Teorija brojeva i šifriranje

Andrej Dujella

PMF-MO, Sveučilište u Zagrebu
e-mail: `duje@math.hr`
URL: `http://web.math.hr/~duje/`

Teorija brojeva

Teorija brojeva je grana matematike koja se ponajprije bavi proučavanjem svojstava cijelih brojeva. Navedimo neke teme i primjere problema iz teorije brojeva.

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

Prosti brojevi:
- Koliko ima prostih brojeva?
- Je li broj $2^{31}-1$ prost?

Faktorizacija:
- Rastaviti na faktore polinom x^4+4.
- Rastaviti na proste faktore broj $2^{32}+1$.

Najveći zajednički djelitelj:

- Odrediti $\mathrm{nzd}(101, 1001)$ (bez faktorizacije – Euklidov algoritam).
- Naći cijele brojeve x i y takve da je $101x - 1001y = \mathrm{nzd}(101, 1001)$.

Diofantske jednadžbe:

$$3x + 5y = 28$$

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

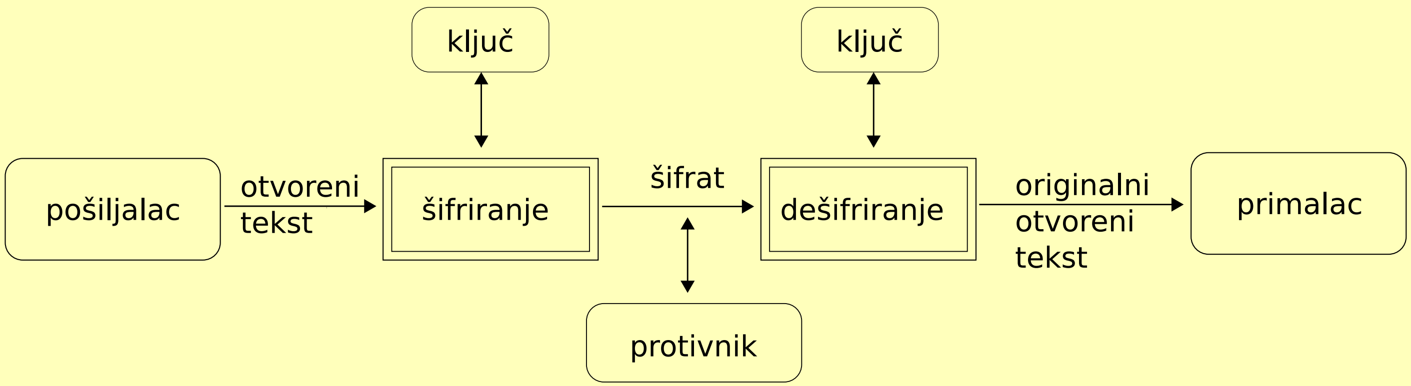
$$y^2 = x^3 + 17$$

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.

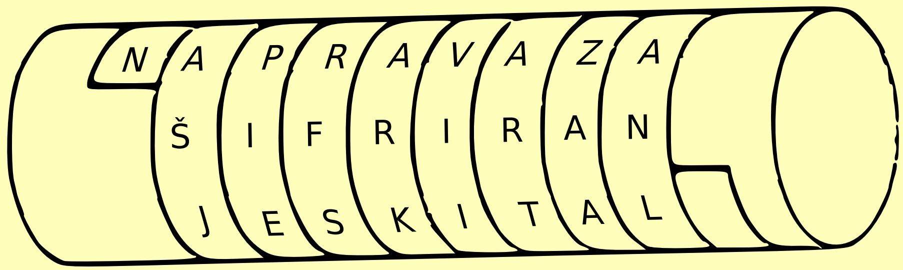


Glavne metode klasične kriptografije:

- 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

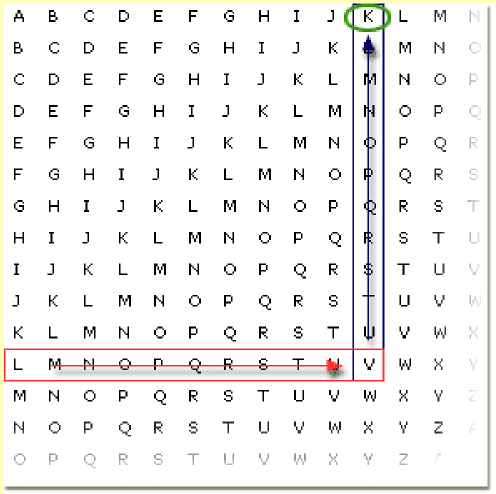
6	1	3	7	5	2	4
S	T	U	P	Č	A	N
A	T	R	A	N	S	P
O	Z	I	C	I	J	A

