

Kriptografija: Umijeće kodiranja



MLADI NADARENI MATEMATIČARI

Marin Getaldić

`mnmm@getaldic.org` • `www.getaldic.org`

Sebastijan Dumančić

Požega, 13. studenog 2010.

Osnovni pojmovi

Skital

Metode šifriranja

Supstitucijske šifre

Statistička analiza teksta

Vigenereova šifra

Transpozicijske šifre

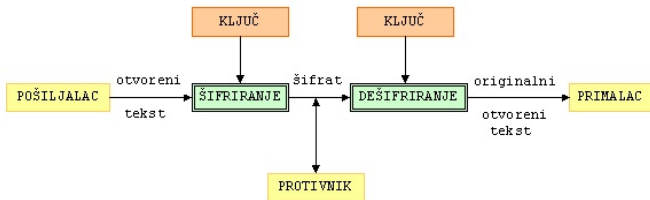
Naprave za šifriranje

Moderna kriptografija

Zagonetke

Osnovni pojmovi

- Kriptografija = tajnopis (grč.)
- Znanstvena disciplina koja se bavi proučavanjem metoda za slanje poruka u takvom obliku da ih samo onaj kome su namijenjene može pročitati
- Osnovni zadatak: omogućiti Alice i Bobu komunikaciju putem nesigurnog kanala tako da Oscar, koji nadzire kanal, ne može pročitati njihove poruke



Slika 1: klasična struktura kriptiranog kanala.

Skital

- Jedna od prvih poznatih metoda šifriranja
- Sparta, 500 pr.Kr



Slika 2: skital.

- Namotavanje pergamenta na štap određene duljine
- Za dekodiranje potrebno je imati štap jednake debljine

Metode šifriranja

- Supstitucija
- Transpozicija
- Blokovske šifre
- Kriptosustavi s javnim ključem
- Kriptosustavi s tajnim ključem

Cezarova šifra

- Slova otvorenog teksta zamjenjuju se slovima što se nalaze x mjesta dalje od njih u alfabetu

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

Slika 3: Primjer Cezarove šifre.

- Definirana je funkcijom: $y = ax + b$
- a mora biti relativno prost s 26
- Slovima se pridodaju numeričke vrijednosti
- Šifrat je $y \bmod 26$

Statistička analiza teksta

- Broji se pojavljivanje svakog slova u šifratu te se uspoređuje s poznatim podacima o distribuciji slova u jeziku
- Bigrami, trigrami

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

Slika 4: Frekvencija slova u hrvatskom jeziku.

Statistička analiza teskta

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
127	91	82	75	70	67	63	61	60	43	40	28	28	24	23	22	20	20	19	15	10	8	2	1	1	1

Slika 5: Frekvencija slova u engleskom jeziku.

- Najfrekventniji bigrami u hrvatskom su : je (2.7%), *na*, *ra*(1.5%), *st*, *an*, *ni*, *ko*, ... (1%).
- a na engleskom: *th*(3.2%), *he*(2.5%), *an*, *in*, *er*, *re*(1%).

- Polialfabetni sustav
- Svako slovo se može preslikati u m mogućih (m je duljina ključa)
- Aritmetička metoda
- $m = \text{BROJ } (1,17,14,19)$
otvoreni tekst = KRIPTOLOGIJA $(10,17,8,15,19,14,11,14,6,8,9,0)$
 $(LIWYUFZXHZXJ)$

- Dugo se smatrala savršenom šifrom
- Kasiskijev test
 - temelji se na traženju ponavljanja
 - n -torke udaljene za neki višekratnik od m

Transpozicijske šifre

- Temelji se na promjeni međusobnih
- Slova ostaju nepromijenjena

ključ	4	3	1	2	5	7	6
Otvoreni tekst	K	R	I	P	T	O	G
	R	A	F	I	J	A	I
	K	R	I	P	T	O	A
	N	A	L	I	Z	A	X

Slika 6: Primjer transpozicijske šifre.

