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/

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).

Navedimo neke teme i primjere problema iz teorije brojeva.

Djeljivost:

- Je li broj 123456789 djeljiv s 9?

- Naći broj koji pri dijeljenju sa 7 daje ostatak 2, pri dijeljenju s 11 daje ostatak 1, a pri dijeljenju s 13 daje ostatak 9.

- Naći ostatak pri dijeljenju broja 2^{100} sa 101.

Prosti brojevi i faktorizacija:

- Prirodan broj $p > 1$ je prost ako je djeljiv samo s 1 i sa samim sobom: $2, 3, 5, 7, 11, 13, 17, 19, \ldots$.
- Koliko ima prostih brojeva?
- Je li broj 91 prost?
- Je li broj $2^{31} - 1$ prost?
- Rastaviti na proste faktore broj 1001.
- Rastaviti na proste faktore broj $2^{32} + 1$.
- Može li se svaki paran broj veći od 2 prikazati kao zbroj dva prosta broja?

($4 = 2+2$, $6 = 3+3$, $8 = 3+5$, $10 = 3+7$, $12 = 5+7$)

Najveći zajednički djelitelj:

- Odrediti $\text{nzd}(901, 1001)$ (bez faktorizacije).

- Naći cijele brojeve x i y takve da je $901x - 1001y = \text{nzd}(901, 1001)$.

Euklidov algoritam:

$$\begin{aligned} 1001 &= 901 \cdot 1 + 100 \\ 901 &= 100 \cdot 9 + 1 \end{aligned}$$

Dakle, $\text{nzd}(901, 1001) = 1$. Nadalje,

$$\begin{aligned} 1 &= 901 - 100 \cdot 9 = 901 - (1001 - 901 \cdot 1) \cdot 9 \\ &= 901 \cdot 10 - 1001 \cdot 9. \end{aligned}$$

Diofantske jednadžbe:

$$3x + 5y = 28$$

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

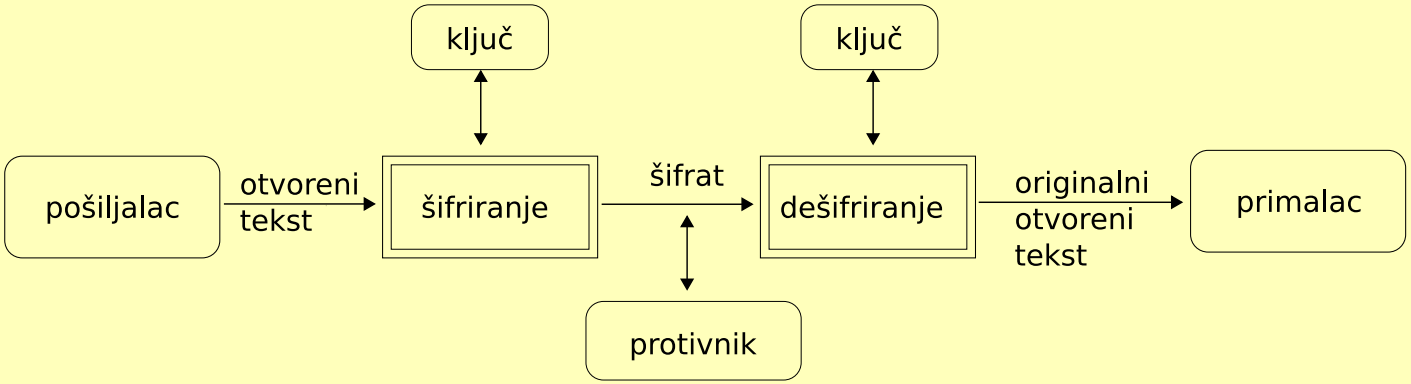
$$y^2 = (x+1)(3x+1)(8x+1)$$

Diofantske aproksimacije:

Nejednadžba $\left|\sqrt{2} - \frac{a}{b}\right| < \frac{1}{2b^2}$ ima beskonačno mnogo rješenja: $\frac{a}{b} = 1, \frac{3}{2}, \frac{7}{5}, \frac{17}{12}, \frac{41}{29}, \frac{99}{70}, \ldots$, a nejednadžba $\left|\sqrt{2} - \frac{a}{b}\right| < \frac{1}{4b^2}$ niti jedno.

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.