TTZASJURINPAČNISAOPAC

Supstitucijske šifre

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

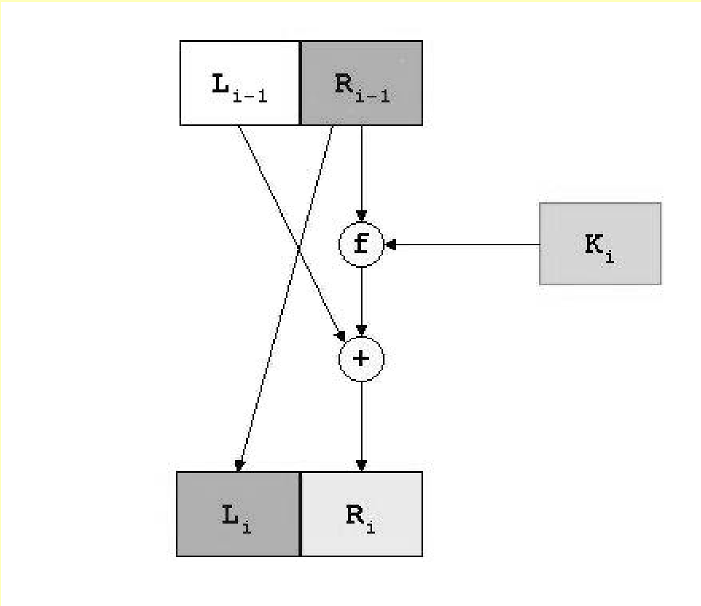
Vigenèreova šifra (16. st. – 19. st.)
- ključna riječ $(k_1, k_2, \ldots, k_m)$,
- slova se pomiču redom za $k_1, k_2, \ldots, k_m, k_1, k_2, \ldots$ mjesta



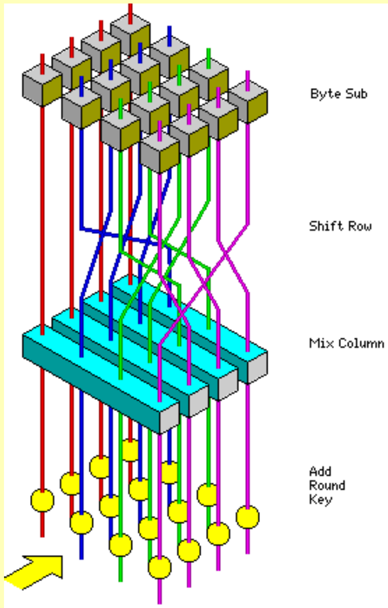
ENIGMA (1920. – 2. svjetski rat)
- najpoznatija naprava za šifriranje
- Vigenèreova šifra s ogromnom ključnom riječi
- Kriptoanaliza: Marian Rejewski i Alan Turing

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: $x^8 + x^4 + x^3 + x + 1$



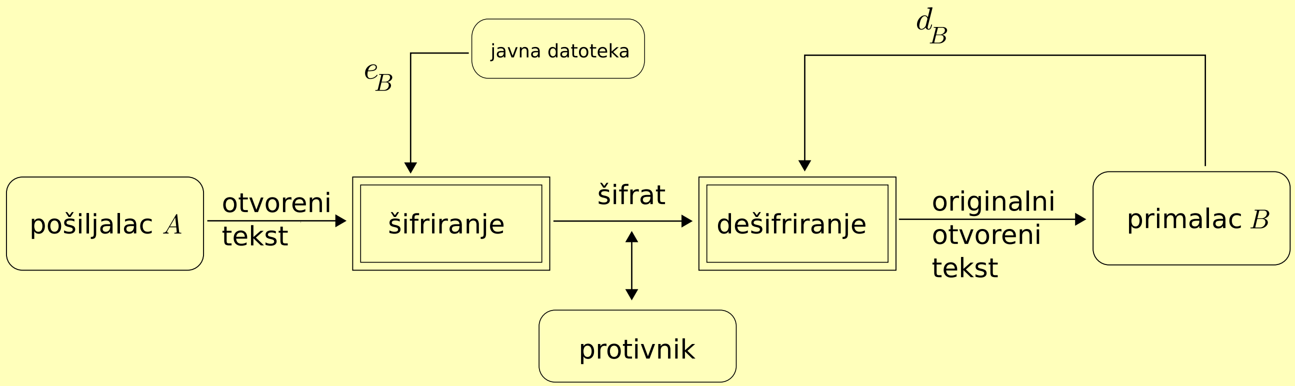
Kriptosustavi s javnim ključem

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.

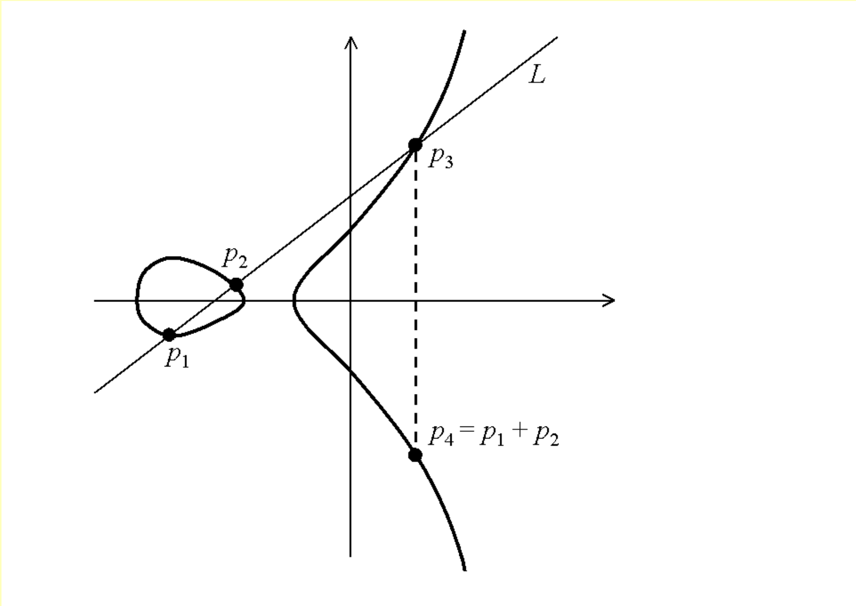
Osnova za kriptosustave s javnim ključem su “teški” matematički problemi:

