Klasična kriptografija

Osnovni pojmovi

Kriptografija je znanstvena disciplina koja se bavi proučavanjem metoda za slanje poruka u takvom obliku da ih onaj kome su namijenjene može pročitati.

Osnovni zadatak je omogućiti dvjema osobama (*pošiljalac* i *primalac*) komuniciranje preko nesigurnog komunikacijskog kanala na način da neka treća osoba (*protivnik*), koja može nadzirati komunkacijski kanal, ne može razumijeti njihove poruke.

Poruku koju pošiljalac želi poslati primaocu zovemo *otvoreni tekst*. Pošiljalac transformira otvoreni tekst koristeći unaprijed dogovoreni *ključ*. Taj postupak zove se *šifriranje* ili *kriptiranje*, a dobiveni tekst *šifrat* ili *kriptogram*. Nakon toga pošiljalac pošalje šifrat preko nekoga komunikacijskog kanala. Protivnik prisluškujući može doznati sadržaj šifrata, ali ne može odrediti otvoreni tekst. Za razliku od njega, primalac zna ključ kojim je poruka šifrirana i može dešifrirati šifrat i odrediti otvoreni tekst.

Kriptoanaliza ili *dekriptiranje* je znanstvena disciplina koja se bavi proučavanjem postupaka za čitanje skrivenih poruka bez poznavanja ključa. *Kriptologija* je pak grana znanosti koja obuhvaća kriptografiju i kriptoanalizu.

Kriptografski algoritam ili *šifra* je matematička funkcija koja se koristi za šifriranje i dešifriranje. Općenito, radi se o dvije funkcije, jednoj za šifriranje, a drugoj za dešifriranje. Te funkcije preslikavaju osnovne elemente otvorenog teksta (najčešće su to slova, hitovi, grupe slova ili bitova) u osnovne elemente šifrata, i obratno. Funkcije se biraju iz određene familije funkcija u ovisnosti o ključu. Skup svih mogućih vrijednosti ključeva nazivamo prostor ključeva. Kriptosustav se sastoji od kriptografskog algoritma, te svih mogućih otvorenih tekstova, šifrata i ključeva. Dakle, imamo sljedeću formalnu definiciju.

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

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

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

(3) $\mathcal{K}$ *je konačan skup svih mogućih ključeva;*

(4) $\mathcal{E}$ *je skup svih funkcija šifriranja;*

(5) $\mathcal{D}$ *je skup svih funkcija dešifriranja;*

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

Najvažnije svojstvo u definiciji je $d_K(e_K(x)) = x$. Iz njega slijedi kako funkcije e_K moraju biti injekcije. Zaista, ako bi bilo

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

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

Klasifikacija kriptosustava

Kriptosustave obično klasificiramo s obzirom na sljedeća tri kriterija:

1. Obzirom na tip operacija koje se koriste pri šifriranju:

a) Supstitucijske šifre: svaki element otvorenog teksta (bit, slovo, grupa bitova ili slova) zamjenjuje se s nekim drugim elementom, prema unaprijed utvrđenoj transformaciji. Ovisno o broju transformacija mogu bit monoalfabetske i polialfabetske. Npr. TAJNA $\rightarrow$ ERMBR.

b) Transpozicijske šifre: elementi otvorenog teksta se premještaju, tj. permutiraju. Npr. TAJNA $\rightarrow$ NAJTA.

c) Postoje i kriptosustavi koji kombiniraju ove dvije metode.

2. Obzirom na način na koji se obrađuje otvoreni tekst:

a) Blokovne šifre: obrađuje se jedan po jedan blok elemenata otvorenog teksta koristeći jedan te isti ključ K.

b) Protočne šifre: elementi otvorenog teksta obrađuju se jedan po jedan koristeći pritom paralelno generirani niz ključeva (engl. keystream).

3. Obzirom na tajnost ključeva:

a) Simetrični kriptosustavi: ključ za dešifriranje može se izračunati poznavajući ključ za šifriranje i obratno. Ovi su ključevi najčešće identični, pa sigurnost ovih kriptosustava leži u tajnosti ključa. Zato se oni zovu i kriptosustavi s tajnim ključem.

b) Kriptosustavi s javnim ključem ili asimetrični kriptosustavi: ključ za dešifriranje ne može se u nekom razumnom vremenu izračunati iz ključa za šifriranje. Ovdje je ključ za šifriranje javni ključ. Naime, bilo tko može šifrirati poruku pomoću njega, ali samo osoba koja ima odgovarajući ključ za dešifriranje (privatni ili tajni ključ) može dešifrirati tu poruku.

