Afina šifra

Da bismo dobili barem malo sigurniju šifru, možemo promatrati funkcije za šifriranje koje će uključivati više od jednog parametra. Najjednostavnija takva funkcija je afina funkcija $e(x) = ax + b$. No, tu se pojavljuje jedan novi problem jer takva funkcija na skupu $\mathbb{Z}_{26}$ ne mora imati inverz (ne mora biti injekcija). Kad bi inverz postojao imali bi:

$$f(f^{-1}(x)) = x \Leftrightarrow af^{-1}(x) + b = x \Leftrightarrow f^{-1}(x) = a^{-1}x - a^{-1}b,$$

tj.

$$f^{-1}(x) = a^{-1}(x - b).$$

Zato parametar a ne može biti proizvoljan, već mora biti relativno prost s modulom 26. Afina šifra definira se na sljedeći način:

Definicija 1.1 *Neka je $\mathcal{P} = \mathcal{C} = \mathbb{Z}_{26}$, te neka je*

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

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

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

Ova šifra naziva se afinom zato što su funkcije šifriranja i dešifriranja afine. Provjerimo je li uvjet $d_K(e_K(x)) = x$ zadovoljen. Zaista,

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

Mogući parametri a 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

Primjer 1.2 *Neka je $K = (7, 3)$. Primjenom afine šifre, šifrirajmo otvoreni tekst OSIJEK.*

Rješenje:

Koristeći ranije navedenu tablicu, slova otvorenog teksta poistovjećujemo s njihovim numeričkim ekvivalentima. Imamo:

$$\begin{aligned} e_K(O) &= (14 \cdot 7 + 3) \bmod 26 = 23 \\ e_K(S) &= (18 \cdot 7 + 3) \bmod 26 = 25 \\ e_K(I) &= (8 \cdot 7 + 3) \bmod 26 = 7 \\ e_K(J) &= (9 \cdot 7 + 3) \bmod 26 = 14 \\ e_K(E) &= (4 \cdot 7 + 3) \bmod 26 = 5 \\ e_K(K) &= (10 \cdot 7 + 3) \bmod 26 = 21, \end{aligned}$$

pa je šifrat XZHOFV.

Primjer 1.3 *Dešifrirajmo šifrat*

OZWHR YEZCV WFCTP CUWRC FPYHW I

dobiven afinom šifrom iz otvorenog teksta na hrvatskom jeziku.

Rješenje:

Imamo $12 \cdot 26 = 312$ mogućih ključeva. To je još uvijek premalo, pa bismo uz pomoć računala sigurno mogli primijeniti "grubu silu", kao u Primjeru 1.4.

No, postoji i elegantniji način ukoliko znamo kojim je jezikom pisan otvoreni tekst. Ovdje nam je poznato da je otvoreni tekst pisan hrvatskim jezikom. Potrebna nam je činjenica da su najfrekventnija slova u hrvatskom jeziku A, I, O, E, N, i to upravo tim redoslijedom. U našem šifratu uočavamo da su najfrekventnija slova C i W, koja se javljaju po 4 puta. Iako je naš šifrat prekratak, možemo ipak očekivati da su ova dva slova šifrati od A, I, O, E ili N, pa pogledajmo kakve smo sreće.

Imamo $e_K(A) = a \cdot 0 + b = b, e_K(I) = 8a + b$. Pretpostavimo da je $e_K(A) = C$ i $e_K(I) = W$. Dobivamo da je $b = 2$ i $8a + b \equiv 22 (\text{mod } 26)$, odnosno $8a \equiv 20 (\text{mod } 26)$. Slijedi nam $a = 9$. Općenito se linearne kongruencije rješavaju pomoću (proširenog) Euklidova algoritma o kojem će biti više riječi kasnije, no u slučaju malog modula, kao što je naš modul 26, dovoljno je uvrstiti sve dopustive (invertibilne) a-ove, te provjeriti koji zadovoljava kongruenciju.

