Kriptoanaliza transpozicijske stupčane šifre

Ante Barbarić

3. studenoga 2021.

Osnovni pojmovi

1. kriptografija
2. pošiljaoc i primaoc
3. otvoreni tekst
4. šifrat
5. ključ

Definicija kriptosustava

Definicija 1. *Kriptosustav je uređena petorka* $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ *za koju vrijedi:*

1. $\mathcal{P}$ *je konačan skup svih mogućih osnovnih elemenata otvorenog teksta;*
2. $\mathcal{C}$ *je konačan skup svih mogućih osnovnih elemenata šifrata;*
3. $\mathcal{K}$ *je 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* $d_K(e_K(n)) = n$ *za svaki otvoreni tekst* $n \in \mathcal{P}$.

Kriptosustavi

Podjela kriptosustava s obzirom na tajnost ključeva:

- simetrični kriptosustavi sa stranim ključem
- asimetrični kriptosustavi s javnim ključem

Transpozicijske šifre

- Podjelu šifri na supstitucijske i transpozicijske uveo je u 16. stoljeću Giovanni Porta.
- Kriptosustavi koje smo do sada promatrali uključuju supstituciju: elementi otvorenog teksta zamjenjivani su različitim elementima šifrata.
- Sada se osnovni elementi otvorenog teksta ostave nepromijenjeni, ali se promjeni njihov međusobni položaj.

Prvi primjer transpozicijskih šifri

- Spartanci su u 5. stoljeću prije Krista upotrebljavali napravu za šifriranje zvanu **skital**
- Drveni štap oko kojeg se namotavala vrpca od pergamenta po kojoj se pisala poruka kako je prikazano na slici

Skital

- Pretpostavimo da na štap možemo napisati četiri slova u krug i pet po dužini
- Neka otvoreni tekst glasi: **Brodovi su usidreni u Mikeni**
- Takav tekst, namotan na skital, bi izgledao na ovaj način:

$$Brodov$$

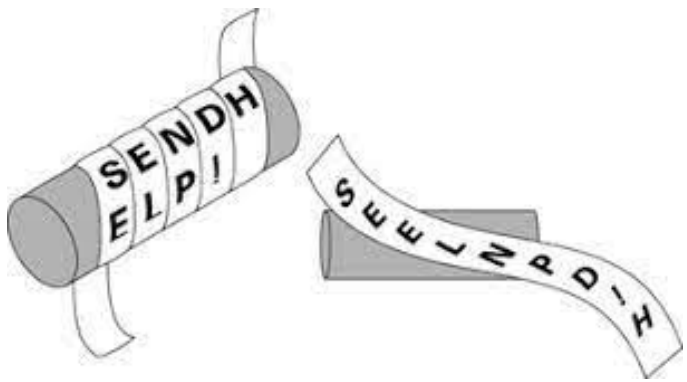
$$isuusi$$

$$dreniu$$

$$Mikeni$$

Skital

- Šifrat koji dobijemo čitajući po stupcima:
  BIDMR SRIOU EKDUN EOSIN VIUI
- Dešifriranje se odvija na način da namotamo tekst na štap i pročitamo uzduž pa bi se svako peto slovo pojavilo u istom retku te bi otvoreni tekst izgledao ovako:
  BRODOVI SU USIDRENI U MIKENI



Definicija transpozicijske šifre

Definicija 2. *Neka je m fiksan prirodan broj. Neka je $\mathcal{P} = \mathcal{C} = \mathbb{Z}_{26}^m$, te neka se $\mathcal{K}$ sastoji od svih permutacija skupa $\{1,2,\ldots,m\}$. Za $\pi \in \mathcal{K}$ definiramo*

$$e_\pi(x_1, x_2, \ldots, x_m) = (x_{\pi(1)}, x_{\pi(2)}, \ldots, x_{\pi(m)})$$
$$d_\pi(y_1, y_2, \ldots, y_m) = (y_{\pi^{-1}(1)}, y_{\pi^{-1}(2)}, \ldots, y_{\pi^{-1}(m)}).$$

Stupčana transpozicija

- Najupotrebljavanija transpozicijska šifra
- U njoj se otvoreni tekst upisuje u pravokutnik po redcima, a zatim se poruka čita po stupcima, ali s promijenjenim poretkom stupaca ovisno o ključu.
- Nadalje, ako se posljednji redak ne ispuni do kraja, onda se prazna mjesta popune proizvoljnim slovima (nulama) koja ne mijenjaju sadržaj poruke.

