



Kriptografija i kriptoanaliza

doc. dr. sc. Ante Đerek i prof. dr. sc. Marin Golub

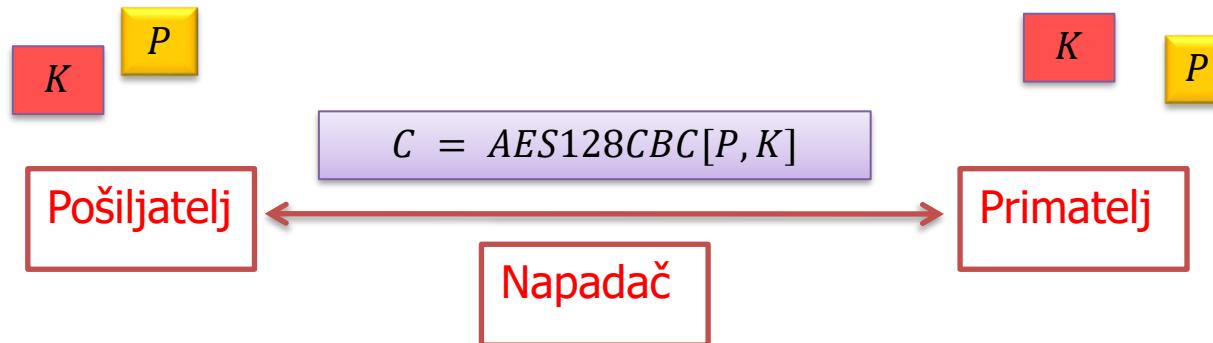
6. **Asimetrični kriptosustavi**

ili sustavi s javnim ključem

Asimetrični kriptosustavi

- Sustavi kriptiranja javnim ključem
- Metode razmjene ključeva
- Digitalni potpisi

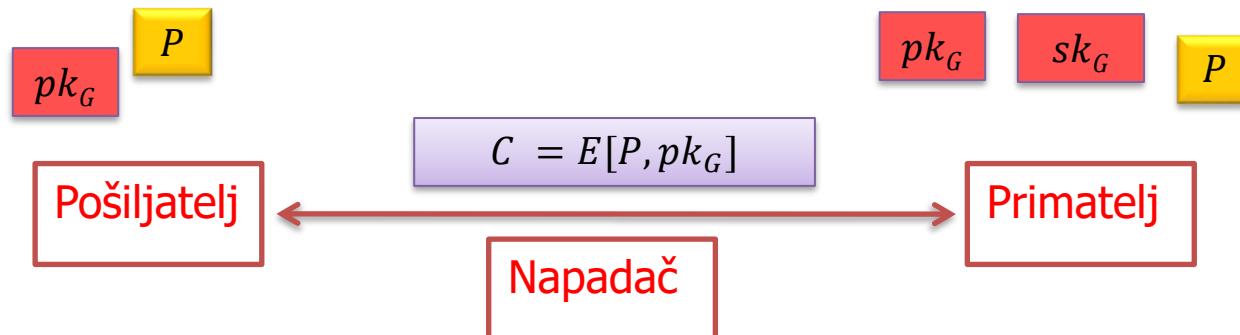
Simetrična enkripcija



- Distribucija ključeva?
- Što ako je primatelj na drugom kontinentu?
- Kako uspostaviti zajednički ključ s poslužiteljem na internetu?

Enkripcija javnim ključem

- Nova ideja: Primatelj ima dva ključa
 - Javni ključ pk_G : Javno poznat (npr. telefonski imenik)
 - Privatni ključ sk_G : Poznat samo Primatejiju
 - Jasni tekst se kriptira s javnim ključem
 - Skriveni tekst se dekriptira s privatnim ključem



Primjena – PGP/GPG

```
$ gpg --list-keys Gledec
pub 1024D/800D81AC 1999-12-03
uid          Gordan Gledec <gordan.gledec@tel.fer.hr>
uid          Gordan Gledec <gordan@tel.fer.hr>
uid          Gordan Gledec <gordan.gledec@fer.hr>
uid          Gordan Gledec <gordan@kaktus.tel.fer.hr>
uid          Gordan Gledec <gordan.gledec@zg.hinet.hr>
sub 1024g/7EBABF31 1999-12-03

$ cat poruka.txt
Napadamo u zoru

$ gpg --armor --encrypt --recipient 0x800D81AC --output poruka.pgp poruka.txt
gpg: 7EBABF31: There is no assurance this key belongs to the named user

pub 1024g/7EBABF31 1999-12-03 Gordan Gledec <gordan.gledec@tel.fer.hr>
  Primary key fingerprint: 8294 3615 5220 2F8A 9A70  3F7A 8B1B 4606 800D 81AC
  Subkey fingerprint: A240 91E6 80BB BF0D 920E  B7AE CF09 55B2 7EBA BF31

It is NOT certain that the key belongs to the person named
in the user ID. If you *really* know what you are doing,
you may answer the next question with yes.

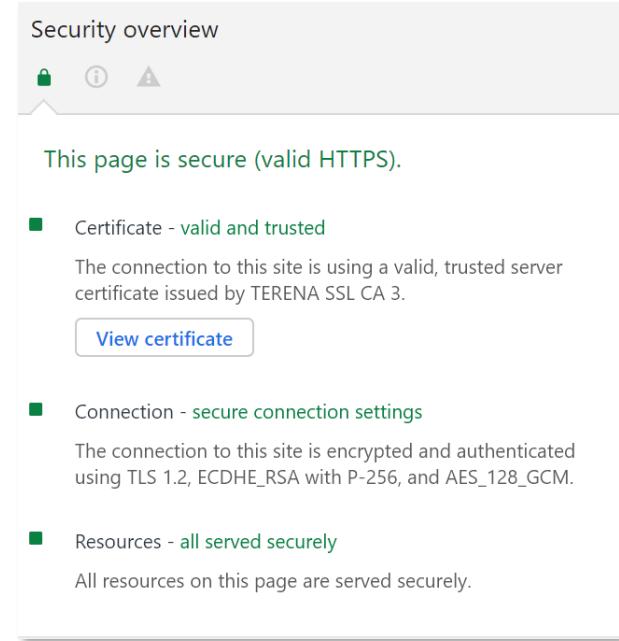
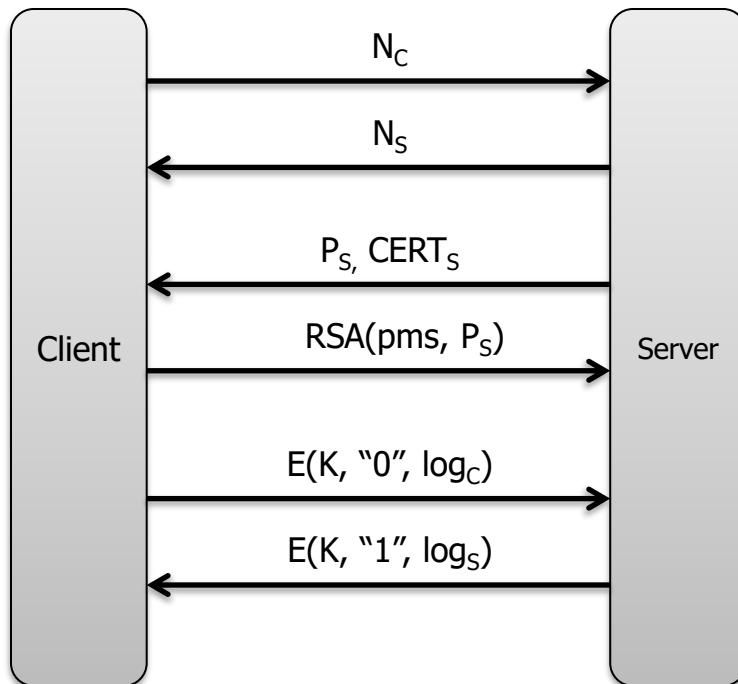
Use this key anyway? (y/N) y
$ cat poruka.pgp
-----BEGIN PGP MESSAGE-----
Version: GnuPG v1

hQEoA88JVbJ+ur8xEAP+PhWVbvpYFuAVLoCBmkid8hPXUTInN0oYSafZ0rSFRQzo
JS+ /qHMu24C8QzQkyyV/9wLWeayk6ApzCZozov3TlpFk9q10HgwfvY+F70T2uz
3jvUKI0c9Y0k8AiFLYgqNogZZ84J45ra00KHSse7whoJto3j1Rm+1qsTFCbjGx0D
/iJAfyg+KdKKfjAUkC0Sm8GH3XHQVrAjCz5Q4KfnTD90QgjOOPgeAO MsqCri+gc9
5gx+dH3Ko989pjWPYNUAkD74evfrOL5cGuG150wV7Xhf4eWwjXmewylaZxECBjkv
NWWDWQRlm42oZ9wk7KkqDFzjALBV/BjDR7RYzH3m7XbQyTAgyQHuzsEP4k16FjCU
P8TKqXci1Ug8eAnSCMkONDqMNYoLrSozBwwPI4IHTj3RI7o=
=H1YL
-----END PGP MESSAGE-----
$
```

Search results for '0x8b1b4606800d81ac'

| Type | bits/keyID | cr. time | exp time | key | expir |
|------|---|------------|----------|--|-----------|
| pub | 1024D/ 800D81AC | 1999-12-03 | | | |
| | | | | Fingerprint=8294 3615 5220 2F8A 9A70 3F7A 8B1B 4606 800D 81AC | |
| uid | Gordan Gledec <gordan@tel.fer.hr> | | | | [selfsig] |
| sig | sig 800D81AC | 1999-12-03 | | | |
| uid | Gordan Gledec <gordan.gledec@fer.hr> | | | | [selfsig] |
| sig | sig 800D81AC | 2001-01-31 | | | |
| uid | Gordan Gledec <gordan.gledec@tel.fer.hr> | | | | [selfsig] |
| sig | sig 800D81AC | 2001-01-31 | | | |
| uid | Gordan Gledec <gordan@kaktus.tel.fer.hr> | | | | [selfsig] |
| sig | sig 800D81AC | 2001-01-31 | | | |
| uid | Gordan Gledec <gordan.gledec@zg.hinet.hr> | | | | [selfsig] |
| sig | sig 800D81AC | 2001-01-31 | | | |
| sub | 1024g/7EBABF31 | 1999-12-03 | | | |
| sig | sbnd 800D81AC | 1999-12-03 | | | [] |

Primjena – TLS protocol (jedna od puno varijanti uspostave ključeva)



Povijest asimetrične kriptografije

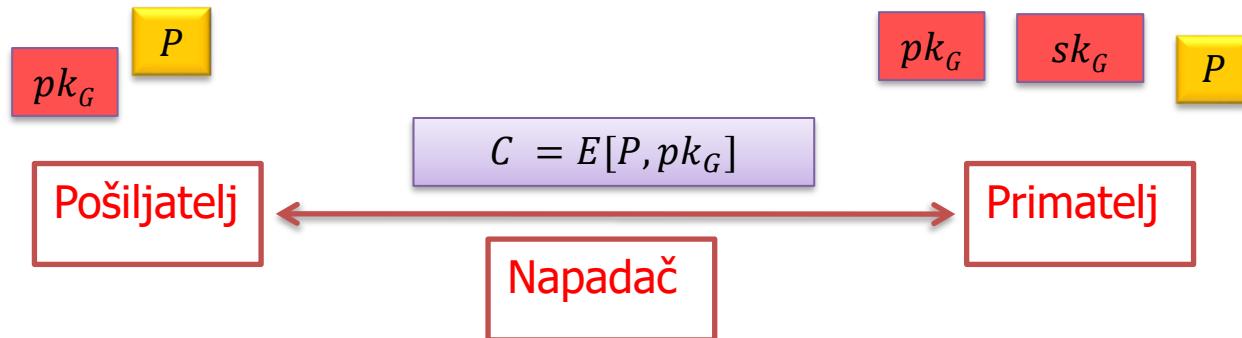
- 1973 – Cocks, „A Note on Non-Secret Encryption”
- 1975 – Merkle, „Secure Communications over Insecure Channels”
- 1976 – Diffie, Hellman, „New Directions in Cryptography”
- 1977 – Rivest, Shamir, Adelman, „A method for obtaining digital signatures and public key cryptosystems”
- 1985 – ElGamal, „A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms”
- 2020 – NIST Post-Quantum Cryptography Standardization Process

Sustav kriptiranja javnim ključem

- Trojka *efikasnih* algoritama G , E i D
 - G – algoritam koji generira par ključeva pk , sk
 - $E(m, pk)$ – algoritam enkripcije
 - $D(c, sk)$ – algoritam dekripcije
- Za svaki par ključeva (pk, sk) generiranih algoritmom G i za svaki jasni tekst p vrijedi $D(E(p, pk), sk) = p$

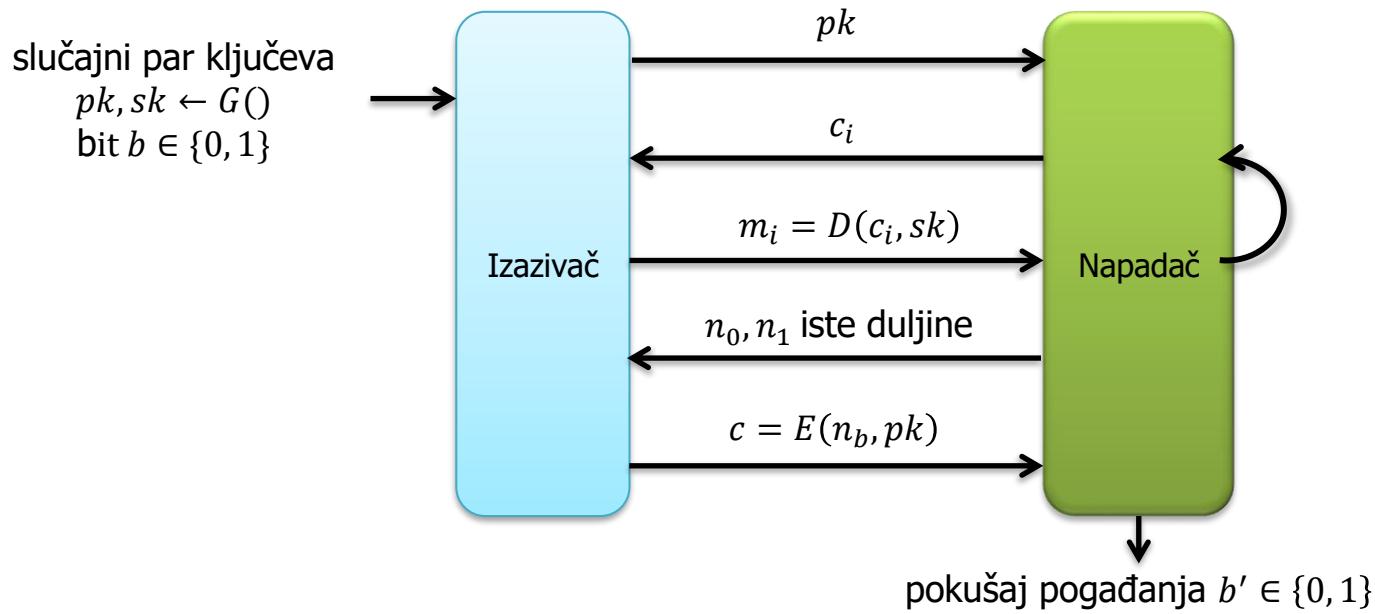
Sustav kriptiranja javnim ključem – sigurnost

- SKJK je *siguran* ako je teško na temelju kriptiranog teksta odrediti bilo što o jasnom tekstu ...
- ... čak i ako napadač ima na raspolaganju:
 - Javni ključ kojim je jasni tekst kriptiran
 - (chosen-plaintext attack).
 - Mogućnost da dobije $p = D(c, sk)$ za proizvoljni c
 - (chosen-ciphertext attack)



Primjer definicije sigurnosti SKJK

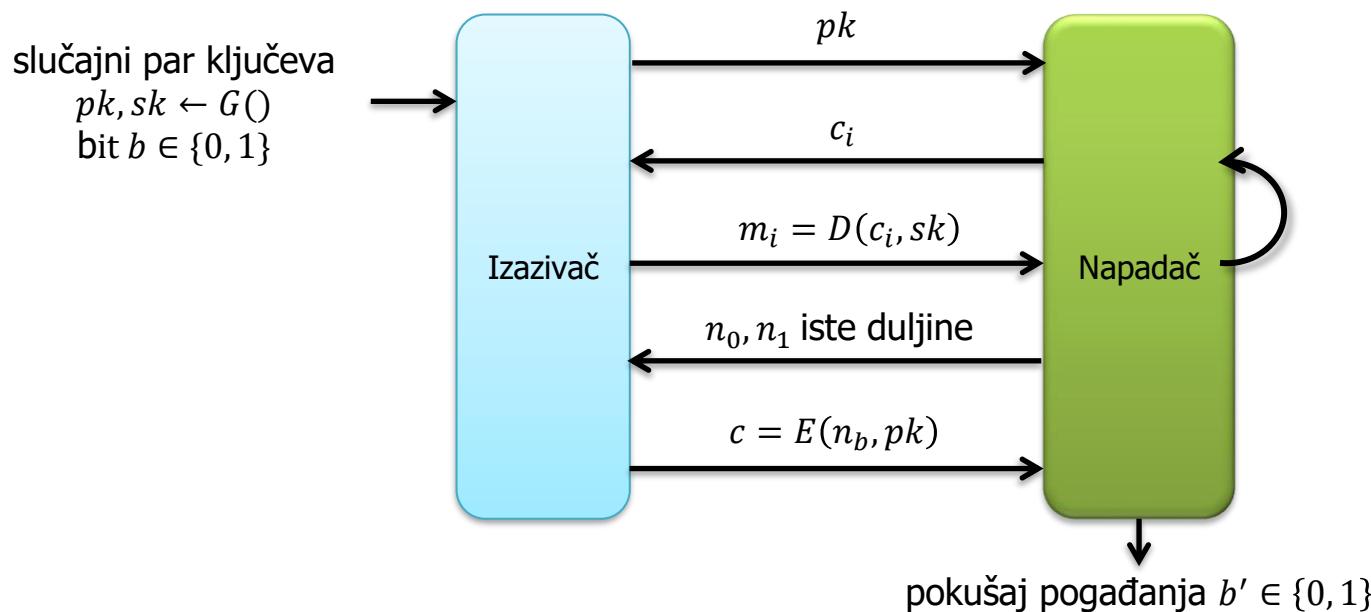
- Semantička sigurnost od napada odabranim skrivenim tekstom (semantic security under chosen-ciphertext attack): Svaki efikasan algoritam ima zanemarivu prednost u sljedećoj igri.



$$\text{Adv}_{SS-CCA1}(A) = |P(W_0) - P(W_1)|$$

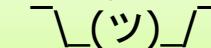
Zadatak: Sigurnost determinističkog SKJK

- Može li deterministički SKJK biti semantički siguran od napada odabranim skrivenim tekstom? Od napada odabranim jasnim tekstom?



Primjeri sustava kriptiranja javnim ključem

- Merkleove slagalice (1974)
 - građene pomoću simetrične šifre, nepraktično
- RSA (1978)
 - teorija brojeva, sigurnost povezana s problemom faktorizacije
- McEliece (1978)
 - teorija kodiranja, sigurnost povezana s problemom dekodiranja općenitog linearog koda
- ElGamal (1985)
 - teorija brojeva ili eliptičke krivulje, sigurnost povezana s problemom diskretnog logaritma

Ne znamo izgraditi dobar sustav kriptiranja javnim ključem pomoću supstitucija, permutacija, operacije XOR 

Teorija brojeva – notacija

- N – prirodni broj
- p, q – prosti brojevi
- $\mathbb{Z}_N = \{0, 1, \dots, N - 1\}$ – *prsten* u kojem se zbraja, oduzima i množi modulo N
- Pišemo $a = b$ u \mathbb{Z}_N umjesto $a \equiv b \pmod{N}$

Aritmetika u \mathbb{Z}_N

$$9 + 8 = 5 \text{ u } \mathbb{Z}_{12}$$

$$5 \cdot 7 = 11 \text{ u } \mathbb{Z}_{12}$$

$$7 - 9 = 10 \text{ u } \mathbb{Z}_{12}$$

Propozicija: Za aritmetiku u \mathbb{Z}_N vrijede uobičajena svojstva komutativnosti, asocijativnosti i distributivnosti (za sada nema dijeljenja u \mathbb{Z}_N).

Najveći zajednički djelitelj

Propozicija: Neka su x i y cijeli brojevi i neka je k njihov *najveći zajednički djelitelj*, $k = \text{nzd}(x, y)$.
Postoje cijeli brojevi a i b tako da vrijedi $ax + by = k$.

- Brojevi a , b i k se mogu efikasno odrediti *proširenim Euklidovim algoritmom*

Dijeljenje u \mathbb{Z}_N

- *Inverz elementa* $x \in \mathbb{Z}_N$ je element $y \in \mathbb{Z}_N$ takav da vrijedi $x \cdot y = 1$ u \mathbb{Z}_N .
- Inverz od x označavamo s x^{-1} (ako postoji)

Inverz od 2 u \mathbb{Z}_{17} ? 9

Inverz od 4 u \mathbb{Z}_{10} ? Ne postoji.

Kriterij invertibilnosti

Propozicija: Broj x ima inverz u \mathbb{Z}_N ako i samo ako je $\text{nzd}(x, N) = 1$.

- Ako je $\text{nzd}(x, N) = 1$ onda vrijedi da postoje a i b takvi da je $ax + bN = 1$ pa je a inverz od x u \mathbb{Z}_N .
- Obratno ako je $xy = 1 + kN$ onda x i N moraju biti relativno prosti zato što svaki broj koji dijeli x i N mora dijeliti i broj 1.

Grupa \mathbb{Z}_N^*

- \mathbb{Z}_N^* je skup svih invertibilnih elemenata $x \in \mathbb{Z}_N$
- Drugim riječima $\mathbb{Z}_N^* = \{x \in \mathbb{Z}_N, \text{nzd}(x, N) = 1\}$
 - Svaki element u \mathbb{Z}_N^* ima inverz koji je također u \mathbb{Z}_N^*
 - Ako su x i y u \mathbb{Z}_N^* onda je i xy u \mathbb{Z}_N^*
 - Stoga je \mathbb{Z}_N^* grupa u odnosu na operaciju množenja

$$\mathbb{Z}_{15}^* = \{1, 2, 4, 7, 8, 11, 13, 14\}$$

Ako je p prost $\mathbb{Z}_p^* = \{1, 2, \dots, p - 1\}$

Eulerova funkcija

- *Eulerova funkcija* $\varphi(N) = |\mathbb{Z}_N^*|$ je broj prirodnih brojeva manjih od N i relativno prostih s N .

$$\varphi(15) = 8$$

Ako je p prost onda $\varphi(p) = p - 1$

Eulerova funkcija

Propozicija: Ako su p i q različiti prosti brojevi onda je $\varphi(pq) = (p - 1)(q - 1)$.

- Razmatram sve brojeve $1, 2, \dots, pq - 1$
- Trebam izbaciti sve višekratnike od p
 - To su $p, 2p, 3p, \dots, (q - 1)p$
- Trebam izbaciti sve višekratnike od q
 - To su $q, 2q, 3q, \dots, (p - 1)q$
- Zašto nisam niti jedan broj izbacio dvaput?
- $\varphi(pq) = pq - 1 - (p - 1) - (q - 1) = (p - 1)(q - 1)$

Eulerov teorem

Teorem (Euler): Za svaki prirodni broj N i za svaki $a \in \mathbb{Z}_N^*$ vrijedi $a^{\varphi(N)} = 1$ u \mathbb{Z}_N .

Teorem (Fermat): Za svaki prosti broj p i za svaki $a \in \mathbb{Z}_p^*$ vrijedi $a^{p-1} = 1$ u \mathbb{Z}_p .

Računanje s velikim brojevima

- Radimo s brojevima veličine 1024-4096 bitova (300-1200 dekadskih znamenki)
- Broj veličine n bitova najčešće pohranjujemo u $\frac{n}{32}$ 32-bitna bloka

```
typedef struct bignum_st BIGNUM;

struct bignum_st
{
    BN_ULONG *d;      /* Pointer to an array of 'BN_BITS2' bit chunks. */
    int top;          /* Index of last used d +1. */
    /* The next are internal book keeping for bn_expand. */
    int dmax;         /* Size of the d array. */
    int neg;          /* one if the number is negative */
    int flags;
};
```

The integer value is stored in `d`, a malloc()ed array of words (`BN ULONG`), least significant word first. A `BN ULONG` can be either 16, 32 or 64 bits in size, depending on the 'number of bits' (`BITS2`) specified in `openssl/bn.h`.

Izvor: [openssl dokumentacija](#)

Aritmetika

- Zbrajanje/oduzimanje?
 - Školski algoritam: $O(n)$
- Množenje?
 - Školski algoritam: $O(n^2)$
 - Karatsuba: $O(n^{\log_2 3}) \approx O(n^{1.58})$
 - Asimptotski bolji algoritmi?
- Dijeljenje s ostatkom?
 - Školski algoritam: $O(n^2)$
 - Optimizacijski trikovi – estimacija kvocijenta, normalizacija
 - Asimptotski bolji algoritmi?

Modularna aritmetika

- Zbrajanje/oduzimanje modulo N ?
 - Školski algoritam: $O(n)$
- Množenje modulo N ?
 - Pomnoži pa izračunaj ostatak: $O(M) + O(D)$
 - Montgomery: $O(n^2)$
- Eksponenciranje modulo N ?
 - Računamo $b^a \text{ mod } N$, gdje su a, b , i N n -bitni brojevi
 - For petlja: $O(a M)$
 - Uzastopno kvadriranje: $O(n M)$

Uzastopno kvadriranje

$$b^{2k} = (b^k)^2$$
$$b^{2k+1} = (b^k)^2 b$$

Neka je $a_m, a_{m-1}, \dots, a_1, a_0$ binarni prikaz od a .

```
d = 1;  
i = m;  
dok je (i >= 0) {  
    d = (d * d) mod n;  
    ako je (a[i] == 1) {  
        d = (d*b) mod n;  
    }  
    i --;  
}
```

Uzastopno kvadriranje – primjer

Primjer 11.4.

Neka su:

$$a = 635 \Rightarrow a = 1001111011_{(2)}$$

$$n = 734$$

$$b = 5$$

$$5^{635} \bmod 734 = ?$$

```
d = 1;  
i = m;  
dok je (i >= 0) {  
    d = (d * d) mod n;  
    ako je (a[i] == 1) {  
        d = (d * b) mod n;  
    }  
    i --;  
}
```

Postupak izračunavanja $b^a \bmod n$:

| | | | | | | | | | | |
|------|---|----|-----|-----|-----|----|-----|-----|-----|-----------|
| i | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 |
| a[i] | 1 | 0 | 0 | 1 | 1 | 1 | 1 | 0 | 1 | 1 |
| d | 5 | 25 | 625 | 685 | 261 | 29 | 535 | 699 | 253 | <u>21</u> |

Kriptosustav “obični RSA”

- *Textbook RSA / Schoolbook RSA*
- Moramo definirati
 - Algoritam G
 - Algoritam E
 - Algoritam D

RSA – generiranje ključeva

Algoritam G:

1. Odaberem velike slučajne proste brojeve p i q
2. Izračunam $N = p \cdot q$
3. Izračunam $\varphi(N) = (p - 1)(q - 1)$
4. Odaberem proizvoljni $e \in \mathbb{Z}_{\varphi(N)}^*$ (u praksi $e = 65537$)
5. Izračunam $d = e^{-1} \in \mathbb{Z}_{\varphi(N)}^*$
6. Javni ključ: $pk = (e, N)$
7. Privatni ključ: $sk = (d, N)$

RSA – generiranje ključeva

Algoritam G:

1. Odaberem velike slučajne proste brojeve p i q
2. Izračunam $N = p \cdot q$
3. Izračunam $\varphi(N) = (p - 1)(q - 1)$
4. Odaberem proizvoljni $e \in \mathbb{Z}_{\varphi(N)}^*$ (u praksi $e = 65537$)
5. Izračunam $d = e^{-1} \in \mathbb{Z}_{\varphi(N)}^*$
6. Javni ključ: $pk = (e, N)$
7. Privatni ključ: $sk = (d, N)$

Ako je moguće N efikasno rastaviti na faktore onda je RSA nesiguran

Ako je moguće efikasno izračunati $\varphi(N)$ onda je RSA nesiguran

Obični RSA – enkripcija i dekripcija

Algoritam E:

- $E(m, (e, N)) = m^e \text{ u } \mathbb{Z}_N$

Algoritam D:

- $D(c, (d, N)) = c^d \text{ u } \mathbb{Z}_N$

e zovemo *javni eksponent*

d zovemo *privatni eksponent*

N zovemo *modul*

Jasni i skriveni tekst su brojevi u \mathbb{Z}_N

RSA – Korektnost

Algoritam G:

1. Veliki slučajni prosti brojeve p i q
2. Izračunam $N = p \cdot q$
3. Izračunam $\varphi(N) = (p - 1)(q - 1)$
4. Odaberem $e \in \mathbb{Z}_{\varphi(N)}^*$
5. Izračunam $d = e^{-1} \in \mathbb{Z}_{\varphi(N)}^*$
6. Javni ključ: $pk = (e, N)$
7. Privatni ključ: $sk = (d, N)$

Algoritam E:

- $E(m, (e, N)) = m^e \in \mathbb{Z}_N$

Algoritam D:

- $D(c, (d, N)) = c^d \in \mathbb{Z}_N$

$$\begin{aligned}D(E(m, (e, N)), (d, N)) &= D(m^e, (d, N)) = (m^e)^d = m^{ed} \\&= m^{1+k\varphi(N)} = m \cdot (m^{\varphi(N)})^k = m \cdot (1)^k = m \in \mathbb{Z}_N\end{aligned}$$

RSA – poruke

- Jasni i skriveni tekst moraju biti u \mathbb{Z}_N^*
- Zašto ovo nije problem?
 - Možete li za veliki RSA modul N pronaći neki broj između 1 i $N - 1$ koji nije u \mathbb{Z}_N^* ?

