Šifriranje matricama

Marko Horvat

Šifriranje

Kriptografija je grana matematike koja se bavi šifriranjem i dešifriranjem tajnih poruka. U zadnje vrijeme kriptografija je sve više na cijeni zbog potrebe očuvanja privatnosti informacija prenošenih javnim putevima komunikacije. U kriptografskom žargonu koristimo, osim izraza *šifre* (eng. *cipher*), izraz *otvoreni tekst* (eng. *plaintext*) za tekst koji nije šifriran i *šifrat* (eng. *ciphertext*) za tekst koji jest šifriran. Pretvaranje otvorenog teksta u šifrat naziva se *šifriranje* (eng. *enciphering*), a šifrata u otvoreni tekst naziva se *dešifriranje* (eng. *deciphering*). Najjednostavniji način šifriranja predstavljaju *supstitucijske šifre* (eng. *substitution ciphers*). Te šifre se baziraju na bijektivnom preslikavanja slova abecede u neke simbole ili druga slova abecede i obrnuto. Upravo zbog objektivno-bijektivnih razloga spomenute su šifre vrlo slabe (npr. Cezarova 3-šifra, u kojoj A prelazi u D, B u E itd.), jer to znači da ih možemo probiti statističkim metodama (npr. traženjem najčešćih bigrama i trigrama u hrvatskom jeziku i sl.).

Jedan od načina da se takvo što spriječi jest uvođenje *Hillove šifre* u kojoj se slova poruke svrstavaju u skupove od po 2, 3 ili n slova, a svaki od tih skupova bit će zamijenjen skupom od novih n slova.

Demonstrirat ćemo šifriranje na Hillovoj 2-šifri (koristit ćemo englesku abecedu):

Korak 1. Izaberemo matricu tipa 2×2 s cjelobrojnim elementima:

$$A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$$

Korak 2. Grupiramo slova otvorenog teksta u parove, dodajući bilo kakvo slovo na kraj ako tekst ima neparni broj slova i zamijenimo svako slovo ostatkom dijeljenja njegovog mjesta u abecedi s brojem 26 (dakle, A zamijenimo s 1, B s 2 itd., a Z s 0.

Korak 3. Svaki par brojeva p_1p_2 zapišemo kao vektor

$$P = \begin{bmatrix} p_1 \\ p_2 \end{bmatrix}$$

i nađemo produkt A_p. Nazvat ćemo p *vektorom otvorenog teksta*, a A_p odgovarajućim *vektorom šifrata*.

Korak 4. Pretvorimo svaki vektor šifrata u njegov abecedni ekvivalent.

Koristeći matricu

$$\begin{bmatrix} 1 & 9 \\ 8 & 5 \end{bmatrix}$$

pronađimo Hillovu šifru za poruku

SKRIVAM SE

Ova poruka ima neparan broj slova, pa ćemo dodati još jedno i grupirati ih u skupove od po 2 slova

SK RI VA MS EE

i konačno ih zamijeniti brojevima na gore opisani način:

19 11 18 9 22 1 13 19 5 5

Kako bismo šifrirali par SK, izračunamo produkt matrice koju smo zadali i vektora tog prvog para:

$$\begin{bmatrix} 1 & 9 \\ 8 & 5 \end{bmatrix} \begin{bmatrix} 19 \\ 11 \end{bmatrix} = \begin{bmatrix} 118 \\ 207 \end{bmatrix}$$

Budući da nam je na raspolaganju 26 slova engleske abecede, od 118 i 207 uzimamo samo ostatak njihovog dijeljenja s 26, tj. 14 i 25. Znači, dobili smo vektor s elementima 14 i 25. Ostala množenja izgledaju ovako:

$$\begin{bmatrix} 1 & 9 \\ 8 & 5 \end{bmatrix} \begin{bmatrix} 18 \\ 9 \end{bmatrix} = \begin{bmatrix} 99 \\ 189 \end{bmatrix} \equiv \begin{bmatrix} 21 \\ 7 \end{bmatrix} \pmod{26}$$

$$\begin{bmatrix} 1 & 9 \\ 8 & 5 \end{bmatrix} \begin{bmatrix} 22 \\ 1 \end{bmatrix} = \begin{bmatrix} 31 \\ 181 \end{bmatrix} \equiv \begin{bmatrix} 5 \\ 25 \end{bmatrix} \pmod{26}$$

