4. poglavje

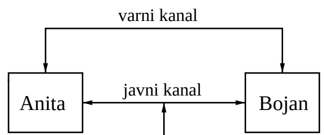
RSA sistem in faktorizacija

- Uvod
  - pomankljivosti simetrične kriptografije
  - kriptografija z javnimi ključi
- Teorija števil
- Opis in implementacija RSA
- Gostota praštevil
- Generiranje praštevil
- Gaussov izrek (o kvadratni recipročnosti)

Uvod

Pomankljivosti simetrične kriptografije

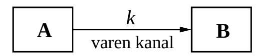
Sodelujoči si delijo *tajno* informacijo.



Dogovor o ključu

Kako Anita in Bojan vzpostavita tajni ključ k?

1. metoda: delitev point-to-point

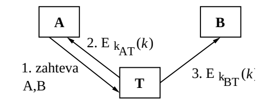


Varni kanal je lahko:
– kurir
– izmenjava na štiri oči (v temnem hodniku/ulici)

To ni praktično za večje aplikacije.

2. metoda: z neodvisnim centrom zaupanja

– *Vsak* uporabnik A deli tajni ključ k_{AT} s centrom zaupanja T za simetrično šifrirno s
– Za vzpostavitev tega ključa mora A obiskati center zaupanja T *samo enkrat.*
– T nastopa kot **center za distribucijo klj** (angl. key distribution centre - KDC):



1. A pošlje T zahtevek za ključ, ki si ga želi d
2. T izbere ključ k, ga zašifrira za A s ključe
3. T zašifrira ključ k za osebo B s ključem k

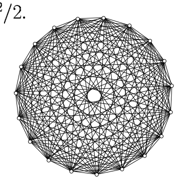
Problemi pri uporabi KDC

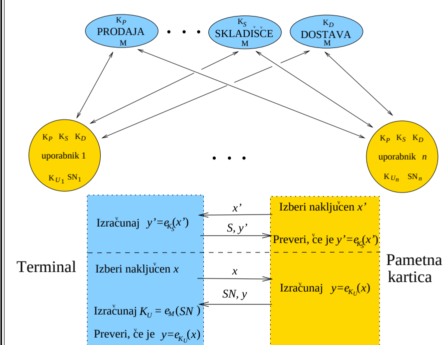
- centru zaupanja T moramo brezpogojno zaupati:
  - to ga naredi za očitno tarčo.
- Zahteva za stalno zvezo (on-line) s centrom T:
  - potencialno ozko grlo,
  - kritično za zanesljivost.

Upravljanje ključev

- v mreži z n uporabniki, mora vsak uporabnik deliti različen ključ z vsakim uporabnikom,
- zato mora hraniti vsak uporabnik $n-1$ različnih tajnih ključev,
- vseh tajnih ključev je $\binom{n}{2} \approx n^2/2$.

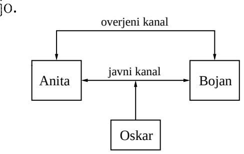
(Tudi preprečevanje tajenja je nepraktično.)





Kriptografija z javnimi klju

Udeleženci si predhodno delijo *overjeno/avt* informacijo.



L. **1976** sta jo predlagala Whitfield **Diffie** in **Hellman** (L. 1970 pa tudi James Ellis, ki je član Communication Electronics Security Gro British Government Communications Headqu

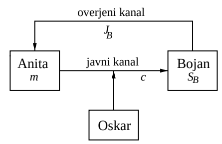
Generiranje para ključev

Vsaka oseba A naredi naslednje:

- generira par ključev (J_A, S_A),
- S_A je A-jev zasebni/tajni ključ,
- J_A je A-jev javni ključ.

Varnostna zahteva: za napadalca mora biti nemogoče priti do kluča S_A iz ključa J_A.

Šifriranje z javnimi ključi



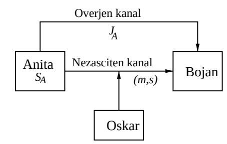
Da bi Bojanu poslala zaupno sporočil m, Anita:

- dobi overjenjo kopijo Bojanovega javnega kjuča J_B,
- izračuna $c = E(J_B, m)$, kjer je E šifrirna funkcija,
- pošlje Bojanu tajnopis c.

Za odšifriranje tajnopisa c Bojan naredi naslednje

- Izračuna $m = D(S_B, c)$, kjer je D odšifrirna funkcija.

Digitalni podpisi



Za podpis sporočila m Anita naredi naslednje:

- Izračuna $s = \mathsf{Sign}(S_A, m)$.
- Pošlje m in s Bojanu.

Bojan preveri Anitin podpis s sporočila m z:

- Pridobi si overjeno kopijo javnega ključa J_A.
- Sprejme podpis, če je $\mathsf{Verify}(J_A, m, s) = \mathsf{Accept}$.