Primjer šifriranja teksta stupčanom transpozicijom

Pogledajmo jedan uvodni primjer.

Primjer 3. *Šifrirajmo otvoreni tekst*

She said don't let go never give up its such a wonderful life.

stupčanom transpozicijom s ključnom riječi FLOWER.

Rješenje

Rješenje:

Ovdje imamo tablicu gdje se u prvom redu nalazi ključ, a ispod njega je napisan otvoreni tekst.

2	3	4	6	1	5
S	H	E	S	A	I
D	D	O	N	T	L
E	T	G	O	N	E
V	E	R	G	I	V
E	U	P	I	T	S
S	U	C	H	A	W
O	N	D	E	R	F
U	L	L	I	F	E

S obzirom na naš ključ, šifrat izgleda ovako (kod transpozicijskih šifri obično se šifrat grupira u blokove od pet slova):

ATNIT ARFSD EVESO UHDTE UUNLE OGRPC DLILE VSWFE SNOGI HEI.

Dekriptiranje transpozicijske šifre

1. Odredimo dimenziju pravkutnika
   - 1.1 broj slova u šifratu se faktorizira
   - 1.2 ako imamo više mogućnosti, upišemo slova šifrata po stupcima u pravokutnike pretpostavljenih dimenzija, te promatramo odnos samoglasnika i suglasnika u svakom retku
2. Odrediti poredak stupaca
   - 2.1 Ako je broj stupaca relativno mali, šifrat možemo dešifrirati tako da jednostavno premještamo stupce dok ne dobijemo smisleni sadržaj u redcima
   - 2.2 Dodatnu pomoć nam mogu dati podatci o frekvencijama bigrama

Primjer dekriptiranja

Primjer 4. *Dešifrirajmo šifrat*

EEBOO EKDSM NJAMR NCPOT SOAEO AULKA DOJSO EKSEA

dobiven stupčanom transpozicijom iz otvorenog teksta na hrvatskom jeziku.

Rješenje dekriptiranja

Rješenje:

U šifratu imamo 40 slova, pa se kao najvjerojatnije dimenzije pravokutnika nameću 5×8 i 8×5 (razumno je pretpostaviti da ni broj stupaca ni broj redaka nisu jako mali - u prvom slučaju bi anagramiranje bilo trivijalno za obaviti, a u drugom duljina ključa ne bi bila bitno kraća od duljine otvorenog teksta). Ako upišemo šifrat u pravokutnike tih dimenzija, dobivamo:

E	S	C	O	J	2:3
E	M	P	A	S	2:3
B	N	O	U	O	3:2
O	J	T	L	E	2:3
O	A	S	K	K	2:3
E	M	O	A	S	3:2
K	R	A	D	E	2:3
D	N	E	O	A	3:2

E	E	N	N	S	A	D	E	4:4
E	K	J	C	O	U	O	K	3:5
B	D	A	P	A	L	J	S	2:6
O	S	M	O	E	K	S	E	4:4
O	M	R	T	O	A	O	A	5:3

Rješenje dekriptiranja

S obzirom na odnos samoglasnika i suglasnika u hrvatskom jeziku možemo zaključiti da je prvi izbor dimenzija vjerojatniji. Sada ovih pet stupaca možemo pokušati "anagramirati" tako da dobijemo smisleni tekst. Na početku nam tu može pomoći već spomenuta frekvencija bigrama.

