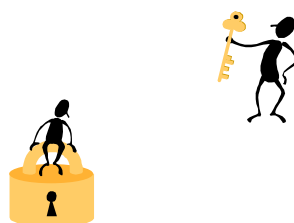


Varne komunikacije

Asimetrični šifrirni algoritmi

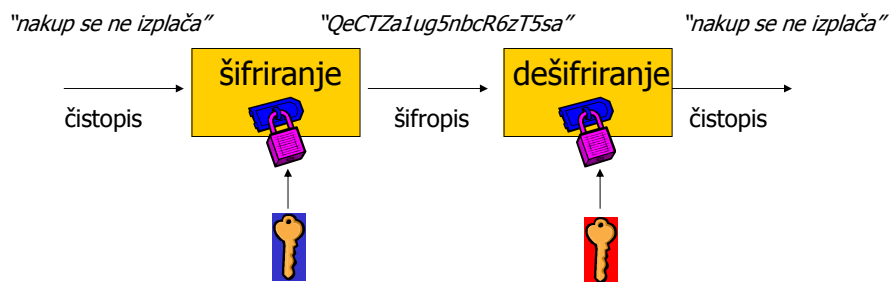
- Asimetrični šifrirni algoritem RSA
 - generacija parov ključev
 - šifriranje in dešifriranje
- Diffie-Hellmanov algoritem (DH)
- ElGamal-ov algoritem



1

Asimetrično šifriranje

- Ključa za šifriranje in dešifriranje nista enaka:



- Pošiljatelj šifrira sporočilo z **javnim** ključem prejemnika.
- Prejemnik dešifrira sporočilo z zasebnim (privatnim) **tajnim** ključem.
- Asimetrični postopki šifriranja so zasnovani na **enosmerni funkciji** s stranskim vhomom (one way trapdoor function).

2

Asimetrični šifrirni algoritem RSA

- RSA algoritem se imenuje po prvih črkah priimkov avtorjev (Ronald Rivest, Adi Shamir, Leonard Adleman), ki so razvili algoritem l. 1977
- Kot vsi asimetrični šifrirni postopki tudi RSA temelji na principu enosmerne funkcije.
- RSA izkorišča težavnosti faktorizacije velikih števil:
 - $15 = 3 * 5$
 - ali znate faktorizirati veliko število ?
109417386415705274218097073220403576120037329454492059909138421314763499842889
34784717997257891267332497625752899781833797076537244027146743531593354333897
=
102639592829741105772054196573991675900716567808038066803341933521790711307779
*
106603488380168454820927220360012878679207958575989291522270608237193062808643



3

RSA algoritem

- **Generacija ključev:**
 - izberemo dve veliki praštevili (p, q)
 - izračunamo produkt $n = p q$ (modul) ,
 - izračunamo produkt $\phi = (p-1) (q-1)$
 - izberemo število e , ki nima skupnega faktorja z ϕ
 - poiščemo število d tako, da daje produkt ($e d$) ostanek 1 pri deljenju z ϕ : $(e d) \bmod \phi = 1$
 - **javni ključ:** (n, e)
 - **tajni ključ:** (n, d)
- **Enkripcija in dekripcija:**
 - šifriramo dolge bloke čistopisa m , šifropis označimo z $E(p)$
 - šifriranje: $E(m) = m^e \bmod n$
 - dešifriranje: $D(E(m)) = E(m)^d \bmod n$
- Na osnovi znanega javnega ključa e , čistopisa m , šifropisa $c = E(m)$ v realnem času ni mogoče ugotoviti tajnega ključa d !!


4

Zgled generacije RSA ključev

- izberemo dve (veliki) praštevili (p, q) $p=17, q=31$
- izračunamo $n = p q$, $\phi = (p-1)(q-1)$ $n=527, \phi=480$
- izberemo število e , ki nima skupnega faktorja z ϕ , veljati mora $\gcd(e, \phi) = 1$; izberemo $e=61$ 
- poiščemo število d tako, da ima produkt $(e d)$ ostanek 1 pri deljenju z ϕ : $(e d) \bmod \phi = 1$
 - veljati mora enačba: $e d = k \phi + 1 \rightarrow d = (k \cdot 480 + 1) / 61$, pri tem pa mora biti k celo število:
 - $d = 7k + (53k + 1) / 61 = 7k + k_1 \rightarrow d = 181$ 
 - $k = (61k_1 - 1) / 53 = k_1 + (8k_1 - 1) / 53 = k_1 + k_2 \rightarrow k = 23$
 - $k_1 = (53k_2 + 1) / 8 = 6k_2 + (5k_2 + 1) / 8 = 6k_2 + k_3 \rightarrow k_1 = 20$
 - $k_2 = (8k_3 - 1) / 5 = k_3 + (3k_3 - 1) / 5 = k_3 + k_4 \rightarrow k_2 = 3$
 - $k_3 = (5k_4 + 1) / 3 = k_4 + (2k_4 + 1) / 3 = k_4 + k_5 \rightarrow k_3 = 2$
 - $k_4 = (3k_5 - 1) / 2 = k_5 + (k_5 - 1) / 2 = k_5 + k_6 \rightarrow k_4 = 1$
 - $k_5 = (2k_6 + 1)$, izberemo $k_6 = 0 \rightarrow k_5 = 1$