Prednosti kriptosistemov z javnimi

- Ni zahteve po varnem kanalu.
- Vsak uporabnik ima 1 par ključev.
- Poenostavljeno upravljanje s ključi.
- Omogoča preprečevanje tajenja.

Pomanjkljivosti kriptosistemov z javni

- Sheme z javnimi ključi so počasnejše.
- Javni ključi so večji od simetričnih.

V praksi uporabljamo skupaj sheme s simetričnimi in javnimi ključi in jim rečemo **hibridne sheme**

Primer: Da bi Bojanu poslala podpisano tajno sporočilo m, Anita naredi naslednje:

- izračuna $s = \mathsf{Sign}(S_A, m)$,
- izbere tajni ključ k simetrične šifrirne sheme (AES),
- pridobi overjeno kopijo Bojanovega javnega ključa J_B,
- pošlje $c_1 = E(J_B, k)$, $c_2 = \mathsf{AES}(k, (m, s))$.

Za odkritje sporočila m in preverjanje avtentičnosti, Bojan:

- odšifrira c_1: $k = D(S_B, c_1)$,
- odšifrira c_2 z uporabo ključa k, da dobi (m, s),
- pridobi overjeno kopijo javnega ključa J_A,
- preveri podpis s sporočila m.

Že l. 1977 so Ronald L. **Rivest**, Adi **Shamir** in Leonard M. **Adleman** naredili prvo realizacijo takšnega kriptosistema (**RSA**)
(tajno pa že l. 1973 **C. Cocks** pri GCHQ).

Temu so sledili številni drugi nesimetrični kriptosistemi, med katerimi pa so danes najbolj pomembni naslednji:

- RSA (faktorizacija),
- Merkle-Hellman Knapsack (metoda nahrbtnika)
- Chor-Rivest
- McEliece (linearne kode),
- ElGamal (diskretni logaritem),
- eliptične krivulje.

Javni kriptosistemi **niso** nikoli brezpogojno varni, zato študiramo računsko/časovno zahtevne sisteme.

Teorija števil

Evklidov algoritem in reševanje Diofantske enačbe

$$ax + by = d, \qquad \text{kjer} \quad D(a,b) \,|\, d.$$

Evklidov algoritem je zasnovan na preprostem dejstvu, da iz $k \,|\, a$ in $k \,|\, b$ sledi $k \,|\, a - b$.

Če je $D(a,b) = 1$ in poznamo eno rešitev (x_0, y_0), tj.

$$ax_0 + by_0 = d,$$

potem ima poljubna rešitev (x, y) naslednjo obliko:

$$x = x_0 - kb, \quad y = y_0 + ka, \qquad \text{za } k \in \mathbb{Z}.$$

Zgodovina Evklidovega algorit

Evklidov algoritem poišče največji skupni delit
naravnih števil in je zasnovan na dejstvu, da č
d deli števili a in b, potem deli tudi njuno razli

V literaturi naletimo nanj prvič 300 p.n.š. v
Evklidovih **Elementov**.

Nakateri strokovnjaki so mnenja, da je njeg
Eudoxus (c. 375 p.n.š.). Gre za *najstarejši* ne
algoritem, ki je preživel do današnjih dni (glej

Eno rešitev lahko poiščemo z
razširjenim Evklidovim algoritmom.

Privzemimo, da je $a > b$ in zapišimo zgornjo enačbo malo bolj splošno (z zaporedji):

$$ap_i + bq_i = r_i.$$

Poiščimo dve trivialni rešitvi:

$$p_1 = 1, \quad q_1 = 0, \quad r_1 = a$$

in

$$p_2 = 0, \quad q_2 = 1, \quad r_2 = b.$$

Zaradi rekurzije

$$r_{i+1} = r_i - s_i r_{i-1}$$

(kjer je s_i izbran tako, da je $r_{i+1} < r_i$)
si lahko izberemo še

$$p_{i+1} = p_i - s_i p_{i-1} \quad \text{in} \quad q_{i+1} = q_i - s_i q_{i-1}.$$

Ko računamo a^{-1} (po modulu praštevila p), računamo samo r_i ter p_i (ne pa tudi q_i).