RSA – Implementacija

Algoritam G:

1. Veliki slučajni prosti brojeve p i q
2. Izračunam $N = p \cdot q$
3. Izračunam $\varphi(N) = (p - 1)(q - 1)$
4. Odaberem $e \in \mathbb{Z}_{\varphi(N)}^*$
5. Izračunam $d = e^{-1} \in \mathbb{Z}_{\varphi(N)}^*$
6. Javni ključ: $pk = (e, N)$
7. Privatni ključ: $sk = (d, N)$

Algoritam E:

- $E(m, (e, N)) = m^e \pmod{N}$

Algoritam D:

- $D(c, (d, N)) = c^d \pmod{N}$

- Množenje, zbrajanje, inverz, modularno eksponenciranje

RSA – Implementacija

Algoritam G:

1. Veliki slučajni prosti brojeve p i q
2. Izračunam $N = p \cdot q$
3. Izračunam $\varphi(N) = (p - 1)(q - 1)$
4. Odaberem $e \in \mathbb{Z}_{\varphi(N)}^*$
5. Izračunam $d = e^{-1} \in \mathbb{Z}_{\varphi(N)}^*$
6. Javni ključ: $pk = (e, N)$
7. Privatni ključ: $sk = (d, N)$

Algoritam E:

- $E(m, (e, N)) = m^e \pmod{N}$

Algoritam D:

- $D(c, (d, N)) = c^d \pmod{N}$

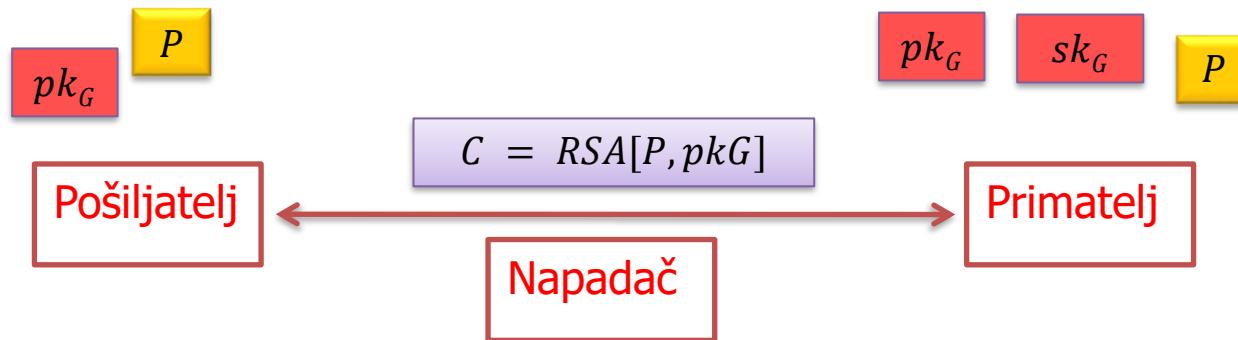
- Složenost enkripcije i dekripcije? Općenito $O(n^3)$
- $e = 63357?$

Generiranje prostih brojeva

- Algoritam
 - Izaberi slučajni broj zadane veličine
 - Provjeri je li izabrani broj prost
- Prosti brojevi su dovoljno *gusti*
- Postoje efikasni algoritmi koji određuju je li broj prost ili složen (npr. Miller-Rabin)

RSA – sigurnost

- Obični RSA *nije* siguran sustav kriptiranja javnim ključem 😞



Zadatak: Obični RSA 1

- Kriptiramo glasove na izborima
 - sudjeluju dva kandidata označena s 1 i 2
 - izborno povjerenstvo objavi svoj javni ključ pk .
 - glasač A izračuna $c_A = E(g_A, pk)$ gdje je $g_A \in \{1, 2\}$
 - glasač A šalje c_A izbornom povjerenstvu

- $E(1, pk) = 1$
- $E(2, pk) \neq 1$
- Napadač može zaključiti za koga je glasač glasao!

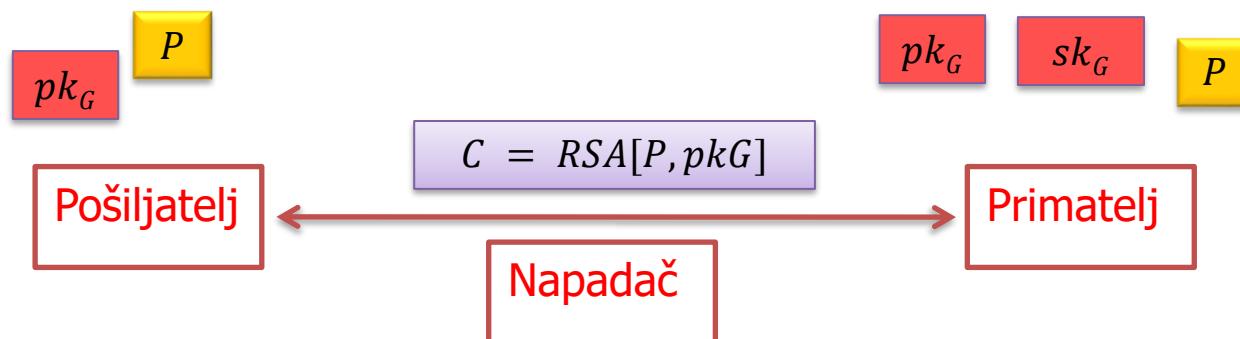
Zadatak: Obični RSA 2

- Kriptiramo datoteku
 - Datoteka se sastoji se od n bajtova b_1, b_2, \dots, b_n
 - kriptiramo svaki bajt zasebno $c_k = E(b_k, pk)$
 - šaljemo c_1, c_2, \dots, c_n Wi-Fi mrežom

- Napadač može za svaki mogući bajt $b = 0, 1, \dots, 255$ izračunati $c = E(b, pk)$
- Kada vidi c_1, c_2, \dots, c_n lagano nalazi b_1, b_2, \dots, b_n

Sustav kriptiranja javnim ključem – sigurnost

- Ako je algoritam enkripcije deterministički onda sustav kriptiranja javnim ključem nikako ne može biti siguran



Zadatak: Obični RSA 3

- Šaljemo 128-bitni AES ključ K koristeći RSA
 - neka je $e = 3$
 - šaljemo $c = E(K, pk)$

- K^3 ima oko manje od 400 bitova
- Prilikom enkripcije se ne dogodi redukcija modulo N
- Napadač može izračunati $K = \sqrt[3]{c}$

Zadatak: Obični RSA 4

- Šaljemo 64-bitni DES ključ K koristeći RSA
 - neka je $e = 65537$
 - šaljemo $c = RSA(K, pk)$

- Ponekad će se slučajno dogoditi da je $K = K_1 \cdot K_2$ gdje su K_1 i K_2 32-bitni brojevi
- $c = K^e = K_1^e \cdot K_2^e$ u \mathbb{Z}_N
- $c \cdot (K_1^e)^{-1} = K_2^e$ u \mathbb{Z}_N
- *Meet-in-the-middle* algoritam nalazi K_1 i K_2 u 2^{32} koraka



Kriptografija i kriptoanaliza

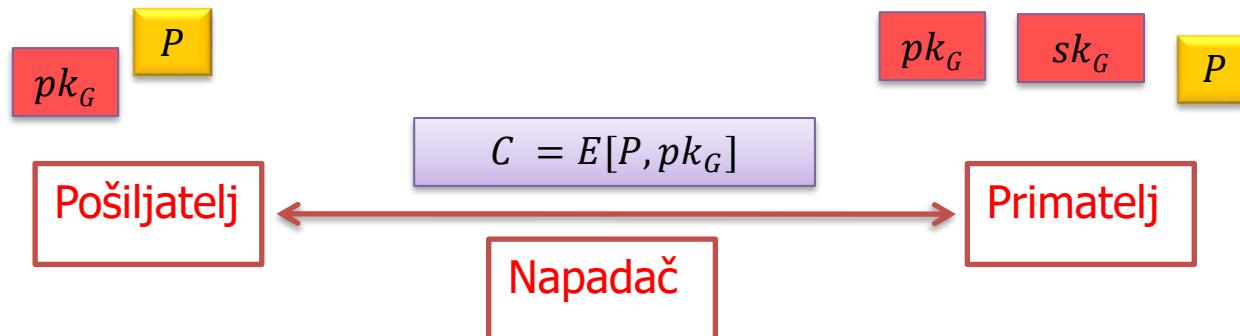
doc. dr. sc. Ante Đerek i prof. dr. sc. Marin Golub

6. **Asimetrični kriptosustavi**

Napadi na kriptosustav RSA

Ponavljanje: Enkripcija javnim ključem

- Nova ideja: Primatelj ima dva ključa
 - Javni ključ pk_G : Javno poznat (npr. telefonski imenik)
 - Privatni ključ sk_G : Poznat samo Primatelu
 - Jasni tekst se kriptira s javnim ključem
 - Skriveni tekst se dekriptira s privatnim ključem

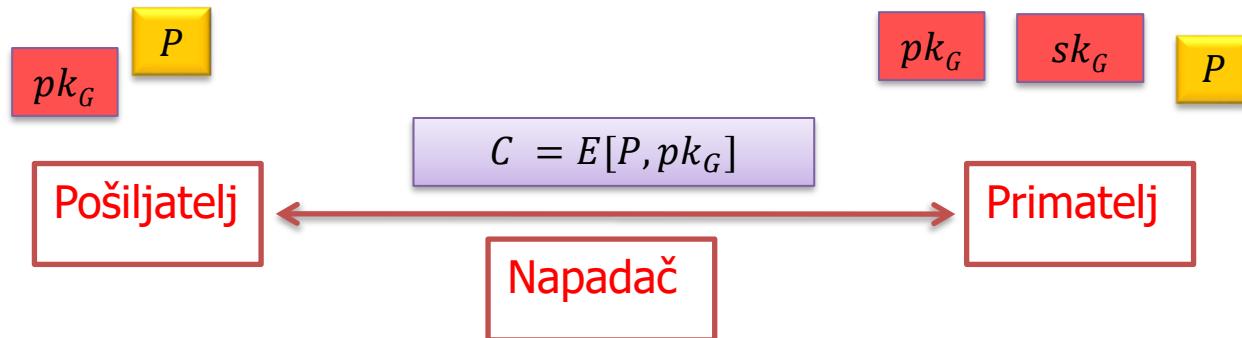


Ponavljanje: Sustav kriptiranja javnim ključem

- Trojka *efikasnih* algoritama G , E i D
 - G – algoritam koji generira par ključeva pk, sk
 - $E(m, pk)$ – algoritam enkripcije
 - $D(c, sk)$ – algoritam dekripcije
- Za svaki par ključeva (pk, sk) generiranih algoritmom G i za svaki jasni tekst p vrijedi $D(E(p, pk), sk) = p$

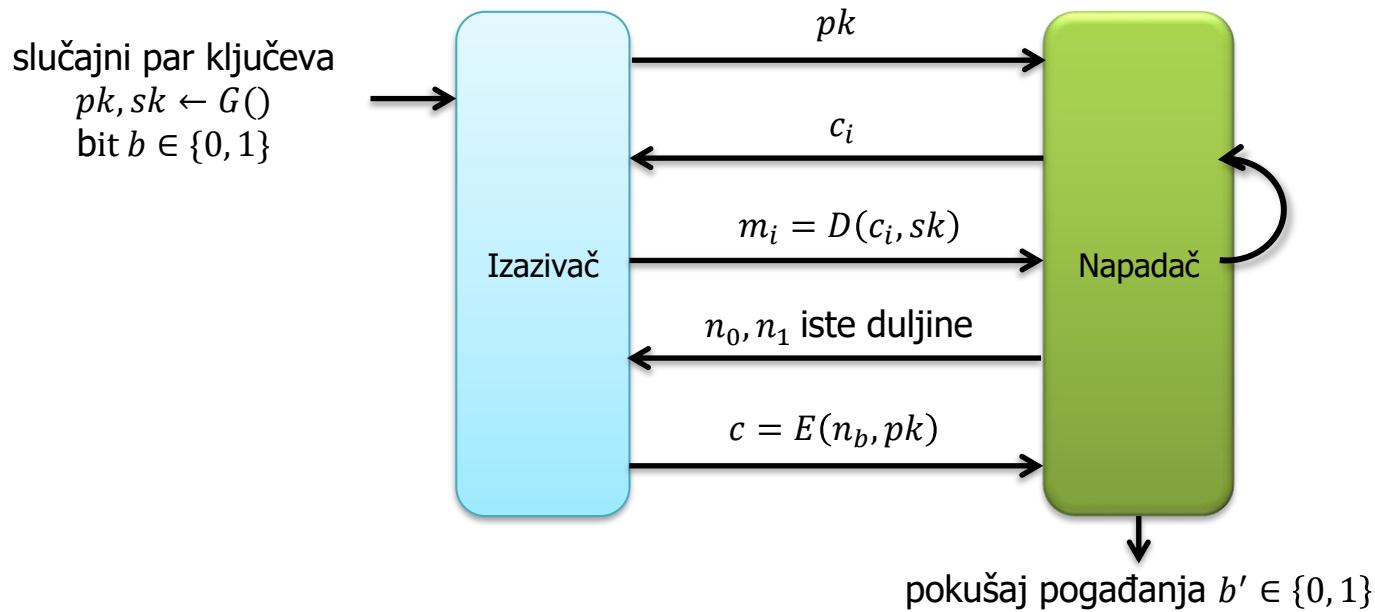
Sustav kriptiranja javnim ključem – sigurnost

- SKJK je *siguran* ako je teško na temelju kriptiranog teksta odrediti bilo što o jasnom tekstu ...
- ... čak i ako napadač ima na raspolaganju:
 - Javni ključ kojim je jasni tekst kriptiran
 - (chosen-plaintext attack).
 - Mogućnost da dobije $p = D(c, sk)$ za proizvoljni c
 - (chosen-ciphertext attack)



Primjer definicije sigurnosti SKJK

- Semantička sigurnost od napada odabranim skrivenim tekstom (semantic security under chosen-ciphertext attack): Svaki efikasan algoritam ima zanemarivu prednost u sljedećoj igri.



$$\text{Adv}_{SS-CCA1}(A) = |P(W_0) - P(W_1)|$$

Ponavljanje: Obični RSA

Algoritam G:

1. Veliki slučajni prosti brojeve p i q
2. Izračunam $N = p \cdot q$
3. Izračunam $\varphi(N) = (p - 1)(q - 1)$
4. Odaberem $e \in \mathbb{Z}_{\varphi(N)}^*$
5. Izračunam $d = e^{-1} \in \mathbb{Z}_{\varphi(N)}^*$
6. Javni ključ: $pk = (e, N)$
7. Privatni ključ: $sk = (d, N)$

Algoritam E:

- $E(m, (e, N)) = m^e \pmod{N}$

Algoritam D:

- $D(c, (d, N)) = c^d \pmod{N}$

Zadatak: Obični RSA 4

- Šaljemo 64-bitni DES ključ K koristeći RSA
 - neka je $e = 65537$
 - šaljemo $c = RSA(K, pk)$

- Ponekad će se slučajno dogoditi da je $K = K_1 \cdot K_2$ gdje su K_1 i K_2 32-bitni brojevi
- $c = K^e = K_1^e \cdot K_2^e$ u \mathbb{Z}_N
- $c \cdot (K_1^e)^{-1} = K_2^e$ u \mathbb{Z}_N
- *Meet-in-the-middle* algoritam nalazi K_1 i K_2 u 2^{32} koraka

RSA – Kombinacija sa simetričnom enkripcijom

- U praksi se RSA gotovo nikad ne koristi za kriptiranje podataka već kriptiranje materijala za ključ.
- Puno konstrukcija.
 - Kriptiranje materijala za ključ
 - Digitalna omotnica

RSA – Kombinacija sa simetričnom enkripcijom

- Dokazivo ispravna konstrukcija, pod određenim jakim pretpostavkama na sigurnost običnog RSA, hash funkcija i simetrične enkripcije.

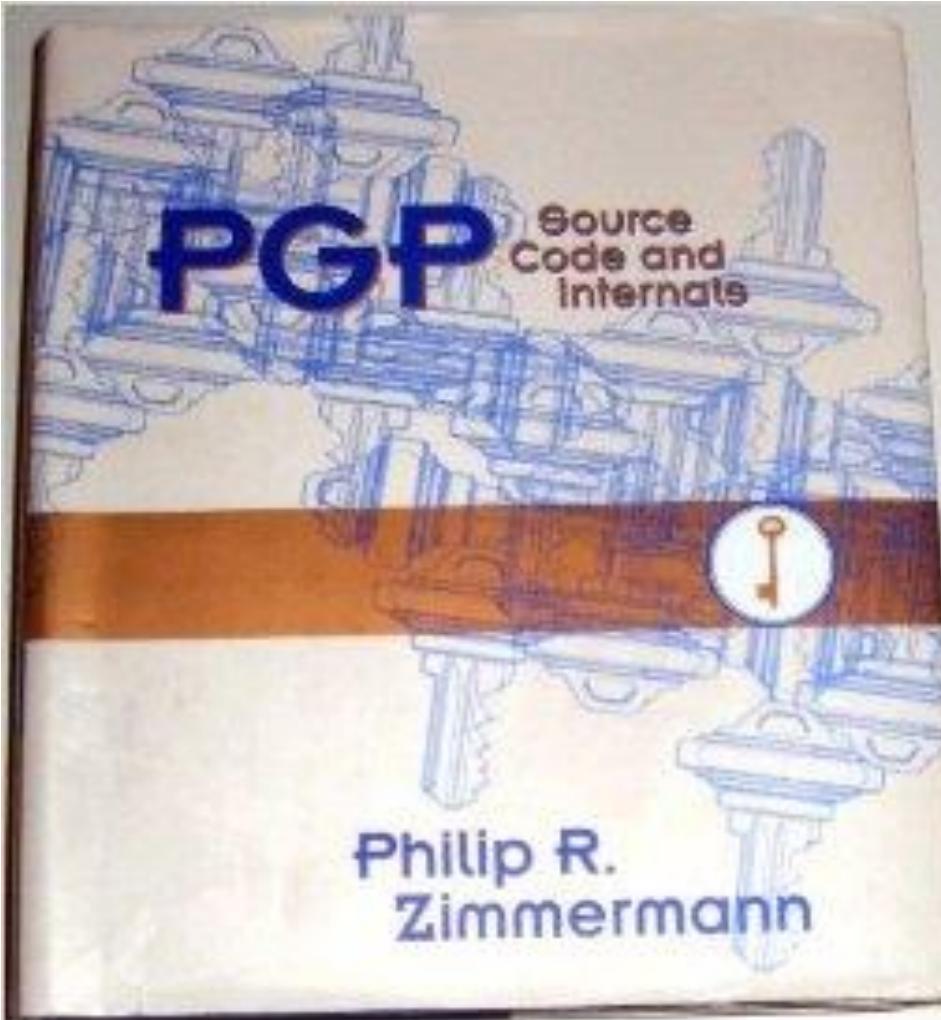
H je hash funkcija, E_s simetrična enkripcija

Algoritam E:

1. Izaberem slučajni $x \in \mathbb{Z}_N$
2. Izračunam $k = H(x)$
3. Izračunam $c_1 = E(x, pk)$
4. Izračunam $c_2 = E_s(m, k)$
5. Skriveni tekst je (c_1, c_2)

RSA – Digitalna omotnica

- Generiramo novi nasumični ključ K
 - Poruku kriptiramo ključem K pomoću simetrične enkripcije.
 - Ključ K kriptiramo sustavom RSA
- $E(Pad(K), pk), E_S(m, K)$
- Primijetite da je digitalna omotnica nije deterministička enkripcija!



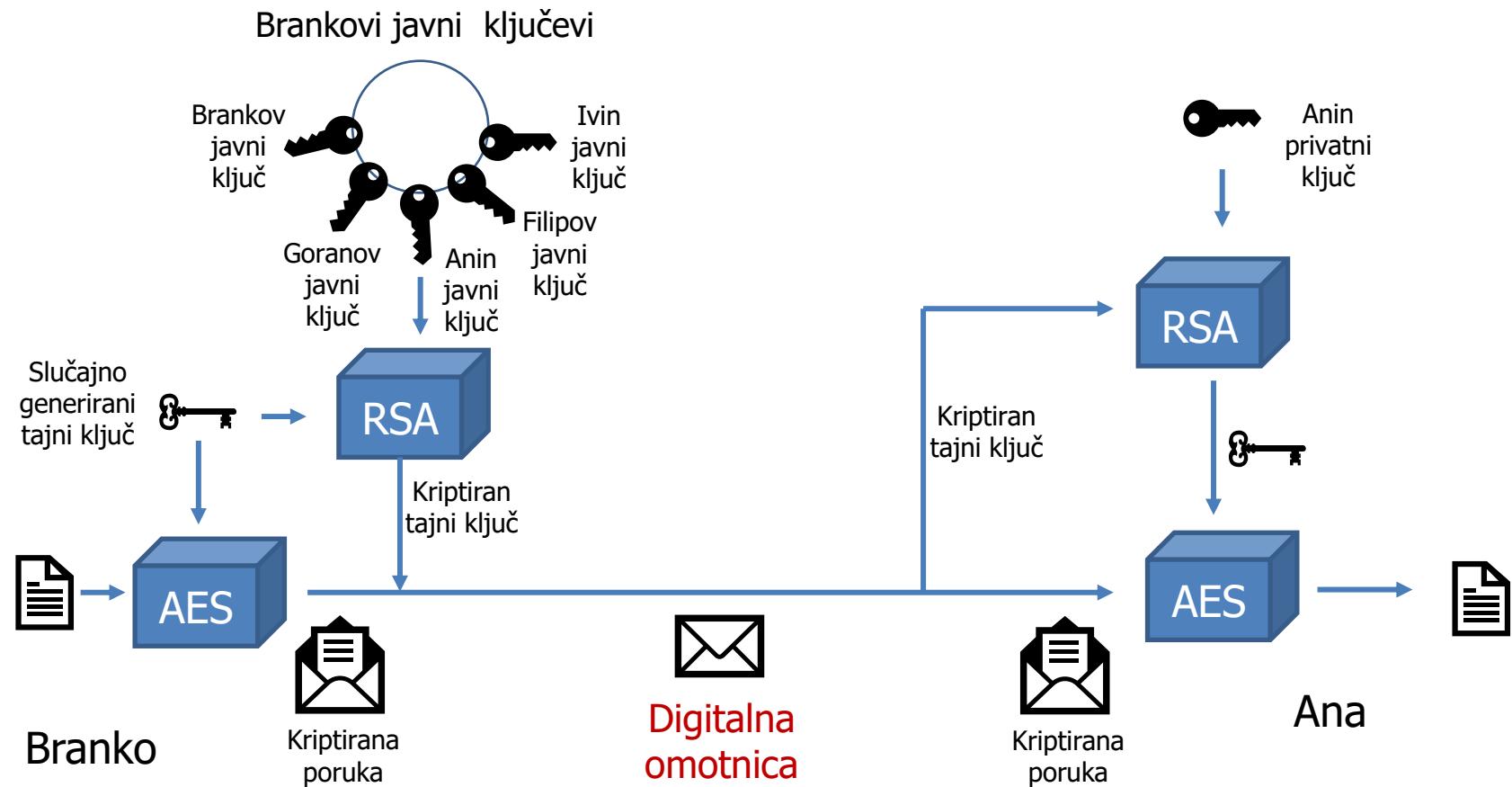
PGP

Source
Code and
Internals



Philip R.
Zimmermann

Kako osigurati tajnost?



RSA – *Padding*

- Jasni tekst se uvijek nadopunjuje na zadanu veličinu!
- Postupak nadopunjavanja (*padding*) igra kritičnu ulogu i pažljivo je osmišljen.
 - PKCS#1 v1.5 (mnoštvo sigurnosnih problema)
 - OAEP

RSA – PKCS#1 v1.5 *Padding*

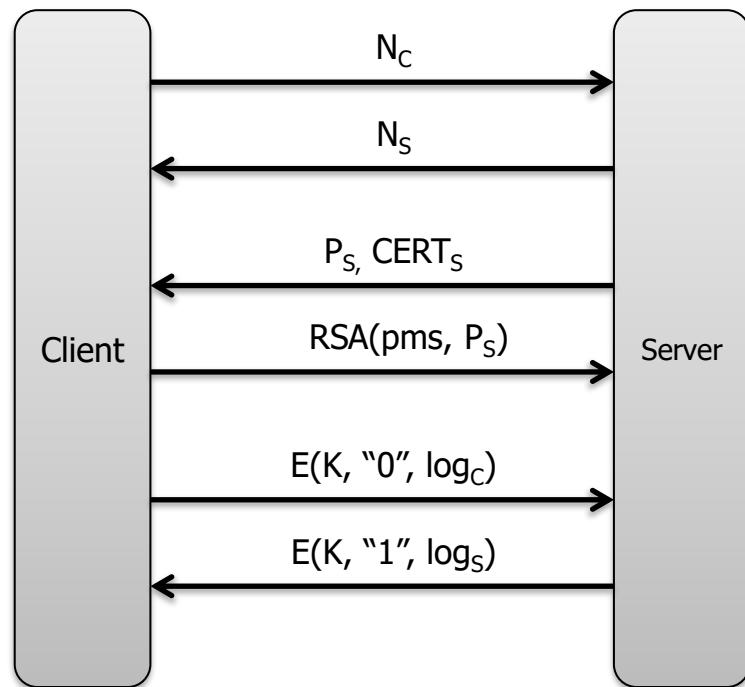
EME-PKCS1-v1_5 encoding:

- a. Generate an octet string PS of length $k - mLen - 3$ consisting of pseudo-randomly generated nonzero octets. The length of PS will be at least eight octets.
- b. Concatenate PS, the message M, and other padding to form an encoded message EM of length k octets as

$$EM = 0x00 \parallel 0x02 \parallel PS \parallel 0x00 \parallel M.$$

Bleichenbacherov napad

- Prepostavimo da TLS poslužitelj koristi PKCS#1 v1.5 *padding*
- Razumna implementacija:
 - Izračunaj $m = c^d \text{ u } \mathbb{Z}_N$
 - Ako m ne počinje s bajtovima 0x00 0x02 vrati klijentu poruku „Bad padding“.
- Dobili smo oracle!
 - Napadač za proizvoljni broj c može saznati da li $c^d \text{ u } \mathbb{Z}_N$ počinje s 0x00 0x02.



Bleichenbacherov napad

- Dobili smo oracle!
 - Napadač za proizvoljni broj c može sazнати да ли $c^d \in \mathbb{Z}_N$ почиње с $0x00$ $0x02$, где је (d, N) privatni ključ.
- Oracle se može iskoristiti – постоји ефикасан алгоритам који након разумног броја упита одређује privatni ključ.
 - Око $2M$ упита потребно за 1024-bitni RSA ključ.
- *Daniel Bleichenbacher, Chosen Ciphertext Attacks Against Protocols Based on the RSA Encryption Standard PKCS #1 (1998)*

Bleichenbacherov napad – pouke?

