni tekst šifriran Polybiusovim kvadratom s ključnom riječi PUSTINJA.*
*Rješenje:*
*Formirajmo Polybiusov kvadrat s ključnom riječi pustinja što je prikazano u Tablici 28.*

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

Tablica 28: *Polybiusov kvadrat s ključnom riječi PUSTINJA*

*Dešifrirajmo prvu riječ. Razdvojimo znamenke na grupe od po dvije. Imamo: 44 21 44. Slovo otvorenog teksta za koje je šifrat 44 naći ćemo tako da pogledamo koje slovo se u tablici nalazi u 4 retku i četvrtom stupcu. To je slovo o. Slovo otvorenog teksta za koje je šifrat 21 čitamo iz tablice tako da nađemo slovo koje se nalazi u drugom retku i prvom stupcu. To je slovo n. Analogno bismo nastavili dalje dok ne dobijemo otvoreni tekst koji glasi:*
***Ono što je bitno, oku je nevidljivo.***

Kao i kod ostalih monoalfabetskih supstitucijskih šifara, napad na ovu šifru je jednostavan. Kriptoanaliza se vrši analizom frekvencija znakova upravo zbog toga jer je svako slovo zamijenjeno točno jednim parom brojeva i taj par brojeva je šifrat samo za to slovo.

## 2.7 Homofona supstitucijska šifra

Homofona supstitucijska šifra puno je složenija varijanta supstitucijske šifre gdje se jedno slovo zamjenjuje s više različitih znakova. Ova vrsta šifre također pripada monoalfabetskoj supstituciji jer slovo šifrata predstavlja točno jedno slovo otvorenog teksta. Drugim riječima, kada slovo šifriramo nekim znakom, ono će uvijek biti šifrirano tim znakom. Jedina razlika s obzirom na prethodno objašnjene kriptosustave je u tome što jedno slovo nema točno jedan šifrat. Naravno, prostor

šifrata ne sastoji se samo od alfabeta, nego mora sadržavati i neke dodatne znakove. Ovakva vrsta šifriranja pojavljuje se oko 1400. godine. Kriptolozi toga vremena znali su nedostatke sigurnosti jednostavnih monoalfabetskih šifri. Ako se jedan znak šifrira jednim znakom, šifra se lako može napasti analizom frekvencije slova, a to je objašnjeno u prethodnom poglavlju. U Tablici 29 dan je primjer homofonog šifriranja.

| 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 |
| 8 | | | | 9 | | | | 1 | | | 6 | |
| | | | | 3 | | | | | | | | |
| n | o | p | q | r | s | t | u | v | w | x | y | z |
| A | B | C | D | E | F | G | H | I | J | K | L | M |
| | | | | | | 4 | | | | | | |
| | | | | | | 5 | | | | | | |

Tablica 29: *Primjer homofone supstitucije*

Slova e i t najfrekventnija su slova engleskog alfabeta. Upravo zbog toga, kako bi se otežao napad na šifrat, ova slova šifriramo s više znakova. Prema tablici 27, slovo e je moguće šifrirati slovom R ili brojevima 9 i 3. Također, postoje tri šifrirna znaka za slovo t. To su G, 4 i 5. Slova a, i i l šifriramo s po dva znaka, dok ostala slova samo jednim znakom.

**Primjer 2.23.** *Šifrirajmo riječ* ***attacker*** *homofonom supstitucijom prema Tablici 29.*
*Rješenje:*
*Neki od mogućih šifrata su:*

***NG48PXRE***
***8548PX3E***
***8558PXRE***

Osnovna ideja ovakve vrste šifriranja je da određenom slovu bude dodijeljen broj znakova koji je ovisan o frekvenciji toga slova. Ako bismo imali otvoreni tekst sa sto slova, idealnu šifru dobili bismo kada bismo slovu e dodijelili 12 znakova, slovu t 8 znakova,... Ovako formiran šifrat nemoguće je dekriptirati.

Ovakvu šifru moguće je formirati uz pomoć slova i znamenaka 0-9 uz upotrebu ključa. Ključ je neka riječ ili rečenica sastavljena od slova i brojeva.