Napomenimo kako je osnovna pretpostavka da kriptoanalitičar zna koji se kriptosustav koristi. To se naziva Kerckhoffsovo načelo, po Nizozemcu Augustu Kerckhoffsu (1835. - 1903.), autoru važne knjige "Vojna kriptografija".

Napadi na kriptosustave

Svaku usmjerenu radnju kriptoanalitičara zovemo *napad*. Razlikujemo četiri osnovna napada:

1. Napad poznatim šifratom:

   Kriptoanalitičar posjeduje samo šifrat od nekoliko poruka šifriranih pomoću istog algoritma. Njegov je zadatak otkriti otvoreni tekst od što više poruka ili u najboljem slučaju otkriti ključ kojim su poruke šifrirane.

2. Napad poznatim otvorenim tekstom:

   Kriptoanalitičar posjeduje šifrat neke poruke, ali i njemu odgovarajući otvoreni tekst. Njegov je zadatak otkriti ključ ili neki algoritam za dešifriranje poruka šifriranih tim ključem.

3. Napad odabranim otvorenim tekstom:

   Kriptoanalitičar ima mogućnost odabira teksta koji će biti šifriran, te može dobiti njegov šifrat. Na taj način, dobrim odabirom skupa poruka može dobiti što više informacija o upotrebljenom ključu. Ovaj napad je jači od prethodnoga, ali je manje realističan.

4. Napad odabranim šifratom:

   Kriptoanalitičar je dobio pristup alatu za dešifriranje, pa može odabrati šifrat, te dobiti odgovarajući otvoreni tekst. Ovaj napad je tipičan kod kriptosustava s javnim ključem. Tu je zadatak kripoanalitičara otkriti ključ za dešifriranje, tj. tajni ključ.

Postoji još jedan (neprimjeren) oblik napada:

(5.) Napad potkupljivanjem, ucjenama, krađama i slično

Ovaj napad ne spada doslovno u kriptoanalizu, ali je vrlo efikasan i često primjenjivan u kombinaciji s "pravim" kriptoanalitičkim napadima.

Povijesni pregled naprava za šifriranje

1.) **Skital**: Spartanci su u 5. stoljeću prije Krista upotrebljavali napravu za šifriranje zvanu skital. To je bio drveni štap oko kojeg se namotavala vrpca od pergamenta, pa se na nju okomito pisala poruka. Nakon upisivanja poruke, vrpca bi se odmotala, a na njoj bi ostali izmiješani znakovi koje je mogao pročitati samo onaj tko je imao štap jednake debljine.

2.) **Jeffersonov kotač za šifriranje**: Napravu je izumio američki državnik Thomas Jefferson krajem 18. stoljeća. Jeffersonov kotač se sastoji od drvenog cilindra s rupom u sredini kroz koju je provučena željezna os. Cilindar je presječen na 26 manjih cilindara (diskova) jednakih širina. Ovi se diskovi mogu neovisno jedan od drugoga okretati oko zajedničke osi. Na vanjštini svakog diska nalazi se 26 jednakih kvadratića. Tih 26 kvadratića se na proizvoljan način popunjava s 26 slova engleskog alfabeta, različito od diska do diska.

Pošiljalac i primalac imaju dva identična kotača. Da bi šifrirao otvoreni tekst, pošiljalac podijeli tekst na blokove od po 26 slova. Blok se šifrira tako da se rotiranjem diskova u jednom od 26 redaka dobije otvoreni tekst. Tada za šifrat možemo izabrati bilo koji od preostalih 25 redaka.

Primalac dešifrira šifrat tako da rotiranjem diskova u jednom retku dobije šifrat. Sada među preostalih 25 redaka potraži onaj koji sadrži neki smisleni tekst i taj redak predstavlja otvoreni tekst.

