Teorija brojeva i kriptografija

Andrej Dujella

PMF-Matematički odsjek, Sveučilište u Zagrebu
HAZU, Razred za matematičke, fizičke i kemijske znanosti
e-mail: duje@math.hr
URL: http://web.math.pmf.unizg.hr/~duje/

1972. – 1979. Osnovna škola Novigrad

Znanstveni skup **NOVIGRAD NEKAD I SAD**

Teorija brojeva

Teorija brojeva je grana matematike koja se ponajprije bavi proučavanjem svojstava cijelih brojeva.

Ima vrlo dugu i bogatu povijest (Euklid, Euler, Gauss).

Dugo je smatrana "najčišćom" granom matematike, u smislu da je bila najdalja od bilo kakvih konkretnih primjena.

Danas je teorija brojeva jedna od najvažnijih grana matematike za primjene u kriptografiji i sigurnoj razmjeni informacija (od 1975. godine nadalje).

Djeljivost:

- Je li broj 123456789 djeljiv s 9?
- Naći ostatak pri dijeljenju broja 2^{100} sa 101.

Prosti brojevi i faktorizacija:

- Je li broj 91 prost?
- Je li broj $2^{31}-1$ prost?
- Rastaviti na proste faktore broj 1001.
- Rastaviti na proste faktore broj $2^{32}+1$.

Diofantske jednadžbe:

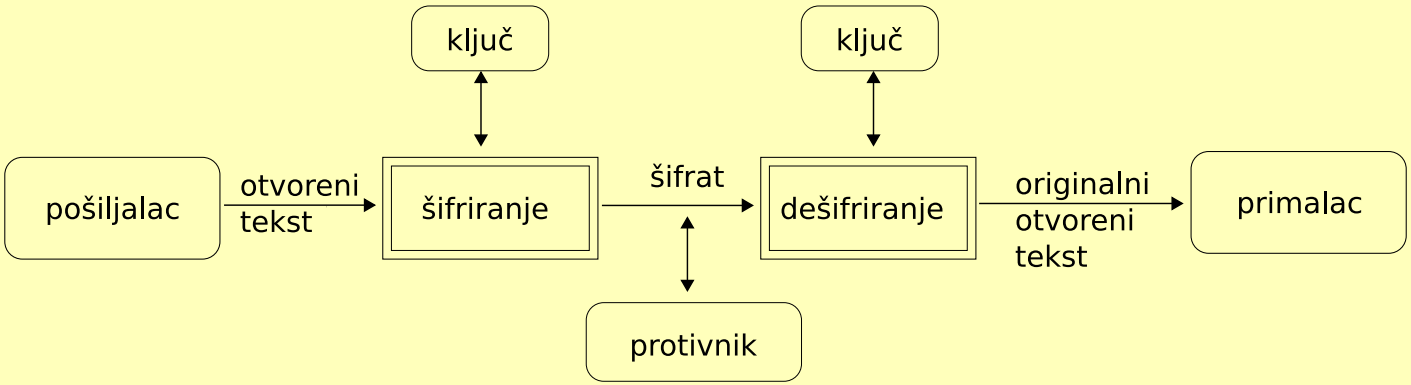
$$3x+5y=28$$

$$x^2-2y^2=1$$

$$y^2=(x+1)(3x+1)(8x+1)$$

Kriptografija

Šifriranje ili kriptografija (tajnopis) je znanstvena disciplina koja se bavi proučavanjem metoda za slanje poruka u takvom obliku da ih samo onaj kome su namijenjene može pročitati.

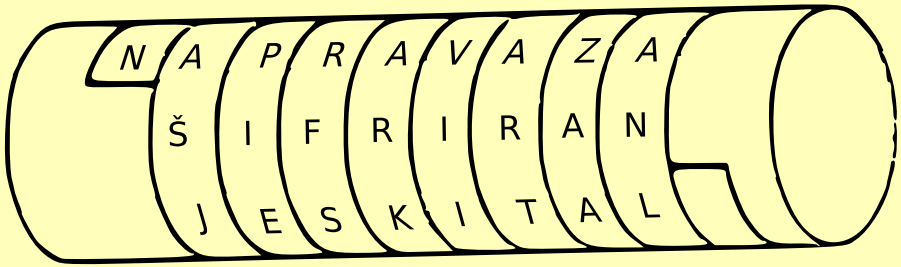


Glavne metode klasične kriptografije:

- transpozicija (premještanje) TAJNA $\mapsto$ JANAT
- supstitucija (zamjena) TAJNA $\mapsto$ UBKOB

Transpozicijske šifre

Skital (Sparta, 5. st. pr. Kr.)