Neka je ključ **4 SEASONS**. Formirajmo homofonu supstitucijsku tablicu što je prikazano u Tablici 30.

| a | b | c | d | e | f | g | h | i | j | k | l | m |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 4 S | E | A | O | N B C D | F | G | H | I J | K | L | M | P |
| n | o | p | q | r | s | t | u | v | w | x | y | z |
| Q R | T U | V | W | X | Y Z | 0 1 2 | 3 | 5 | 6 | 7 | 8 | 9 |

Tablica 30: Primjer homofone supstitucije s ključnom riječi

Kao i ranije, frekventnija slova imaju više šifrata. U tablicu upisujemo ključnu riječ bez ponavljanja slova, nakon čega zapisujemo slova i brojeve koji se ne pojavljuju u ključnoj riječi. Slovo a moguće je šifrirati s 4 i S, slovo b šifriramo samo s E, slovo e zamijenjujemo jednim od slova N, B, C, D,...

Formirajmo homofonu supstitucijsku tablicu prilagođenu frekvencijama slova hrvatskoga jezika. Koristit ćemo 22 slova otvorenog teksta. Kao što je ranije objašnjeno, slova č i ć poistovijetit ćemo sa slovom c, slova đ, š i ž sa slovima d, s, z. Slova dž, lj i nj rastavit ćemo na dva slova d i z, l i j te n i j. Neka je ključ **4 GODIŠNJA DOBA**.

| a | b | c | d | e | f | g | h | i | j |
|---|---|---|---|---|---|---|---|---|---|
| 4 G O D | I | S | N | J A | B | C | E | F H K | L |
| k | l | m | n | o | p | r | s | t | u | v | z |
| M | P | R | T U | V Z 0 | 1 | 2 | 3 5 | 6 | 7 | 8 | 9 |

Tablica 31: Primjer homofone supstitucije s ključnom riječi

**Primjer 2.24.** *Šifrirajmo otvoreni tekst*

***Ono što je bitno, oku je nevidljivo.***

*homofonom supstitucijskom šifrom pomoću Tablice 31.*
*Rješenje:*
*Jedan od mogućih šifrata je:*
***0TZ 36Z LJ IF6TV, ZM7 LA TA8FNPLF8Z.***

**Primjer 2.25.** *Dešifrirajmo šifrat*

***94 VTJ MZLF 1767L7, 98HLA9NA 57 8ZNHSK***

*ako je poznato da je otvoreni tekst šifriran pomoću Tablice 31.*
*Rješenje:*
*Otvoreni tekst glasi:*
***Za one koji putuju, zvijezde su vodiči.***

Jedan suvremeni način izrade homofonske šifre, Grandpre šifra, uključuje odabir deset riječi od deset slova, takvih da prva slova tih riječi čine jedanaestu riječ. Riječi bi trebale sadržavati svih 26 slova abecede. Slova tih riječi tvore matricu $10 \times 10$. Slova otvorenog teksta zamijene se dvoznamenkastim brojevima određenim retkom i stupcem u kojem se nalaze te tako dobivamo šifrat. U Tablici 32 prikazan je jedan primjer Grandpre šifriranja.

| | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
|---|---|---|---|---|---|---|---|---|---|---|
| 0 | B | L | I | Z | Z | A | R | D | L | Y |
| 1 | L | I | Q | U | I | F | Y | I | N | N |
| 2 | A | M | B | E | R | J | A | C | K | S |
| 3 | C | O | L | L | O | Q | U | I | U | M |
| 4 | K | I | C | K | B | O | X | I | N | G |
| 5 | J | A | W | B | O | N | I | N | G | S |
| 6 | A | N | T | I | H | I | J | A | C | K |
| 7 | C | O | M | P | L | E | X | I | N | G |
| 8 | K | I | B | B | I | T | Z | E | R | S |
| 9 | S | U | B | J | E | C | T | I | V | E |

Tablica 32: *Primjer Grandpre šifre*

Slovo a može se zamijeniti s: 05, 20, 26, 51, 60, 67. Slovo b se mijenja s 00, 22, 44, 53, 82, 83, 92. Slovo W se šifrira samo s 52.

