Teorija kodiranja in kriptografija 2013/2014

Kriptosistemi z javnim ključem

Arjana Žitnik

Univerza v Ljubljani, Fakulteta za matematiko in fiziko

Ljubljana, 25. 3. 2014

Vsebina

- Kriptosistemi z javnim ključem
- RSA - opis
- Parametri RSA

Simetrični in asimetrični kriptosistemi

Kriptosistem $\mathcal{S}$ je simetričen, če poznamo učinkovit algoritem, ki za vsak kodirni ključ $e \in \mathcal{K}$ izračuna pripadajoči dekodirni ključ $d \in \mathcal{K}$.

Kriptosistem $\mathcal{S}$, ki ni simetričen, imenujemo asimetričen kriptosistem ali kriptosistem z javnim ključem.

Pripomba: če $d = e$, je kriptosistem simetričen.
Velja tudi obratno: v simetričnem kriptosistemu lahko privzamemo $d = e$, saj lahko računanje ključa iz e vgradimo v dekodirno funkcijo.

Kriptosistemi z javnim ključem - ideja

Naj bo $\mathcal{S}$ asimetričen kriptosistem.

- kodirni ključ e je javen: vsakdo lahko šifrira
- dekodirni ključ d je tajen: dešifrira lahko samo lastnik ključa

Zato pri asimetričnem kriptosistemu $\mathcal{S}$ imenujemo kodirni ključ tudi javni ključ, dekodirni ključ pa zasebni ključ. Sam kriptosistem pa tudi kriptosistem z javnim ključem.

Pri simetričnem kriptosistemu lahko izmenjava ključa predstavlja veliko težavo.
Pri kriptosistemih z javnim ključem naj bi bila ta težava odpravljena.

Varnost kriptosistemov z javnim ključem

Varnost temelji na tem, da samo iz javnega ključa e ne moremo v ”razumnem” času izračunati zasebnega ključa d.

To ponavadi pomeni, da je za izračun zasebnega ključa potrebno rešiti ”težak” matematičen problem, na primer:

- Problem razcepa sestavljenega števila:
  za dano število $n = p \cdot q$, kjer sta p in q veliki praštevili, poišči p in q.
- Problem diskretnega logaritma.

Uporaba asimetričnega kriptosistema

- Boris si izbere javni kodirni ključ $e \in \mathcal{K}$
  in pripadajoči dekodirni ključ $d \in \mathcal{K}$.
- Boris javni ključ e objavi,
  zasebni ključ d pa zadrži zase.
- Kdorkoli želi poslati Borisu tajno sporočilo, ga šifrira z Borisovim javnim ključem e.
- Kriptogram lahko dešifrira le, kdor pozna Borisov zasebni ključ d.

Kriptosistem RSA

RSA so objavili Rivest, Shamir, Adleman leta 1978.

- $n = p \cdot q$, kjer sta p in q veliki praštevili, $p \neq q$.
- $m = \varphi(n) = (p-1)(q-1)$.

Potem je kriptosistem RSA podan z

- $\mathcal{B} = \mathcal{C} = \mathbb{Z}_n$,
- $\mathcal{K} = \{n\} \times \mathbb{Z}_m^*$
- $E_{(n,e)}(x) \equiv x^e \pmod{n}$
- $D_{(n,d)}(y) \equiv y^d \pmod{n}$

Kodirnemu ključu (n, e) pripada dekodirni ključ (n, d), kjer je $d = e^{-1} \in \mathbb{Z}_m^*$ oziroma $e \cdot d \equiv 1 \pmod{m}$.

Varnost RSA

Varnost RSA temelji na domnevi, da so naslednji problemi težki:

- *RSAdecrypt:* iz $x^e \pmod{n}$ izračunaj x.
- *RSAkey:* iz (n, e) izračunaj d.
- *RSAfactor:* iz $n = p \cdot q$ izračunaj p in q.

Velja:

$$RSAdecrypt \Longleftarrow RSAkey \Longleftrightarrow RSAfactor$$

Faktorizacija je kvečjemu težja kot dešifriranje.
Prednost: če imamo na voljo stroj za dešifriranje, ne moremo izračunati ključa!

Osnovna varianta RSA ni varna

Osnovna varianta RSA ni varna pred raznimi napadi:

- Vsakdo lahko preveri, ali za prestreženi kriptogram c velja

$$c \equiv x^e \pmod{n}$$

  za dani x.

- Multiplikativna lastnost RSA:

$$\begin{aligned} c_1 &\equiv x_1^e \pmod{n} \\ c_2 &\equiv x_2^e \pmod{n} \\ c &\equiv (x_1 \cdot x_2)^e \pmod{n} \end{aligned} \quad \Longrightarrow \quad c \equiv c_1 \cdot c_2 \pmod{n}$$

Rešitev: v šifriranje je treba vnesti naključnost!

RSA v praksi

Najprej izberemo praštevili p in q in izračunamo $n = p \cdot q$.