- Šifrat je: *IFILPIPIRARAKRKNTJTZGIAXOAOA*

Cardanova rotacijska rešetka

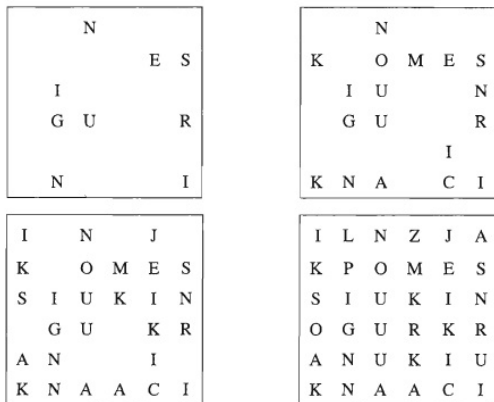
- Temelji se na izboru određenih elemenata iz geometrijske rešetke
- Kvadratna rešetka se dijeli na četiri jednaka kvadrata koja permutiraju skup brojeva
- Svaki kvadrat je rotiran za 90° od prethodnog kvadrata

Cardanova rotacijska rešetka

1	2	3	7	4	1
4	5	6	8	5	2
7	8	9	9	6	3
3	6	9	9	8	7
2	5	8	6	5	4
1	4	7	3	2	1

Slika 7: Cardanova rešetka.

Cardanova rotacijska rešetka

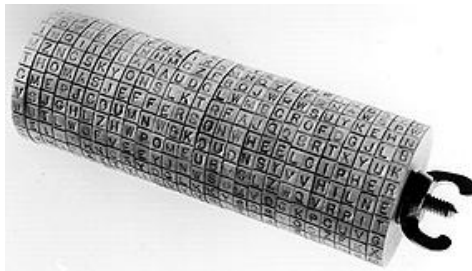


Slika 8: Enkripcija pomoću Cardanove rešetka.

- Šifriranje $\Rightarrow$ matematička funkcija
- Dešifriranje $\Rightarrow$ inverzna funkcija funkciji šifriranja

Naprave za šifriranje

- Jeffersonov kotač za šifriranje



Slika 9: Jeffersonov kotač.

Naprave za šifriranje

- Hebernov električni stroj za kodiranje



Slika 10: Hebernov električni stroj.

Naprave za šifriranje

- ENIGMA



Slika 11: ENIGMA.

Moderna kriptografija

- Algoritamska teorija brojeva
- Pseudoslučajni brojevi
- DES, RSA kriptosustavi
- Kriptosustavi zasnovani na problemu diskretnog logaritma
- Hash funkcije
- ...

- Šifrat: OZWHR YEZCV WFCTP CUWRC FPYHWI
- Afina šifra ($a = 3, b = 7$)
- Rješenje: KRIPTOGRAFIJA ZNAČI TAJNOPIS

- Šifrat: TQCWT QCKIQ RWNOQ OBCEW OQVKB UKAPK
OQOQB CQPQA JGDUQ EQORW TSJGR WEQKY WGTWC
JKRBI KZGVO GBQ
- Statistička analiza teksta
- Matematika je znanstvena disciplina nastala proučavanjem brojeva i geometrijskih odnosa.

- Šifrat: GSIQI TUKQI EAOHR VUGLT AZGHX UHLPJ MRTTN
QRBZI AVBTG QTBY MYAIV OMZTA IXJBT EDEWV QWADV
WGOOK NQNTC IPEGP Y BOK USECN WELLC PZUMI
VWFUI JMYAT UEXIS LMZTN PGUJH TMERX JSYSI VWABG
VWFDT ZILNT IEDEF JMFAM PNQZB RSDIZ PRMLG
VKFED ZXMVX VQMJX WSLEE QRMAE PRUJX IMFNT

- Kasiskijev test
- potrebno je uočiti ponavljanja: MYA s početkom na pozicijama 50 i 115 ($115 - 50 = 65 = 5 \cdot 13$)
MZT s početkom na pozicijama 56 i 125 ($125 - 56 = 69 = 3 \cdot 23$)
EDE ($160 - 65 = 95 = 5 \cdot 19$)
IVW ($143 - 108 = 35 = 5 \cdot 7$)
VWF ($149 - 109 = 40 = 5 \cdot 8$)
- Rješenje: Uspjeh u rješavanju nepoznatih šifara mjeri se ovim četirima pokazateljima, redom kako su ovdje navedeni: upornošću, pažljivim postupcima analize, intuicijom i srećom. Sposobnost da se zna barem čitati jezik originalnog teksta veoma je poželjna, ali nije bitna

- Šifrat: AAOSA JRTIE EAAAU SCEAE IANPI JAJJN FVSOI
RZVPH NIONA RNZIJ INUSS NTRZU TIC
- Transpozicijska šifra: dimenzije 7x9, ključna riječ: 5 1 6 4 2 7 3
- Otvoreni tekst: ZA RJEŠAVANJE NEPOZNATIH ŠIFARA
NAJVAŽNIJI SU UPORNOST, INTUICIJA I SREĆA.

- Šifrat: TCPNP RLGCL YYTVL OGTHP
- Cezarova šifra; A odgovara pomaknutoj abecedi od L
- Otvoreni tekst: I REČE GAVRAN NIKAD VIŠE