Za svaki od parova stupaca, pogledajmo koliko se od tako dobivenih pet bigrama nalazi među prethodnih 36 najfrekventnijih. Tako dobijemo sljedeću tablicu:

	1	2	3	4	5
1	-	1	2	0	1
2	0	-	3	1	5
3	2	1	-	0	1
4	2	2	1	-	3
5	2	2	0	1	-

Rješenje dekriptiranja

Možemo primijetiti da je broj pet najveći od svih brojeva u tablici. Stoga možemo krenuti od pretpostavke da stupci 2 i 5 dolaze jedan do drugoga (u tom poretku). Obzirom na stupac 5 dalje možemo iz tablice pretpostaviti da je do stupca 5 stupac 1. Preostaje nam još za smjestiti stupce 3 i 4. Imamo dvije mogućnosti: 42513 i 32514. Sada lako provjerimo da prvi izbor daje rješenje šifrata. Odnosno,

Osjećam se puno bolje otkako sam se odrekao nade.

Uvod u stupčanu transpoziciju s dva ključa

- Stupčana transpozicija se može lako razbiti ukoliko treća strana dođe u posjed šifriranog teksta
- Ona može lako pogoditi dimenzije pravokutnika i slagati anagrame dok se ne dobije neka smislena cjelina, tako da joj je to veliki nedostatak.
- Sigurnost transpozicijskih šifara se može znatno povećati korištenjem više koraka transpozicije(npr. dvostruke transpozicijske šifre)

Stupčana transpozicija s dva ključa

- Stupčana transpozicija se stoga upotrebljavala do 50-ih godina prošlog stoljeća, a onda je poboljšana sa stupčanom šifrom s dva ključa.
- Stupčana šifra s dva ključa jedna je od najpopularnijih šifri zbog svoje jednostavnosti i visoke razine sigurnosti.
- Dva ključa K1 i K2 moraju biti unaprijed dogovoreni i odabrani.
- Šifrirajmo otvoreni tekst na engleskom jeziku: **This is a secret text encrypted by the double transposition cipher** koristeći ključeve K1=KEYWORD i K2=SECRET.

3	2	7	6	4	5	1
K	E	Y	W	O	R	D
T	H	I	S	I	S	A
S	E	C	R	E	T	T
E	X	T	E	N	C	R
Y	P	T	E	D	B	Y
T	H	E	D	O	U	B
L	E	T	R	A	N	S
P	O	S	I	T	I	O
N	C	I	P	H	E	R

Tablica 2: *Prvi korak šifriranja*

1	2	3	4	5	6	7
D	E	K	O	R	W	Y
A	H	T	I	S	S	I
T	E	S	E	T	R	C
R	X	E	N	C	E	T
Y	P	Y	D	B	E	T
B	H	T	O	U	D	E
S	E	L	A	N	R	T
O	O	P	T	I	I	S
R	C	N	H	E	P	I

Tablica 3: *Drugi korak šifriranja*

5	2	1	4	3	6
S	E	C	R	E	T
A	T	R	Y	B	S
O	R	H	E	X	P
H	E	O	C	T	S
E	Y	T	L	P	N
I	E	N	D	O	A
T	H	S	T	C	B
U	N	I	E	S	R
E	E	D	R	I	P
I	C	T	T	E	T
S	I				

Tablica 4: *Treći korak šifriranja*

1	2	3	4	5	6
C	E	E	R	S	T
R	T	B	Y	A	S
H	R	X	E	O	P
O	E	T	C	H	S
T	Y	P	L	E	N
N	E	O	D	I	A
S	H	C	T	T	B
I	N	S	E	U	R
D	E	I	R	E	P
T	C	E	T	I	T
	I			S	

Tablica 5: *Četvrti korak šifriranja*

- Završni šifrat pročitamo redom po stupcima:
  RHOTN SIDTT REYEH NECIB XTPOC SIEYE CLDTE RTAOH EITUE ISSPS NABRP T.

Literatura

- https://repozitorij.mathos.hr/islandora/object/mathos
- http://www.mathos.unios.hr/ mdjumic/uploads/diplomski/
- https://web.math.pmf.unizg.hr/ duje/kript/transp.html
- https://stackoverflow.com/
- https://github.com/
- https://crypto.interactive-maths.com/columnar-transposition-cipher.html