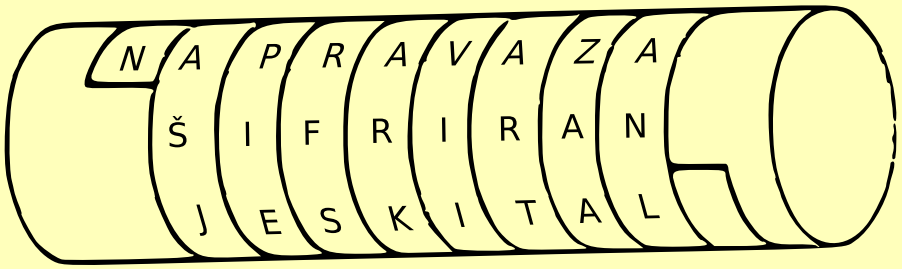


Glavne metode klasične kriptografije:

- 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

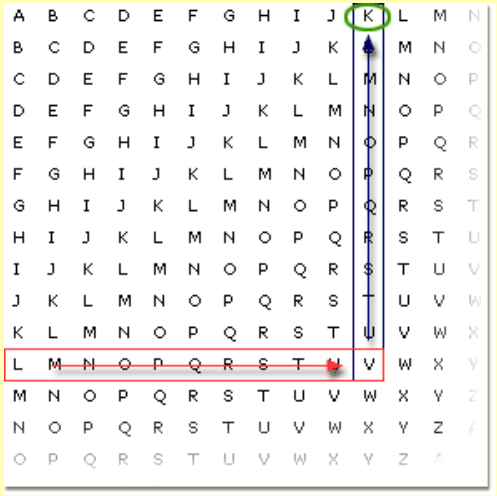
6	1	3	7	5	2	4
S	T	U	P	Č	A	N
A	T	R	A	N	S	P
O	Z	I	C	I	J	A

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

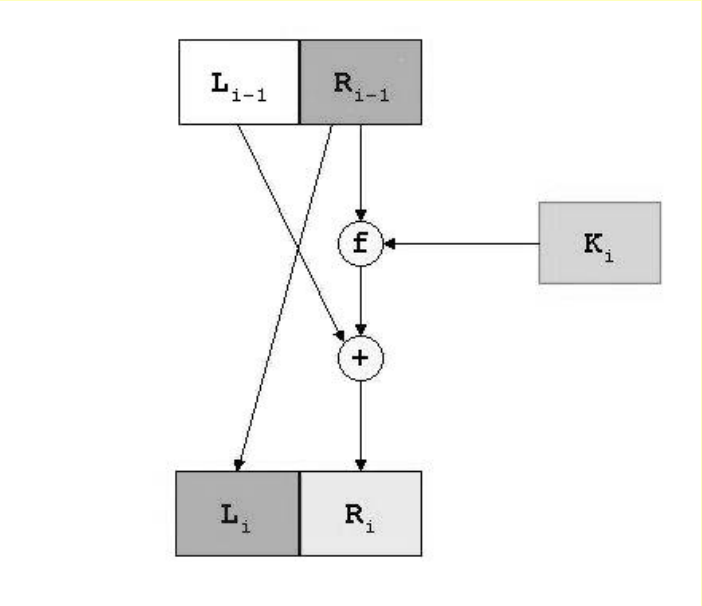


ENIGMA (1920. – 2. svjetski rat)

- najpoznatija naprava za šifriranje
- Vigenèreova šifra s ogromnom ključnom riječi
- Kriptoanaliza: Marian Rejewski i Alan Turing

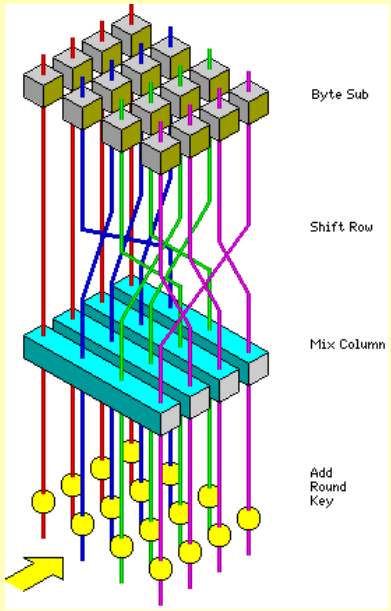
DES – Data Encryption Standard (1976. – 1998.)