Stupčana transpozicija

Poruka se piše po redcima, a čita po stupcima, ali s promijenjenim poretkom stupaca

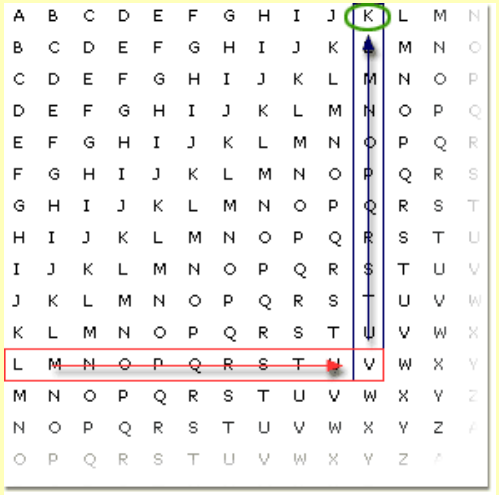
6	1	3	7	5	2	4
S	T	U	P	Č	A	N
A	T	R	A	N	S	P
O	Z	I	C	I	J	A

TTZASJURINPAČNISAOPAC

Supstitucijske šifre

Cezarova šifra (1. st. pr. Kr.)
- svako slovo se pomakne za k mjesta u alfabetu,
- Cezar je koristio šifru s $k = 3$

Vigenèreova šifra (16. st. – 19. st.)
- ključna riječ $(k_1, k_2, \ldots, k_m)$,
- slova se pomiču redom za $k_1, k_2, \ldots, k_m, k_1, k_2, \ldots$ mjesta



ENIGMA (1920. – 2. svjetski rat)

- najpoznatija naprava za šifriranje
- Kriptoanaliza: Marian Rejewski i Alan Turing

Hrvatska:

- Ivan Krstitelj Prus: Cryptographia nova seu Ars cryptographica noviter inventa (Nova kriptografija ili nedavno izmišljena kriptografska vještina, 1732.)

- Jules Verne: Mathias Sandorf - roman u kojem se opisuju urote u Austro-Ugarskoj, koje uključuju slanje šifriranih poruka; važan dio radnje se odvija u Hrvatskoj, posebno u Dubrovniku te pazinskom Kaštelu (može se možda usporediti s romanom Kletva Augusta Šenoe, čiji se dio radnje odvija u novigradskoj Fortici)

Razmjena ključeva

Sigurnost svih do sada navedenih kriptosustava leži u tajnosti ključa.

Problem: Kako sigurno razmijeniti ključ?

Ideja: Korištenje tzv. jednosmjernih funkcija, tj. funkcija koje se računaju lako, ali se njihov inverz računa jako teško.

Osnova za rješenje problema razmjene ključeva su "teški" matematički problemi:

- faktorizacija velikih složenih brojeva
- problem diskretnog logaritma (DLP)

$$a^x \equiv b \pmod{p}$$

- eliptički diskretni logaritam (ECDPL)

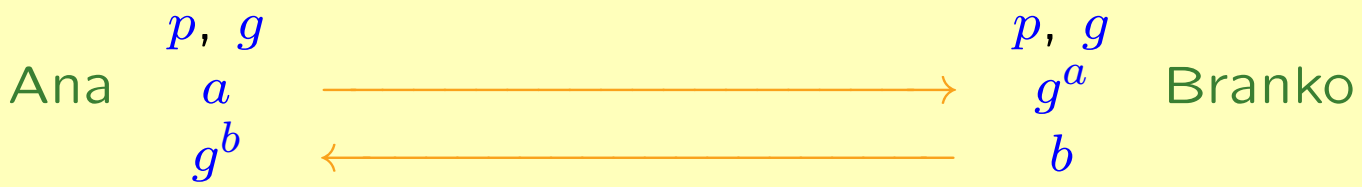
Diffie–Hellmanov protokol za razmjenu ključeva

p je veliki prosti broj; g je generator modulo p, tj. broj sa svojstvom da brojevi $\{g, g^2, \ldots, g^{p-1}\}$ daju različite ostatke pri dijeljenju s p (često se može uzeti da je $g = 2$)

Primjer: Grupa $\mathbb{Z}_{11}^* = \{1, 2, \ldots, 10\}$ (operacija je množenje modulo 11); generator je $g = 2$.

x	1	2	3	4	5	6	7	8	9	10
2^x	2	4	8	5	10	9	7	3	6	1

Ana i Branko žele se dogovoriti o jednom tajnom broju iz skupa $\{1, 2, \ldots, p-1\}$, preko nesigurnog komunikacijskog kanala kojeg prisluškuje Eva.



Eva: p, g, g^a, g^b

Ana: $(g^b)^a = g^{ab}$ ↘

Branko: $(g^a)^b = g^{ab}$ ↗

razmijenili su ključ

Eva: g^a, g^b ? g^{ab}

Da bi protokol funkcionirao, prost broj p treba izabrati tako da je potenciranje modulo p lako, a logaritmiranje teško (p mora imati barem 300 znamenaka).