Formirajmo jednu tablicu za Grandpre šifriranje pomoću riječi hrvatskog jezika što je prikazano u Tablici 33.

| | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
|---|---|---|---|---|---|---|---|---|---|---|
| 0 | S | U | G | L | A | S | N | O | S | T |
| 1 | K | O | M | B | I | N | E | Z | O | N |
| 2 | L | A | N | S | I | R | A | N | J | E |
| 3 | A | P | S | O | R | P | C | I | J | A |
| 4 | D | A | L | M | A | T | I | N | A | C |
| 5 | A | N | E | M | O | M | E | T | A | R |
| 6 | T | E | R | M | O | M | E | T | A | R |
| 7 | E | V | A | L | U | A | C | I | J | A |
| 8 | L | E | B | D | J | E | L | I | C | A |
| 9 | J | E | D | I | N | S | T | V | E | N |

Tablica 33: *Primjer Grandpre šifre*

**Primjer 2.26.** *Šifrirajmo otvoreni tekst*

***Ono što je bitno, oku je nevidljivo.***

*Grandpre šifrom pomoću Tablice 33.*
*Rješenje:*
*Jedan od mogućih šifrata je:*
***540607 329633 7866 8246095107, 331001 3816 062971448373847777100.***

**Primjer 2.27.** *Dešifrirajmo šifrat*

***1704 071516 10113814 310145743874, 1771148416179183700574 711183467634.***

*dobiven Grandpre šifrom pomoću Tablice 33.*
*Rješenje:*
*Nađimo otvoreni tekst prve riječi. Podijelimo 1704 u grupe od po dva slova: 17 04. Prvo slovo dobit ćemo tako da u tablici nađemo slovo koje se nalazi u retku označenom s 1 i stupcu označenom sa 7. To je slovo z. Drugo slovo je slovo koje se nalazi u retku označenom s 0 i stupcu označenom s 4. To je slovo a. Ponavljamo dalje dok ne dobijemo otvoreni tekst:*
***Za one koji putuju, zvijezde su vodiči.***

Američki kriptograf, Herbert Osborn Yardley, u knjizi *The American Black Chamber* ilustrirao je homofonu šifru s ključem koji se mogao lako mijenjati. Slova

otvorenog teksta zamijenjena su dvoznamenkastim brojevima 00-99. Ispod alfabeta ispisani su dvoznamenkasti brojevi u četiri retka. U prvom retku su brojevi 01-26, u drugom 27-52, u trećem 53-78. U četvrtom retku nalaze se brojevi 79-99 iza kojih slijedi 00 pa četiri prazna mjesta. Ključ se sastoji od četiri slova. $i$-to slovo ključa određuje poziciju početka ispisivanja niza znamenki u $i$-tom retku, $i = 1, 2, 3, 4$. Nakon što ispisivanjem znamenki dođemo do kraja retka, dalje ih zapisujemo od početka tog istog retka sve dok ne dođemo do pozicije početka ispisivanja znamenki. U sljedećoj tablici dan je primjer ovakve vrste šifre s ključem THAT.

| a | b | c | d | e | f | g | h | i | j | k | l | m |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 08 | 09 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 |
| 46 | 47 | 48 | 49 | 50 | 51 | 52 | 27 | 28 | 29 | 30 | 31 | 32 |
| 53 | 54 | 55 | 56 | 57 | 58 | 59 | 60 | 61 | 62 | 63 | 64 | 65 |
| 86 | 87 | 88 | 89 | 90 | 91 | 92 | 93 | 94 | 95 | 96 | 97 | 98 |
| n | o | p | q | r | s | t | u | v | w | x | y | z |
| 21 | 22 | 23 | 24 | 25 | 26 | 01 | 02 | 03 | 04 | 05 | 06 | 07 |
| 33 | 34 | 35 | 36 | 37 | 38 | 39 | 40 | 41 | 42 | 43 | 44 | 45 |
| 66 | 67 | 68 | 69 | 70 | 71 | 72 | 73 | 74 | 75 | 76 | 77 | 78 |
| 99 | 00 | | | | | 79 | 80 | 81 | 82 | 83 | 84 | 85 |

Tablica 34: *Primjer homofone supstitucije s ključnom riječi*

Slovo a moguće je šifrirati bojevima 08, 46, 53 i 86, slovo b brojevima 09, 47, 54 i 87, ...