Zgled za razširjeni algoritem:

$4864 = 1{\cdot}3458{+}1406$	$p_2 := p_1 - 1 \cdot p_0 = 1$
$3458 = 2{\cdot}1406{+}646$	$p_3 := p_2 - 2 \cdot p_1 = -2$
$1406 = 2{\cdot}646{+}114$	$p_4 := p_3 - 2 \cdot p_2 = 5$
$646 = 5{\cdot}114{+}76$	$p_5 := p_4 - 5 \cdot p_3 = -27$
$114 = 1{\cdot}76{+}38$	$p_6 := p_5 - 1 \cdot p_4 = 32$
$76 = 2{\cdot}38{+}0$	$p_7 := p_6 - 2 \cdot p_5 = -91$

$4864 = 1{\cdot}3458{+}1406$	$p_2 = 1$
$3458 = 2{\cdot}1406{+}646$	$p_3 = -2$
$1406 = 2{\cdot}646{+}114$	$p_4 = 5$
$646 = 5{\cdot}114{+}76$	$p_5 = -27$
$114 = 1{\cdot}76{+}38$	$p_6 = 32$ q_6
$76 = 2{\cdot}38{+}0$	$p_7 = -91$

$$4864 \cdot (-91) + 3458 \cdot (128) = 38$$

Lehmerjev algoritem deli z majhnimi namesto velikimi števili (izboljšave J. Sorenson, Jaebelan,...).

Dobro vprašanje je kako prenesti te ideje v GF(2^n).

R. Schroeppel je že naredil prvi korak s svojim algoritmom **almost inverse**.

Kitajski izrek o ostankih. *Če so števila $m_1, m_2, ..., m_r$ paroma tuja, tj. $D(m_i, m_j) = 1$ za $i \neq j$, in $a_1, a_2, ..., a_r \in \mathbb{Z}$, potem ima sistem kongruenc*

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_r \pmod{m_r} \end{aligned}$$

enolično rešitev po modulu $M = m_1 \cdot m_2 \cdots m_r$,

$$x = \sum_{i=1}^{r} a_i \cdot M_i \cdot y_i \pmod{M},$$

kjer je $M_i = M/m_i$, $y_i = M_i^{-1} \bmod m_i$, $i = 1, ..., r$.

(angl. Chinese Reminder Theorem oziroma CRT)

Red elementa g v končni multiplikativni grupi je najmanjše celo število m tako, da $g^m = 1$.

Lagrangev izrek: *Naj bo G multiplikativna grupa reda n in $g \in G$, potem red g deli n.*

Naj bo p praštevilo. Generatorju multiplikativne grupe $\mathbb{Z}_p^*$ pravimo **primitiven element**.

DN: Koliko primitivnih elementov ima $\mathbb{Z}_p$?
Naj bo α primitiven element, potem za $\forall \beta \in \mathbb{Z}_p^*$ obstaja tak $i \in \{0, 1, \ldots, p-2\}$, da je $\beta = \alpha^i$.
Pokaži, da je red elementa β enak $\dfrac{p-1}{D(p-1, i)}$.

Eulerjevo funkcijo φ definiramo s

$$\varphi(n) = |\{x \in \mathbb{N} \mid x < n \text{ in } D(x,n) = 1$$

Potem za praštevilo p, naravno število n in p
tuji si števili a in b velja

$$\varphi(p^n) = p^n - p^{n-1} \quad \text{in} \quad \varphi(ab) = \varphi(a)\varphi($$

Če poznamo faktorizacijo števila n, poznam
$\varphi(n)$.

Fermatov izrek
Za praštevilo p in $b \in \mathbb{Z}_p$ velja $b^p \equiv b \pmod{p}$.

Eulerjev izrek
Če je $a \in \mathbb{Z}_n^*$ oziroma $D(n,a)=1$, potem velja

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

Opis in implementacija RSA

Generiranje ključev: najprej izberemo

praštevili p, q ter izračunamo $n := pq$, in
šifrirni eksponent e, tako da je $D(e,\varphi(n))$=1,

nato pa izračunamo odšifrirni eksponent d iz kongruence

$$ed \equiv 1 \pmod{\varphi(n)}$$

z razširjenim Evklidovim algoritmom
(ali pa potenciranjem).

Javni ključ je (e,n), **zasebni ključ** pa (d,p,q).

Šifriranje: $E(e,n)(x) = x^e \pmod{n}$.
Odšifriranje: $D(d,p,q)(y) = y^d \pmod{n}$.

Šifriranje in odšifriranje sta inverzni operaciji.
Za $x \in \mathbb{Z}_n^*$ to sledi iz Eulerjeve kongruence:

$$(x^e)^d \equiv x^{r\varphi(n)+1} \equiv (x^{\varphi(n)})^r x \equiv x \pmod{n},$$

za $x \in \mathbb{Z}_n \backslash \mathbb{Z}_n^*$ pa se prepričajte sami za DN.

Generiranje podpisa:
za podpis sporočila $m \in \{0,1\}^*$, Anita:

1. izračuna $M = H(m)$,
   kjer je H zgoščevalna funkcija (npr. SHA
2. izračuna $s = M^d$ mod n,
3. Anitin podpis za m je s.

Preverjanje podpisa:
Bojan preveri Anitin podpis s za m, tako da:

1. vzame overjeno kopijo Anitinega javnega ključa (n,e),
2. izračuna $M = H(m)$,
3. izračuna $M' = s^e$ mod n,
4. sprejme (m,s) če in samo če je $M = M'$.