3.) **Hebernov električni stroj za kodiranje**: Izumio ga Amerikanac Edward Hugh Hebern 1915. godine. To je bio električni uređaj kojim su se dva električna pisaća stroja spajala pomoću 26 žica, ali s razbacanim rasporedom, pa kad bi se udarila tipka na pisaćem stroju za otvoreni tekst, drugi bi stroj automatski otipkao šifrat tog slova. Budući da se položaj žica nije mijenjao tijekom šifriranja jedne poruke, šifra koja se tako dobivala je bila obična monoalfabetska šifra. Jedina novost je bila u tome što je postupak šifriranja automatiziran.

Međutim, dvije godine kasnije, Hebern je u uređaj ugradio 5 tzv. rotora. Rotori su na svakoj strani imali po 26 električnih kontakata. Svaki je kontakt na jednoj strani nasumce žicom spojen s nekim kontaktom na drugoj strani. Kao što smo već rekli, ovo predstavlja jednu monoalfabetsku supstituciju. Rotiranjem rotora i to tako da najprije prvi napravi cijeli krug, drugi se pomakne za jedno mjesto, itd., dobivamo polialfabetsku supstituciju s periodom 26^5.

4.) **ENIGMA**: Rotorska naprava koju je izumio i patentirao Nijemac Arthur Scherbius 1918. godine. Od 1926. godine započela je njezina uporaba u njemačkoj vojsci. Do masovne uporabe ENIGME došlo je neposredno prije i za vrijeme Drugog svjetskog rata. Razbijanje njezine šifre (kombinacijom kriptoanalize i klasične špijunaže) imalo je važnu ulogu za tijek i ishod Drugog svjetskog rata.

Postojale su različite (vojne i komercijalne) inačice ENIGME. Posebno je bila poznata japanska inačica ENIGME, koju su Amerikanci nazvali PURPLE.

Enigma se sastojala od tipkovnice s 26 tipki poput pisaćeg stroja, zaslona s 26 žaruljica za prikaz šifriranog izlaza, tri mehanička rotora (šifrarnika) i električne prespojne ploče. Pritiskom na tipku kroz mrežu kontakata rotora i prespojne ploče zatvorio bi se strujni krug i upalila bi se odgovarajuća žaruljica koja označava šifrirano slovo.

Mehanički rotori sastojali su se od diskova s 26 kontakata. Svaki kontakt na jednoj strani diska bio je povezan s nekim drugim kontaktom na suprotnoj strani. Većina modela ENIGME sastojala se od tri rotora koji su smješteni u ležište tako da se kontakti susjednih stranica međusobno dodiruju, tj. "izlaz" jednog rotora predstavljao je "ulaz" drugog. Izlaz trećeg (zadnjeg) rotora bio je povezan na reflektor - statičan mehanički disk sličan rotoru, s međusobno prespojenim električnim kontaktima samo na jednoj strani. Njegova je zadaća bila da električni signal šalje natrag kroz rotore, no drugim putem. Prvi se rotor nakon svakog šifriranog slova okretao za jedan kontakt, a kad bi učinio potpun krug, mehanička je poluga okretala sljedeći rotor za jedan kontakt. Tri ožičena rotora s 26 kontakata daju $26^3 = 17576$ mogućih kombinacija. To nije dovoljno velik broj da bi dao zadovoljavajuću sigurnost.

Naravno, sigurnost se mogla povećati dodavanjem novih rotora, no to bi povećalo veličinu i težinu samog uređaja, što bi znatno smanjilo njegovu atraktivnost. Scherbius je povećao sigurnost ENIGME povećavajući broj mogućih početnih postavki na dva različita načina: izmjenjivim rotorima i prespojnom pločom.

Budući da su rotori mehanički gotovo identični, a njihovi električni spojni putevi različiti, njihovom međusobnom zamjenom mijenja se i način šifriranja samog stroja. Broj mogućih permutacija triju rotora je $3! = 6$ (mogući rasporedi rotora

su 123, 132, 213, 231, 312, 321). Znatno veći doprinos sigurnosti donosi prespojna ploča, koja korisniku omogućuje da doda kablove, koji imaju efekt zamjene nekih slova prije ulaska u prvi rotor. Na primjer, kabel se može koristiti za zamjenu slova "A" i "D", tako da kad korisnik pritisne tipku "A", električni signal zapravo slijedi put kroz rotore koji bi bez prespojne ploče bio put slova "D", i obrnuto. U ranoj fazi Drugog svjetskog rata operateri ENIGME koristili su 6 prespojnih kabela, što znači da je bilo moguće zamijeniti 6 parova slova, ostavljajući preostalih 14 slova da se šifriraju bez utjecaja prespojne ploče. Broj načina na koji možemo odabrati 6 parova slova između 26 slova je

$$\binom{26}{2} \cdot \binom{24}{2} \cdot \binom{22}{2} \cdot \binom{20}{2} \cdot \binom{18}{2} \cdot \binom{16}{2} /6! = 100\,391\,791\,500.$$