$$\begin{bmatrix} 1 & 9 \\ 8 & 5 \end{bmatrix} \begin{bmatrix} 13 \\ 19 \end{bmatrix} = \begin{bmatrix} 184 \\ 199 \end{bmatrix} \equiv \begin{bmatrix} 2 \\ 17 \end{bmatrix} \pmod{26}$$

$$\begin{bmatrix} 1 & 9 \\ 8 & 5 \end{bmatrix} \begin{bmatrix} 5 \\ 5 \end{bmatrix} = \begin{bmatrix} 50 \\ 65 \end{bmatrix} \equiv \begin{bmatrix} 5 \\ 13 \end{bmatrix} \pmod{26}$$

Navedeni vektorski parovi određuju slova:

NY NG EY EQ EM

Najčešće uzimamo poruku bez razmaka:

NYNGEYEQEM

Dešifriranje

Sad ćemo se pozabaviti *recipročnim inverzom* broja a.

> **Definicija:** Ako je $a \in \mathbb{Z}_m$ gdje je $\mathbb{Z}_m$ skup cijelih brojeva $0, 1, 2, \ldots, m-2, m-1$, onda je broj a^{-1} *recipročni inverz* ostatka dijeljenja a sa m ako vrijedi $aa^{-1} = a^{-1}a = 1 (\mathrm{mod}\ m)$.

Dokazat ćemo da ako a i m nemaju zajedničkih prostih faktora, onda a ima jedinstveni recipročni inverz modulo m; obrnuto, ako a i m imaju zajednički prosti faktor, a nema recipročni inverz modulo m.

Dokaz. Neka je $\mathrm{nzd}(a, m) = 1$. Pretpostavimo suprotno tj. da ne postoji b takav da je

$$ab \equiv 1 \pmod{n}.$$

Neka je $b_i = i$ za $i = 1, 2, \ldots, m-1$ i c_i takav da je

$$ab_i = c_i \pmod{m}.$$

S obzirom da ni a ni b_i nisu djeljivi s m tada vrijedi da je $c_i \neq 0$. Kako imamo $m-1$ broj ostataka $(c_1, c_2, \ldots, c_{m-1})$, koji mogu biti samo u skupu ostataka $(2, 3, \ldots, m-1)$, znači (po Dirichletovom pravilu) da postoje $k \neq j$ takvi da je $c_k = c_j$. Oduzimanjem k-te i j-te jednadžbe dobivamo

$$a(b_k - b_j) \equiv c_k - c_j \equiv 0 \pmod{m}.$$

Kako je $1 \leq |b_k - b_j| \leq m-1$, to znači da postoji b_l takav da je $ab_l \equiv 0 \pmod{m}$, što je kontradikcija (jer smo rekli da takav broj ne postoji)! Ako je $\text{nzd}(a,b) = d > 1$, tada je uvijek $ab \equiv d \cdot k \neq 1 \pmod{m}$, $k \in \mathbb{Z}$. ■

Recipročni inverz broja a modulo m dobivamo tako da postavimo modularnu jednadžbu

$$ax = 1(\text{mod } m)$$

Nećemo ovdje zbog kompleksnosti predstaviti opće metode rješavanja ovakvih jednadžbi, nego ćemo proći sve cijele brojeve od 0 do 26 kao moguća rješenja, što je srećom moguće jer ih je vrlo malo. Prema tome, možemo sastaviti sljedeću tablicu recipročnih inverza modulo 26:

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

Ova nam tablica pomaže pri traženju inverza matrice kojom smo šifrirali, i to modulo 26. Ako se elementi kvadratne matrice

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

nalaze u Z_{26} i ostatak $\det(A) = ad - bc$ modulo 26 nije djeljiv s 2 ili 13, inverz od $A(\text{mod } 26)$ jest:

$$A^{-1} = (ad - bc)^{-1} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} (\text{mod } 26)$$

Nađimo inverz matrice

$$A = \begin{bmatrix} 1 & 9 \\ 8 & 5 \end{bmatrix}$$

modulo 26.