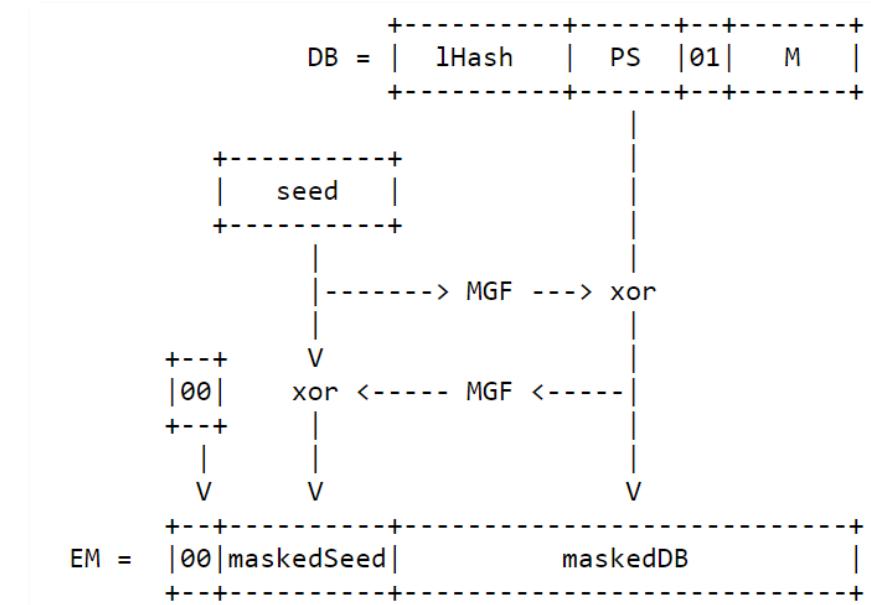
- Implementacija ne smije napadaču (tj. Korisniku) otkrivati detalje greške.
- Napad odabranim skrivenim tekstom je stvarno razumna definicija sigurnosti.

In any case, a TLS server MUST NOT generate an alert if processing an RSA-encrypted premaster secret message fails, or the version number is not as expected. Instead, it MUST continue the handshake with a randomly generated premaster secret. It may be useful to log the real cause of failure for troubleshooting purposes; however, care must be taken to avoid leaking the information to an attacker (through, e.g., timing, log files, or other channels.)

Izvor: <https://datatracker.ietf.org/doc/html/rfc5246>

RSA – OAEP *Padding*

- *Optimal asymmetric encryption padding*
 - Struktura slična Feistelovoj mreži
- Dokazano sigurna (u smislu semantičke sigurnosti protiv napada odabranim skrivenim tekstrom) pod jakim pretpostavkama sigurnosti običnog RSA i hash funkcija.
 - Osnovna ideja: „*all-or-nothing security*“ – ako napadač ne sazna sve bitove od EM onda ne može saznati ništa o m .

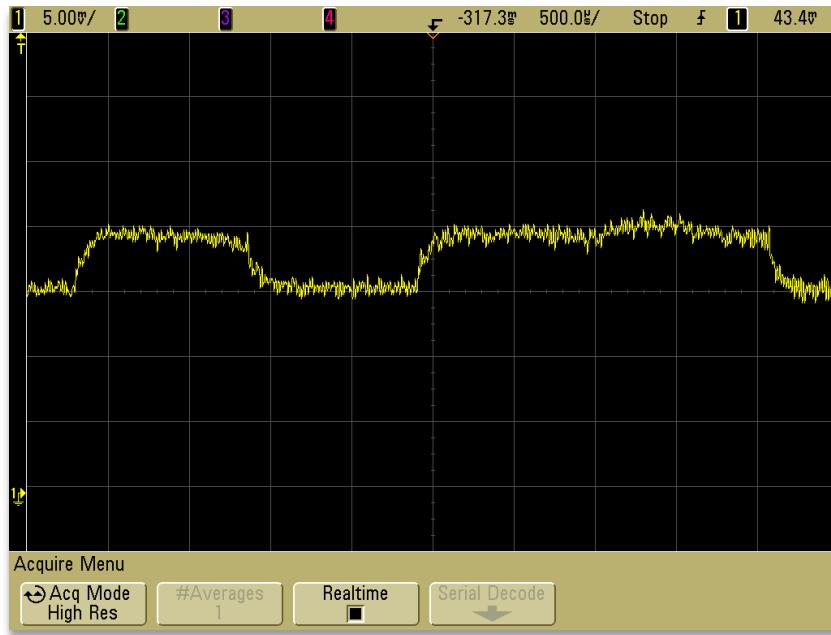


Izvor: ietf.org

Side channel napadi na RSA

```
// Modularno eksponenciranje
// b^a mod n, a u binarnom zapisu

d = 1;
i = m;
dok je (i >= 0) {
    d = (d * d) mod n;
    ako je (a[i] == 1) {
        d = (d*b) mod n;
    }
    i--;
}
```



Izvor:
wikipedia.org

Napadi na RSA

- Matematički napadi:
 - Wienerov napad na mali privatni eksponent.
 - Franklinov and Reiterov napad na povezane poruke.
 - ...
- Implementacijski napadi:
 - Napadi mjerenjem vremena.
 - Napadi u slučaju sitnih grešaka pri računanju.
 - ...
- Izvor: *Dan Boneh, Twenty years of attacks on the RSA cryptosystem*

RSA – sigurnost

- Obični RSA je nesiguran!
- Ako se RSA ispravno koristi smatramo ga sigurnim!
- Puno implementacijskih napada!
- Najbolji poznati općeniti napad:
 - Faktorizacija modula
 - Na primjer, algoritmom GNFS (General Number Field Sieve)
 - U 2020. najveći faktorizirani modul je veličine 829 bitova.

RSA – faktorizacija modula

paul zimmermann Paul.Zimmermann at inria.fr

Fri Feb 28 16:48:03 CET 2020

- Previous message: [\[Cado-nfs-discuss\] move to gitlab](#)
- **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#)

Date: February 28, 2020

For the past three months, ever since the DLP-240 record announced in December 2019 [1], we have been in a historically unique state of affairs: the discrete logarithm record (in a prime field) has been larger than the integer factorization record. We are pleased to rectify this situation with the factorization of RSA-250 from the RSA challenge list:

```
RSA-250 =
21403246502407449612644230728393335630086147151447550177977549208814180234471401366433
      =
64135289477071580278790190170577389084825014742943447208116859632024532344630238623598
      *
33372027594978156556226010605355114227940760344767554666784520987023841729210037080257
```

This computation was performed with the Number Field Sieve algorithm, using the open-source CADO-NFS software [2].

The total computation time was roughly 2700 core-years, using Intel Xeon Gold 6130 CPUs as a reference (2.1GHz):

```
RSA-250 sieving: 2450 physical core-years
RSA-250 matrix:   250 physical core-years
```

RSA – faktorizacija modula

paul zimmermann Paul.Zimmermann at inria.fr

Fri Feb 28 16:48:03 CET 2020

- Previous message: [\[Cado-nfs-discuss\] move to gitlab](#)
- **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#)

Date: February 28, 2020

For the past three months, ever since the DLP-240 record announced in December 2019 [1], we have been in a historically unique state of affairs: the discrete logarithm record (in a prime field) has been larger than the integer factorization record. We are pleased to rectify this situation with the factorization of RSA-250 from the RSA challenge list:

```
RSA-250 =
21403246502407449612644230728393335630086147151447550177977549208814180234471401366433
      =
64135289477071580278790190170577389084825014742943447208116859632024532344630238623598
      *
33372027594978156556226010605355114227940760344767554666784520987023841729210037080257
```

This computation was performed with the Number Field Sieve algorithm, using the open-source CADO-NFS software [2].

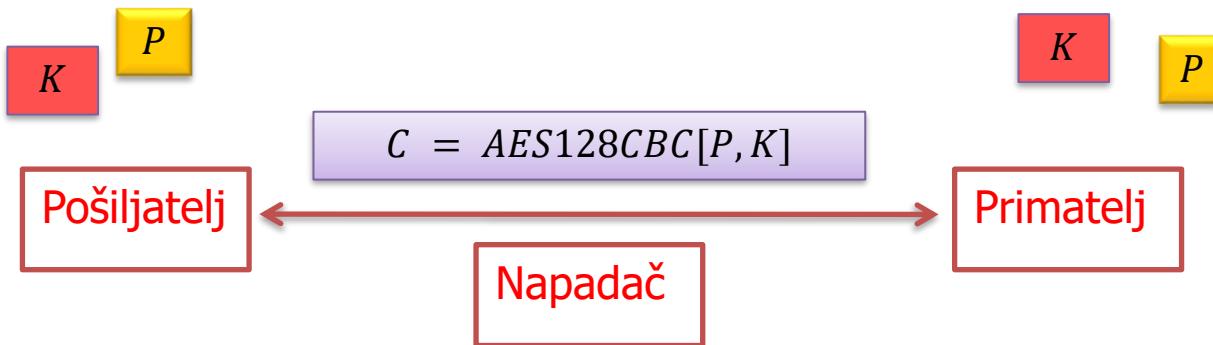
The total computation time was roughly 2700 core-years, using Intel Xeon Gold 6130 CPUs as a reference (2.1GHz):

```
RSA-250 sieving: 2450 physical core-years
RSA-250 matrix:   250 physical core-years
```

6. **Asimetrični kriptosustavi**

Digitalni potpis zasnovan na RSA

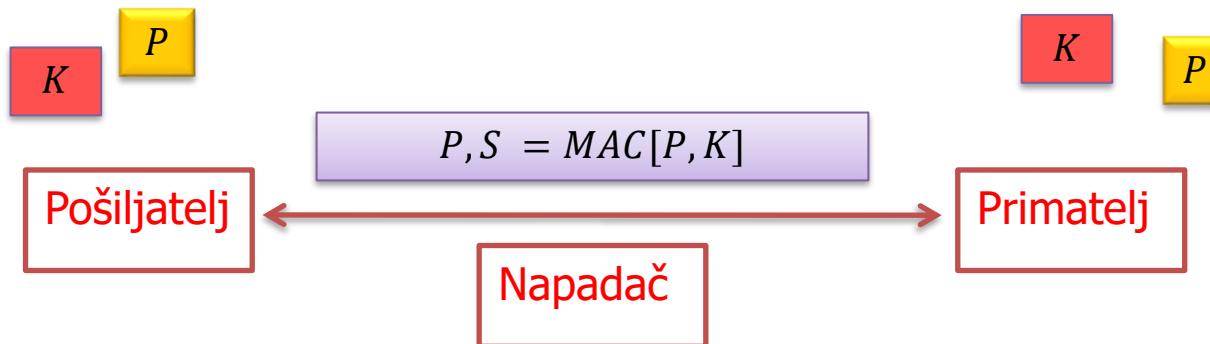
Enkripcija ne rješava sve probleme!



- Ako ste primili i uspješno dekriptirali poruku možete li biti sigurni da znate:
 - Tko je generirao poruku?
 - Je li dekriptirana poruka identična originalnoj?

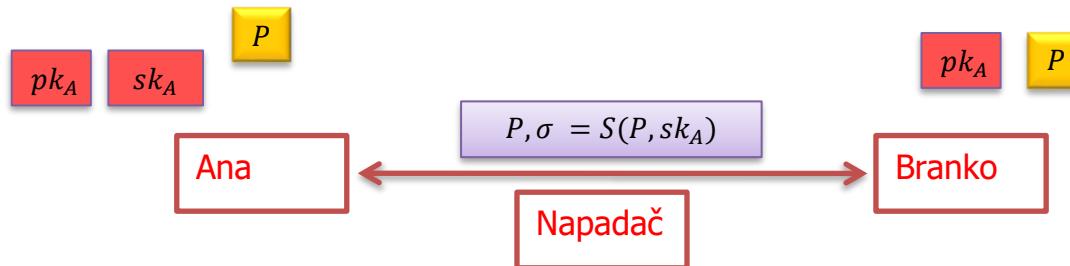
MAC / Autentificirana enkripcija

- Kod za integritet poruke (*Message Authentication Code*)
- Autentificirana enkripcija

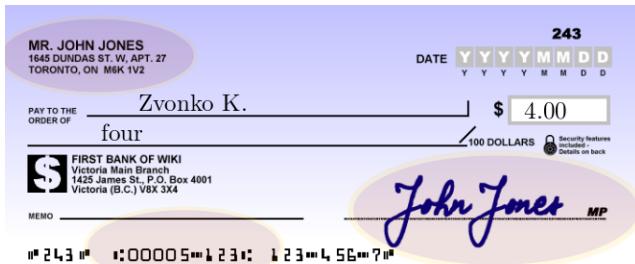


Javni i tajni ključevi

- Stara ideja: Svatko ima dva ključa
 - Javni ključ pk_A : Javno poznat (npr. telefonski imenik)
 - Privatni ključ sk_A : Poznat samo Ani
 - Ana *generira* potpis svojim privatnim ključem sk_A
 - Branko *provjerava* potpis Aninim javnim ključem pk_A



Digitalni vs analogni potpis – autentičnost

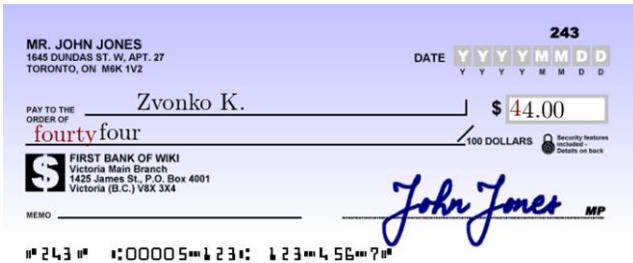


Izvor: wikipedia.org

- Svatko može provjeriti ispravnost digitalnog potpisa ako ima na raspolaganju javni ključ tobožnjeg potpisnika.
- Provjera ispravnosti je garancija da je potpis stvarno generiran odgovarajućim privatnim ključem.
- Veza između ključeva i identiteta?

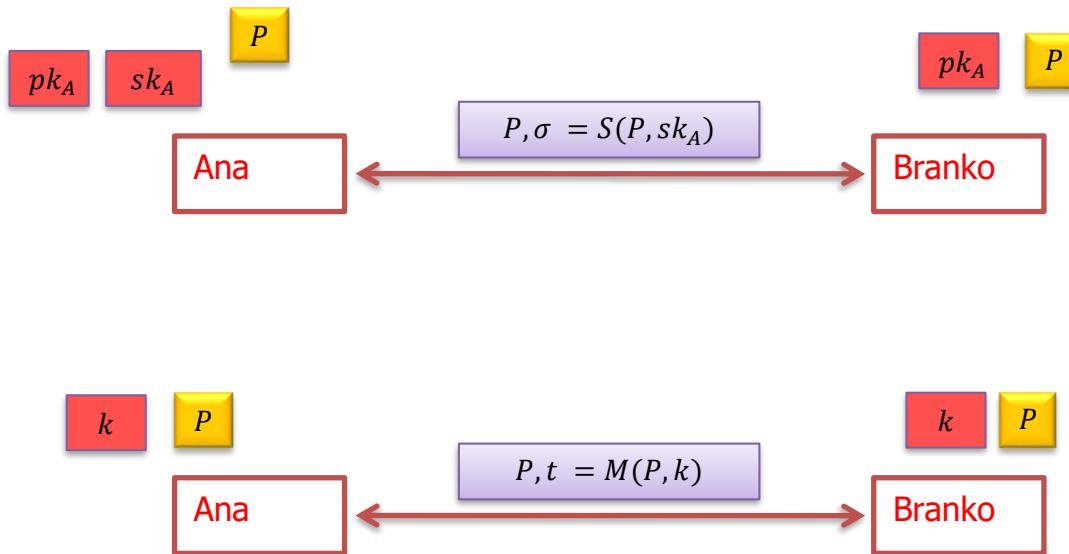
Digitalni vs analogni potpis – integritet

- Digitalni potpis je vezan uz dokument.
- Ispravan potpis garantira integritet dokumenta.



Izvor: wikipedia.org

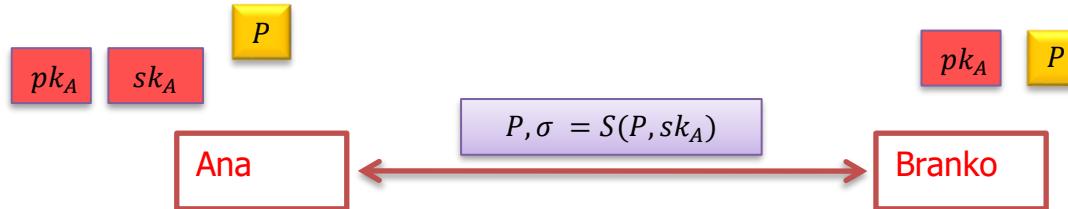
Digitalni potpis vs MAC – neporecivost (non-repudiation)



- Moguće je trećoj strani dokazati da je pošiljatelj potpisao poruku!
- Veza između ključeva i identiteta?
- „Netko me je hakirao“ obrana?

Sustav digitalnog potpisa

- Trojka efikasnih algoritama G , S i V
 - G – algoritam koji generira par ključeva pk , sk
 - $S(m, sk)$ – algoritam potpisivanja
 - $V(m, \sigma, pk)$ – algoritam verifikacije
- Za svaki par ključeva (pk, sk) generiranih algoritmom G i za svaki jasni tekst p vrijedi $V(p, S(p, sk), pk) = 1$

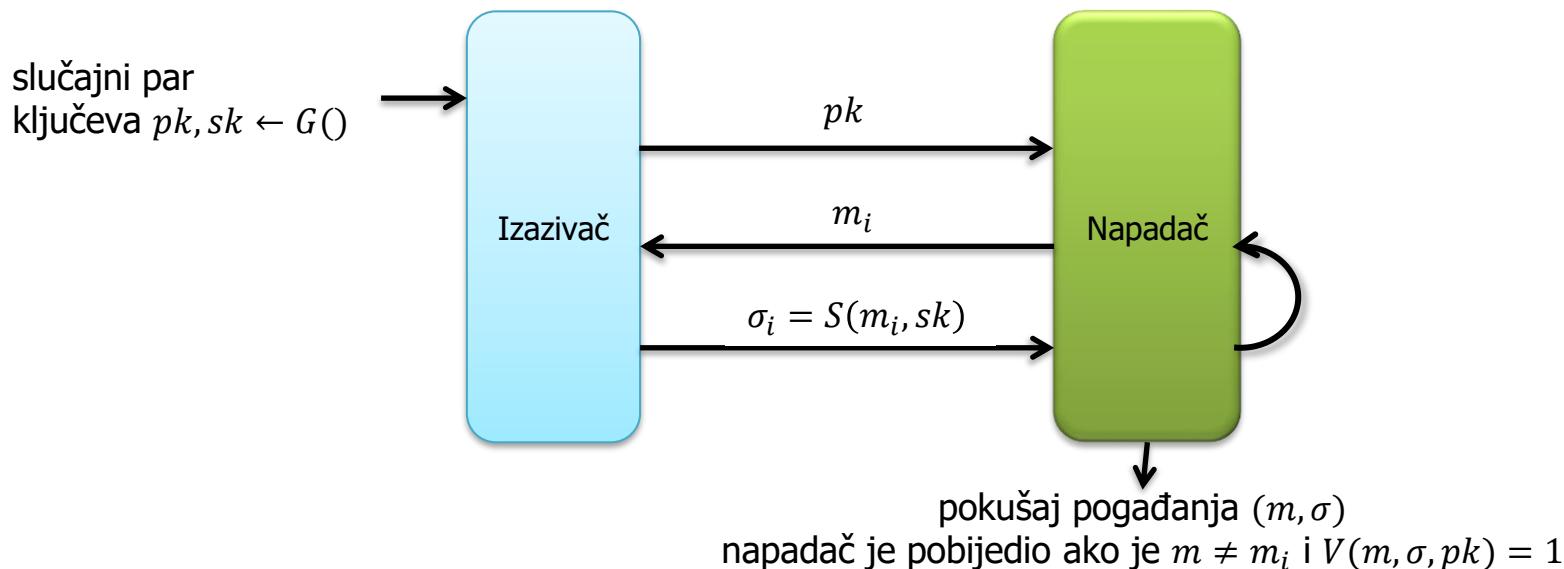


Sustav digitalnog potpisa – sigurnost

- SDP je siguran ako je teško odrediti bilo koju poruku p i bilo koji potpis (niz bitova) σ takav da
 - $V(p, \sigma, pk) = 1$
 - p nikad nije potpisan s privatnim ključem sk
- ... čak i ako napadač ima na raspolaganju:
 - Javni ključ pk
 - Mogućnost da dobije potpis $S(p, sk)$ za proizvoljnu poruku p (chosen message attack)

Primjer definicije sigurnosti digitalnog potpisa

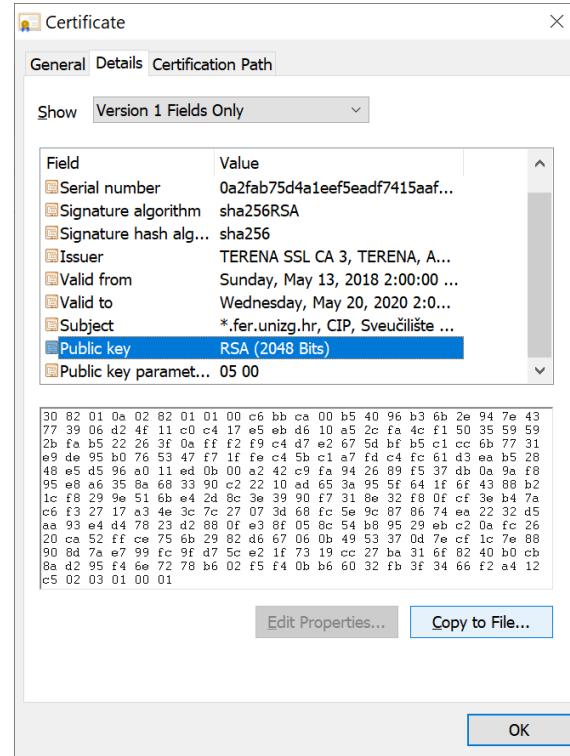
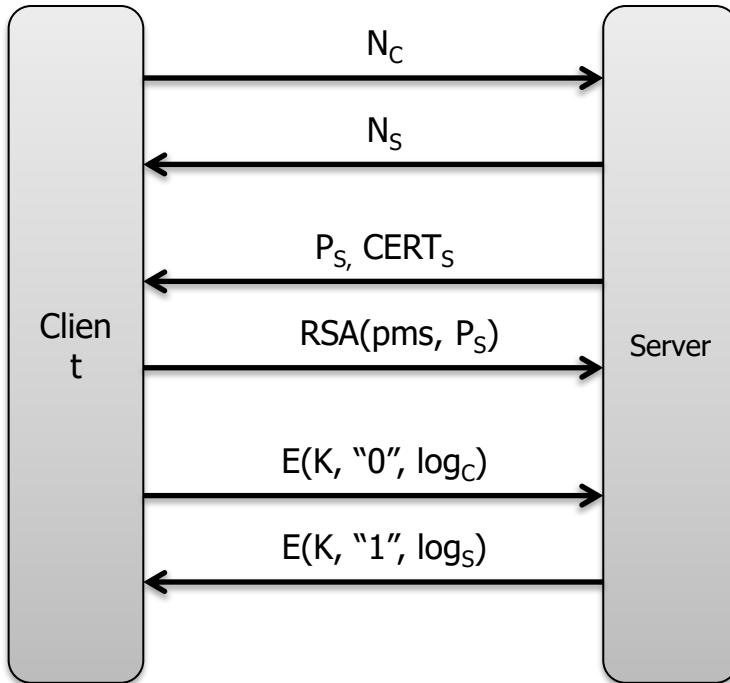
Nemogućnost krivotvorenja potpisa bilo kakve poruke pod napadom odabranom porukom (*existential unforgeability under chosen message attack*): Mti jedan algoritam koji koristi razumne resurse ne može pobijediti u sljedećoj igri s vjerojatnošću nezanemarivo većom od nule.



Digitalni potpis – primjene

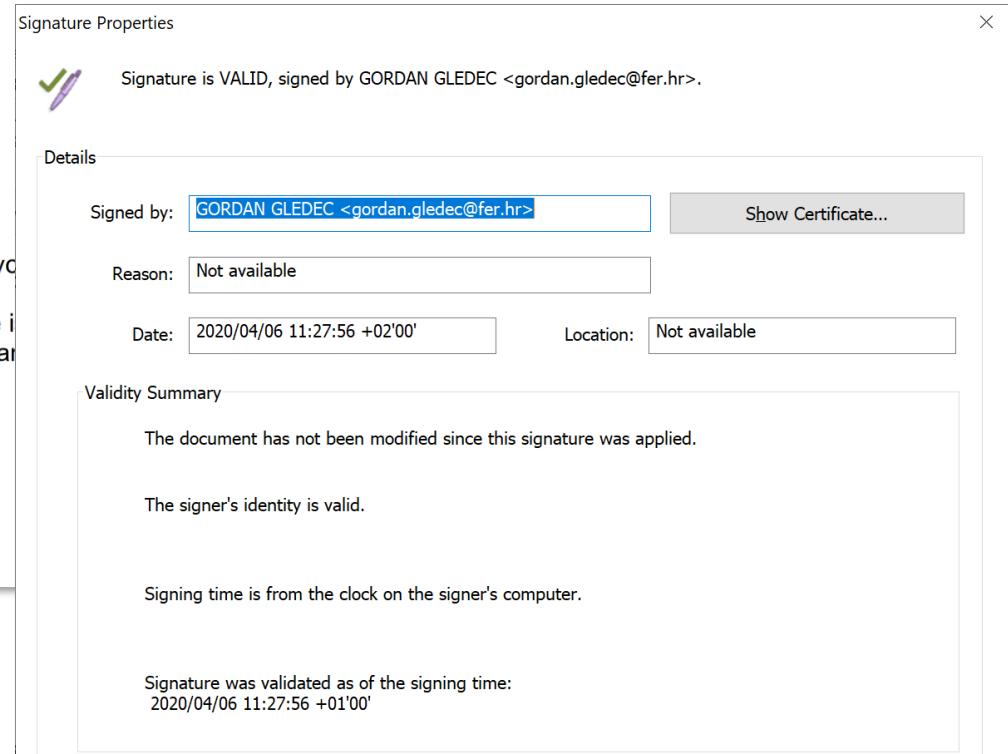
- Potpisivanje digitalnih dokumenata
- Sigurnosni protokoli (TLS, ...)
- Autentifikacija email-a
- Provjera autentičnosti softvera (apk, exe, firmware, ...)
- Kriptovalute
- ...

Primjena – TLS protokol



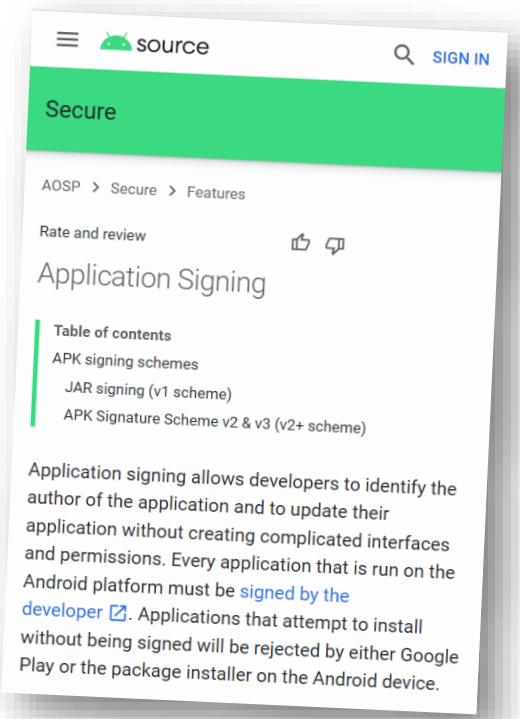
Primjena – e-Dokumenti

- ovisno o razvoju situacije, razmotrit će se uvođenje novih mera.
- II. Ova odluka je privremenog karaktera, donosi se i u okolnosti navedenih u točki I., stupa na snagu dan



Primjena – Android mobilne aplikacije

- Svaka mobilna aplikacija mora biti digitalno potpisana od strane autora!
- Operacijski sustav ne dopušta instaliranje i pokretanje nepotpisane aplikacije.
- Aplikacija može biti potpisana *bilo kojim* ključem.
 - Ključ je dio paketa koji sadrži aplikaciju i potpis.
- Aplikacije potpisane istim ključem mogu dijeliti podatke.