Dakle, dobili smo da je $e_K(x) = (9x + 2) \bmod 26$. Tada je $d_K(y) = 3(y - 2) \bmod 26$. Primijenimo li funkciju d_K na naš šifrat, dobivamo otvoreni tekst s umetnutim razmacima i dijakritičkim znakovima:

KRIPTOGRAFIJA ZNAČI TAJNOPIS.

Napomena 1.4 *Ako pretpostavimo kako pri šifriranju uzastopno koristimo dvije afine šifre, tj. funkcije šifriranja* $e_K^{(1)}(x) = (ax + b) \bmod 26$ *i* $e_K^{(2)}(x) = (mx + n) \bmod 26$*, zapitajmo se je li to prednost u odnosu na šifriranje jednom afinom funkcijom. Naime, primjenom jedne funkcije šifriranja pa onda druge, dobivano funkciju*

$$[m(ax + b) + n] \bmod 26 = [(am)x + (bm + n)] \bmod 26,$$

a to je opet afina funkcija. Dakle, uzastopno šifriranje s dvije afine funkcije isto je kao i šifriranje s jednom. Osim toga, ako je $(a, 26) = 1$ *i* $(m, 26) = 1$*, onda je i* $(am, 26) = 1$*.*

Zadatak 1.5 *Dešifrirajte šifrat*

MCCLL IMIPP ISKLN UHCGI MCKBI XCUMT IPLKX
LRIGW MCXLA MWALV CCDGJ KXYCR

dobiven primjenom afine šifre ako je poznato da je otvoreni tekst pisan engleskim jezikom.

Rješenje:

Primjenom analize frekvencije slova, uočavamo kako se slova C, I, L pojavljuju 9, 7, 7 puta redom. Kako znamo da je otvoreni tekst pisan engleskim jezikom, a najfrekventnija slova su E, T, A, O, I, N, tim redom, pretpostavimo da je

$$e_K(E) = C, \quad \text{tj.} \quad 2 = 4a + b.$$

Kako je sljedeće najfrekventnije slovo T, pretpostavit ćemo da je ono šifrirano s I ili L. Probajmo najprije s I. Slijedi

$$e_K(T) = I, \quad \text{tj.} \quad 8 = 19a + b.$$

Dakle, slijedi sustav kongruencija

$$\begin{aligned} 4a + b &\equiv 2 (\text{mod } 26) \\ 19a + b &\equiv 8 (\text{mod } 26) \end{aligned}$$

Oduzimanjem slijedi linearna kongruencija

$$15a \equiv 6 (\text{mod } 26),$$

tj. $a = 16$. Prisjetimo se definicije afine šifre. Postoji uvjet $(a, 26) = 1$. Dakle, odabir $e_K(T) = I$ nam nije dobar, pa probajmo s

$$e_K(T) = L, \quad \text{tj.} \quad 11 = 19a + b.$$

Dobivamo sustav kongruencija

$$\begin{aligned} 4a + b &\equiv 2 (\text{mod } 26) \\ 19a + b &\equiv 11 (\text{mod } 26) \end{aligned}$$

odnosno linearnu kongruenciju

$$15a \equiv 9 (\text{mod } 26),$$

tj. $a = 11$, pa je pripadni $b = 10$. Dakle, ključ bi mogao biti $K = (a, b) = (11, 10)$, pa bi funkcija dešifriranja mogla biti

$$d_K(y) = 19(y - 10) \text{ mod } 26.$$

Sada elementima šifrata pridružimo njihove numeričke ekvivalente i redom dobivamo elemente otvorenog teksta:

$$\begin{aligned} M &\to M \\ C &\to E \\ C &\to E \\ L &\to T \\ L &\to T \\ I &\to O \\ M &\to M \\ I &\to O \\ P &\to R \\ P &\to R \\ I &\to O \\ S &\to W \\ K &\to A \\ L &\to T \\ N &\to F \\ &\vdots \end{aligned}$$

Dakle, otvoreni tekst je

MEET TOMORROW AT FIVE, COME ALONE, IMPORTANT DOCUMENTS MUST BE EXCHANGED.