5

RSA šifriranje sporočila

- javni RSA ključ: $(n, e) = (527, 61)$ 
- sporočilo v čistopisu: $m = 40$
- šifriranje sporočila: $c = E(m) = m^e \bmod n$

$$c = 40^{61} \bmod 527$$

upoštevamo lastnost: $e = 61 = 1 + 4 + 8 + 16 + 32$

$$40^1 \bmod 527 = 40$$

$$40^2 \bmod 527 = (40^1 \bmod 527)^2 \bmod 527 = 19$$

$$40^4 \bmod 527 = (40^2 \bmod 527)^2 \bmod 527 = 361$$

$$40^8 \bmod 527 = (40^4 \bmod 527)^2 \bmod 527 = 152$$

$$40^{16} \bmod 527 = (40^8 \bmod 527)^2 \bmod 527 = 443$$

$$40^{32} \bmod 527 = (40^{16} \bmod 527)^2 \bmod 527 = 205$$

$$40^{64} \bmod 527 = (40^{32} \bmod 527)^2 \bmod 527 = 392$$

$$40^{128} \bmod 527 = (40^{64} \bmod 527)^2 \bmod 527 = 307$$


$$c = ((40^1 \bmod 527)(40^4 \bmod 527)(40^8 \bmod 527)(40^{16} \bmod 527)(40^{32} \bmod 527)) \bmod 527$$

$$c = (40 \cdot 361 \cdot 152 \cdot 443 \cdot 205) \bmod 527 = 350$$

- šifrirano sporočilo: $c = 350$

6

RSA dešifriranje sporočila

- tajni RSA ključ: $(n, d)=(527,181)$ 
- sporočilo v šifropisu: $c = 350$
- dešifriranje sporočila: $m = D(c) = c^d \bmod n$
 $m = 350^{181} \bmod 527$

upoštevamo lastnost: $d=181=1+4+16+32+128$

$$350^1 \bmod 527 = 350$$

$$350^2 \bmod 527 = (350^1 \bmod 527)^2 \bmod 527 = 236$$

$$350^4 \bmod 527 = (350^2 \bmod 527)^2 \bmod 527 = 361$$

$$350^8 \bmod 527 = (350^4 \bmod 527)^2 \bmod 527 = 152$$

$$350^{16} \bmod 527 = (350^8 \bmod 527)^2 \bmod 527 = 443$$

$$350^{32} \bmod 527 = (350^{16} \bmod 527)^2 \bmod 527 = 205$$

$$350^{64} \bmod 527 = (350^{32} \bmod 527)^2 \bmod 527 = 392$$

$$350^{128} \bmod 527 = (350^{64} \bmod 527)^2 \bmod 527 = 307$$

$$c = ((350^1 \bmod 527)(350^4 \bmod 527)(350^{16} \bmod 527)(350^{32} \bmod 527)(350^{128} \bmod 527)) \bmod 527$$

$$c = (350 * 361 * 443 * 205 * 307) \bmod 527 = 40$$

- dešifrirano sporočilo: $m = 40$

7

Diffie - Hellmanov algoritem

- glavna parametra sta lahko enaka za vse uporabnike:
 - (g, p) : "generator" g in veliko praštevilo p
- varnost DH algoritma temelji na težavnosti računanja diskretnega logaritma:
 - za vsako število $0 < n < p$ lahko najdemo potenco k , tako da velja:
 - $n = g^k \bmod p$
 - število k pa zelo težko poiščemo iz (n, g, p) !!
- A in B najprej vsak na svoji strani izbereta tajni ključ tk_a in tk_b
- A in B izračunata javna ključa jk_a in jk_b :
 - $jk_a = g^{tk(a)} \bmod p$
 - $jk_b = g^{tk(b)} \bmod p$
- A in B si izmenjata ključa $n_a \leftrightarrow n_b$ in izračunata skupni ključ:
 - uporabnik A izračuna sejni ključ: $tk_{Ab} = jk_b^{tk(a)} \bmod p$
 - uporabnik B izračuna sejni ključ: $tk_{Ba} = jk_a^{tk(b)} \bmod p$
- oba sejna ključa sta enaka: $g^{tk(b)tk(a)} \bmod p = g^{tk(a)tk(b)} \bmod p$