**Primjer 2.28.** *Šifrirajmo otvoreni tekst*

***Ono što je bitno, oku je nevidljivo.***

*pomoću Tablice 34.*
*Rješenje:*
*Šifrat za slovo o može biti 22, 34,67 ili 00. Dakle, slovo o šifriramo bilo kojim od ovih dvoznamenkastih brojeva. Slično vrijedi i za ostala slova otvorenog teksta. Jedan od mogućih šifrata je:*
***222134 260134 1712 0916012100, 676340 6250 339074618964618100.***

**Primjer 2.29.** *Dešifrirajmo šifrat*

***0708 222112 18342916 688079739573, 4541282990785657 2640 473411285594***

*ako je poznato da je šifriran pomoću Tablice 34.*
*Rješenje:*
*Dešifrirajmo prvu riječ 0708. Podijelimo broj u grupe od po dvije znamenke te dešifriramo znamenku po znamenku. 07 je šifrat za slovo z, a 08 šifrat za slovo a. Dakle, prva riječ je riječ za. Analogno dešifriramo ostatak šifrata. Dobivamo otvoreni tekst:* ***Za one koji putuju, zvijezde su vodiči.***

Kako je frekventnijim slovima dodijeljeno više znakova, sama analiza frekvencija slova nije dovoljnaza za otkrivanje otvorenog teksta. Ako u šifratu postoji N znakova, onda prostor ključeva homofonske supstitucije ima $26^N$ elemenata. Razbiti šifrat pogađanjem ključeva je nemoguć, no ipak je moguće razbiti ovakvu vrstu šifre.

Neka su slova šifrirana dvoznamenkastim brojevima te neka:

- Znak 10 u šifratu ima frekvenciju 10%;
- Znak 11 u šifratu ima frekvenciju 1%;
- Znak 12 u šifratu ima frekvenciju 5%;
- Znak 13 u šifratu ima frekvenciju 1%;
- Znak 14 u šifratu ima frekvenciju 5%.

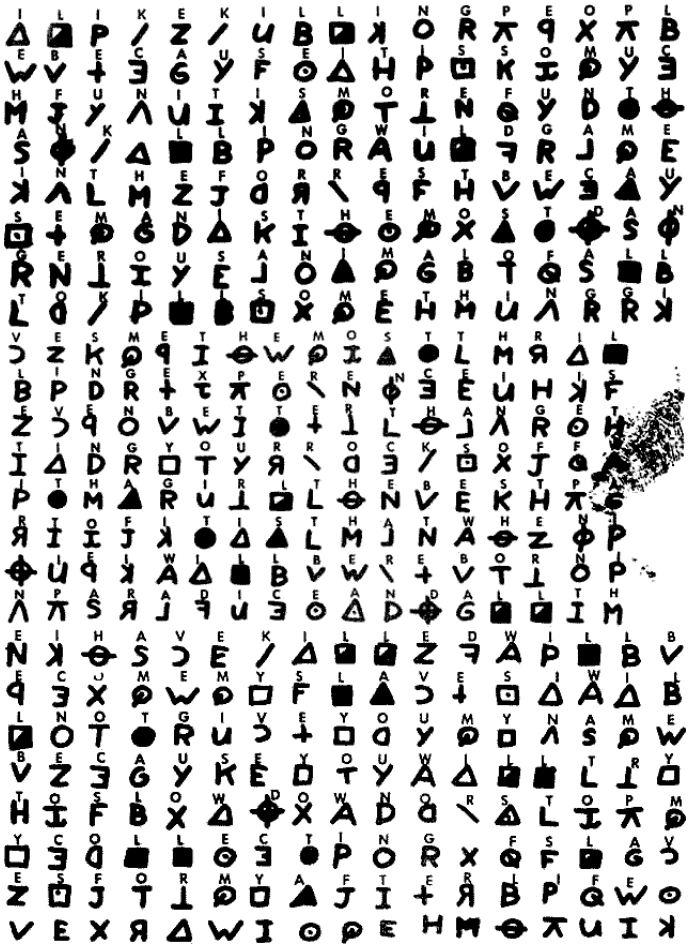
Kako se slovo E u engleskom jeziku pojavljuje s frekvencijom 12%, postoje dvije moguće kombinacije iz gore navedenih simbola kojima je šifrirano slovo E:

- znak 10 + znak 11 + znak 13;
- znak 11 + znak 12 + znak 13 + znak 14.

Dakle, isprobavanjem svih mogućih kombinacija frekvencija znakova moguće je doći do šifri za najfrekventnije znakove. Kod napada na šifrat pomažu i visoko frekventni $n$-grami koji se sastoje od nisko frekventnih slova. U literaturi, bigram $QU$ je najčešći uzorak napada na homofonski šifrat kada je tekst pisan na engleskom jeziku. Njegova frekvencija je 0.2%, no frekvencije slova Q i U su izrazito male tako da će ta slova vjerojatno biti supstituirana s po jednim znakom. Dakle, ako se neki skup od dva znaka u šifratu pojavljuje s frekvencijom 0.2%, pretpostavlja se da je to šifra za $QU$.