- kombinira se supstitucija i transpozicija,
- ključna riječ ima 56 bitova,
- 16 rundi šifriranja



AES – Advanced Encryption Standard (2000. –)

- koristi operacije u polju $GF(2^8)$,
- elementi polja su polinomi stupnja ≤ 7 s koeficijentima iz $\{0, 1\}$,
- operacije su zbrajanje polinoma u $\mathbb{Z}_2[X]$ (1+1=0) i množenje polinoma modulo fiksni polinom osmog stupnja: $x^8 + x^4 + x^3 + x + 1$



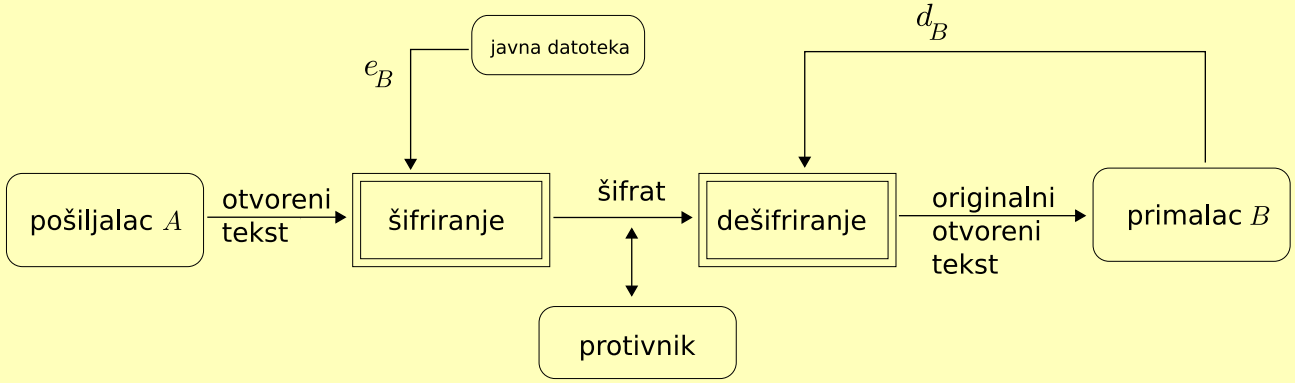
Kriptosustavi s javnim ključem

Sigurnost svih do sada navedenih kriptosustava leži u tajnosti ključa.

Problem: Kako sigurno razmijeniti ključ?

Ideja: javni ključ e_K za šifriranje, tajni (osobni) ključ d_K za dešifriranje.

Ovdje e_K mora biti tzv. jednosmjerna funkcija, tj. nju se računa lako, a njezin inverz jako teško.



Kriptosustavi s javnim ključem su puno sporiji od modernih simetričnih kriptosustava (npr. AES-a). Zato se u praksi ne koriste za šifriranje poruka, već za:

- razmjenu ključeva,
- digitalni potpis: $z = d_A(e_B(x))$, $e_A(z) = e_B(x)$.

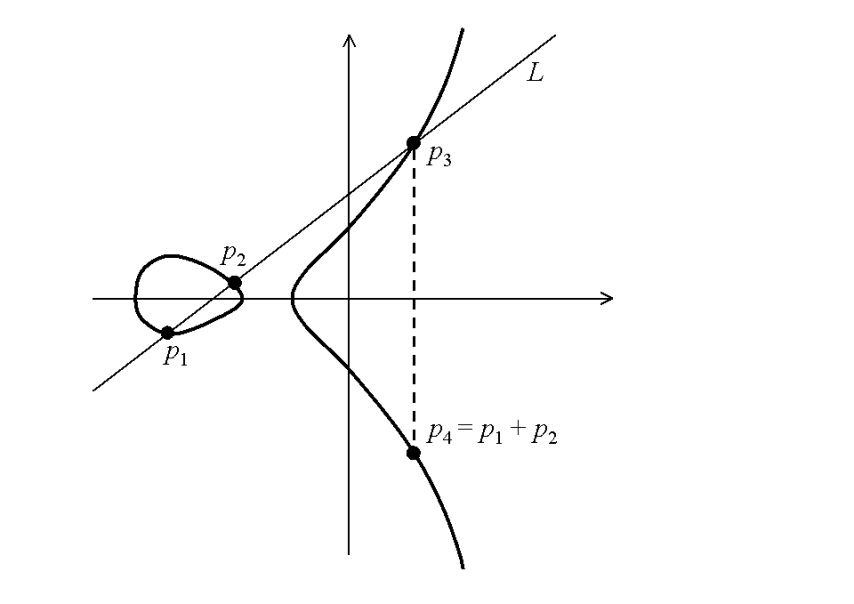
Osnova za kriptosustave s javnim ključem su "teški" matematički problemi:

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

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

- eliptički diskretni logaritam (ECDPL)

Eliptička krivulja: $y^2 = x^3 + ax + b$



ECDLP: $xP = \underbrace{P + \cdots + P}_{x \text{ pribrojnika}} = Q$ (nad $\mathbb{F}_p$ ili $\mathbb{F}_{2^k}$)

ECDLP je teži od DLP $\Rightarrow$ ista sigurnost uz kraći ključ ($1024 \longleftrightarrow 160$)

Diffie–Hellmanov protokol za razmjenu ključeva

G je konačna ciklička grupa s generatorom g, tj. $G = \{g, g^2, \ldots, g^{|G|}\}$

Ana i Branko žele se dogovoriti o jednom tajnom elementu grupe G, preko nesigurnog komunikacijskog kanala kojeg prisluškuje Eva.

Primjer: Grupa $\mathbb{F}_{11}^* = \{1, 2, \ldots, 10\}$ (operacija je množenje modulo 11) je ciklička grupa s generatorom 2.

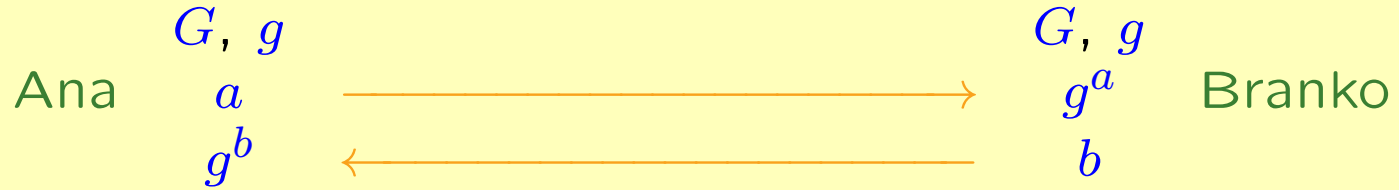
x	1	2	3	4	5	6	7	8	9	10
2^x	2	4	8	5	10	9	7	3	6	1

Primjer: Grupa točaka na eliptičkoj krivulji

$$E: \quad y^2 = x^3 + x + 3$$

nad poljem $\mathbb{F}_7 = \{0, 1, 2, 3, 4, 5, 6\}$ je ciklička grupa s generatorom $P = (4, 1)$.

x	1	2	3	4	5	6
xP	$(4, 1)$	$(6, 6)$	$(5, 0)$	$(6, 1)$	$(4, 6)$	$\mathcal{O}$



Eva: G, 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, grupa G treba biti takva da je u njoj potenciranje lako, a logaritmiranje teško.

Primjeri takvih grupa jesu multiplikativna grupa konačnog polja $\mathbb{F}_q^*$ i grupa $E(\mathbb{F}_q)$ točaka na eliptičkoj krivulji nad konačnim poljem (q mora imati barem 300 znamenaka).

RSA kriptosustav

(Rivest, Shamir, Adleman (1977))

- izaberemo tajno dva velika prosta broja p i q,
- izračunamo $n = p \cdot q$ i $\varphi(n) = (p-1)(q-1) = n + 1 - p - q$ (Eulerova funkcija),
- izaberemo e tako da je $e < \varphi(n)$ i $\text{nzd}(e, \varphi(n)) = 1$,
- izračunamo tajno d takav da je $d \cdot e \equiv 1 \pmod{\varphi(n)}$ (linearna diofantska jednadžba $d \cdot e - t \cdot \varphi(n) = 1$ – prošireni Euklidov algoritam.

(n, e) – javni ključ

(p, q, d) – tajni (osobni) ključ

šifriranje: $e_K(x) = x^e \bmod n$

dešifriranje: $d_K(y) = y^d \bmod n$

Provjera: $d_K(e_K(x)) \equiv d_K(x^d) \equiv x^{de} \equiv x^{t\varphi(n)+1} \equiv (x^{\varphi(n)})^t \cdot x \equiv x \bmod n$ (Eulerov teorem)

- sigurnost leži u teškoći faktorizacije velikih brojeva

- Teško je faktorizirati veliki prirodan broj n.