8

DH - primer generacije sejnega ključa

- parametra g in p sta: $g=23$, $p=31$
- A in B izbereta tajni ključ tk_a in tk_b
 - $tk_a = 9$
 - $tk_b = 3$
- A in B izračunata javna ključa jk_a in jk_b :
 - $jk_a = g^{tk(a)} \bmod p = 23^9 \bmod 31 = 27$
 - $jk_b = g^{tk(b)} \bmod p = 23^3 \bmod 31 = 15$
- A in B izmenjata javna ključa jk_a , jk_b in izračunata skupni ključ:
 - A: $tsk_{ab} = jk_b^{tk(a)} \bmod p = 15^9 \bmod 31 = 29$
 - B: $tsk_{ba} = jk_a^{tk(b)} \bmod p = 27^3 \bmod 31 = 29$

9

ElGamal-ov algoritem

- imenuje se po avtorju: Taher ElGamal
- varnost ElGamal algoritma temelji na težavnosti računanja diskretnega logaritma:
 - skupina uporabnikov izbere veliko praštevilo p in naključno število g
 - vsak uporabnik naključno izbere število x in izračuna par y :
 $y = g^x \bmod p$
 - tajni ključ sestavljajo števila (x, g, p)
 - javni ključ so števila (y, g, p)
 - če je p zelo veliko število, potem iz (y, g, p) zelo težko izračunamo eksponent x !!
- ElGamal algoritem za enkripcijo
- ElGamal algoritem za digitalni podpis

10

ElGamal-ovo šifriranje

- veliko praštevilo p in naključno število g sta javna
- uporabnika A in B naključno izbereta tajna ključa in generirata javna ključa:

- $jk_a = g^{tk(a)} \bmod p$
- $jk_b = g^{tk(b)} \bmod p$

- pošiljatelj A:



- izbere naključno število k , $\gcd(k, p-1)=1$
- na osnovi čistopisa m , naključnega števila k in javnega ključa prejemnika jk_b izračuna dvodelni šifropis (a, b) :

$$a = g^k \bmod p$$

$$b = (jk_b^k m) \bmod p$$

- prejemnik B:

- dešifriranje sporočilo na osnovi tajnega ključa prejemnika x :

$$m = b a^{p-1-tk(b)} \bmod p$$

11

ElGamal-ovo šifriranje - zgled

- javni števili za več uporabnikov: $p=31$ in $g=9$
- uporabnik B naključno izbere tajni ključ in generirata javni ključ:

- $tk_b = 3$
- $jk_b = g^{tk(b)} \bmod p = 16$

- pošiljatelj A:

- izbere naključno število $k=7$, $\gcd(7, 30)=1$
- na osnovi čistopisa $m=23$, naključnega števila k in javnega ključa prejemnika jk_b izračuna dvodelni šifropis (a, b) :

$$a = g^k \bmod p = 9^7 \bmod 31 = 10$$

$$b = (jk_b^k m) \bmod p = (16^7 23) \bmod 31 = 29$$

- prejemnik B:

- dešifriranje sporočilo na osnovi tajnega ključa prejemnika x :

$$m = b a^{p-1-tk(b)} \bmod p = 29 10^{27} \bmod 31 = 23$$

12

ElGamal-ov digitalni podpis

- izbran in objavljen je par števil (g, p)
- podpisnik izračuna dvodelni podpis sporočila m na osnovi svojega tajnega ključa (x, g, p) in naključnega števila k tako da:
 - izbere naključno število k , ki izpolnjuje pogoj $\gcd(k, p-1)=1$
 - izračuna prvi del podpisa a :
$$a = g^k \bmod p$$
 - In izračuna drugi del podpisa b :
$$m = (x a + k b) \bmod (p-1)$$
 - javni ključ podpisnika je $y = g^x \bmod p$
- prejemnik preverja digitalni podpis (a, b) sporočila m s pomočjo javnega ključa pošiljatelja y :
$$y^a a^b \bmod p = g^m \bmod p \quad ?$$



13

ElGamal-ov digitalni podpis - zgled

- izbran in objavljen je par števil $(g=2, p=11)$
- podpisnik izračuna dvodelni podpis sporočila $m=5$ na osnovi svojega tajnega ključa $(x=8, g=2, p=11)$ tako da:
 - izbere naključno število $k=9$, $\gcd(9, 10)=1$
 - izračuna prvi del podpisa a :
$$a = g^k \bmod p = 2^9 \bmod 11 = 6$$
 - izračuna drugi del podpisa b :
$$m = (x a + k b) \bmod (p-1) \rightarrow b=3$$
 - javni ključ podpisnika je $y = g^x \bmod p = 2^8 \bmod 11, y=3$
- prejemnik preverja digitalni podpis $(a=6, b=3)$ sporočila m s pomočjo javnega ključa pošiljatelja $y=3$:
$$y^a a^b \bmod p = g^m \bmod p \quad ?$$

levo: $y^a a^b \bmod p = 3^6 6^3 \bmod 11 = 10$

desno: $g^m \bmod p = 2^5 \bmod 11 = 10$

14