Od 1939. godine standardizirano je korištenje 10 prespojnih kabela, što je davalo 150 738 274 937 250 mogućih kombinacija. Možda je zanimljivo spomenuti da se maksimalni broj kombinacija dobiva korištenjem točno 11 prespojnih kabela, tako da nije najjasnije zašto je u ovoj kasnijoj verziji izabran broj 10 (moguće da je došlo do greške u proračunu kombinacija).

U svakom slučaju, već kod korištenja 6 prespojnih kabela, ukupan broj postavki ENIGME je vrlo velik (veći od 10^{16}), pa je napad ispitivanjem svih mogućih kombinacija postao nemoguć. Pa ipak, dvije grupe matematičara-kriptoanalitičara uspjele su pronaći način za dekriptiranje ENIGME. Bile su to poljska grupa, koju je predvodio Marian Rejewski, te britanska grupa, koju je predvodio Alan Turing.

Prvi napredak u kriptoanalizi ENIGME ostvaren je godine 1931. akcijom francuske obavještajne službe, koja je stupila u vezu s bratom načelnika sektora veze njemačke vojske, Hansom-Thilom Schmidtom. Uz naknadu od 10 000 tadašnjih njemačkih maraka Schmidt je Francuzima dostavio upute za uporabu ENIGME. Budući da su Francuzi i Poljaci po završetku Prvog svjetskog rata potpisali ugovor o vojnoj suradnji, ti su dokumenti dostavljeni poljskom uredu za kriptografiju.

Rejewski je uočio da broj elemenata u ciklusima ovisi isključivo o rotorima, a ne o prespojnoj ploči. Ukupan broj postavki rotora je 105456, što je velik broj, ali ne i ogroman.

Zahvaljući Schmidtovoj špijunaži, Poljaci su bili u stanju napraviti repliku ENIGME, te katalogizirati koje postavke rotora daju kakve rastave na produkte ciklusa (za to im je trebala godina dana). Nakon toga, dešifriranje je bilo dosta lako. Trebalo je još odrediti veze na prespojnoj ploči. Ako se krene u dešifriranje s prespojnom pločom bez ikakvih veza, dobit će se uglavnom nerazumljiv tekst. No, vjerojatno će se naići i na djelove teksta koji su "skoro čitljivi", tj. u kojima je dosta jasno koja slova treba zamijeniti da bi se dobio otvoreni tekst. I tako se otkrivaju slova koja su povezana kablovima na prespojnoj ploči. Na ovaj su način Poljaci nekoliko godina uspijevali redovito dešifrirati njemačke poruke, sve dok 1939. godine Nijemci nisu značajno povećali broj mogućih ključeva, uvođenjem većeg broja rotora (pet) i većeg broja veza na prespojnoj ploči (deset).

Supstitucijske šifre

Definicija 1.2 *Supstitucijske šifre su šifre kod kojih se svaki element otvorenog teksta zamjenjuje nekim drugim elementom.*

Frekvencija slova

Navest ćemo sada osnovne podatke o frekvenciji slova u hrvatskom jeziku u promilima ($1‰ = 0.1\%$). Poredak slova od najfrekventnijih do najmanje frekventnih:

A(115), I(98), O(90), E(84), N(66), S(56), R(54), J(51), T(48), U(43), D(37), K(36), V(35), L(33), M(31), P(29), C(28), Z(23), G(16), B(15), H(8), F(3).

Najfrekventniji bigrami u hrvatskom jeziku su:

JE(27) NA(15), RA(15), ST, AN, NI, KO, OS, TI, IJ, NO, EN, PR(10).

Dakle, najfrekventniji bigram je JE, iako J nije najfrekventnije slovo. Uočimo kako su najfrekventniji bigrami oblika samoglasnik-suglasnik ili obratno. Najfrekventniji recipročni bigrami su:

NA i AN, te NI i IN(9).

Najfrekventniji trigrami u hrvatskom jeziku su:

IJE(6), STA, OST, JED, KOJ, OJE, JEN s frekvencijama između 3 i 4.