- Možda i nije; npr. $n = 10^{200} = 2^{200} \cdot 5^{200}$,
$n = 9999 \cdots 9919 = x^2 - 9^2 = (x-9)(x+9)$

- Teško je faktorizirati n koji je produkt dva velika pažljivo odabrana prosta broja p i q (sa stotinjak znamenaka)

- Kako naći (tajno) veliki prosti broj?
Čini se ("školskim" načinom) da je to podjednako teško kao faktorizirati veliki broj slične veličine.

- Testiranje prostosti – može se puno brže nego "školski". Postoje polinomijalni ("efikasni") algoritmi koji ne koriste definiciju prostih brojeva, već neka njihova svojstva koja su jednostavna za provjeru. Mali Fermatov teorem:
$a^{p-1} \equiv 1 \pmod{p}$,
$x^2 \equiv 1 \pmod{p} \Rightarrow x \equiv \pm 1 \pmod{p}$.

- Faktorizacija: ne može puno brže nego "školski" (po onome što je danas poznato). Najbolji poznati algoritmi su subeksponencijalni. Osnovna ideja je izračunati $\text{nzd}(n, y)$ za prikladno odabrani y (tako da rezultat bude $\neq 1, n$).

"Dječja" kriptografija - kriptosustavi primjereni učenicima različitih uzrasta koji dovoljno poznaju matematiku i informatiku da bi razumjeli kako šifrirati poruku, ali još ne poznaju algoritme pomoću kojih se može lako razbiti šifru.

M. R. Fellows, N. Koblitz, *Combinatorially based cryptography for children (and adults)*, Congr. Numerantium 99 (1994), 9–41.
http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.26.3311

N. Koblitz, *Cryptograpy as a teaching tool*, Cryptologia 21 (1997) 317–326.
http://www.math.washington.edu/~koblitz/crlogia.html

M. Barun, A. Dujella, Z. Franušić, *Kriptografija u školi*, Poučak 33 (2008), 40–52.
https://web.math.pmf.unizg.hr/ fran/clanci/kripto-poucak4.pdf

"Dječji" RSA:

Ana izabire cijele brojeve a, b, a', b' i postavlja sljedeće vrijednosti:

$$\begin{aligned} M &= ab - 1, \\ e &= a'M + a, \\ d &= b'M + b, \\ n &= (ed - 1)/M = a'b'M + ab' + a'b + 1. \end{aligned}$$

Njen javni ključ je (n, e), a tajni d. Definirajmo sljedeće funkcije

$$\begin{aligned} e_A(x) &= ex \bmod n, \\ d_A(y) &= dy \bmod n, \end{aligned}$$

gdje je x prirodan broj, $0 \leq x < n$, koji predstavlja poruku, tj. otvoreni tekst.

Funkcije e_A i d_A su međusobno inverzne. Zaista, neka je $0 \leq x < n$. Tada je

$$\begin{aligned} d_A(e_A(x)) &\equiv dex \equiv (b'M + b)(a'M + a)x \\ &\equiv (a'b'M^2 + ab'M + a'bM + ab)x \\ &\equiv (Mn + 1)x \equiv x \pmod{n}. \end{aligned}$$

Branko odabire cijele brojeve a_1, b_1, a_1', b_1', te, na isti način kao i Ana, generira brojeve e_1, d_1, n_1. Analogno su definirane funkcije $e_B(x) = e_1 x \bmod n_1$ i $d_B(y) = e_1 y \bmod n_1$. Brankov javni ključ je (n_1, e_1), a tajni d_1.

Pretpostavimo da Ana želi Branku poslati poruku x. Ana šifrira tako što redom računa vrijednosti

$$y = d_A(x),$$
$$z = e_B(y),$$

te Branku šalje poruku z. Primivši poruku z, Branko ju dešifrira na sljedeći način:

$$e_A(d_B(z)) = e_A(d_B(e_B(y))) = e_A(y) = x.$$

Ovaj kriptosustav može se razbiti pronalaženjem prirodnog broja d takvog da je $de \equiv 1 \pmod{n}$ (čak ne nužno onog d kojeg Ana koristi kao svoj tajni ključ).

To je moguće efikasno napraviti pomoću Euklidovog algoritma, no taj algoritam vjerojatno nije poznat onima kojima je ovaj sustav namijenjen. Otvoreno je pitanje može li se ovaj sustav razbiti bez primjene neke verzije Euklidovog algoritma.

Ovaj kriptosustav možda može poslužiti kao dodatna motivacija za uvođenje Euklidovog algoritma u nastavu matematike ili informatike.