Izvor: source.android.com

Primjena – COVID potvrde

Vaccination example

V1-BE-12345678
ASBCD-56789-44

Name DOE Joe
Date of Birth 1987-06-05
Passport number PF12345678
Certificate issued 2021-06-02

Dose 1/2

Date 2021-02-03
Brand Pfizer Oy

Batch AB123CD
Adm. centre Hospital 1

Country Belgium
Issued by National health service

ME-telecom

Vaccination example

Level:
Standard

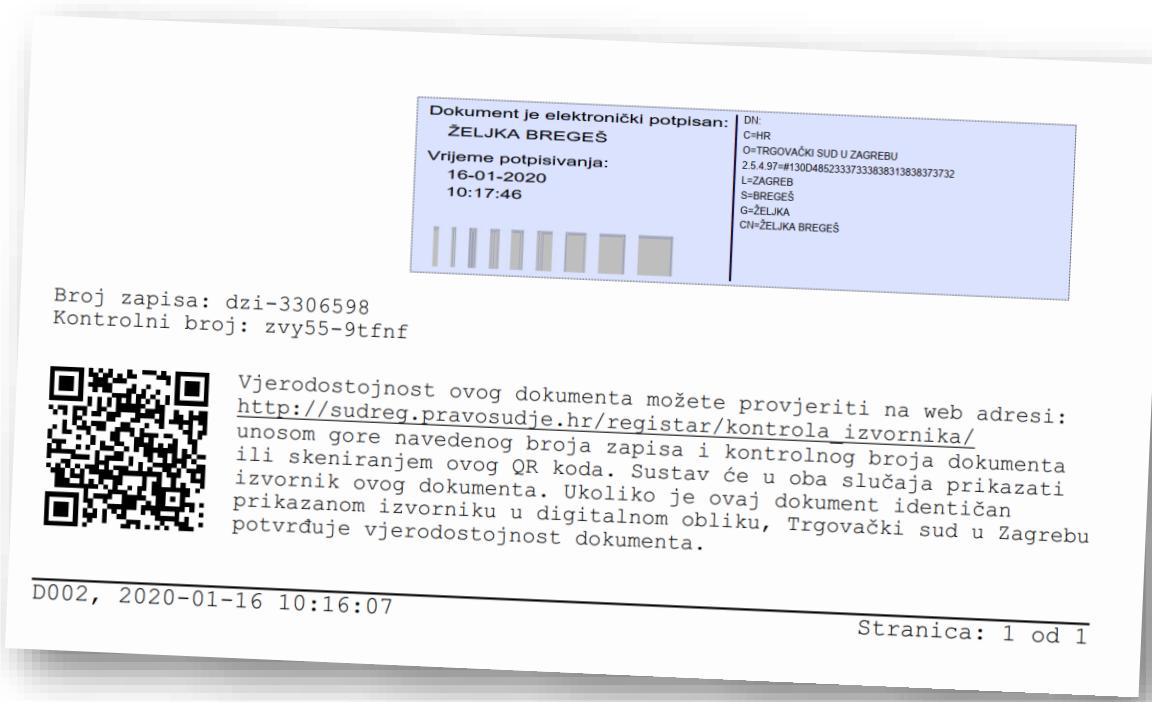
Name Doe Joe
Date of Birth 1987-06-05
Passport number PF12345678
Certificate issued 2021-06-02

Dose 1/2
Type C19-mRNA
Date 2021-02-24
Brand Pfizer Oy

Izvor: Interoperability of health certificates Trust framework

Što sve *nije* digitalni potpis?

- Tekst koji kaže da je dokument digitalno potpisan.
- Broj koji omogućuje dohvaćanje originalnog dokumenta online.
- QR kod.
- Slika analognog potpisa.
- ...



Primjeri sustava digitalnog potpisa

- RSA (1978)
 - teorija brojeva, sigurnost povezana s problemom faktorizacije
- McEliece (1978)
 - teorija kodiranja, sigurnost povezana s problemom dekodiranja općenitog linearног koda
- ElGamal (1985)
 - teorija brojeva ili eliptičke krivulje, sigurnost povezana s problemom diskretnog logaritma
- Schnorr (1991)
 - Jednostavan i efikasan sustav, sigurnost povezana s problemom diskretnog logaritma
- DSA (1992)
 - vrlo slično ElGamalovim potpisima

Digitalni potpisi i asimetrične šifre

Alice signs a message—"Hello Bob!"—by appending to the original message a version encrypted with her private key. Bob receives both the message and signature. He uses Alice's public key to verify the authenticity of the message, i.e. that the message, decrypted using the public key, exactly matches the original message.

- Digitalni potpis nije enkripcija sažetka poruke privatnim ključem!
- Često (ali ne i uvijek) se ista matematička ideja može iskoristiti za izgradnju asimetrične šifre i digitalnog potpisa.
 - RSA šifra i RSA potpis
 - Diffie-Hellman: ElGamal šifra, DSA potpis

Izvor: https://en.wikipedia.org/wiki/Digital_signature (ožujak 2021.)

„Obični RSA“ digitalni potpis

Algoritam S:

- $S(m, (d, N)) = m^d \text{ u } \mathbb{Z}_N$

Algoritam V:

- $V(m, \sigma, (e, N)) = (\sigma^e == m \text{ u } \mathbb{Z}_N) ? 1 : 0$

Zadatak: Obični RSA potpis 1

- Može li napadač na temelju javnog ključa (e, N) pronaći bilo koju poruku i njen ispravan potpis?

- Odaberem proizvoljni $x \in \mathbb{Z}_N$
- Izračunam $y = x^e$ u \mathbb{Z}_N
- x je ispravan potpis za poruku y .

Zadatak: Obični RSA potpis 2

- Pretpostavimo da napadač ima dvije poruke i njihove ispravne potpise, može li ih kombinirati tako da dobije ispravan potpis za neku novu poruku?

- $m_1, \sigma_1 = m_1^d \text{ u } \mathbb{Z}_N$
- $m_2, \sigma_2 = m_2^d \text{ u } \mathbb{Z}_N$
- $\sigma_1 \cdot \sigma_2 = m_1^d \cdot m_2^d = (m_1 \cdot m_2)^d \text{ u } \mathbb{Z}_N$
- $\sigma_1 \cdot \sigma_2$ je ispravan potpis od $m_1 \cdot m_2$

Zadatak: Obični RSA potpis 3

- Napadač ima mogućnost dobiti potpis za točno jednu poruku koja izgleda slučajno. Želi iskoristiti tu mogućnost kako bi dobio potpis konkretnе poruke m po njegovom izboru.

RSA digitalni potpis

H – kriptografska funkcija sažetka

Pad – funkcija nadopunjavanja

Algoritam S:

- $S(m, (d, N)) = Pad(H(m))^d \text{ u } \mathbb{Z}_N$

Algoritam V:

- $V(m, \sigma, (e, N)) = (Unpad(\sigma^e \text{ u } \mathbb{Z}_N) == H(m)) ? 1 : 0$

Zadatak: Obični RSA potpis 3

- Zašto isti napad više ne radi?

RSA digitalni potpis – Padding

- Hash poruke se uvijek nadopunjuje na zadalu veličinu!
- Postupak nadopunjavanja (*padding*) igra kritičnu ulogu i pažljivo je osmišljen.
 - PKCS#1 v1.5 (mnoštvo sigurnosnih problema)
 - PSS

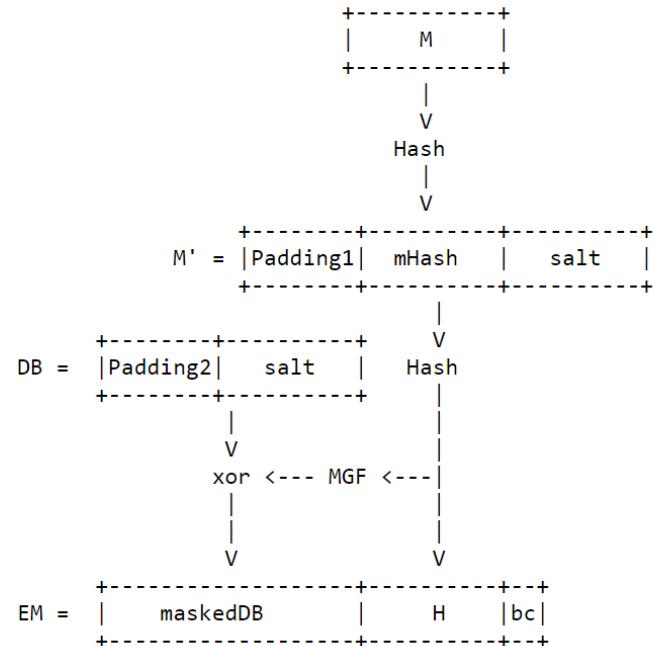
RSA – PKCS#1 v1.5 Padding

4. Generate an octet string PS consisting of emLen - tLen - 3 octets with hexadecimal value 0xff. The length of PS will be at least 8 octets.
5. Concatenate PS, the DER encoding T, and other padding to form the encoded message EM as

```
EM = 0x00 || 0x01 || PS || 0x00 || T.
```

RSA – PSS Padding

- *Probabilistic signature scheme*
- Dokazano sigurna pod jakim pretpostavkama sigurnosti običnog RSA i hash funkcija.
- *Mihir Bellare , Phillip Rogaway, PSS: Provably Secure Encoding Method for Digital Signatures (1998)*



Izvor: <https://datatracker.ietf.org/doc/html/rfc8017>



Kriptografija i kriptoanaliza

doc. dr. sc. Ante Đerek i prof. dr. sc. Marin Golub

prosinac 2023.

Diffie-Hellmanova razmjena ključeva

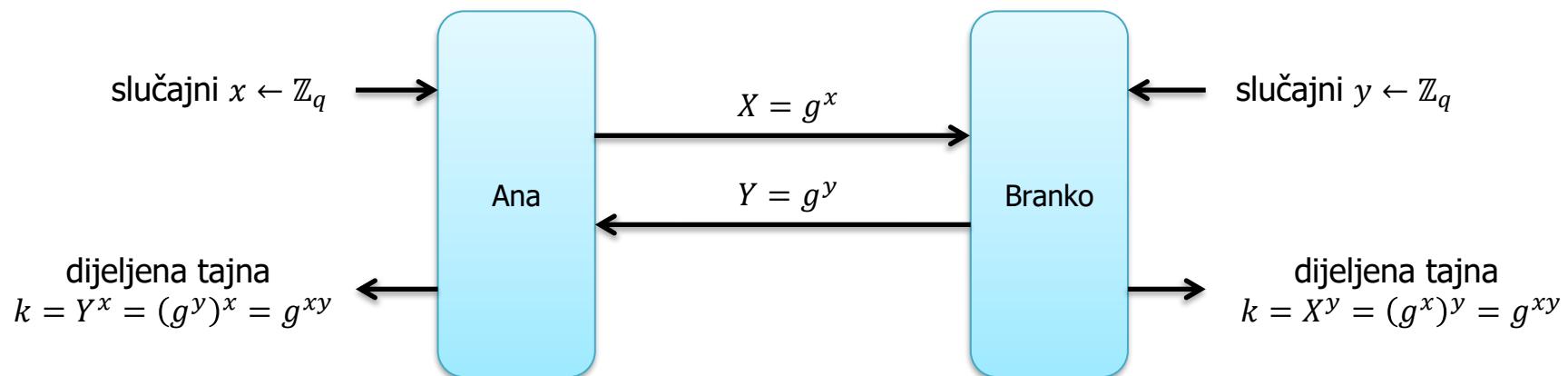
Globalni, javno poznati parametri (*domain parameters*):

- p – jako veliki prosti broj (npr. 2048 bitova)
- q – veliki prost broj koji dijeli $p - 1$ (npr. 256 bitova)
- g – element od \mathbb{Z}_p^* reda q

Sve operacije se rade u \mathbb{Z}_p (odnosno modulo p).

Nazivlje:

- g – generator
- x – privatni ključ
- g^x – javni ključ



Diffie-Hellmanova razmjena ključeva – sigurnost

- Neformalno, Diffie-Hellmanova razmjena ključeva je *sigurna* ako je teško na temelju $X = g^x$ i $Y = g^y$ odrediti bilo što o $k = g^{xy}$.
- Pažnja: razmatramo sigurnost samo protiv *pasivnog* napadača.

Ponavljanje: Grupe

Grupe. Grupa je matematička struktura koja se sastoji od nepraznog skupa G i binarne operacije $\circ : G \times G \rightarrow G$. To znači da za svaka dva elementa $x, y \in G$ definiran njihov umnožak $x \circ y \in G$. Pri tome zahtjevamo da vrijede sljedeća svojstva

1) **Asocijativnost.** Za sve $x, y, z \in G$ vrijedi

$$(x \circ y) \circ z = x \circ (y \circ z).$$

2) **Postojanje neutralnog elementa.** Postoji element $e \in G$ takav da za svaki $x \in G$ vrijedi

$$e \circ x = x \circ e = x.$$

3) **Postojanje inverznog elementa.** Za svaki $x \in G$ postoji element $x^{-1} \in G$ takav da je

$$x \circ x^{-1} = x^{-1} \circ x = e.$$

Ako je k tome za svaka dva elementa $x, y \in G$ ispunjeno $x \circ y = y \circ x$, onda za G kažemo da je **komutativna** ili **Abelova** grupa.

Primjeri grupa

- $(\mathbb{Z}, +)$ je grupa
- $(\mathbb{Q} \setminus \{0\}, *)$ je grupa
- $(\mathbb{Z}_N, +)$ je grupa
- $(\mathbb{Z}_N^*, *)$ je grupa
- ...
- $(\mathbb{N}, +)$ nije grupa
- $(\mathbb{Q}, *)$ nije grupa
- $(\mathbb{Z}_N, *)$ nije grupa ako je N složen.
- ...

Notacija

- Aditivna notacija:

$$0, a + b, -a, k a = a + a + \cdots + a$$

- Multiplikativna notacija:

$$1, a * b, a^{-1}, a^k = a * a * \cdots * a$$

Konačne Abelove groupe

- Grupa je *konačna* ako ima konačan broj elemenata.
- Grupa je komutativna ili Abelova ako za svaki $g, h \in G$ vrijedi $g * h = h * g$.
- U ovom predmetu kada kažemo grupa mislimo na konačnu Abelovu grupu.

Red elementa

- Ako je G grupa i $g \in G$.
- *Red elementa* g je veličina skupa $\{g^k : k \in \mathbb{N}\}$
 - Oznaka: $\text{ord}(g)$
- Alternativno: red elementa g je najmanji prirodni broj k za koji vrijedi $g^k = 1$.

Zadatak

- Zašto alternativna definicija reda ima smisla? Je li u konačnoj grupi moguće da je $g^k \neq 1$ za sve prirodne brojeve k ?

Cikličke grupe

- Neka je G grupa koja se sastoji od n elemenata. Ako postoji element $g \in G$ reda n onda kažemo da je G *ciklička grupa*.
 - $\text{ord}(g) = |G|$
 - $G = \{1, g, g^2, g^3, \dots\}$
- Takav element g nazivamo *generator* ili *primitivni element* grupe G .

Primjeri cikličkih grupa

- $(\mathbb{Z}_N, +)$ je ciklička grupa
 - Npr. 1 je generator
- Ako je G bilo koja konačna grupa i $g \in G$ onda je $H = \{g, g^2, g^3, \dots\}$ ciklička grupa. H je podgrupa od G .
- Teorem: $(\mathbb{Z}_p^*, *)$ je ciklička grupa ako je p prost.

Svojstva

- $g^{-a} := (g^{-1})^a$

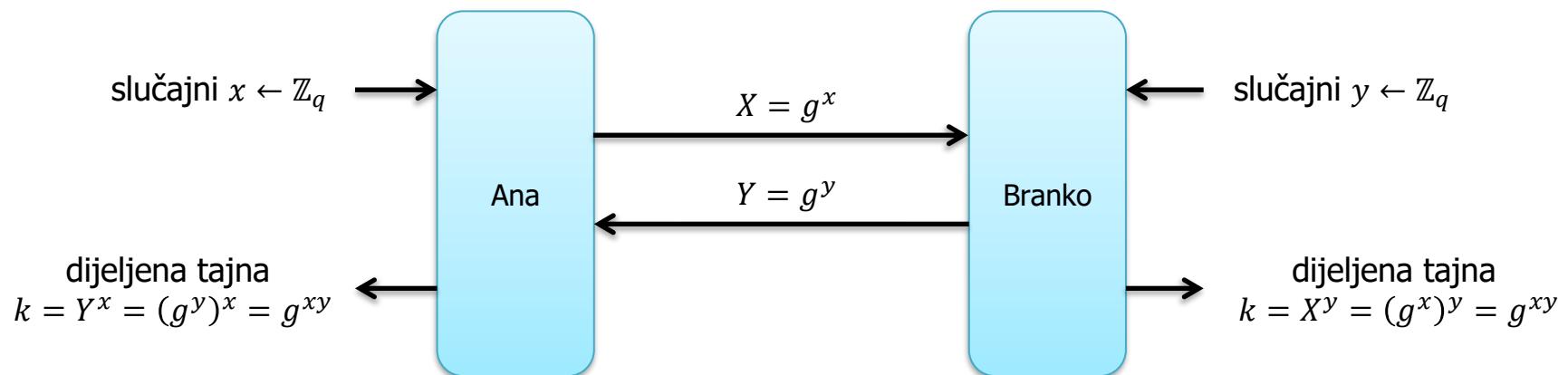
Diffie-Hellmanova razmjena ključeva u grupi G

Globalni, javno poznati parametri (*domain parameters*):

- G – konačna ciklička grupa reda q
- g – generator od G

Nazivlje:

- g – generator
- x – privatni ključ
- g^x – javni ključ



Diffie-Hellmanova razmjena ključeva – sigurnost

- Diffie-Hellmanova razmjena ključeva je sigurna ako napadač na temelju G, g, g^x, g^y ne može ...
 - ... odrediti g^{xy} . (*computational Diffie-Hellman assumption*)
 - ... odrediti nikakve informacije o g^{xy} . (*decisional Diffie-Hellman assumption*)

Diskretni logaritam

- Diskretni logaritam u grupi G :
 - $\text{Dlog}_g(h)$ je broj $k \in \mathbb{Z}$ takav da vrijedi $g^k = h$.
- Diskretni logaritam je jedinstven modulo red elementa g .

Zadatak

- Koliko je $D\log_3(11) \cup \mathbb{Z}_{17}^*$?
- Koliko je $D\log_2(5) \cup \mathbb{Z}_{17}^*$?

Problem diskretnog logaritma

- Neformalno, problem diskretnog logaritma je *težak* u za grupu G i generator g ako ne postoji efikasan algoritam koji računa diskretne logaritme.
- Odnos između diskretnog logaritma i Diffie-Hellmana
 - Trivijalno: Ako je diskretni logaritam lagan onda Diffie-Hellmanova razmjena ključeva nije sigurna!
 - Iskustvo: Tamo gdje je diskretni logaritam težak je i Diffie-Hellmanova razmjena ključeva sigurna!

Kada je DH siguran?

- *Prime-order subgroup*
 - G je $(\mathbb{Z}_p^*, *)$ gdje je p prost
 - p je veličine npr. 2048 bitova
 - g je reda q gdje je q prost
 - q je veličine npr. 256 bitova
 - Nivo sigurnosti je oko pola veličine od q (128 bitova)
- *Safe prime* (TLS)
 - G je $(\mathbb{Z}_p^*, *)$ gdje je p prost, i $(p - 1)/2$ je također prost
 - p je veličine > 2048 bitova
 - g je reda $(p - 1)/2$
 - Nivo sigurnosti je oko 100 bitova
- ...

Primjer – Diffie-Hellman parametri za TLS

The hexadecimal representation of p is:

```
FFFFFFFF FFFFFFFF ADF85458 A2BB4A9A AFDC5620 273D3CF1
D8B9C583 CE2D3695 A9E13641 146433FB CC939DCE 249B3EF9
7D2FE363 630C75D8 F681B202 AEC4617A D3DF1ED5 D5FD6561
2433F51F 5F066ED0 85636555 3DED1AF3 B557135E 7F57C935
984F0C70 E0E68B77 E2A689DA F3EFE872 1DF158A1 36ADE735
30ACCA4F 483A797A BC0AB182 B324FB61 D108A94B B2C8E3FB
B96ADAB7 60D7F468 1D4F42A3 DE394DF4 AE56EDE7 6372BB19
0B07A7C8 EE0A6D70 9E02FCE1 CDF7E2EC C03404CD 28342F61
9172FE9C E98583FF 8E4F1232 EEF28183 C3FE3B1B 4C6FAD73
3BB5FCBC 2EC22005 C58EF183 7D1683B2 C6F34A26 C1B2EFFA
886B4238 61285C97 FFFFFFFF FFFFFFFF
```

The generator is: g = 2

The group size is: q = (p-1)/2

The hexadecimal representation of q is:

```
7FFFFFFF FFFFFFFF D6FC2A2C 515DA54D 57EE2B10 139E9E78
EC5CE2C1 E7169B4A D4F09B20 8A3219FD E649CEE7 124D9F7C
BE97F1B1 B1863AEC 7B40D901 576230BD 69EF8F6A EAEB2B0
9219FA8F AF833768 42B1B2AA 9EF68D79 DAAB89AF 3FABE49A
CC278638 707345BB F15344ED 79F7F439 0EF8AC50 9B56F39A
98566527 A41D3CBD 5E0558C1 59927DB0 E88454A5 D96471FD
DCB56D5B B06BFA34 0EA7A151 EF1CA6FA 572B76F3 B1B95D8C
8583D3E4 770536B8 4F017E70 E6FBF176 601A0266 941A17B0
C8B97F4E 74C2C1FF C7278919 777940C1 E1FF1D8D A637D6B9
9DDAE5E 17611002 E2C778C1 BE8B41D9 6379A513 60D977FD
4435A11C 30942E4B FFFFFFFF FFFFFFFF
```

Izvor: <https://datatracker.ietf.org/doc/html/rfc7919>

Diffie-Hellman parametri

Diffie–Hellman Set-up

1. Choose a large prime p .
2. Choose an integer $\alpha \in \{2, 3, \dots, p - 2\}$.
3. Publish p and α .

large enough so that the index-calculus method cannot compute the DLP. By consulting Table 6.1 we see that a security level of 80 bit is achieved by primes of lengths 1024 bit, and for 128 bit security we need about 3072 bit. An additional requirement is that in order to prevent the Pohlig–Hellman attack, the order $p - 1$ of the cyclic group must not factor in only small prime factors. Each of the subgroups formed by the factors of $p - 1$ can be attacked using the baby-step giant-step method or Pollards’s rho method, but not by the index-calculus method. Hence, the smallest prime factor of $p - 1$ must be at least 160 bit long for an 80-bit security level, and at least 256 bit long for a security level of 128 bit.

Diffie-Hellman – sigurnost

- Računanje diskretnog logartima je najbolji poznati općeniti napad
 - Baby-step giant-step
 - Pollardov ρ algoritam
 - Index calculus
 - General Number Field Sieve (jednako kao i za faktorizaciju)
 - U 2021. najveći izračunati Dlog je bio modulo 795-bitni prost broj.

Emmanuel Thomé [Emmanuel Thomé at inria.fr](#)
Mon Dec 2 13:52:33 CET 2019

- Next message: [\[Cado-nfs-discuss\] malloc Hash_init error](#)
- Messages sorted by: [\[date\]](#) [\[thread\]](#) [\[subject\]](#) [\[author\]](#)

Dear cado-nfs-discuss subscribers,

We are pleased to announce the factorization of RSA-240, from RSA's challenge list, and the computation of a discrete logarithm of the same size (795 bits).

RSA-240 =
12462036678171878406583504460810659043482037465167880575481878883289660
= 509435952285839914555051023580843714132648382024111473186660296521821206
* 24462420883831815056781313902400289665380209257893140145204122133655847;

Let $p = \text{RSA-240} + 49204$ be the first safe prime above RSA-240. We chose p as a target the encoding of the sentence "The magic words are still Squeamish Ossifrage" (in reference to the factorization of RSA-129 [1]):

```
target_str="The magic words are still Squeamish Ossifrage"
target_hex=`echo -n $target_str | xxd -p -c 256`
target_hex=${target_hex^^}
target=`echo "ibase=16; $target_hex" | BC_LINE_LENGTH=0 bc`
```

target = 774356626343973985966622216006087686926705588649958206166317147722421706

we have with generator $g = 5$:

```
log(target) =
92603135928144195363094953317328555029610991914376116167294204758987445
```

which can be checked with $5^{926\dots716} \equiv \text{target} \pmod p$.

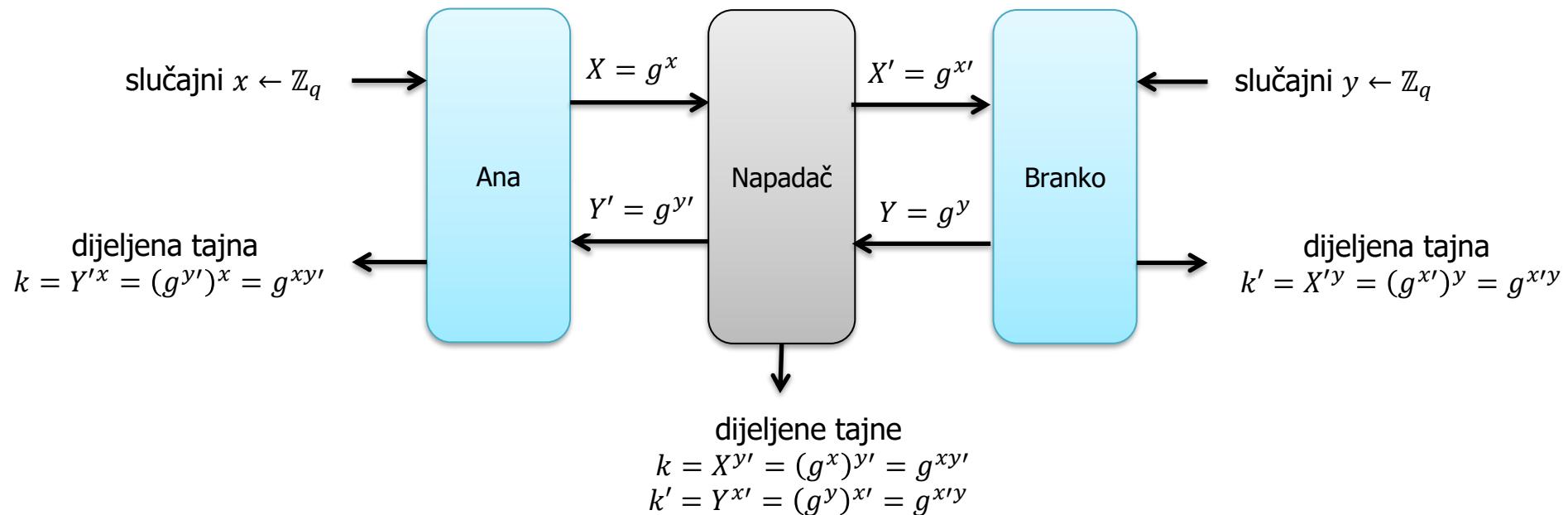
The previous records were RSA-768 (768 bits) in December 2009 [2], and a 768-bit prime discrete logarithm in June 2016 [3].

Izvor: Arhiva mailing liste cado-nfs-discuss

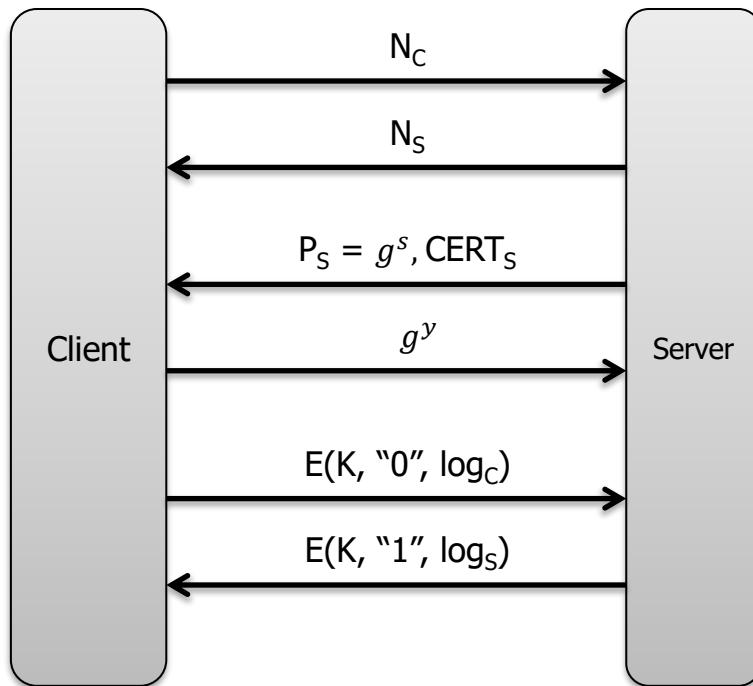
Aktivni napad

- Pažnja: Diffie-Hellmanova razmjena ključeva je sigurna samo protiv *pasivnog* napadača!
- U protokolima se koristi zajedno s digitalnim potpisima, ili nekim drugim mehanizmom za osiguravanje autentičnosti.