$$\det(A) = ad - bc = 1 \cdot 5 - 9 \cdot 8 = -67$$

Ne možemo koristiti tablicu koju smo napravili jer je broj -67 izvan njezinog opsega. Ali, koji je ostatak dijeljenja negativnog cijelog broja pozitivnim cijelim brojem? Postoji li neki poučak s time u vezi? Naravno da postoji:

Teorem o ostatku: Za svaki cijeli broj a i djelitelj m neka je

$$R = \text{ostatak od } \frac{|a|}{m}$$

Onda je ostatak ra modulo m jednak:

$$r = \begin{cases} R & \text{ako } a \geq 0 \\ m - R & \text{ako } a < 0 \wedge R \neq 0 \\ 0 & \text{ako } a < 0 \wedge R = 0 \end{cases}$$

To svojstvo primijenimo na broj -67:

$$(-67)^{-1} = 19(\text{mod } 26)$$

Iz gore navedene jednakosti dobivamo:

$$A^{-1} = 19 \begin{bmatrix} 5 & -9 \\ -8 & 1 \end{bmatrix} = \begin{bmatrix} 95 & -171 \\ -152 & 19 \end{bmatrix} = \begin{bmatrix} 17 & 11 \\ 4 & 19 \end{bmatrix} (\text{mod } 26)$$

Dobro je ovdje napraviti provjeru:

$$AA^{-1} = \begin{bmatrix} 1 & 9 \\ 8 & 5 \end{bmatrix} \begin{bmatrix} 17 & 11 \\ 4 & 19 \end{bmatrix} = \begin{bmatrix} 53 & 182 \\ 156 & 183 \end{bmatrix} \pmod{26} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \pmod{26}$$

Za kraj ćemo se pokušati vratiti na otvoreni tekst koji smo šifrirali. Na raspolaganju su nam cijeli šifrat i šifra. Krenimo od šifrirane poruke, praveći se da ne znamo njezin pravi sadržaj:

NYNGEYEQEM

Grupirajmo opet slova u parove:

NY NG EY EQ EM

Zamijenimo slova brojčanim ekvivalentima iz tablice:

14 25 14 7 5 25 5 17 5 13

Da bismo dobili parove u otvorenom tekstu, pomnožimo svaki vektor šifrata inverzom matrice A:

$$\begin{bmatrix} 17 & 11 \\ 4 & 19 \end{bmatrix} \begin{bmatrix} 14 \\ 25 \end{bmatrix} = \begin{bmatrix} 513 \\ 531 \end{bmatrix} = \begin{bmatrix} 19 \\ 11 \end{bmatrix} \pmod{26}$$

$$\begin{bmatrix} 17 & 11 \\ 4 & 19 \end{bmatrix} \begin{bmatrix} 21 \\ 7 \end{bmatrix} = \begin{bmatrix} 434 \\ 217 \end{bmatrix} = \begin{bmatrix} 18 \\ 9 \end{bmatrix} \pmod{26}$$

$$\begin{bmatrix} 17 & 11 \\ 4 & 19 \end{bmatrix} \begin{bmatrix} 5 \\ 25 \end{bmatrix} = \begin{bmatrix} 360 \\ 495 \end{bmatrix} = \begin{bmatrix} 22 \\ 1 \end{bmatrix} \pmod{26}$$

$$\begin{bmatrix} 17 & 11 \\ 4 & 19 \end{bmatrix} \begin{bmatrix} 2 \\ 17 \end{bmatrix} = \begin{bmatrix} 221 \\ 331 \end{bmatrix} = \begin{bmatrix} 13 \\ 19 \end{bmatrix} \pmod{26}$$

$$\begin{bmatrix} 17 & 11 \\ 4 & 19 \end{bmatrix} \begin{bmatrix} 24 \\ 13 \end{bmatrix} = \begin{bmatrix} 551 \\ 343 \end{bmatrix} = \begin{bmatrix} 5 \\ 5 \end{bmatrix} \pmod{26}$$

Prema tablici, odgovarajuća slova jesu:

SK RI VA MS EE,

odnosno, poruka glasi:

SKRIVAM SE.

KAKO ISKORISTITI OVU METODU ŠIFRIRANJA NA RAČUNALU, SAZNAJTE NA STRANICI 24. U ČLANKU „MATRICE U MAPLE-U”