Zadatak 1.6 *Dešifrirajte šifrat*

TFYYX WQNKR NEOPU PFSNV CFRBR UPAWQ POPMZ PTCPT FCRAP TFHIB UFHRW FAPPW NUFCP OPACF CBZPC NTPTA BABMB RPRUA POCNZ OPMZP VNZP

dobiven primjenom afine šifre ako je poznato da je otvoreni tekst pisan hrvatskim jezikom.

Rješenje:
Primjenom analize frekvencije slova, uočavamo kako se slova P, F, C, N, R, A pojavljuju 19, 9, 8, 7, 7, 7 puta redom. Kako znamo da je otvoreni tekst pisan hrvatskim jezikom, a najfrekventnija slova su A, I, O, E, N, S, tim redom, pretpostavimo da je

$$e_K(A) = P, \quad \text{tj.} \quad 15 = 0a + b,$$

pa je $b = 15$. Kako je sljedeće najfrekventnije slovo F, pretpostavit ćemo da je ono šifrat od I ili O ili E, ili N ili S. Probajmo najprije s I. Slijedi

$$e_K(I) = F, \quad \text{tj.} \quad 5 = 8a + b.$$

Dakle, slijedi linearna kongruencija

$$18a \equiv 10 (\text{mod } 26),$$

tj. $a = 15$. Sada je funkcija dešifriranja dana sa

$$d_K(y) = 7(y - 15) \text{ mod } 26.$$

Redom dobivamo slova otvorenog teksta CILL .... Kako je otvoreni tekst pisan na hrvatskom jeziku vidimo da nam je potreban novi odabir za slovo kojemu je F šifrat. Probajmo s O. Dakle,

$$e_K(O) = F, \quad \text{tj.} \quad 5 = 14a + b,$$

pa slijedi linearna kongruencija

$$12a \equiv 10 (\text{mod } 26),$$

tj. $a = 3$. Sada je funkcija dešifriranja dana sa

$$d_K(y) = 9(y - 15) (\text{mod } 26).$$

Dobiva se otvoreni tekst

KOD DULJIH ŠIFRATA OBIČNO SE STAVLJA RAZMAK NAKON SVAKOG PETOG SLOVA ALI TO NARAVNO NEMA NIKAKVE VEZE SA STVARNIM RAZMACIMA.

Zadatak 1.7 *Dekriptirajte šifrat*

ODMFG BPUFE KCFGV LPAXU PLMDQ PCXSP VRFSF WPUDH
GXLVG DCFPU MSXCS DTGPV LFMDV GROSD TSFPS GXKSX GR

dobiven primjenom afine šifre ako je poznato da je otvoreni tekst pisan hrvatskim jezikom.

Rješenje:

Primjenom analize frekvencije slova, uočavamo kako se slova P, F, G, S, D pojavljuju 9, 8, 8, 8, 7 puta redom. Najfrekventnija slova u hrvatskom jeziku su A, I, O ,E, N, S, pa opet treba napraviti razne kombinacije šifrata i vidjeti koja će nas funkcija dešifriranja dovesti do rješenja. Ovdje je dobra kombinacija

$$e_K(I) = P, \quad \text{tj.} \quad 15 = 8a + b,$$

i

$$e_K(A) = F, \quad \text{tj.} \quad 5 = 0a + b,$$

pa je $b = 5$. Dakle, slijedi linearna kongruencija

$$8a \equiv 10 (\text{mod } 26),$$

tj. $a = 11$. Sada je funkcija dešifriranja dana sa

$$d_K(y) = 19(y - 5) \bmod 26.$$

Otvoreni tekst je

PODATCI ZA HRVATSKI JEZIK DOBIVENI SU ANALIZOM TEKSTOVA
IZ DNEVNOG TISKA DOSTUPNOG NA INTERNETU.