Napad čovjeka u sredini

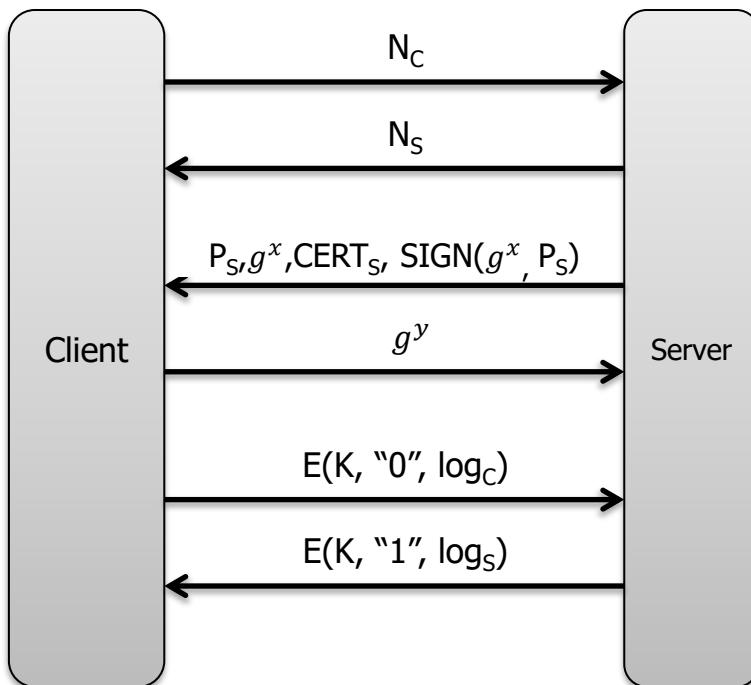


Primjena – TLS protokol – statični Diffie-Hellman



- *Fixed Diffie-Hellman*
- Javni ključ poslužitelja je zapravo Diffie-Hellman vrijednost g^s .
- Ključevi za sjednicu se generiraju na temelju Diffie-Hellman tajne i razmijenjenih *nonce* vrijednosti
- Rijetko se koristi i ne preporuča se

Primjena – TLS protokol – privremeni Diffie-Hellman



- *Ephemeral Diffie-Hellman*
- Prilikom uspostave sjednice poslužitelj i klijent razmjenjuju nove Diffie-Hellman vrijednosti.
- Ključevi za sjednicu se generiraju Diffie-Hellman tajne i razmijenjenih *nonce* vrijednosti
- Unaprijed sigurnost (*perfect forward secrecy*)
 - Ako napadač u budućnosti kompromitira dugoročne ključeve poslužitelja, ne može dešifrirati podatke iz starih sjednica.

Primjene

- Mnoštvo kriptografskih primitiva je bazirano na Diffie-Hellman ideji i/ili na diskretnim logaritmima
 - ElGamal asimetrična šifra
 - ElGamal digitalni potpis
 - DSA potpis
 - Schnorrovi potpisi
 - ...

ElGamalov SKJK

- Taher Elgamal (1985)
- Baziran na Diffie-Hellmanovoj razmjeni ključeva.
 - Privatni ključ je Diffie-Hellman privatni ključ
 - Javni ključ je Diffie-Hellman javni ključ
- Za svaku novu poruku, pošiljatelj generira privremene Diffie-Hellman vrijednosti i poruku kriptira tajnom dobivenom iz svojeg privremenog privatnog ključa i primateljevog dugotrajnog javnog ključa.

Obični ElGamal – generiranje ključeva

Domenski parametri:

- G ciklička grupa reda q
- g generator grupe G

Algoritam G:

1. Odaberem slučajni $a \in \mathbb{Z}_q$
2. Izračunam $A = g^a$
3. Javni ključ je $A \in G$
4. Privatni ključ je $a \in \mathbb{Z}_q$

Obični ElGamal – enkripcija i dekripcija

Algoritam E:

Ulaz: poruka $m \in G$ i javni ključ $A \in G$

1. Odaberem slučajni $y \in \mathbb{Z}_q$
2. Izračunam $Y = g^y$
3. Izračunam $k = A^y$
4. Izračunam $c = mk$

Rezultat je par (Y, c)

Algoritam D:

Ulaz: (Y, c) i privatni ključ $a \in \mathbb{Z}_q$

1. Izračunam $k = Y^a$
 2. Izračunam $m = ck^{-1}$
- Rezultat je m

$$D(E(m, pk), sk) = D(E(m, g^a), a) = D((g^y, mg^{ay}), a) = mg^{ay}(g^{ya})^{-1} = m$$

Obični ElGamal – operacije

- Moramo znati efikasno
 - Izvršiti operaciju grupe
 - „Potenciranje“ u grupi – uzastopno kvadriranje
 - Traženje inverza u grupi – svodi se na potenciranje obzirom da je poznat red grupe

Zadatak – ElGamal

- Možemo li isti privremeni par ključeva (y, g^y) koristiti dva puta?

Obični ElGamal – sigurnost

- U slučaju napada odabranim jasnim tekstrom (napadač ima samo javni ključ) ElGamal je siguran ako je Diffie-Hellmanova razmjena ključeva sigurna.
- U slučaju napada odabranim skrivenim tekstrom: *otvoren problem* – nemamo napade niti dokaz.

ElGamal u praksi

- Iako obični ElGamal ima puno bolja sigurnosna svojstva nego obični RSA, u praksi također gotovo nikad ne kriptiramo poruke već ga kombiniramo sa simetričnom šifrom.

Diffie-Hellman na eliptičkim krivuljama

- Pitanje za matematičare: u kojim je još grupama operacija efikasna, a problem diskretnog logaritma se čini težak?
 - Odgovor: Eliptičke krivulje zajedno s operacijom „zbrajanja” točaka.

Asimetrični kriptosustavi zasnovani na eliptičkim krivuljama (ECC)

- Sigurnost asimetričnih algoritama oslanja se na teško rješive probleme diskretnog logaritma u grupi točaka na eliptičkoj krivulji.
- Ovakve sustave su predložili 1985. godine Victor Miller i Neal Koblitz (nezavisno).
- Svaki sustav zasnovan na Diffie-Hellmanovoj razmijeni ključeva može se ostvariti nad eliptičkim krivuljama.
 - ECDH (Elliptic Curve Diffie-Hellman)
 - EC ElGamalov kriptosustav
 - ECDSA (Elliptic Curve Digital Signature Algorithm)
 - ...
- Postoje eliptičkih krivulja primjene u kriptografiji koje nisu samo generalizacija algoritama na poljima – *pairing based cryptography*.

Pojednostavljena definicija eliptičke krivulje

- Eliptička krivulja E nad poljem K je skup svih točaka $(x, y) \in K \times K$ koje zadovoljavaju jednadžbu:

$$y^2 = x^3 + a x + b.$$

- Detalji:
 - U kriptografiji će K uglavnom biti \mathbb{Z}_p gdje je p prost broj ili Galoisovo polje $GF(2^m)$.
 - U E dodamo još jedan element kojeg označavamo s 0 i nazivamo se *točka u beskonačnosti*.
 - a i b su parametri za koje vrijedi $4a^3 + 27b^2 \neq 0$ u K .

Opći oblik eliptičke krivulje (Weierstrassova forma)

$$y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6$$

$a_1, a_2, a_3, a_4, a_6 \in K$ (K je algebarski zatvoreno polje)

- eliptička krivulja se može definirati nad proizvoljnim poljem K :
 - polje racionalnih brojeva Q
 - polje realnih brojeva R
 - polje kompleksnih brojeva C
 - konačno polje Z_p^* .
- *Eliptička krivulja ili nesingularna kubna krivulja* (engl. *nonsingular cubic curve*) je skup svih rješenja glatke Weierstrasseove jednadžbe
- Rješenje je točka na eliptičkoj krivulji.

Primjer – eliptička krivulja nad \mathbb{R}

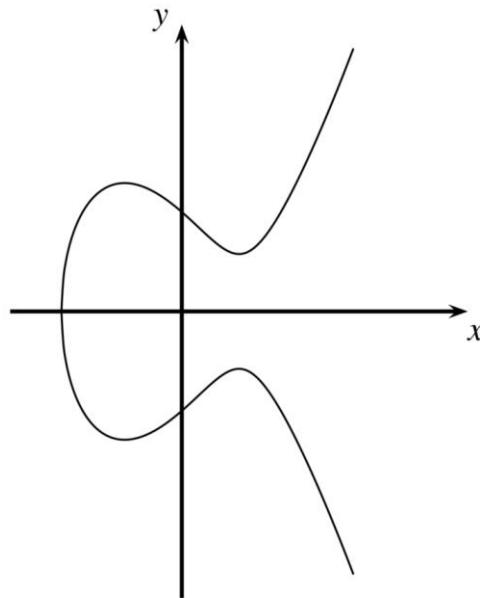
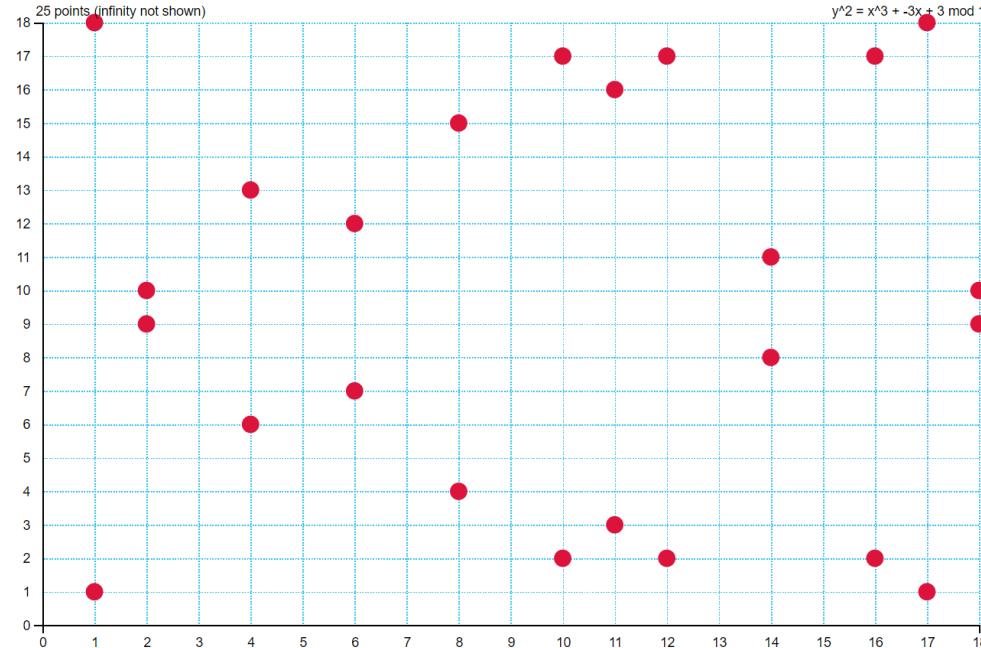


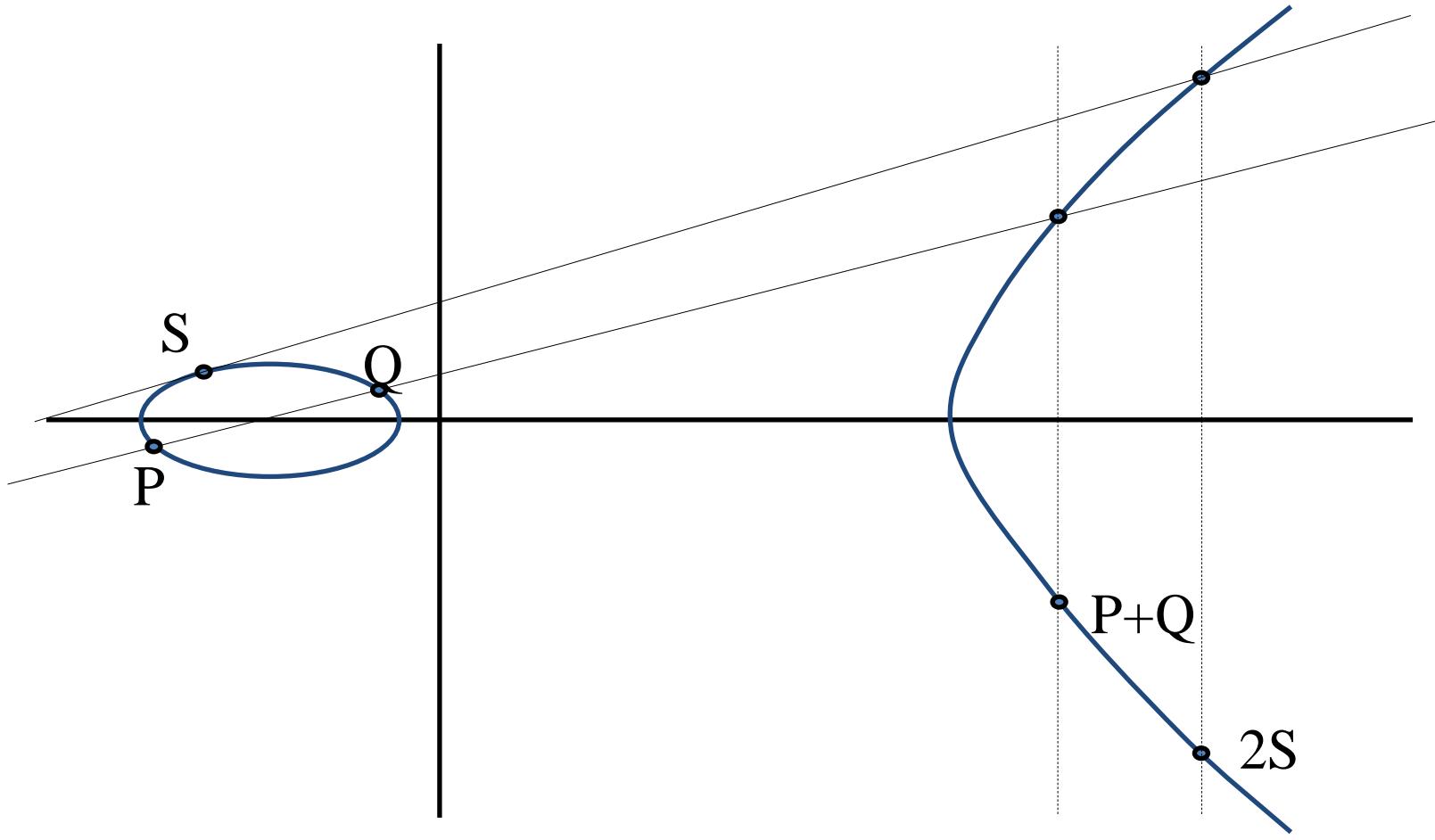
Fig. 9.3 $y^2 = x^3 - 3x + 3$ over \mathbb{R}

Primjer – ista krivulja nad \mathbb{Z}_{19}

Draw the elliptic curve $y^2 = x^3 + ax + b \pmod{r}$, where $a: -3$ $b: 3$ $r: 19$ **DRAW!**



Operacija „zbrajanja“



Operacija „zbrajanja”

$$x_3 = s^2 - x_1 - x_2 \bmod p$$

$$y_3 = s(x_1 - x_3) - y_1 \bmod p$$

$$s = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} \bmod p & ; \text{if } P \neq Q \text{ (point addition)} \\ \frac{3x_1^2 + a}{2y_1} \bmod p & ; \text{if } P = Q \text{ (point doubling)} \end{cases}$$

- Teorem: Eliptička krivulja s ovako definiranom operacijom zbrajanja čini grupu.
- Teorem: Broj točaka na eliptičkoj krivulji nad \mathbb{Z}_p je između $p + 1 - 2\sqrt{p}$ i $p + 1 + 2\sqrt{p}$.

Diskretni logaritam

- Diskretni logaritam u grupi G :
 - $\text{Dlog}_g(h)$ je broj $k \in \mathbb{Z}$ takav da vrijedi $g^k = h$.
- Diskretni logaritam u grupi G točaka na eliptičkoj krivulji
 - $\text{Dlog}_g(h)$ je broj $k \in \mathbb{Z}$ takav da vrijedi $kg = h$.
- Pažnja: ovo je ista stvar, samo kod eliptičkih krivulja koristimo aditivnu notaciju!

Eliptičke krivulje – sigurnost diskretnog logaritma

- Index calculus i GNFS nisu primjenjivi nad eliptičkim krivuljama.
- Za pažljivo odabранe krivulje najbolji poznati algoritmi za diskretni logaritam trebaju oko \sqrt{n} koraka gdje je n veličina krivulje.
 - Baby-step giant-step
 - Pollardov ρ algoritam

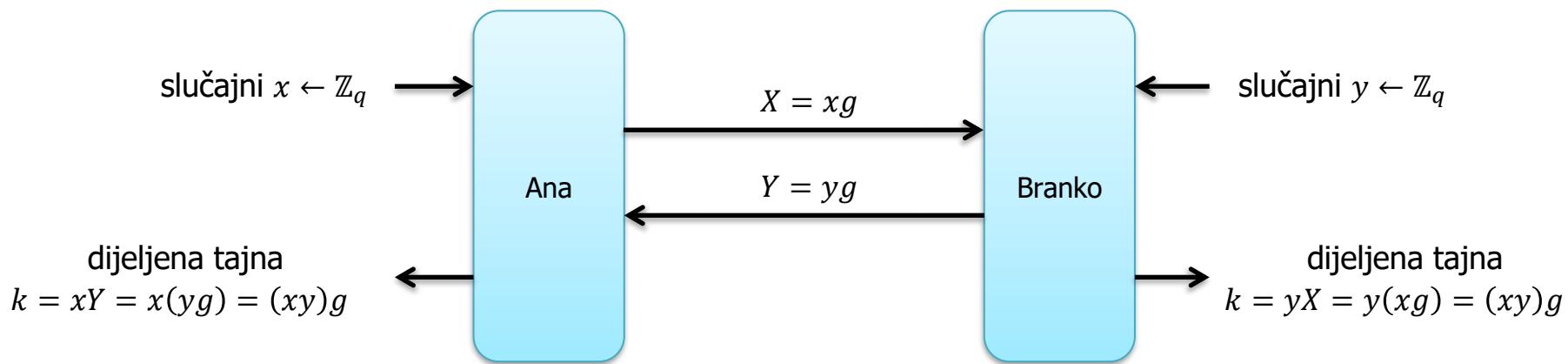
Diffie-Hellmanova razmjena nad eliptičkim krivuljama (ECDH)

Globalni, javno poznati parametri (*domain parameters*):

- G – eliptička krivulja reda q
- g – generator od G

Nazivlje:

- g – generator
- x – privatni ključ
- g^x – javni ključ



Primjer – krivulja secp256k1

The elliptic curve domain parameters over \mathbb{F}_p associated with a Koblitz curve **secp256k1** are specified by the sextuple $T = (p, a, b, G, n, h)$ where the finite field \mathbb{F}_p is defined by:

$$\begin{aligned} p &= \text{FFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFE} \\ &\quad \text{FFFFFC2F} \\ &= 2^{256} - 2^{32} - 2^9 - 2^8 - 2^7 - 2^6 - 2^4 - 1 \end{aligned}$$

The curve E : $y^2 = x^3 + ax + b$ over \mathbb{F}_p is defined by:

$$\begin{aligned} a &= 00000000 00000000 00000000 00000000 00000000 00000000 00000000 \\ &\quad 00000000 \\ b &= 00000000 00000000 00000000 00000000 00000000 00000000 00000000 \\ &\quad 00000007 \end{aligned}$$

The base point G in compressed form is:

$$\begin{aligned} G &= 02\ 79BE667E\ F9DCBBAC\ 55A06295\ CE870B07\ 029BFCDB\ 2DCE28D9 \\ &\quad 59F2815B\ 16F81798 \end{aligned}$$

and in uncompressed form is:

$$\begin{aligned} G &= 04\ 79BE667E\ F9DCBBAC\ 55A06295\ CE870B07\ 029BFCDB\ 2DCE28D9 \\ &\quad 59F2815B\ 16F81798\ 483ADA77\ 26A3C465\ 5DA4FBFC\ 0E1108A8\ FD17B448 \\ &\quad A6855419\ 9C47D08F\ FB10D4B8 \end{aligned}$$

Finally the order n of G and the cofactor are:

$$\begin{aligned} n &= \text{FFFFFFF FFFFFFFF FFFFFFFF FFFFFFFE BAAEDCE6 AF48A03B BFD25E8C} \\ &\quad \text{D0364141} \\ h &= 01 \end{aligned}$$

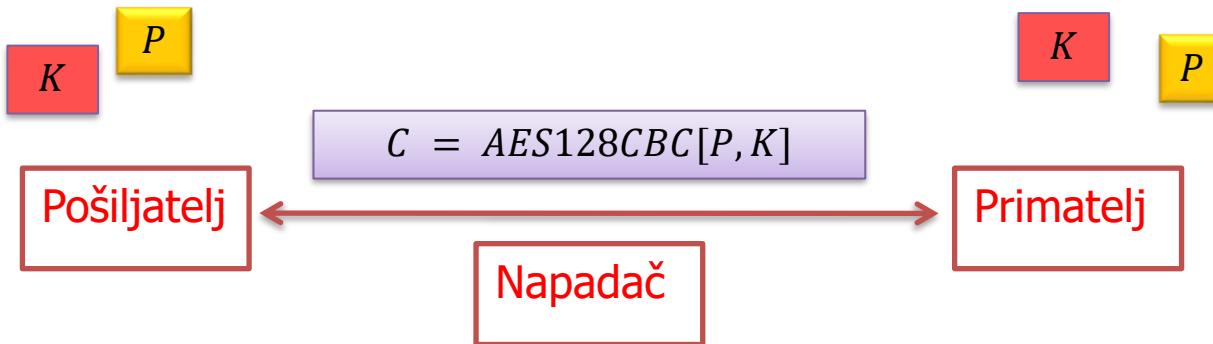
Izvor: Standards for Efficient Cryptography SEC 2: Recommended Elliptic Curve Domain Parameters Certicom Research

6. **Asimetrični kriptosustavi**

Digitalni potpis zasnovan na RSA

Digitalni potpis zasnovan na
diskretnom logaritmu

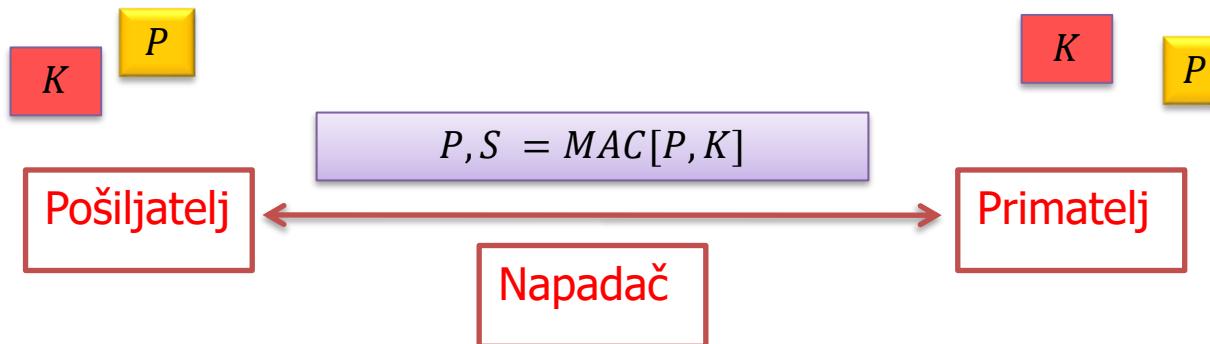
Enkripcija ne rješava sve probleme!



- Ako ste primili i uspješno dekriptirali poruku možete li biti sigurni da znate:
 - Tko je generirao poruku?
 - Je li dekriptirana poruka identična originalnoj?

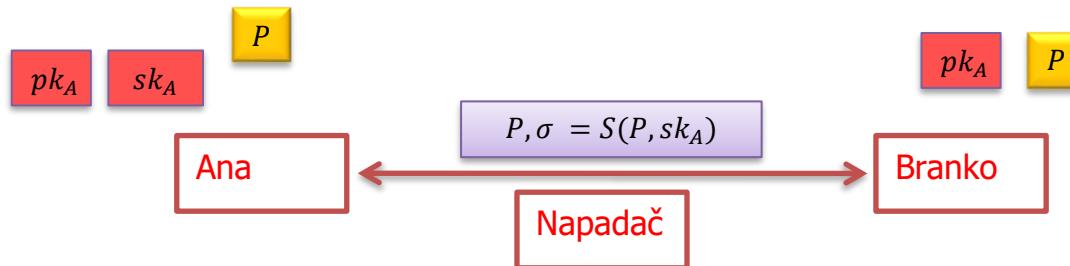
MAC / Autentificirana enkripcija

- Kod za integritet poruke (*Message Authentication Code*)
- Autentificirana enkripcija

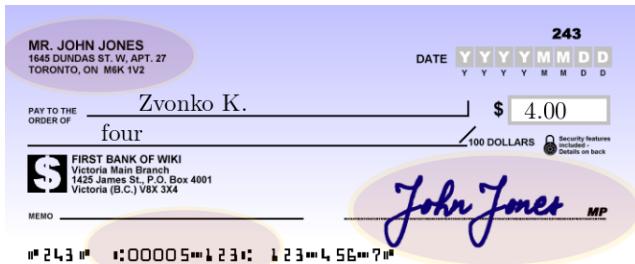


Javni i tajni ključevi

- Stara ideja: Svatko ima dva ključa
 - Javni ključ pk_A : Javno poznat (npr. telefonski imenik)
 - Privatni ključ sk_A : Poznat samo Ani
 - Ana *generira* potpis svojim privatnim ključem sk_A
 - Branko *provjerava* potpis Aninim javnim ključem pk_A



Digitalni vs analogni potpis – autentičnost

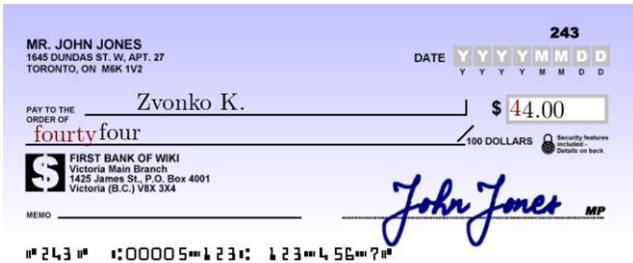


Izvor: wikipedia.org

- Svatko može provjeriti ispravnost digitalnog potpisa ako ima na raspolaganju javni ključ tobožnjeg potpisnika.
- Provjera ispravnosti je garancija da je potpis stvarno generiran odgovarajućim privatnim ključem.
- Veza između ključeva i identiteta?

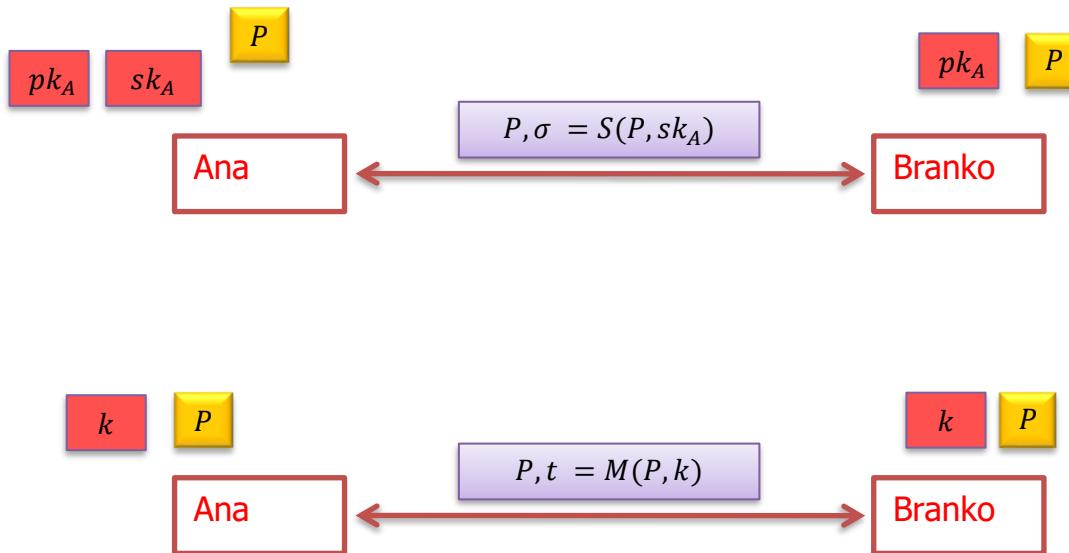
Digitalni vs analogni potpis – integritet

- Digitalni potpis je vezan uz dokument.
- Ispravan potpis garantira integritet dokumenta.



Izvor: wikipedia.org

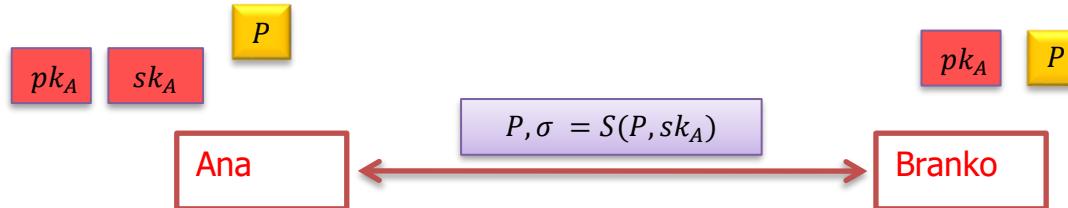
Digitalni potpis vs MAC – neporecivost (non-repudiation)



- Moguće je trećoj strani dokazati da je pošiljatelj potpisao poruku!
- Veza između ključeva i identiteta?
- „Netko me je hakirao“ obrana?