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

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

- eliptički diskretni logaritam (ECDPL)

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



ECDLP: $[x]P = Q$ (nad $\mathbb{Z}_p$ ili $GF(2^n)$)

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.
$G = \{g, g^2, \ldots, g^{|G|}\}$

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

	G, g		G, g	
Alica	a	$\longrightarrow$	g^a	Bob
	g^b	$\longleftarrow$	b	

Eva: G, g, g^a, g^b

Alica: $(g^b)^a = g^{ab}$ $\searrow$

razmijenili su ključ

Bob: $(g^a)^b = g^{ab}$ $\nearrow$

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.

Primjer: Grupa $\mathbb{Z}_{11}^* = \{1, 2, \ldots, 10\}$ (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

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 $\mathrm{nzd}(e, \varphi(n)) = 1$,
- 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.

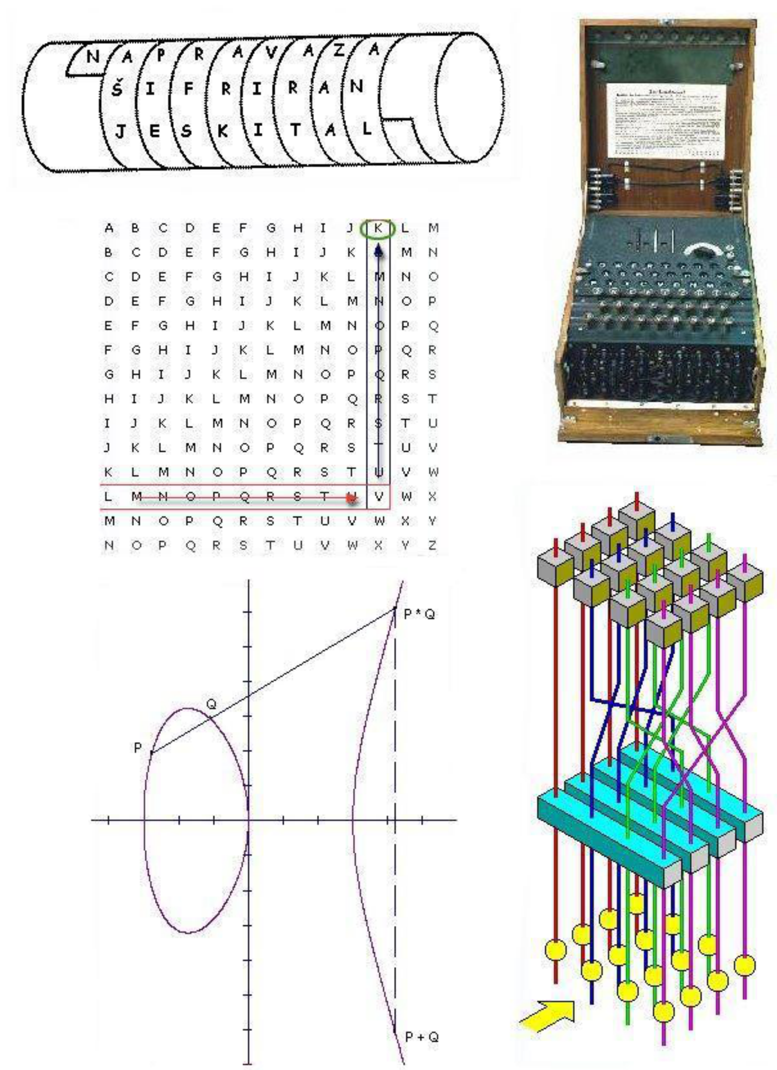
- Možda i nije; npr. $n = 10^{200} = 2^{200} \cdot 5^{200}$,
$n = 9999 \cdots 9919 = x^2 - 9^2 = (x - 9)(x + 9)$

- 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 $\mathrm{nzd}(n, y)$ za prikladno odabrani y (tako da rezultat bude $\neq 1, n$).



109417386415705274218097073220403576120037329454492059909138421314763499842889\
34784717997257891267332497625752899781833797076537244027146743531593354333897 =
102639592829741105772054196573991675900716567808038066803341933521790711307779 ×
106603488380168454820927220360012878679207958575989291522270608237193062808643.