## 2.8 Pisma ubojice Zodiaca

Serijski ubojica nazvan Zodiac krajem 1960-ih te početkom 1970-ih godina ubijao je u Sjevernoj Kaliforniji. Njegov identitet do danas nije otkriven. Sam si je dao ime Zodiac u nizu zaprepaštujućih pisama poslanih u lokane novine. Ubojica je obećao da će, ukoliko novine objave njegova pisma, otkriti svoj identitet. Ukoliko to ne naprave, nastavit će ubijati tijekom vikenda. Četiri su različite šifre kojima su pisana pisma. Prva šifrirana komunikacija sastojala se od tri pisma poslanih 31. srpnja 1969. godine. Pisma su sadržavala ukupno 408 znakova od kojih su 54 različita. Šifra je nazvana Z408. Na sljedećoj slici prikazani su šifrati triju pisama te je iznad znakova napisano pripadno slovo otvorenog teksta.



Slika 11: *Šifrat Z408*

Za šifriranje slova e, ubojica je koristio 7 simbola prikazanih na Slici 12.

Slika 12: *Šifrirni znakovi za slovo e*

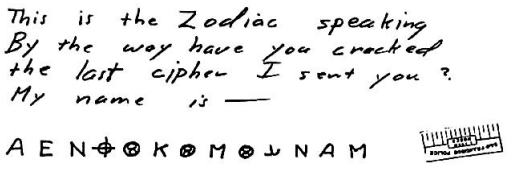
Poruka je šifrirana homofonom supstitucijom. Trebalo je svega nekoliko dana da se dešifrira ovaj šifrat, no zadnjih 18 simbola ostalo je neobjašnjeno. U pismu su se nalazile brojne gramatičke pogreške. Na primjer, pojavljuje se riječ *paradice* što bi trebalo pisati *paradise* (raj). U pismima koja su dekriptirana, nije otkriven Zodiacov identitet, kao što je ubojica obećao. Posljednjih 18 simbola nije dekriptirano. Neki ljudi tvrde kako su ti simboli šifra za identitet ubojice, no moguće je i da su ispisani znakovi slučajnim redoslijedom.

Dana 8. studenog 1969. godine, Zodiac je poslao šifrat koji se sastoji od 340 znakova, od kojih su 63 različita, koji do danas nije dekriptiran. Ova šifra nazvana je Z340. Šifrat je prikazan na Slici 13.

Slika 13: *Šifrat Z340*

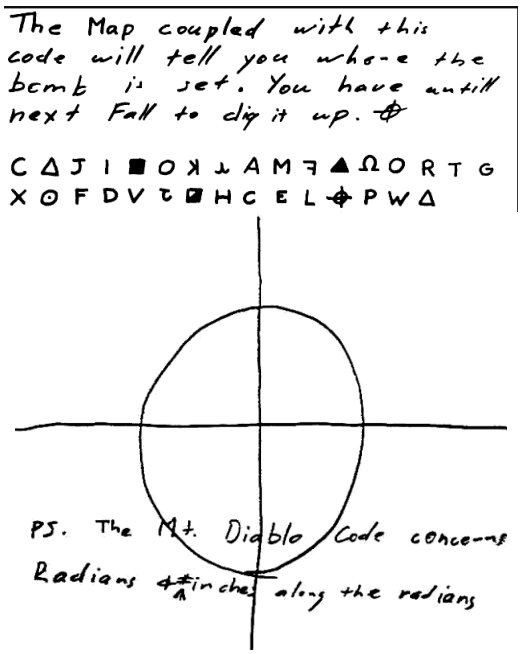
Dana 20. travnja Zodiac je poslao pismo u kojem tvrdi da je otvoreni tekst

šifrata zapravo jegov identitet. Pismo sadrži 13 šifrirnih znakova koji još uvijek nisu dekriptirani. Šifra je nazvana Z13. Na Slici 13 prikazano je Zodiacovo pismo sa Z13 šifrom.




Slika 14: *Šifrat Z13*

Dana 26. lipnja 1970. godine Zodiac je poslao posljednji šifrat. Ubojica tvrdi da otvoreni tekst šifrata sadrži informacije o lokaciji postavljene bombe. Šifrat se sastoji od 36 šifrirnih znakova. Šifra je nazvana Z32 te još uvijek nije dekriptirana.