Poredak slova od najfrekventnijih do najmanje frekventnih u engleskom jeziku:

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),

a trigrami

THE(35), ING(11), AND(10), ION, TIO, ENT, ERE, HER (7).

Poredak slova od najfrekventnijih do najmanje frekventnih u njemačkom jeziku:

E(175), N(98), I(77), R(75), S(68), A(65), T(61), D(48), H(42), U(42), L(35), G(31), O(30), C(27), M(26), B(19), F(17), W(15), K(15), Z(11), P(10), V(9), J(3), Y(1), X(0), Q(0).

Najfrekventniji bigrami su

ER(41), EN(40), CH(24), DE, EI, ND, TE, IN, IE, GE(15),

a trigrami

EIN(12), ICH(11), NDE(9), DIE, UND, DER, CHE, END(8).

Cezarova i afina šifra

Znameniti Rimski vojskovođa i državnik Gaj Julije Cezar u komunikaciji sa svojim prijateljima koristio se šifrom u kojoj su se slova otvorenog teksta zamjenjivala slovima koja su se nalazila tri mjesta dalje od njih u alfabetu ($A \mapsto D, B \mapsto E, \dots$). Pretpostavljamo da se alfabet ciklički nastavlja, tj. da nakon zadnjeg slova Z ponovno dolaze $A, B, \dots$.

Danas se Cezarovom šifrom nazivaju i šifre istoga oblika s pomakom različitim od 3. Da bismo Cezarovu šifru precizno definirali, uvest ćemo prirodnu korespondenciju između slova alfabeta $A - Z$ i cijelih brojeva $0 - 25$.

Skup $\{0, 1, \dots, 25\}$ označavat ćemo sa $\mathbb{Z}_{26}$ i pretpostavljat ćemo da su na njemu definirane operacije $+, -, \cdot$ na isti način kao u skupu $\mathbb{Z}$, ali tako da se rezultat (ukoliko nije iz skupa $\{0, 1, \dots, 25\}$) na kraju zamijeni s njegovim ostatkom pri dijeljenju s 26. Koristit ćemo oznaku $(a \pm b) \bmod 26$, $(a \cdot b) \bmod 26$ ili $a \pm_{26} b$, $a \cdot_{26} b$. Npr. $10 +_{26} 23 = 7$, $12 -_{26} 14 = 24, 5 \cdot_{26} 6 = 4$. Skup $\mathbb{Z}_{26}$ uz tako definirane operacije $+$ i $\cdot$ čini prsten (dakle, operacije $+_{26}, -_{26}$ i $\cdot_{26}$ su zatvorene, komutativne i asocijativne, a vrijedi i distributivnost množenja prema zbrajanju).

Broj 0 je neutralni element za zbrajanje, tj. $a +_{26} 0 = 0 +_{26} a = a$, te svaki element a ima suprotni element (aditivni inverz) $-a$ (za $a \neq 0$ to je broj $26 - a$, jer vrijedi $a +_{26} (26 - a) = (26 - a) +_{26} a = 26 \bmod 26 = 0$. Nadalje, broj 1 je neutralni element za množenje, jer $a \cdot_{26} 1 = 1 \cdot_{26} a = a$, no samo neki elementi a imaju multiplikativni inverz a^{-1}, tj. element za koji vrijedi $a \cdot_{26} a^{-1} = a^{-1} \cdot_{26} a = 1$. To su oni elementi iz $\mathbb{Z}_{26}$ koji su relativno prosti s 26. Naime, kongruencija $ax \equiv 1 (\mathrm{mod}\ 26)$ ima rješenje ako i samo ako $(a, 26) | 1$, tj. $(a, 26) = 1$. Dakle, elementi i pripadni multiplikativni inverzi dani su u sljedećoj tablici:

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

Potpuno analogno definira se skup $\mathbb{Z}_m$ i operacije na njemu, za proizvoljan prirodan broj m. Dakle, Cezarovu šifru možemo definirati na sljedeći način:

Definicija 1.3 *Neka je* $\mathcal{P} = \mathcal{C} = \mathcal{K} = \mathbb{Z}_{26}$. *Za* $0 \leq K \leq 25$ *definiramo*

$$\begin{aligned} e_K(x) &= (x + K) \bmod 26 \\ d_K(y) &= (y - K) \bmod 26. \end{aligned}$$

Šifra je definirana nad $\mathbb{Z}_{26}$, pa imamo sljedeću korespondenciju koja za svako slovo daje njegov numerički ekvivalent:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19

U	V	W	X	Y	Z
20	21	22	23	24	25.