Sustav digitalnog potpisa

- Trojka efikasnih algoritama G , S i V
 - G – algoritam koji generira par ključeva pk , sk
 - $S(m, sk)$ – algoritam potpisivanja
 - $V(m, \sigma, pk)$ – algoritam verifikacije
- Za svaki par ključeva (pk, sk) generiranih algoritmom G i za svaki jasni tekst p vrijedi $V(p, S(p, sk), pk) = 1$

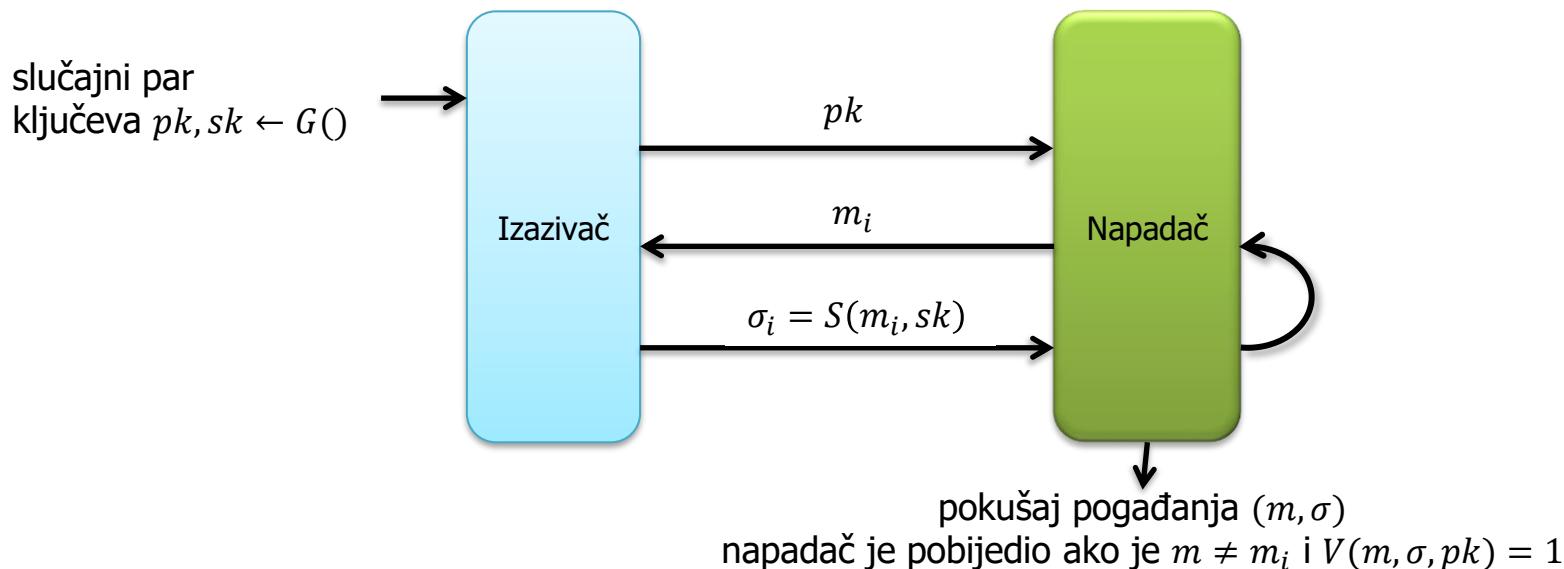


Sustav digitalnog potpisa – sigurnost

- SDP je siguran ako je teško odrediti bilo koju poruku p i bilo koji potpis (niz bitova) σ takav da
 - $V(p, \sigma, pk) = 1$
 - p nikad nije potpisan s privatnim ključem sk
- ... čak i ako napadač ima na raspolaganju:
 - Javni ključ pk
 - Mogućnost da dobije potpis $S(p, sk)$ za proizvoljnu poruku p (chosen message attack)

Primjer definicije sigurnosti digitalnog potpisa

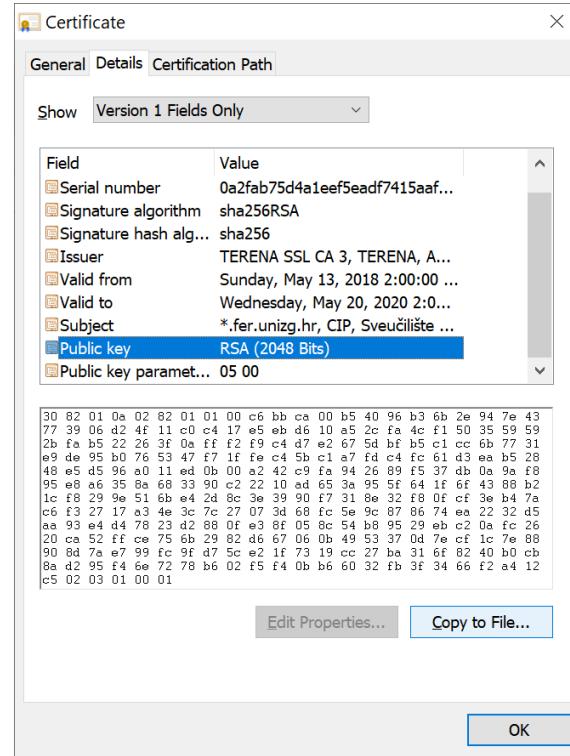
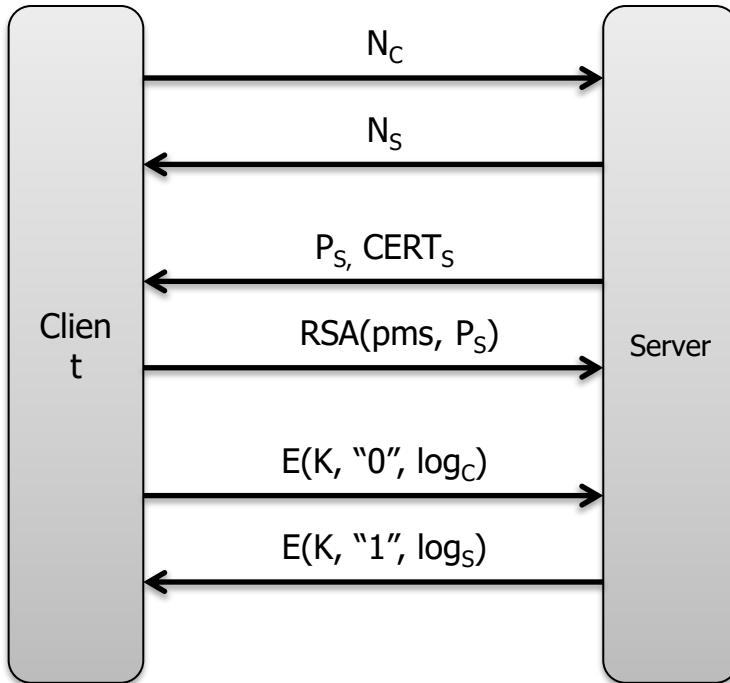
Nemogućnost krivotvorenja potpisa bilo kakve poruke pod napadom odabranom porukom (*existential unforgeability under chosen message attack*): Mti jedan algoritam koji koristi razumne resurse ne može pobijediti u sljedećoj igri s vjerojatnošću nezanemarivo većom od nule.



Digitalni potpis – primjene

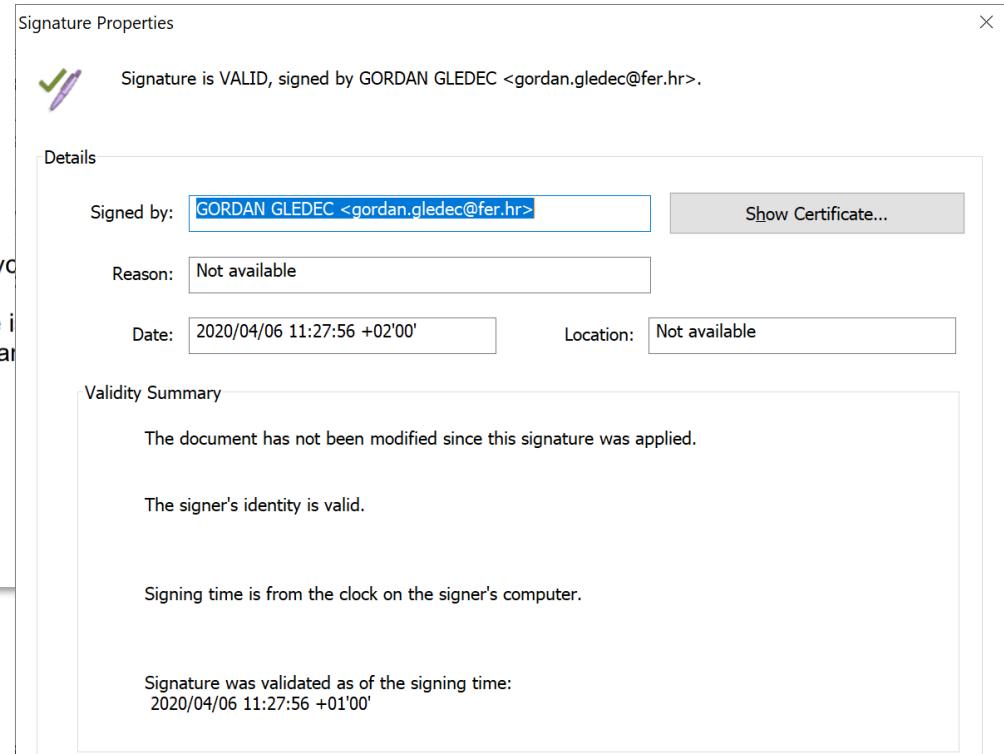
- Potpisivanje digitalnih dokumenata
- Sigurnosni protokoli (TLS, ...)
- Autentifikacija email-a
- Provjera autentičnosti softvera (apk, exe, firmware, ...)
- Kriptovalute
- ...

Primjena – TLS protokol



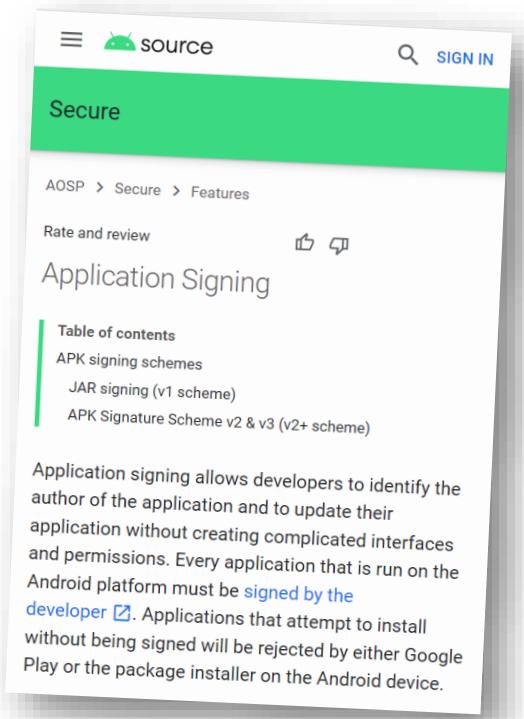
Primjena – e-Dokumenti

- ovisno o razvoju situacije, razmotrit će se uvođenje novih mera.
- II. Ova odluka je privremenog karaktera, donosi se i u okolnosti navedenih u točki I., stupa na snagu dan



Primjena – Android mobilne aplikacije

- Svaka mobilna aplikacija mora biti digitalno potpisana od strane autora!
- Operacijski sustav ne dopušta instaliranje i pokretanje nepotpisane aplikacije.
- Aplikacija može biti potpisana *bilo kojim* ključem.
 - Ključ je dio paketa koji sadrži aplikaciju i potpis.
- Aplikacije potpisane istim ključem mogu dijeliti podatke.



Izvor: source.android.com

Primjena – COVID potvrde

Vaccination example

V1-BE-12345678
ASBCD-56789-44

Name DOE Joe
Date of Birth 1987-06-05
Passport number PF12345678
Certificate issued 2021-06-02

Dose 1/2

Date 2021-02-03
Brand Pfizer Oy

Batch AB123CD
Adm. centre Hospital 1

Country Belgium
Issued by National health service

The smartphone screen displays a digital vaccination certificate. At the top, it says "Vaccination example". Below that is a large QR code. To the right of the QR code, the text "Level: Standard" is shown. Further down, the same personal and vaccination details are listed again. At the bottom of the screen, there is a blue downward-pointing triangle icon.

ME-telecom

Vaccination example

Level:
Standard

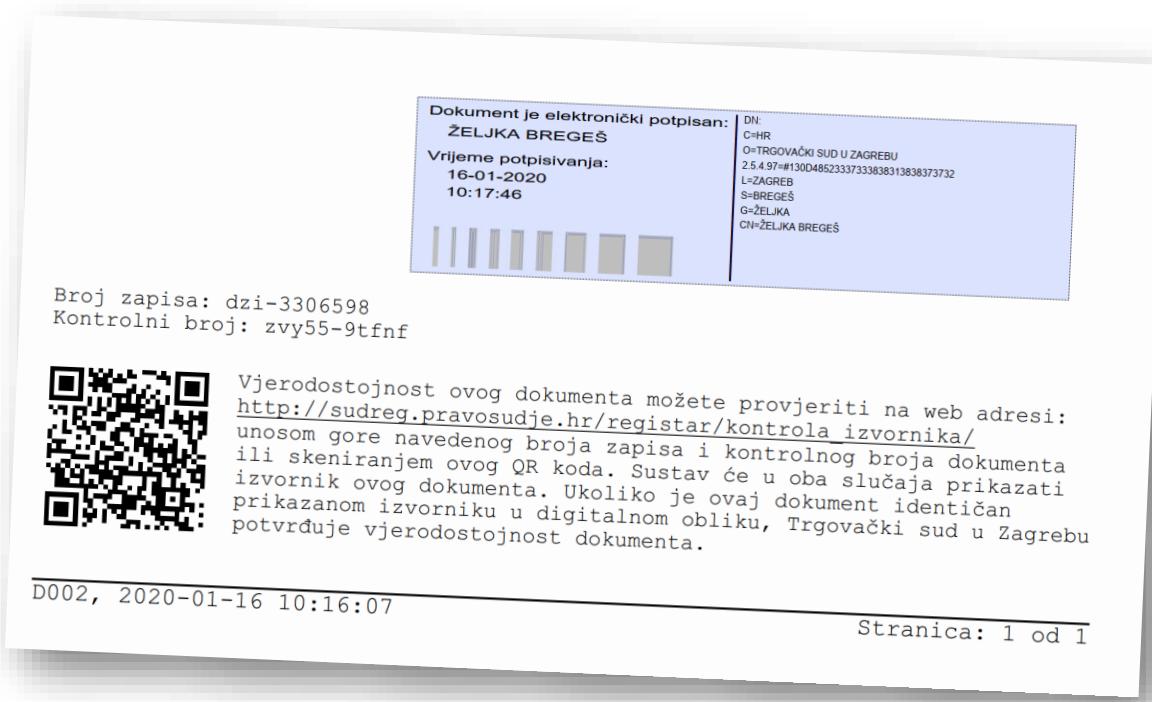
Name Doe Joe
Date of Birth 1987-06-05
Passport number PF12345678
Certificate issued 2021-06-02

Dose 1/2
Type C19-mRNA
Date 2021-02-24
Brand Pfizer Oy

Izvor: Interoperability of health certificates Trust framework

Što sve *nije* digitalni potpis?

- Tekst koji kaže da je dokument digitalno potpisan.
- Broj koji omogućuje dohvaćanje originalnog dokumenta online.
- QR kod.
- Slika analognog potpisa.
- ...



Primjeri sustava digitalnog potpisa

- RSA (1978)
 - teorija brojeva, sigurnost povezana s problemom faktorizacije
- McEliece (1978)
 - teorija kodiranja, sigurnost povezana s problemom dekodiranja općenitog linearног koda
- ElGamal (1985)
 - teorija brojeva ili eliptičke krivulje, sigurnost povezana s problemom diskretnog logaritma
- Schnorr (1991)
 - Jednostavan i efikasan sustav, sigurnost povezana s problemom diskretnog logaritma
- DSA (1992)
 - vrlo slično ElGamalovim potpisima

Digitalni potpisi i asimetrične šifre

Alice signs a message—"Hello Bob!"—by appending to the original message a version encrypted with her private key. Bob receives both the message and signature. He uses Alice's public key to verify the authenticity of the message, i.e. that the message, decrypted using the public key, exactly matches the original message.

- Digitalni potpis nije enkripcija sažetka poruke privatnim ključem!
- Često (ali ne i uvijek) se ista matematička ideja može iskoristiti za izgradnju asimetrične šifre i digitalnog potpisa.
 - RSA šifra i RSA potpis
 - Diffie-Hellman: ElGamal šifra, DSA potpis

Izvor: https://en.wikipedia.org/wiki/Digital_signature (ožujak 2021.)

„Obični RSA” digitalni potpis

Algoritam S:

- $S(m, (d, N)) = m^d \pmod{N}$

Algoritam V:

- $V(m, \sigma, (e, N)) = (\sigma^e \equiv m \pmod{N}) ? 1 : 0$

Zadatak: Obični RSA potpis 1

- Može li napadač na temelju javnog ključa (e, N) pronaći bilo koju poruku i njen ispravan potpis?

- Odaberem proizvoljni $x \in \mathbb{Z}_N$
- Izračunam $y = x^e$ u \mathbb{Z}_N
- x je ispravan potpis za poruku y .

Zadatak: Obični RSA potpis 2

- Pretpostavimo da napadač ima dvije poruke i njihove ispravne potpise, može li ih kombinirati tako da dobije ispravan potpis za neku novu poruku?

- $m_1, \sigma_1 = m_1^d \text{ u } \mathbb{Z}_N$
- $m_2, \sigma_2 = m_2^d \text{ u } \mathbb{Z}_N$
- $\sigma_1 \cdot \sigma_2 = m_1^d \cdot m_2^d = (m_1 \cdot m_2)^d \text{ u } \mathbb{Z}_N$
- $\sigma_1 \cdot \sigma_2$ je ispravan potpis od $m_1 \cdot m_2$

Zadatak: Obični RSA potpis 3

- Napadač ima mogućnost dobiti potpis za točno jednu poruku koja izgleda slučajno. Želi iskoristiti tu mogućnost kako bi dobio potpis konkretnе poruke m po njegovom izboru.

RSA digitalni potpis

H – kriptografska funkcija sažetka

Pad – funkcija nadopunjavanja

Algoritam S:

- $S(m, (d, N)) = Pad(H(m))^d \text{ u } \mathbb{Z}_N$

Algoritam V:

- $V(m, \sigma, (e, N)) = (Unpad(\sigma^e \text{ u } \mathbb{Z}_N) == H(m)) ? 1 : 0$

Zadatak: Obični RSA potpis 3

- Zašto isti napad više ne radi?

RSA digitalni potpis – Padding

- Hash poruke se uvijek nadopunjuje na zadalu veličinu!
- Postupak nadopunjavanja (*padding*) igra kritičnu ulogu i pažljivo je osmišljen.
 - PKCS#1 v1.5 (mnoštvo sigurnosnih problema)
 - PSS

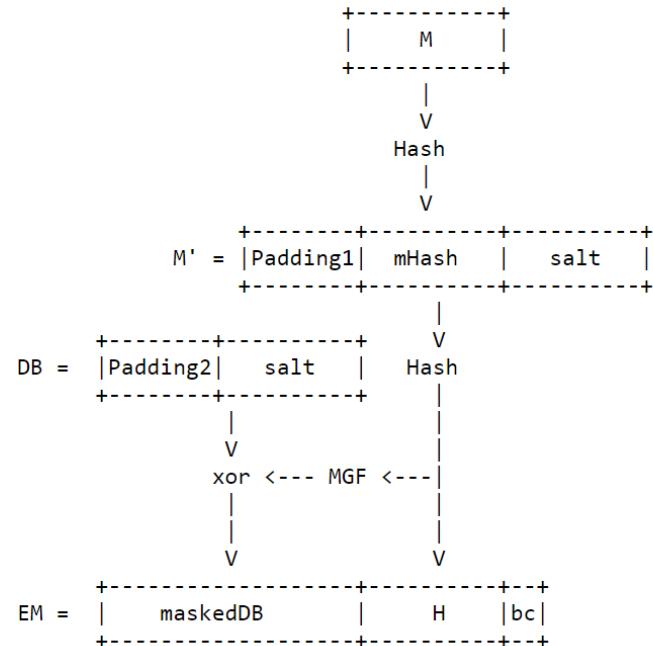
RSA – PKCS#1 v1.5 Padding

4. Generate an octet string PS consisting of emLen - tLen - 3 octets with hexadecimal value 0xff. The length of PS will be at least 8 octets.
5. Concatenate PS, the DER encoding T, and other padding to form the encoded message EM as

```
EM = 0x00 || 0x01 || PS || 0x00 || T.
```

RSA – PSS Padding

- *Probabilistic signature scheme*
- Dokazano sigurna pod jakim pretpostavkama sigurnosti običnog RSA i hash funkcija.
- *Mihir Bellare , Phillip Rogaway, PSS: Provably Secure Encoding Method for Digital Signatures (1998)*



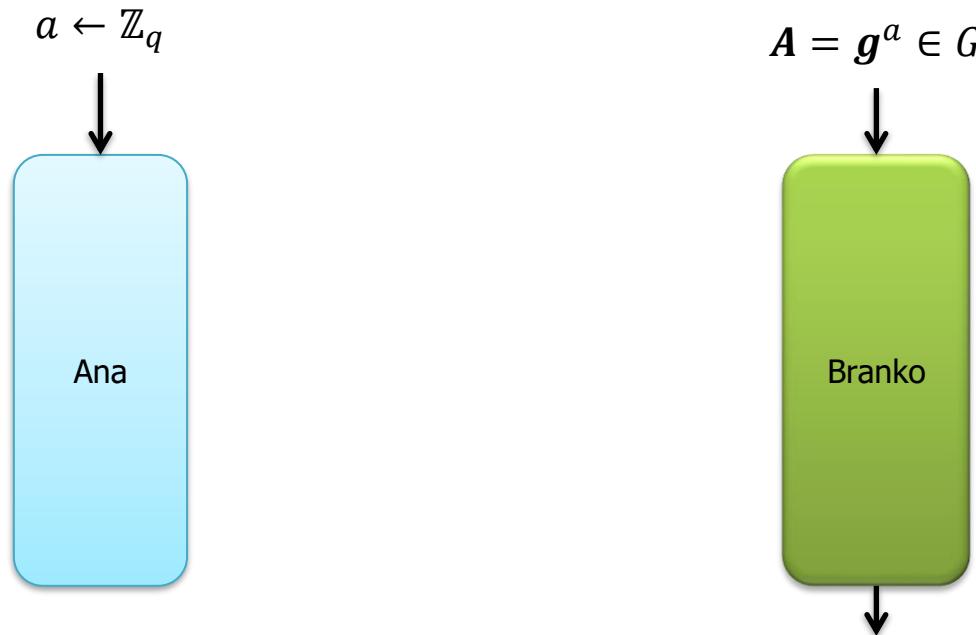
Izvor: <https://datatracker.ietf.org/doc/html/rfc8017>

Digitalni potpisi zasnovani na problemu diskretnog logartima

- Puno konstrukcija!
 - ElGamalov potpis
 - Schnorrov potpis
 - DSA
 - ...

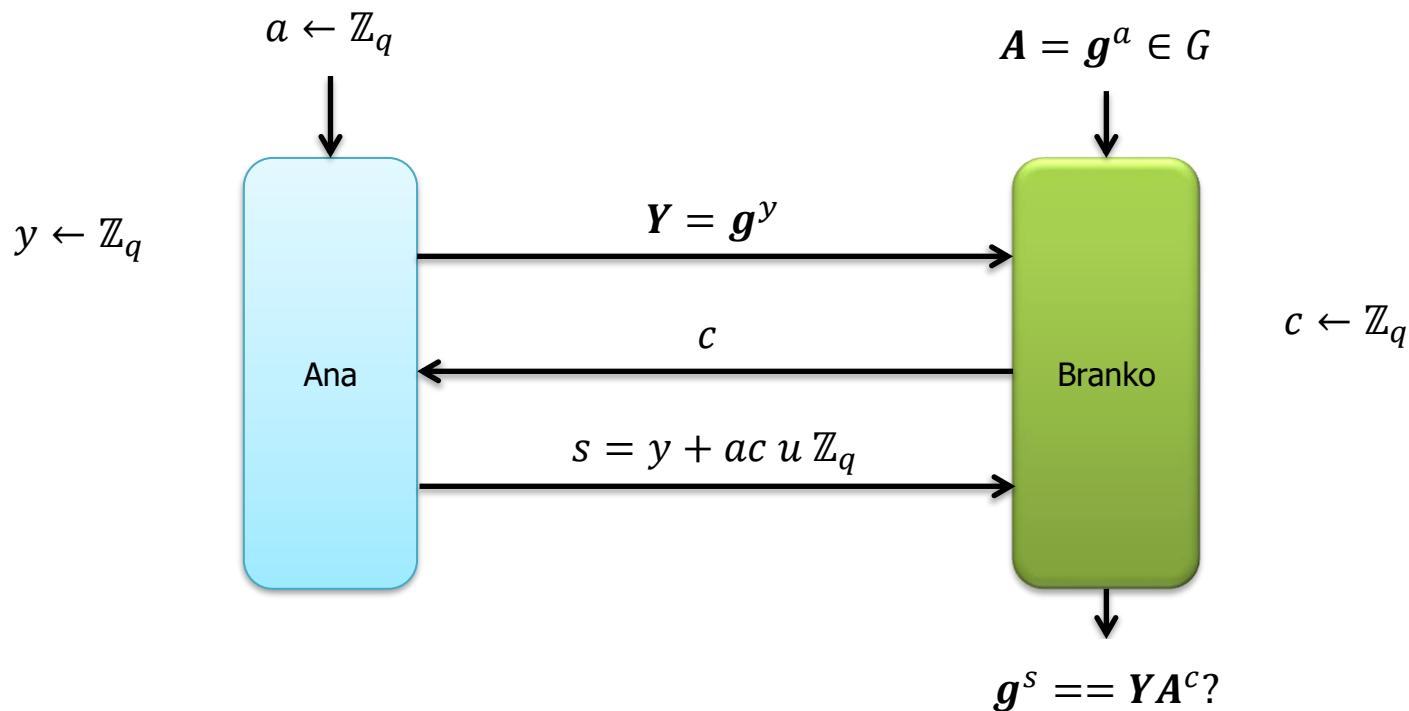
Schnorrov identifikacijski protokol

Kako Ana može dokazati Branku da posjeduje privatni ključ $a \in \mathbb{Z}_q$ koji odgovara javnom ključu $A = g^a \in G$, a da Branko ili napadač koji promatra promet ne može saznati ništa o privatnom ključu?

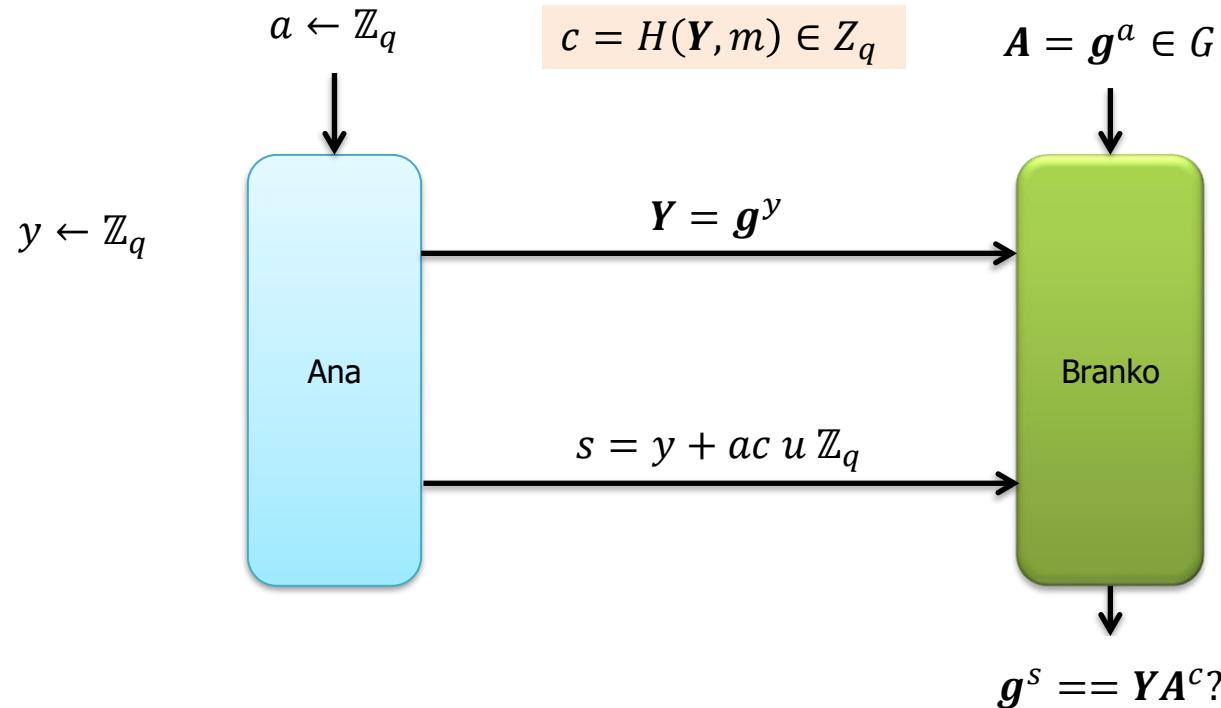


Schnorrov identifikacijski protokol

Kako Ana može dokazati Branku da posjeduje privatni ključ $a \in \mathbb{Z}_q$ koji odgovara javnom ključu $A = g^a \in G$, a da Branko ili napadač koji promatra promet ne može saznati ništa o privatnom ključu?