Slika 15: *Šifrat Z32*

Kroz cijelu povijest čovječanstva postojala je potreba za sigurnom komunikacijom. Još prije 3000 godina Egipćani i Indijci bavili su se ovim problemom. Prvi tragovi šifriranja potječu još od 1900. godine pr. Kr. U 6. stoljeću pr. Kr. u zapisu dijela Biblije korištena je jednostavna šifra koja koristi alfabet ispisan naopako. Monoalfabetska supstitucijska šifra sastoji se od zamjene slova nekim drugim znakom koje je zamjena samo za to slovo. Ova šifra pruža vrlo nisku komunikacijsku sigurnosti. Čak i bez uporabe računala, šifrat se lako dekriptira, posebno za dulje tekstove. S tehnološkog stajališta, monoalfabetske supstitucijske šifre su vrlo jednostavne i zastarjele. Ove šifre postale su izvor enigmatske zabave za velik broj ljubitelja enigmatike. Također, ovakve vrste šifri mogu poslužiti za tajno komuniciranje običnog čovjeka. Postoje brojne aplikacije za šifriranje poruka ovakvim šiframa pri komuniciranju. Homofona supstitucijska šifra znatno otežava dekriptiranje šifrata. Pisma serijskog ubojice Zodiaca šifrirana homofonom supstitucijom već 50-ak godina nisu dekriptirana.

# 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.

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

[4] H. Fouche Gaines,*Cryptanalysis a study of ciphers and their solution*, Dover Publication, New York, 1956.

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

[6] B. Širola, *Algebarske strukture*, PMF-Matematički odjel, Sveučilište u Zagrebu, skripta.

# Sažetak

U ovom radu bavili smo se analizom monoalfabetskih supstitucijskih šifri. Najprije smo naveli definicije i rezultate iz algebre i teorije brojeva što je potrebno kako bi se uspješno pratio sadržaj rada. Definirali smo monoalfabetske supstitucijske šifre te na primjerima pokazali šifriranje i dešifriranje teksta korištenjem raznim tipovima šifri. Naveli smo neke inačice monoalfabetskih šifri kao što su hebrejska, Cezarova, afina, pigpen šifra te Polybiusov kvadrat. Svaku od ovih šifri pokrijepili smo raznim primjerima. Objasnili smo i homofonu supstitucijsku šifru te njene razne inačice. Na kraju rada, spomenuli smo šifru kojom se koristio serijski ubojica Zodiac, čiji šifrati već desetke godina nisu dekriptirani.

# Ključne riječi:

Monoalfabetska supstitucijska šifra, hebrejska šifra, Cezarova šifra, Cezarova šifra s ključnom riječi, afina šifra, pigpen šifra, Polybiusov kvadrat, homofona supstitucijska šifra, grandpre šifra, homofona supstitucijska šifra s ključnom riječi, Zodiac šifra

# Summary

In this paper, we analized a monoalphabetic substitution ciphers. First of all, we gave defnitions and results from algebra and number theory, usefull fot successfully reading the content of the paper. We defined the monoalphabetic substitution ciphers. Through the different types of examples we illustrated encryption and decryption of plain text. Moreover, we mentioned some versions of the monoalfabetic codes such as Hebrew code, Caesar cipher, Afine cipher, Pigpen code and Polybius square. Each of them is confirmed by various type of examples. Besides that, we explained the homophonic substitution cipher and some of its variants. At the end, we mentioned the code used by the serial killer Zodiac, whose ciphertext has not been decrypted for decades.

# Keywords:

Monoalphabetic substitution cipher, Hebrew cipher, Caesar cipher, Caesar cipher with keyword, Affine cipher, Pigpen cipher, Polybius square, homophonic substitution cipher, grandpre cipher, homophonic substitution cipher with keyword, Zodiac cipher

# Životopis

Rođena sam 28. rujna 1991. godine u Zagrebu. Godine 2006. završila sam Osnovnu školu u Novskoj gdje sam upisala i Srednju ekonomsku školu. Nakon završene srednje škole, upisala sam se na Odjel za matematiku na Sveučilištu u Rijeci gdje sam, u razdoblju od 2010. do 2014. godine, pohađala preddiplomski studij matematike. Nakon završetka preddiplomskog studija, upisala sam diplomski studij matematike, smjer: financijska matematika i statistika na Odjelu za matematiku Sveučilišta J. J. Strossmayera u Osijeku.