U Cezarovoj šifri osnovni elementi otvorenog teksta su slova (odnosno njihovi numerički ekvivalenti), a ključ K određuje za koliko mjesta udesno ćemo pomicati slova pri šifriranju. Očito je $d_K(e_K(x)) = x$, što se i zahtijeva u definiciji kriptosustava. Za $K = 3$ dobiva se originalna Cezarova šifra.

Primjer 1.4 *Dešifrirajmo šifrat $PWNUY\ TLWFK\ NOF$ dobiven Cezarovom šifrom.*

Rješenje:

Budući je prostor ključeva jako mali (ima ih 26), zadatak se može riješiti "grubom silom", tj. tako da ispitamo sve moguće ključeve sve dok ne dođemo do smislenog teksta:

$$\begin{aligned} K &= 0: \quad PWNUY, \dots \\ K &= 1: \quad OVMTX, \dots \\ K &= 2: \quad NULSV, \dots \\ K &= 3: \quad MTKRV, \dots \\ K &= 4: \quad LSJQU, \dots \\ K &= 5: \quad KRIPTOGRAFIJA \end{aligned}$$

Dakle, funkcija dešifriranja je $d_K(y) = (y-5) \bmod 26$. Drugim riječima, odredimo numerički ekvivalent šifrata, na njega primjenimo funkciju d_K i dobivenom broju pridružimo odgovarajuće slovo:

$$\begin{aligned} P \mapsto 15 &\mapsto 10 \mapsto K \\ &\vdots \\ F \mapsto 5 &\mapsto 0 \mapsto A. \end{aligned}$$

Primjer 1.5 *Pretpostavimo da smo presreli poruku $FQOCU\ DEM$ za koju znamo da je otvoreni tekst na engleskom jeziku šifriran Cezarovom šifrom. Želimo ju dešifrirati.*

Rješenje:

Potrebno je opet pronaći ključ K. Jedan od načina je analiza frekvencije slova. Najfrekventnija slova u engleskom alfabetu su redom

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

Kako je E najfrekventnije slovo engleskog alfabeta, razumno je pretpostaviti da je E i najfrekventnije slovo otvorenog teksta. Time smo izbor ključa sveli na 8 kombinacija.

(1) Ako je E šifrirano s F, funkcija šifriranja slijedi iz

$$5 = (4 + \underline{1}) \bmod 26,$$

pa je ključ $K = 1$ i dešifriramo sa

$$d_K(y) = (y-1) \bmod 26.$$

Dobivamo otvoreni tekst $EPNB\dots$.

(2) Ako je E šifrirano s Q, funkcija šifriranja slijedi iz

$$16 = (4 + \underline{12}) \bmod 26,$$

pa je ključ $K = 12$ i dešifriramo sa

$$d_K(y) = (y-12) \bmod 26.$$

Dobivamo otvoreni tekst $TECQ\dots$.

$\vdots$

(5) Ako je E šifrirano s U, funkcija šifriranja slijedi iz

$$20 = (4 + \underline{16}) \bmod 26,$$

pa je ključ $K = 16$ i dešifriramo sa

$$d_K(y) = (y - 16) \bmod 26.$$

Dobivamo otvoreni tekst $PAY|ME|NOW$.

Zadatak 1.6 *Dešifrirajte poruku*

$$PXPXK\ XENVD\ RUXVT\ NLXHY\ MAXYK\ XJNXG\ VRFXM\ AHW$$

šifriranu Cezarovom šifrom iz otvorenog teksta na engleskom jeziku.

Rješenje:

Najfrekventnije slovo je X. Prema tome, razumno je opet pretpostaviti da je slovo E šifrirano s X, tj. da je funkcija šifriranja dobivena iz

$$23 = (4 + \underline{19}) \bmod 26.$$

Dakle, ključ bi mogao biti $K = 19$ i funkcija dešifriranja mogla bi biti

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

Dobiva se otvoreni tekst

$$WE|WERE|LUCKY|BECAUSE|OF|THE|FREQUENCY|METHOD.$$