Schnorrov potpis



Schnorr – generiranje ključeva

Domenski parametri:

- G ciklička grupa reda q , gdje je q prost broj
- g generator grupe G
- H sigurna kriptografska hash funkcija

Algoritam G:

1. Odaberem slučajni $a \in \mathbb{Z}_q$
2. Izračunam $A = g^a$
3. Javni ključ je $A \in G$
4. Privatni ključ je $a \in \mathbb{Z}_q$

Schnorr – potpisivanje i verifikacija

Algoritam S:

Ulaz: poruka $m \in \{0,1\}^*$ i privatni ključ $a \in \mathbb{Z}_q$

1. Odaberem slučajni $y \in \mathbb{Z}_q$
2. Izračunam $\mathbf{Y} = \mathbf{g}^y$
3. Izračunam $c = H(\mathbf{Y}, m)$
4. Izračunam $s = y + a c \in \mathbb{Z}_q$

Potpis je par (\mathbf{Y}, s)

Algoritam V:

Ulaz: poruka m , potpis (\mathbf{Y}, s) i javni ključ \mathbf{A}

1. Izračunam $c = H(\mathbf{Y}, m)$
2. Provjerim je li $\mathbf{g}^s = \mathbf{Y}\mathbf{A}^c$

Schnorrov potpis

- Dokaziva jaka sigurnosna svojstva pod razumnim pretpostavkama o sigurnosti diskretnog logaritma i hash funkcije.
- Zaštićen patentima zbog čega nije često korišten u praksi (patent istekao 2008. godine).
 - Bitcoin dodao podršku za Schnorrove potpise 2021. godine.
- Zanimljiva svojstva agregacije potpisa.
- Pažnja: u literaturi se pojavljuje nekoliko inačica s različitim detaljima (npr. $s = y - a c$ umjesto $s = y + a c$)

Digital Signature Algorithm – DSA

- Standard od 1994. godine
 - Predložen od strane NIST-a
- Baziran na Diffie-Hellmanovoj razmjeni ključeva.
- Vrlo široko korišten:
 - TLS
 - Bitcoin, Ethereum
 - ...

Digital Signature Algorithm – DSA

4 The Digital Signature Algorithm (DSA)

Prior versions of this standard specified the DSA. This standard no longer approves DSA for digital signature generation. DSA may be used to verify signatures generated prior to the implementation date of this standard. See FIPS 186-4 [20] for the specifications for DSA.

7. The Edwards-Curve Digital Signature Algorithm (EdDSA)

The Edwards-curve Digital Signature Algorithm (EdDSA) is a digital signature scheme using a variant of a Schnorr signature based on twisted Edwards curves. See SP 800-186 for details on curves approved for use with EdDSA.

Prehash EdDSA (HashEdDSA) is a version of EdDSA where the EdDSA signature is generated on the hash of the message rather than the message itself. Prehash EdDSA is described in Section 7.8.

DSA – generiranje ključeva

Domenski parametri:

- G ciklička grupa reda q , gdje je q prost broj
- g generator grupe G
- H sigurna kriptografska hash funkcija
- F jednostavna funkcija koja preslikava elemente grupe G u \mathbb{Z}_q

Algoritam G:

1. Odaberem slučajni $a \in \mathbb{Z}_q$
2. Izračunam $A = g^a$
3. Javni ključ je $A \in G$
4. Privatni ključ je $a \in \mathbb{Z}_q$

DSA – potpisivanje i verifikacija

Algoritam S:

Ulaz: poruka $m \in \{0,1\}^*$ i privatni ključ $a \in \mathbb{Z}_q$

1. Odaberem slučajni $y \in \mathbb{Z}_q$
2. Izračunam $\mathbf{Y} = \mathbf{g}^y$
3. Izračunam $r = F(\mathbf{Y})$
4. Izračunam $s = y^{-1}(H(m) + ar) \in \mathbb{Z}_q$
5. Ako su r ili s jednaki 0 onda sve ponovi

Potpis je par (r, s)

Algoritam V:

Ulaz: poruka m , potpis (r, s) i javni ključ \mathbf{A}

1. Izračunam $t = H(m)s^{-1} \in \mathbb{Z}_q$
2. Izračunam $u = rs^{-1} \in \mathbb{Z}_q$
3. Izračunam $\mathbf{h} = \mathbf{g}^t \mathbf{A}^u$
4. Provjerim je li $r = F(\mathbf{h})$

Zadatak: Korektnost DSA

- Pokaži da se ispravno potpisane poruke uspješno verificiraju.

DSA na Z_p^*

- DSA nije definiran dok ne kažemo kako točno radi funkcija F .
- Ako je radimo u Z_p^* onda je $F(h) = h \bmod q$.

DSA Signature Generation

1. Choose an integer as random ephemeral key k_E with $0 < k_E < q$.
2. Compute $r \equiv (\alpha^{k_E} \bmod p) \bmod q$.
3. Compute $s \equiv (SHA(x) + d \cdot r) k_E^{-1} \bmod q$.

DSA na Z_p^*

- *Prime-order subgroup*
 - Računamo u $(Z_p^*, *)$ gdje je p prost (p je veličine npr. 3072 bitova)
 - g je reda q gdje je q prost (q je veličine npr. 256 bitova)
 - Nivo sigurnosti je oko pola veličine od q (128 bitova)
- Efikasnost računanja
 - Generiranje ključa
 - modularno eksponenciranje (eksponent veličine 256 bitova, modul veličine 3072 bita)
 - Potpisivanje, provjera potpisa
 - modularno eksponenciranje (eksponent veličine 256 bitova, modul veličine 3072 bita)
 - Modolarno zbrajanje, množenje, inverz (modul veličine 256 bitova)

Zadatak: Playstation 3 napad

- Što može poći po krivu ako prilikom potpisivanja uvijek koristimo isti y (umjesto da ga biramo svaki put slučajno)?

ECDSA

- DSA nije definiran dok ne kažemo kako točno radi funkcija F .
- Na eliptičkim krivuljama je $F((x, y)) = x \bmod q$.

ECDSA Signature Generation

1. Choose an integer as random ephemeral key k_E with $0 < k_E < q$.
2. Compute $R = k_E A$.
3. Let $r = x_R$.
4. Compute $s \equiv (h(x) + d \cdot r) k_E^{-1} \bmod q$.

Napadi kvantnim računalima

Pregled osnovnih pojmove napada
kvantnim računalima, kvantne i
postkvantne kriptografije

Kvantna mehanika – osnovni pojmovi

- Disclaimer: predavač nije fizičar i nema pojma o kvantnoj mehanici 😞
- Superpozicija (*superposition*)
 - Sustav može biti istovremeno u više stanja
 - Kvantni bit (*qubit*): $\alpha_0 |0\rangle + \alpha_1 |1\rangle$
- Kvantno sprezanje (*entanglement*)
 - Dva ili više qubita mogu biti spregnuti tako su im stanja međuvisna
 - *Sustav od dva qubita*: $\alpha_{00}|0\rangle|0\rangle + \alpha_{01}|0\rangle|1\rangle + \alpha_{10}|1\rangle|0\rangle + \alpha_{11}|1\rangle|1\rangle$
- Kvantna vrata
 - Rade na kvantnim bitovima
 - Npr. X vrata: $X(\alpha|0\rangle + \beta|1\rangle) = \beta|0\rangle + \alpha|1\rangle$.

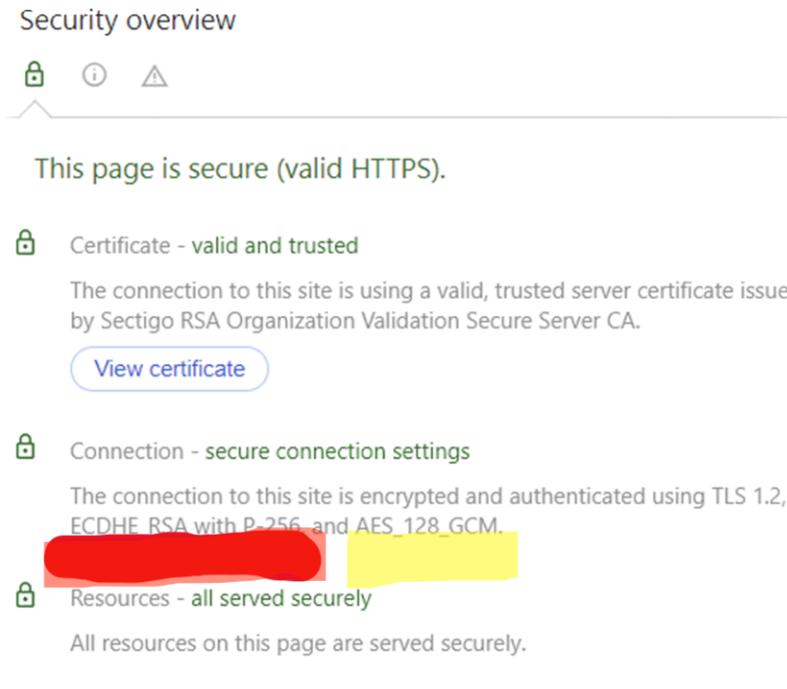
Kvantna računala

- Kvantni sklopovi
 - Grade se od kvantnih vrata
 - Mogu sve što i „obični“ logički sklopovi (ali ne direktno)
- Kvantni paralelizam (puno, puno pojednostavljeno)
 - Klasični algoritam: pokreni algoritam za jedan ulaz
 - Kvantni algoritam: stanje je superpozicija svih mogućih ulaza, pokreni algoritam i izračunaj izlaz za sve moguće ulaze, odaberi željeni izlaz
- Teškoće
 - Ne možemo očitati stanje cijelog spregnutog sustava
 - *No cloning theorem* – nemoguće je kopirati kvantne bitove

Napadi na kriptografiju kvantnim računalima

- Peter Shor (1997). „Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer”
 - RSA, Diffie-Hellman i povezane sheme su potpuno razbijene.
- Lov K. Grover (1998). „A framework for fast quantum mechanical algorithms”
 - Napad u $2^{n/2}$ koraka na bilo koju blok šifru s veličinom ključa n
- Obrane
 - Simetrična kriptografija: veći ključevi (npr. 256 umjesto 128 bitova)
 - Asimetrična kriptografija: novi algoritmi, procesi standardizacije u tijeku

Osnovni kriptografski algoritmi – napadi



Simetrični algoritmi – smanjena razina sigurnosti!

- Simetrične šifre
- Kriptografske funkcije sažetka
- Kodovi za integritet poruke

Asimetrični algoritmi – potpuno razbijeni

- Asimetrične šifre
- Digitalni potpisi
- Diffie-Hellmanova razmjena ključeva

Koliko je opasna ova prijetnja?

- Mišljenja variraju između:
 - Napadi kvantnim računalima su novi izmišljeni Y2K problem!
 - Kinezi već razbijaju kriptografiju kvantnim računalima.
- Ozbiljne institucije smatraju:
 - Praktični napada kvantnim računalima mogući u narednim desetljećima.
 - Potrebno je već danas krenuti s procesima prelaska na post-kvantne algoritme.

Quantum supremacy

- Nije svako „kvantno računalo“ pogodno za napade na kriptografske algoritme!
- Već postoje demonstracije kvantnih računala koja **određene specifične probleme** mogu riješiti brže nego klasična računala.
- Arute, F., et al. (2019). "Quantum supremacy using a programmable superconducting processor." *Nature*, 574(7779), 505-510. DOI: 10.1038/s41586-019-1666-5.
 - 53-qubitno kvantno računalo
 - Problem: „sampling the output of a pseudo-random quantum circuit“
 - Kvantno računalo: 200 sekundi – klasično superračunalo trebalo 10000 godina

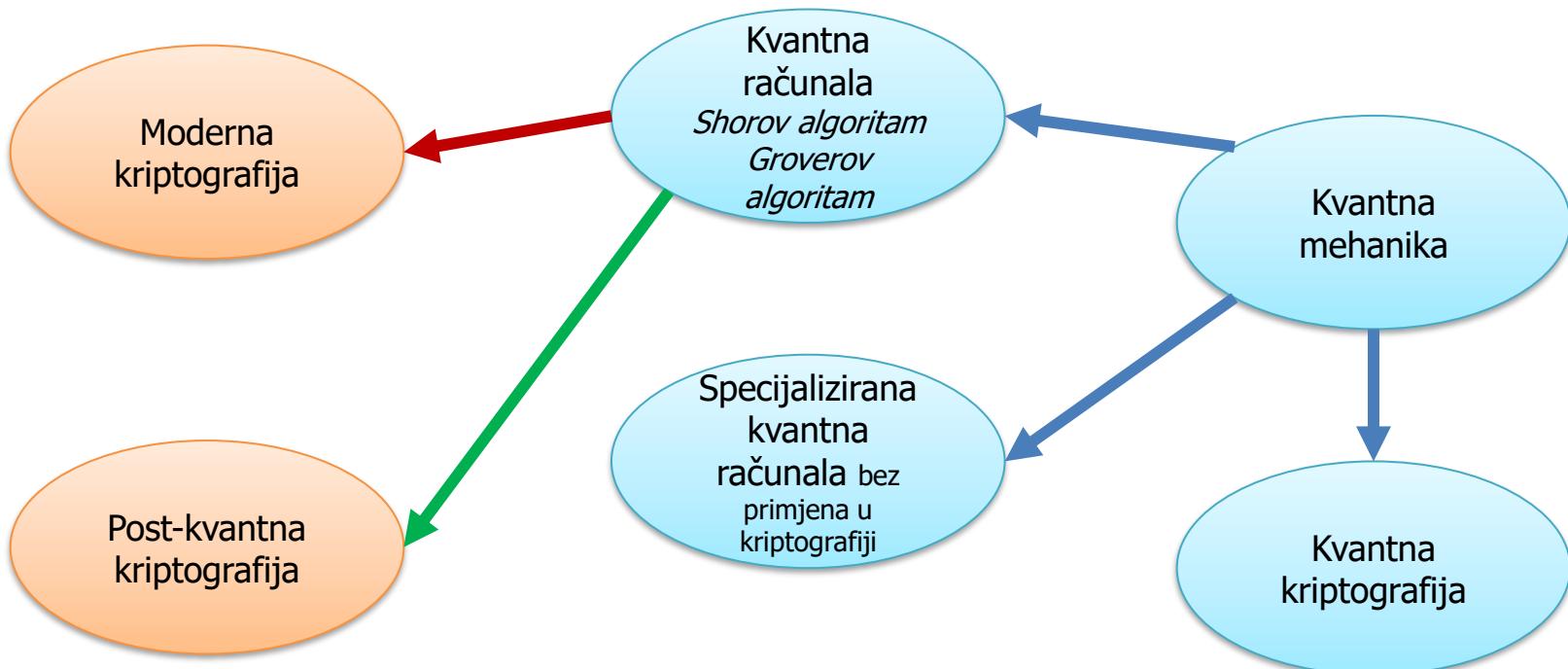
Post-kvantna kriptografija

- Algoritmi koji su (vjerujemo) otporni na napade kvantnim računalima
- Algoritmi su namijenjeni običnim, klasičnim, računalima.
- Tri klase:
 - Zasnovani na hash funkcijama
 - Zasnovani na rešetkama
 - Zasnovani na izogenijama
- Aktivno područje znanstvenog istraživanja
- Postupci standardizacije u tijeku
- Upitna sigurnost!

Kvantna kriptografija – *Quantum Key Distribution*

- Sigurna razmjena ključeva temeljena na principima kvantne mehanike
- Nije zasnovana na kvantnim računalima!
- Primjer: BB84 protokol
 - Ideja: Ako Alice i Bob uspješno završe protokol mora biti da nitko nije kopirao (mjerio) kvantne bitove koje su razmijenili jer bi mjerjenje narušilo uspješno izvođenje protokola.
- Nedostaci:
 - Specijalizirana oprema
 - Potrebna direktna veza između sudionika

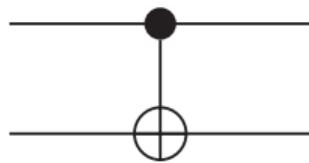
Mapa osnovnih pojmoveva



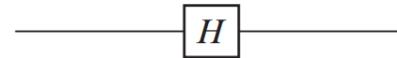
Podsjetnik – osnovni pojmovi

- Superpozicija (*superposition*)
 - Sustav može biti istovremeno u više stanja
 - Kvantni bit (*qubit*): $\alpha_0|0\rangle + \alpha_1|1\rangle$
- Kvantno sprezanje (*entanglement*)
 - Dva ili više qubita mogu biti spregnuti tako su im stanja međuvisna
 - *Sustav od dva qubita*: $\alpha_{00}|0\rangle|0\rangle + \alpha_{01}|0\rangle|1\rangle + \alpha_{10}|1\rangle|0\rangle + \alpha_{11}|1\rangle|1\rangle$
- Kvantna vrata
 - Rade na kvantnim bitovima
 - Npr. X vrata: $X(\alpha|0\rangle + \beta|1\rangle) = \beta|0\rangle + \alpha|1\rangle$.

Kvantna vrata – primjeri



Hadamardova vrata



CNOT

| Input | Output |
|--------------|--------------|
| $ 00\rangle$ | $ 00\rangle$ |
| $ 01\rangle$ | $ 01\rangle$ |
| $ 10\rangle$ | $ 11\rangle$ |
| $ 11\rangle$ | $ 10\rangle$ |

$$H(|0\rangle) = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

$$H(|1\rangle) = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

Kvantna vrata – ograničenja

- Funkcija koju računaju kvantna vrata mora biti:
 - *linear operator* na prostoru kvantnog stanja, što više *unitarni operator*
 - *Invertibilna*
- Nemoguće kopiranje qbitova!
- Jedna posljedica: Nije moguće direktno implementirati I vrata jer se gubi informacija.

| Operator | Gate(s) | Matrix |
|----------------------------|---------|--|
| Pauli-X (X) | | $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ |
| Pauli-Y (Y) | | $\begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$ |
| Pauli-Z (Z) | | $\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$ |
| Hadamard (H) | | $\frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$ |
| Phase (S, P) | | $\begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$ |
| $\pi/8$ (T) | | $\begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}$ |
| Controlled Not (CNOT, CX) | | $\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$ |
| Controlled Z (CZ) | | $\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}$ |
| SWAP | | $\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$ |
| Toffoli (CCNOT, CCX, TOFF) | | $\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$ |

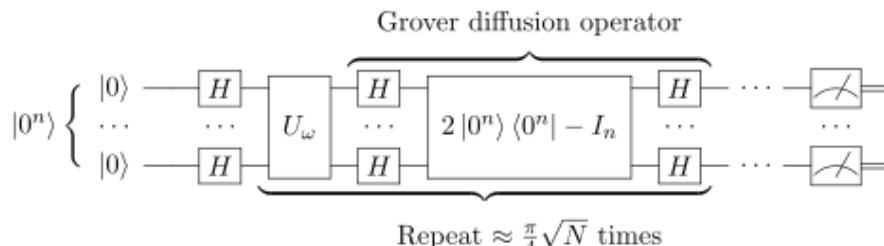
Nestrukturirano pretraživanje

- Problem nestruktuiranog pretraživanja:
 - Zadana je funkcija $f: \{1, \dots, N\} \rightarrow \{0, 1\}$
 - Za samo jedan ulaz x vrijedi $f(x) = 1$
 - Potrebno je pronaći x sa što manje evaluacija funkcije f
 - Funkcija f je crna kutija, možemo je evaluirati ali ne znamo kako radi iznutra
- Klasično računalo treba $O(N)$ koraka

| 1 | 2 | 3 | 4 | ... | x | ... | N-2 | N-1 | N |
|---|---|---|---|-----|---|-----|-----|-----|---|
| 0 | 0 | 0 | 0 | ... | 1 | ... | 0 | 0 | 0 |

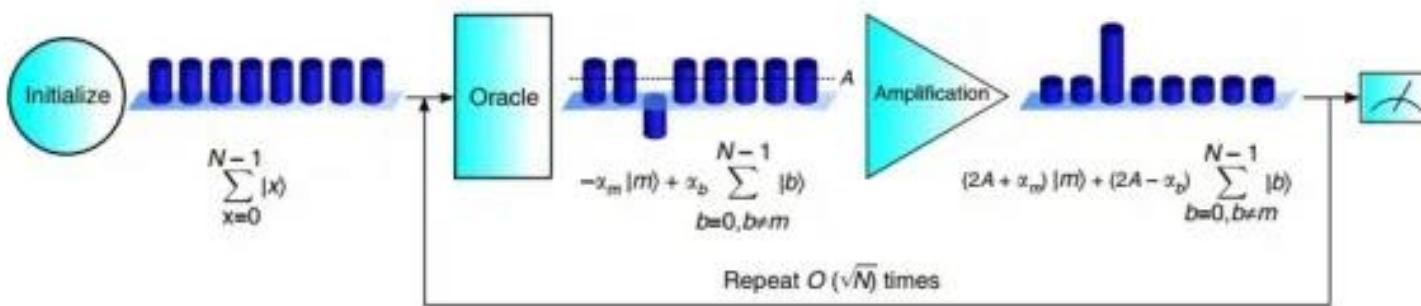
Groverov algoritam

- Lov K. Grover (1998). „A framework for fast quantum mechanical algorithms“
- Kvantni sklop za nestrukturirano pretraživanje
 - Radi u $O(\sqrt{N})$ koraka!
 - Pronalazi x s velikom vjerojatnošću.



wikipedia.org

Groverov algoritam – koraci



Demystifying Grover's Algorithm: a way quantum computing can serve power and energy applications, March 27, 2023 Abhishek Jadhav

Groverov algoritam – posljedice

- Brute-force napad na simetrične kriptosustave je problem nestrukturiranog pretraživanja!
 - $c = AES(k, m)$
 - $f(k) = AES(k, m) == c?$
- Ključ veličine n bitova se može pronaći u $2^{n/2}$ koraka!

Traženje perioda

- Problem traženja perioda:
 - Zadana je funkcija $f: \mathbb{Z}_N \rightarrow S$
 - Funkcija je periodička s periodom π ako vrijedi $f(x + \pi) = f(x)$ za svaki x
 - Potrebno je pronaći najmanji period sa što manje evaluacija funkcije f
 - Funkcija f je crna kutija, možemo je evaluirati ali ne znamo kako radi iznutra
- Klasično računalo treba $O(N)$ koraka

| 0 | 1 | 2 | 3 | 2 | 5 | 6 | 7 | 8 | ... |
|---|---|---|---|---|---|---|---|---|-----|
| 1 | 5 | 3 | 1 | 5 | 3 | 1 | 5 | 3 | ... |

Shorov algoritam

- Peter Shor (1997). „Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer”
- Pronalazi period funkcije u $O(\log^2 N)$ koraka
 - Zasnovan na kvantnoj Fourierovoj transformaciji.
- Problem faktoriziranja brojeva se može efikasno (i klasično) svesti na problem traženja perioda!
- Problem diskretnog logaritma se može efikasno (i klasično) svesti na problem traženja perioda!

Napadi kvantnim računalima – posljedice

| Cryptographic Algorithm | Type | Purpose | Impact from large-scale quantum computer |
|--|---------------|-------------------------------|--|
| AES | Symmetric key | Encryption | Larger key sizes needed |
| SHA-2, SHA-3 | ----- | Hash functions | Larger output needed |
| RSA | Public key | Signatures, key establishment | No longer secure |
| ECDSA, ECDH (Elliptic Curve Cryptography) | Public key | Signatures, key exchange | No longer secure |
| DSA (Finite Field Cryptography) | Public key | Signatures, key exchange | No longer secure |

Chen, Lily, et al. *Report on post-quantum cryptography*. Vol. 12. Gaithersburg, MD, USA: US Department of Commerce, NIST, 2016.

Napadi „kvantnim računalima” u praksi

- 2001 – faktoriziran broj 15
 - Vandersypen, Lieven MK, et al. "Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance." *Nature* 414.6866 (2001): 883-887.
- 2012 – faktoriziran broj 15
 - Martin-Lopez, Enrique, et al. "Experimental realization of Shor's quantum factoring algorithm using qubit recycling." *Nature photonics* 6.11 (2012): 773-776.
- 2012 – faktoriziran broj 21
 - Lucero, Erik, et al. "Computing prime factors with a Josephson phase qubit quantum processor." *Nature Physics* 8.10 (2012): 719-723.

Cilj!

Public-Key: (4096 bit)

Modulus:

```
00:b4:73:d2:d6:65:d3:02:ef:58:3a:f4:82:82:d3:  
a7:eo:8a:60:b2:3a:f5:b1:65:38:a7:24:0e:21:6b:  
7d:ea:9:a0:9d:33:a2:74:cd:ae:91:ba:94:b5:cc:6:  
80:b5:71:df:48:71:ca:75:4b:a7:bf:ff:26:eb:84:  
fe:fb:9:72:16:c8:c2:7e:86:d4:bf:af:ee:63:35:b9:  
c0:e4:da:05:4f:b8:48:9e:22:28:ff:55:05:23:6b:  
81:4e:b3:17:11:2c:2a:25:1f:4:e1:df:61:c8:3c:  
f2:56:69:d0:55:7d:96:10:b2:a8:7:b5:90:5b:a6:  
5e:53:8b:41:e3:c7:87:c7:31:bd:34:39:ec:19:21:  
d9:80:c4:e8:0d:db:da:03:0c:00:f4:aa:b5:82:06:  
25:0c:c5:d9:1a:62:9d:fd:0a:49:05:fc:1c:be:93:  
46:fc:ce:89:91:ff:cd:cc:5f:48:5f:dc:38:0d:75:  
6f:d2:2d:ab:cc:22:12:78:88:12:1f:fe:0:d5:4e:77:  
bc:2c:89:4d:76:7a:88:9b:5d:07:da:b3:67:98:1:  
39:ce:7a:46:ab:cf:f6:7d:57:25:13:fa:84:c4:03:  
70:af:0c:76:0c:d2:40:24:7c:59:df:77:37:59:50:  
b1:25:46:4e:42:1d:08:22:09:72:55:c4:42:ea:6f:  
6f:65:59:d4:4e:e0:3d:a3:ab:70:7:c6:69:09:30:55:  
76:62:89:f3:6f:d2:0:a6:b3:6e:19:3d:96:86:7a:  
66:94:cd:f2:cc:7a:f0:07:08:b3:69:ae:1b:ff:1c:  
71:18:a2:44:f9:db:d6:0d:84:10:81:74:49:61:62:  
d7:10:f0:01:a6:45:c0:b5:d0:52:f4:51:86:3d:e2:  
f7:16:29:5a:fa:4a:9e:27:4b:8e:46:f1:72:3e:a7:  
f5:a4:0c:e0:0b:17:9a:22:ff:f9:7:ea:ab:35:8e:01:  
84:d5:75:93:7f:e6:75:a8:7a:64:de:62:3a:02:47:  
1:a:0:23:c4:4c:3f:d0:dc:4e:33:7:6c:bb:fa:f6:  
18:10:2b:34:30:5f:c7:33:50:99:02:e9:b1:59:46:  
55:65:a6:ba:4:83:18:8b:cd:1:f1:ca:18:e2:d9:  
20:e6:b7:84:87:1f:0b:56:7c:4d:31:54:26:f2:99:  
56:c8:a6:59:a6:85:33:f2:90:cc:28:5a:c8:6c:a4:  
cb:a6:47:46:4:9a:55:39:84:64:8d:77:e7:0a:3d:  
c3:d0:12:f7:76:a8:cc:1c:b3:1f:58:85:3a:4:36:  
8:dec:9a:ec:0:e:7:1:c9:9f:4f:fb:d0:7a:07:0c:  
c6:05:b0:ab:8d:ba:72:5d:4e:23:d9:6f:0c:5c:f8:  
a6:72:d1
```

Exponent: 65537 (0x10001)

Što kažu vjerodostojni izvori?

- National Institute of Standards and Technology (NIST) – **20 godina**
 - Chen, Lily, et al. Report on post-quantum cryptography. Vol. 12. Gaithersburg, MD, USA: US Department of Commerce, NIST, 2016
- The European Union Agency for Cybersecurity (ENISA) – **ne znamo, ali želimo biti spremni**
 - POST-QUANTUM CRYPTOGRAPHY, Current state and quantum mitigation, MAY 2021, v2
- Bundesamt für Sicherheit in der Informationstechnik (BSI) – **10-20 godina**
 - Studie: Entwicklungsstand Quantencomputer Version 2.0, Datum, 13.11.2023

Teško je pronaći potpuno objektivne izvore!