- Praštevili p in q morata biti dovolj veliki, da je faktorizacija n prezahtevna.
  Za dolgoročno varnost ne zadošča več, da sta p in q dolgi po 512 bitov.
- Kako poiskati p in q:
  - generiramo naključna števila prave velikosti, dokler ne naletimo na praštevilo.
  - Obstoj praštevil nam zagotavlja izrek o gostoti praštevil
  - Za preverjanje praštevilskosti ponavadi uporabimo verjetnostni algoritem.

RSA v praksi - nadaljevanje

Nato izberemo šifrirni eksponent e:

- Šifrirni eksponent e mora biti tuj proti $m = \varphi(n)$ (da obstaja d)
- Za šifrirni eksponent e se pogosto izbira $e \in \{5, 17, 2^{16} + 1$, da je šifriranje hitro.
- Zaradi napada s skupnim eksponentom ni dobro, da je e premajhen.

RSA v praksi - implementacija

Osnovna varianta RSA ni varna: pri impementaciji je potrebno vnesti naključnost, glej standard PKCS#1, v. 2.1, kjer je uporabljena shema OAEP (Optimal Asymmetric Encryption Padding).

Uporabljeni algoritmi:

- generator slučajnih števil,
- test praštevilskosti
- aritmetika za delo z velikimi števili:
  - seštevanje, množenje, modularna redukcija
  - (razširjeni) evklidov algoritem (inverz)
  - potenciranje (kvadriraj in zmnoži)

Izrek o gostoti praštevil

Izrek (de la Vallée Poussin, Hadamard, 1896)

Naj bo $\pi(x)$ število praštevil, manjših od x. Potem je

$$\lim_{x\to\infty} \frac{\pi(x)}{x/\ln x} = 1$$

Vprašanje: kolikšna je verjetnost, da je naključno izbrano liho število n praštevilo? Približno

$$\frac{n/\ln n}{n/2} = \frac{2}{\ln n}.$$

Za 512-bitno število je ta verjetnost približno

$$\frac{2}{\ln(2^{512})} \approx 0.0056.$$

Preverjanje praštevilskosti

Kako težko je preveriti, ali je dano število praštevilo?

- obstaja polinomski algoritem
  (Agrawal, Kayal, Saxena, 2002)
- hitrejši in lažje razumljivi so verjetnostni algoritmi, ki z določeno verjetnostjo vrnejo napačen odgovor.
  - Solovay-Strassen
  - Miller-Rabin

Fermatov test praštevilskosti

Izrek (Fermat)

Naj bo p praštevilo in a tuj s p. Potem velja

$$a^{p-1} \equiv 1 \pmod{p}$$

Lahko se zgodi, da je $a^{p-1} \equiv 1 \pmod{p}$ in a tuj s p, vendar p ni praštevilo. Potem je p psevdopraštevilo za bazo a.

Število p je Charmichaelovo število, če ni praštevilo in je $a^{p-1} \equiv 1 \pmod{p}$ za vsak a, ki je tuj s p.

Primer

$p = 561$ je najmanjše Charmichaelovo število.

Takih števil je relativno veliko, zato naslednji test ni dovolj zanesljiv.

Fermatov test praštevilskosti - algoritem

Parametri: k - število ponovitev

Vhod: liho število n.

Izhod: TRUE, če je n psevdopraštevilo in
FALSE, sicer

Postopek:
za $i = 1, 2, \ldots k$ ponovi
naključno izberi naravno število $a < n$
če velja $a^{n-1} \not\equiv 1 \pmod{n}$
vrni FALSE, končaj
vrni TRUE

Izrek

Izrek

Naj bo n praštevilo in a tuj z n. Zapišimo $n-1 = 2^s \cdot d$, kjer je d liho število. Potem

$$a^d \equiv 1 \pmod{n}$$

ali pa obstaja $r \in \{0, 1, \ldots, s-1\}$, da je

$$a^{2^r \cdot d} \equiv -1 \pmod{n}$$

Primer

561 *je Charmichaelovo število.*
$a = 2$ *je priča, da je* 561 *sestavljeno.*

Izrek

Izrek

Naj bo $n \geq 3$ liho sestavljeno število. Potem je v množici $\{1, 2, \ldots, n-1\}$ največ $(n-1)/4$ števil, ki so tuja z n in niso priča, da je n sestavljeno.

Torej: naključno izbrano število $a \in \{1, 2, \ldots, n-1\}$ ni priča z verjetnostjo manj kot $1/4$.

Miller-Rabinov test

Parametri: k - število ponovitev

Vhod: liho število n.

Izhod: TRUE, če je n psevdopraštevilo in
FALSE, če je n sestavljeno

Postopek:

$n = 2^s \cdot d + 1$, kjer je d liho število

za $j = 1, 2, \ldots k$ ponovi

naključno izberi naravno število $a < n$

če je $\gcd(a, n) \neq 1$, vrni FALSE, končaj

$x = a^d \pmod{n}$

če $x \neq 1$

$i = 0$

dokler $x \neq n - 1 \pmod{\ }n$

$x = x^2 \pmod{n}$

$i = i + 1$

če $i = s$ ali $x = 1$

vrni FALSE, končaj

vrni TRUE