Research suggests that by 2026, there is a 1 in 7 chance that quantum computers will break the most used cryptographic systems, which will go as high as 50% by 2031.¹ However, research published² in early 2023 by Chinese scholars suggests that it could happen even before.

A quantum cybersecurity agenda for Europe. Governing the transition to post-quantum cryptography, Andrea García Rodríguez, Publisher European Policy Centre

The question of when a large-scale quantum computer will be built is complicated and contentious. While in the past it was less clear that large quantum computers are a physical possibility, many scientists now believe it to be merely a significant engineering challenge. Some experts even predict that within the next 20 or so years, sufficiently large quantum computers will be built to break essentially all public key schemes currently in use [2]. It has taken almost 20 years to deploy our modern public key cryptography infrastructure. It will take significant effort to ensure a smooth and secure migration from the current widely used cryptosystems to their quantum computing resistant counterparts. Therefore, regardless of whether we can estimate the exact time of the arrival of the quantum computing era, we must begin now to prepare our information security systems to be able to resist quantum computing.

Chen, Lily, et al. *Report on post-quantum cryptography*. Vol. 12. Gaithersburg, MD, USA: US Department of Commerce, NIST, 2016.

I have estimated a one in seven chance that some of the fundamental public-key cryptography tools upon which we rely today will be broken by 2026 and a 50% chance by 2031. [1,2] Although the quantum attacks are happening yet, critical decisions need to be taken *today* in order to be able to respond to these threats in the future, and organizations are already being differentiated by how well they can articulate their readiness.

Mosca, Michele (2016), Quantum Computing: A New Threat to Cybersecurity. Global Risk Institute.



evolutionQ provides scalable defense-in-depth with PQC and QKD software solutions for resilience and quantum-safe security.

OUR STORY

About evolutionQ

evolutionQ was co-founded by leading quantum-safe cryptography experts, Dr. Michele Mosca, Dr. Norbert Lütkenhaus, and Dr. David Jao.

Zdrava doza skepticizma

- Sasvim je moguće da su praktični napadi kvantnim računalima
jako jako daleko!
- Postoje puno ozbiljniji sigurnosni problemi kojima bi trebalo
posvetiti više pažnje!

On the Heffalump Threat

Peter Gutmann

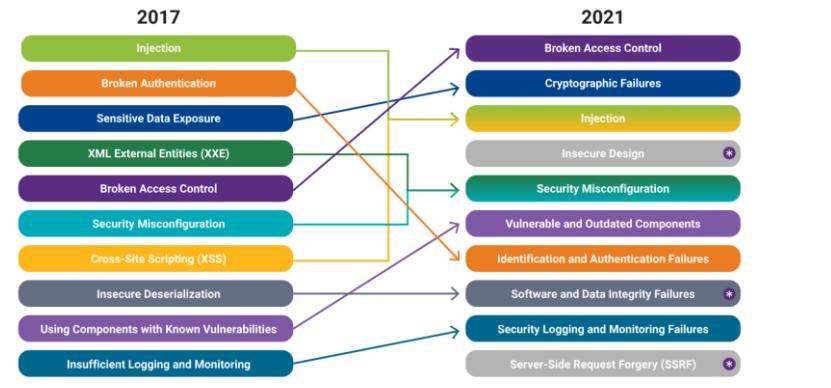
University of Auckland

pgut001@cs.auckland.ac.nz

Abstract

Over the last few years a new type of attack has been receiving a lot of attention. Unfortunately the technical details can be quite confusing to laypeople. This paper explains it in easy-to-understand terms.

<https://www.cs.auckland.ac.nz/~pgut001/>



<https://www.synopsys.com/glossary/what-is-owasp-top-10.html>

Proliferacija post-kvantnih rješenja!

- Oprez: vrlo popularno područje za znanstvena istraživanja i komercijalne proizvode upitne kvalitete!

The collage consists of three separate journal article snippets:

- drones** (top left):
Article
A Quantum-Resistant Identity Authentication and Key Agreement Scheme for UAV Networks Based on Kyber Algorithm
Tao Xia ^{1,*†}, Menglin Wang ^{1,*}, Jun He ^{1,†}, Gang Yan
Security and Communication Networks
- MDPI** (top right):
Post-Quantum Lattice-Based Secure Framework Using Aggregate Signature for Ambient Intelligence Assisted Blockchain-Based IoT Applications
Prithwi Bagchi, Basudeb Bera, Ashok Kumar Das, Sachin Shetty, Pandi Vijayakumar, and Marimuthu Karuppiah
- Post-Quantum Secure Identity-Based Random Integer Lattices for IoT-enabled AI Applications** (bottom center):
Dharminder Dharminder, Ashok Kumar Das , Sourav Saha, Basudeb Bera, Athanasios V. Vasilakos
First published: 06 July 2022 | <https://doi.org/10.1155/2022/5498058> | Citations: 3
Academic Editor: Wenbo Shi

Regulativa (EU)

- (3) The future potential development of quantum computers capable of breaking today's encryption makes it necessary for Europe to look for stronger safeguards, ensuring the protection of sensitive communications and the long-term integrity of confidential information, i.e., by switching to Post-Quantum Cryptography as swiftly as possible. This new type of cryptography will remove the known vulnerabilities of current asymmetric cryptography and enhance the robustness against the threats posed by the malicious use of quantum computers.

- (5) Member States should consider migrating their current digital infrastructures and services for public administrations and other critical infrastructures to Post-Quantum Cryptography as soon as possible, inducing a fundamental shift in cryptographic algorithms, protocols and systems. As highlighted in the Commission's recent White Paper "How to master Europe's digital infrastructure needs", this requires a coordinated effort involving government agencies, standardization bodies, industry stakeholders, researchers and cybersecurity professionals.

EUROPEAN COMMISSION RECOMMENDATION of 11.4.2024 on a
Coordinated Implementation Roadmap for the transition to Post-
Quantum Cryptography

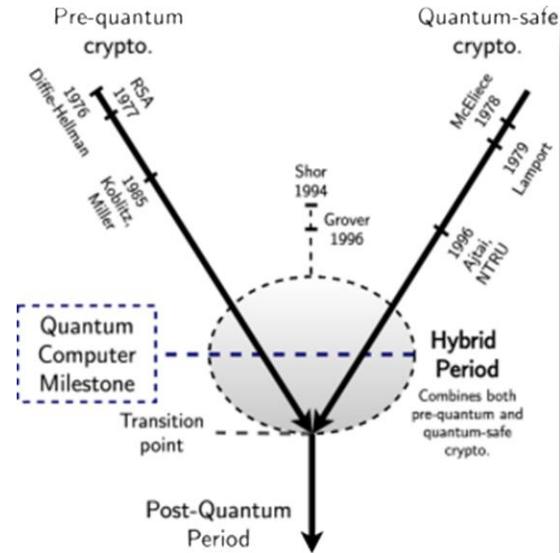
Napadač iz budućnosti!

- Problem: današnji kriptirani podaci mogu biti dekriptirani u budućnosti kada kvantna računala postanu dostupna i praktična!
 - *Store now – decrypt later* napad
- Potreba za zaštitom post-kvantnim algoritmima postoji već danas!
- Napad nije primjenjiv na sve kriptografske ključeve/algoritme/sustave.
 - Npr. kompromis FINA CA privatnog ključa



Hibridna faza

- Prijelazna faza u kojoj se kombiniraju klasični kriptografski algoritmi i post-kvantni algoritmi
 - Jednostavni primjer: dvostruka enkripcija
- Omogućuje postupni prijelaz na sigurnije kriptografske algoritme
- Smanjuje rizik od neočekivanih slabosti u novim algoritmima



A. Giron, R. Custodio, and F. Rodríguez-Henríquez.
Post-quantum hybrid key exchange: a systematic
mapping study. *Journal of Cryptographic Engineering*,
13 (1):71–88, 2023.

Post-kvantna kriptografija

Cilj

- Tražimo post-kvantne inačice asimetričnih algoritama!
 - Asimetrične šifre
 - Digitalni potpisi
 - Diffie-Hellmanova razmjena ključeva
- Novi pojam – *key encapsulation mechanism*
 - Zamjena za asimetričnu šifru
- Novi pojam – *key exchange mechanism*
 - Zamjena za Diffie-Hellmanovu razmjenu ključeva

Sustav enkapsulacije ključa (KEM)

Asimetrična enkripcija

- Trojka *efikasnih* algoritama G , E i D
 - G – algoritam koji generira par ključeva pk, sk
 - $E(m, pk)$ – algoritam enkripcije
 - $D(c, sk)$ – algoritam dekripcije

Sustav enkapsulacije ključa

- Trojka *efikasnih* algoritama G , E i D
 - G – algoritam koji generira par ključeva pk, sk
 - $E(pk)$ – algoritam enkapsulacije koji generira skriveni tekst c i k
 - $D(c, sk)$ – algoritam dekapsulacije
- Vrijedi $D(c, sk) = k$

NIST Standardizacija – kratki pregled

- 2016 – poziv za prijedloge za algoritme asimetrične kriptografije
- 2022 – objavljeni kandidati za standarizaciju
 - Key encapsulation mechanisms: CRYSTALS-Kyber
 - Digitalni potpis: CRYSTALS-Dilithium, Falcon, SPHINCS+
 - Kandidati: BIKE, SIKE, Classic McEliece, HQC
- 2023 – SIKE potpuno razbijen (Castryck and Decru)

NIST Standardizacija – epilog

- FIPS 203: Module-Lattice-Based Key-Encapsulation Mechanism Standard, August 13, 2024
 - ML-KEM
 - Zasnovan na jednoj od inačica CRYSTALS-KYBER KEM prijedloga
- FIPS 204: Module-Lattice-Based Digital Signature Standard, August 13, 2024
 - ML-DSA
 - Zasnovan na jednoj od inačica CRYSTALS-DILITHIUM prijedloga
- FIPS 205, Stateless Hash-Based Digital Signature Standard, August 13, 2024
 - SLH-DSA
 - Zasnovan na SPHINCS+ prijedlogu

ML-KEM veličina ključa i razina sigurnosti

ML-KEM comes equipped with three parameter sets:

- ML-KEM-512 (security category 1)
- ML-KEM-768 (security category 3)
- ML-KEM-1024 (security category 5)

| Level | Security Description |
|-------|---|
| I | At least as hard to break as AES128 (exhaustive key search) |
| II | At least as hard to break as SHA256 (collision search) |
| III | At least as hard to break as AES192 (exhaustive key search) |
| IV | At least as hard to break as SHA384 (collision search) |
| V | At least as hard to break as AES256 (exhaustive key search) |

Table 3. Sizes (in bytes) of keys and ciphertexts of ML-KEM

| | encapsulation key | decapsulation key | ciphertext | shared secret key |
|-------------|-------------------|-------------------|------------|-------------------|
| ML-KEM-512 | 800 | 1632 | 768 | 32 |
| ML-KEM-768 | 1184 | 2400 | 1088 | 32 |
| ML-KEM-1024 | 1568 | 3168 | 1568 | 32 |

Performance

| Algorithm | Public key (bytes) | Ciphertext (bytes) | Key gen. (ms) | Encaps. (ms) | Decaps. (ms) |
|------------------|-----------------------|-----------------------|------------------|-----------------|-----------------|
| ECDH NIST P-256 | 64 | 64 | 0.072 | 0.072 | 0.072 |
| SIKE p434 | 330 | 346 | 13.763 | 22.120 | 23.734 |
| Kyber512-90s | 800 | 736 | 0.007 | 0.009 | 0.006 |
| FrodoKEM-640-AES | 9,616 | 9,720 | 1.929 | 1.048 | 1.064 |

Table 1: Key exchange algorithm communication size and runtime

| Algorithm | Public key (bytes) | Signature (bytes) | Sign (ms) | Verify (ms) |
|------------------|-----------------------|----------------------|--------------|----------------|
| ECDSA NIST P-256 | 64 | 64 | 0.031 | 0.096 |
| Dilithium2 | 1,184 | 2,044 | 0.050 | 0.036 |
| qTESLA-P-I | 14,880 | 2,592 | 1.055 | 0.312 |
| Picnic-L1-FS | 33 | 34,036 | 3.429 | 2.584 |

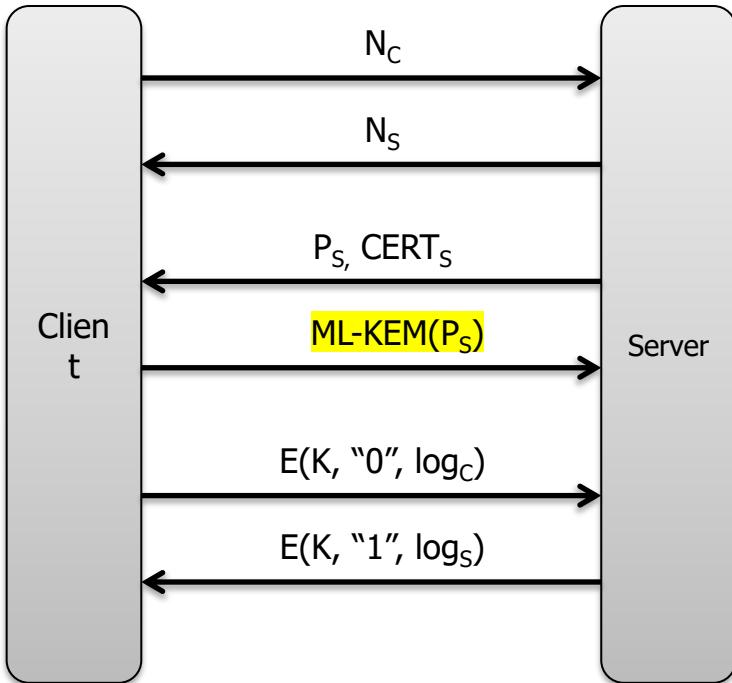
Table 2: Signature scheme communication size and runtime

Paquin, Christian, Douglas Stebila, and Goutam Tamvada. "Benchmarking post-quantum cryptography in TLS." *Post-Quantum Cryptography: 11th International Conference, PQCrypto 2020, Paris, France, April 15–17, 2020, Proceedings 11*. Springer International Publishing, 2020.

Post-kvantna kriptografija

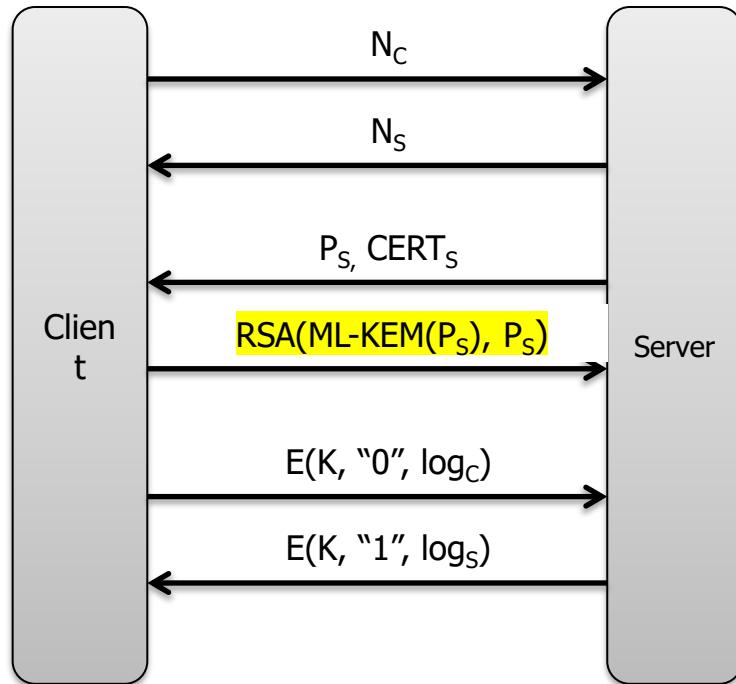
- Zamjena za klasične asimetrične algoritme!
- Standardi postoje, ali treba proći 10-20 godina prije nego što ćemo ih smatrati sigurnima.
- Veći ključevi i slabije performanse za istu razinu sigurnosti (na klasičnim računalima) u usporedbi s asimetričnim algoritmima koje zamjenjuju.
- Još nemamo post-kvantnu varijantu Diffie-Hellmanove zamjene ključeva – potrebno je redizajnirati neke protokole i sustave.

Zadatak – PQ TLS – V1



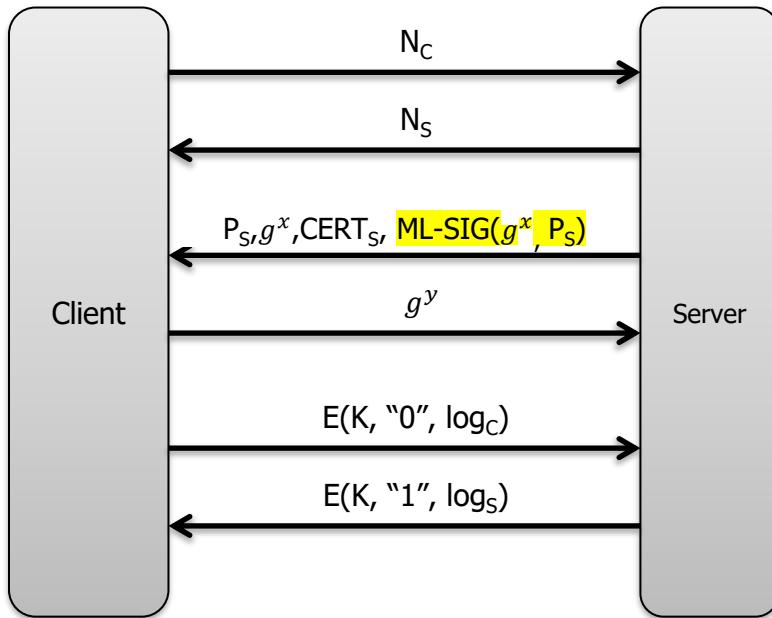
- Obzirom da nemam zamjene za post-
kvantni Diffie-Hellman
biram RSA varijantu i
prelazim na KEM!
- Prednosti i mane?

Zadatak – PQ TLS – V2



- Od viška glava ne boli?
- Prednosti i mane?

Zadatak – PQ TLS – V3



- Prednosti i mane?

7. Kriptografija prilagođena uređajima s ograničenim mogućnostima

Lightweight Cryptography

Kriptografija prilagođena ugrađenim
sistavima i Internetu stvari

Natječaj

- <https://csrc.nist.gov/Projects/Lightweight-Cryptography/>
- za ograničene računalne resurse, primjerice
 - ugrađene sustave
 - Internet stvari
- Na NIST-ovoj radionici 20.6.2015. "Lightweight Cryptography Workshop 2015" iskazuje se potreba za novim oblikom kriptografije koja djeluje u okruženju s ograničenim računalnim resursima.
- NIST raspisuje natječaj 27.8.2018.
- 25.2.2019. je pristiglo 57 kandidata od kojih 56 zadovoljava uvjete natječaja
- 29.3.2021. objavljeno 10 finalista
- 7.2.2023. NIST je odabrao algoritam **ASCON**

Uvjeti natječaja 1/3

- algoritam ili skup algoritama koji osim
 - simetrične i
 - autentifikacijske kriptografije (*Authenticated Encryption with Associated Data, AEAD*)
- mogu opcionalno imati funkcionalnost
 - izračunavanja sažetka (*hash*)
- zahtjevi za spremnikom (RAM i ROM) trebaju biti što je moguće manji
- moraju se moći izvoditi i u sljedećim sklopoškim okruženjima
 - FPGA
 - ASIC
 - 8, 16 i 32-bitnim mikrokontrolerima

Uvjeti natječaja 2/3

- veličina ključa 128 bita ili više
- složenost napada grubom silom ne smije biti manja od 2^{112}
- ako algoritam podržava veći ključ od 128 bita tada mora imati
 - mogućnost veličine ključa od 256 bita i
 - složenost napada grubom silom mora biti najmanje 2^{224}
- najmanja veličina parametara:
 - *nonce* treba biti veličine najmanje 96 bita
 - *tag* najmanje 64 bita
- najveća duljina poruke ne smije biti manja od $2^{50}-1$

Uvjeti natječaja 3/3

Simetrični i autentifikacijski algoritam, AEAD

- ulaz u AEAD se sastoji od 4 dijela
 - jasni tekst varijabilne duljine
 - pridruženi podaci (*associated data*) varijabilne duljine
 - *nonce*
 - ključ
- izlaz je kriptirani tekst i *tag*

Funkcija za izračunavanje sažetka poruke, *hash*

- opcionalna
- izlaz mora biti minimalno 256 bita
- napad grubom silom mora biti najmanje složenosti 2^{112}

18.4.2019. objavljeno 56 kandidata za prvi krug natječaja

| ACE | ASCON | Bleep64 | CiliPadi | CLAE | CLX | COMET | DryGASCON |
|---------------------------|--------------------------------------|-----------|-----------|----------------------|-----------------|------------------|------------------|
| Elephant | ESTATE | FlexAEAD | ForkAE | Fountain | GAGE and InGAGE | GIFT-COFB | Gimli |
| Grain-128AEAD | HERN & HERON | HYENA | ISAP | KNOT | LAEM | Lilliput-AE | Limdolen |
| LOTUS-AEAD and LOCUS-AEAD | mixFeed | ORANGE | Oribatida | PHOTON-Beetle | Pyjamask | Qameleon | Quartet |
| REMUS | Romulus | SAEAES | Saturnin | Shamash & Shamashash | SIMPLE | SIV-Rijndael256 | SIV-TEM-PHOTON |
| SKINNY-AEAD /SKINNY-HASH | SNEIK | SPARKLE | SPIX | SpoC | Spook | Subterranean 2.0 | SUNDAE-GIFT |
| Sycon | TGIF (Thank Goodness It's Friday) | TinyJambu | Triad | TRIFLE | WAGE | Xoodyak | Yarará and Coral |

30.8.2019. objavljeno

32 kandidata za drugi krug natječaja

od čega 12 kandidata imaju mogućnost izračunavanja sažetka

| ACE | ASCON | Bleep64 | CiliPadi | CLAE | CLX | COMET | DryGASCON |
|----------------------------------|--|------------------|------------------|---------------------------------|------------------------|-------------------------|-------------------------|
| Elephant | ESTATE | FlexAEAD | ForkAE | Fountain | GAGE and InGAGE | GIFT-COFB | Gimli |
| Grain-128AEAD | HERN & HERON | HYENA | ISAP | KNOT | LAEM | Lilliput-AE | Limdolen |
| LOTUS-AEAD and LOCUS-AEAD | mixFeed | ORANGE | Oribatida | PHOTON-Beetle | Pyjamask | Qameleon | Quartet |
| REMUS | Romulus | SAEAES | Saturnin | Shamash & Shamashash | SIMPLE | SIV-Rijndael256 | SIV-TEM-PHOTON |
| SKINNY-AEAD /SKINNY-HASH | SNEIK | SPARKLE | SPIX | SpoC | Spook | Subterranean 2.0 | SUNDAE-GIFT |
| Sycon | TGIF (Thank Goodness It's Friday) | TinyJambu | Triad | TRIFLE | WAGE | Xoodyak | Yarará and Coral |

29.3.2021. objavljeno 10 finalista

od čega 4 kandidata imaju mogućnost izračunavanja sažetka

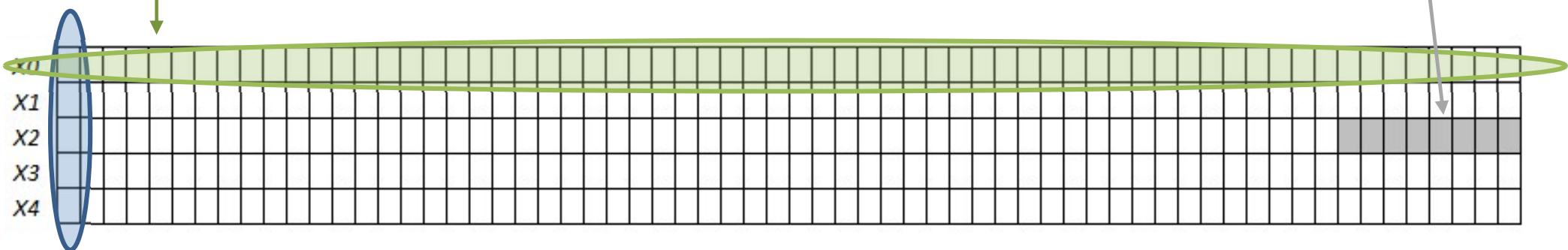
| ACE | ASCON | Bleep64 | Clipadi | CLAE | CLX | COMET | DryGASCON |
|---------------------------|-------------------------------------|------------------|-------------|----------------------|-----------------|--|------------------|
| Elephant | ESTATE | FlexAEAD | ForkAE | Fountain | GAGE and InGAGE | GIFT-COFB | Gimli |
| Grain-128AEAD | HERN & HERON | HYENA | ISAP | KNOT | LAEM | Lilliput-AE | Lindolen |
| LOTUS-AEAD and LOCUS-AEAD | mixFeed | ORANGE | Oribatida | PHOTON-Beetle | Pyjamask | Qameleon | Quartet |
| REMUS | Romulus | SAEAES | Saturnin | Shamash & Shamashash | SIMPLE | STV-Rijndael256 | STV-TEM-PHOTON |
| SKINNY-AEAD /SKINNY-HASH | SNEIK | SPARKLE | SPIX | SpoC | Spook | Subterranean 2.0 | SUNDAE-GIFT |
| Sycon | TGIF (Thank Goddess It's Friday) | TinyJambu | Triad | TRIPLE | WAGE | Xoodyak Joan Daemen ... | Yarara and Coral |

ASCON

- pobjednik u natječaju CAESAR i u NIST-ovom natječaju za kriptografiju prilagođenu uređajima s ograničenim mogućnostima (*lightweight crypto*)
- uz autentifikacijsko kriptiranje (ASCON-128 i ASCON-128a) omogućuje i izračunavanje sažetka poruke (ASCON-HASH i ASCON-XOF)
- jasni tekst M i pridruženi podaci AD (*Associated Data*) se dijele na blokove od po
 - $r=64$ bita = ASCON-128 (broj rundi $b=6$) ili
 - $r=128$ bitova = ASCON-128a (broj rundi $b=8$)
- ključ K je veličine 128 bita kao i *nonce* N i *tag* T
- kriptiranje ili sažimanje obavlja se iterativnom uporabom samo jedne „lagane“ (*lightweight*) funkcije permutacije p koja se sastoji od
 - zbrajanja s konstantom
 - supstitucije (*nonlinear substitution layer*)
 - linearne difuzije (*linear diffusion layer*)

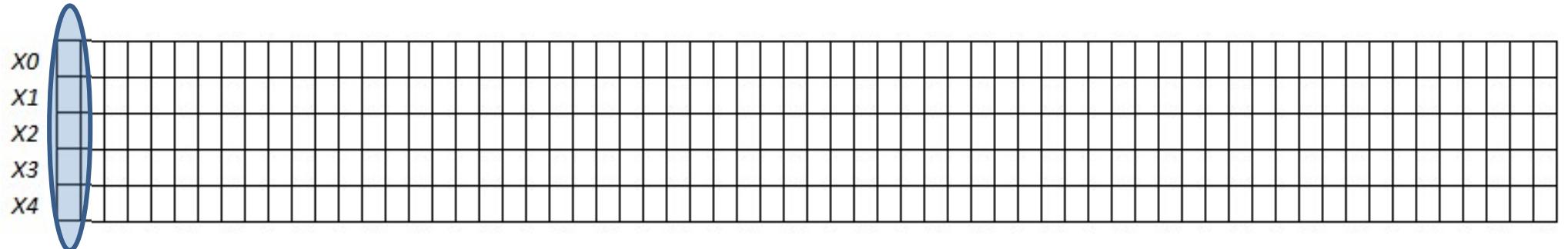
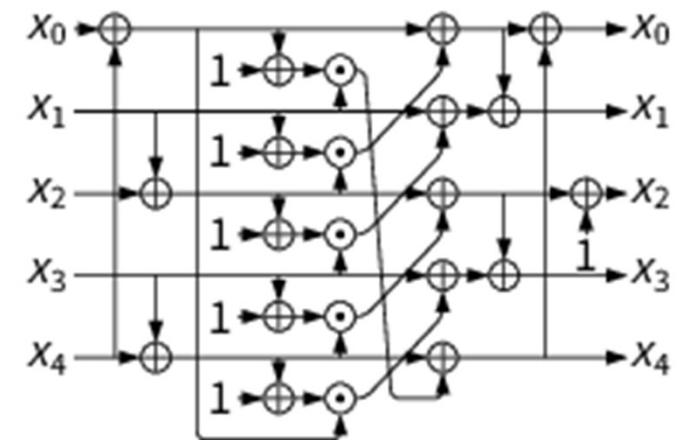
ASCON – permutacija p

- zbrajanja s konstantom Cr (jedan bajt) i to samo nad $X2$
- supstitucije (*nonlinear substitution layer*)
 - S-BOX
 - djeluje nad svim stupcima stanja što se može paralelizirati
- linearne difuzije (*linear diffusion layer*)
 - djeluje nad retcima stanja što se također može paralelizirati



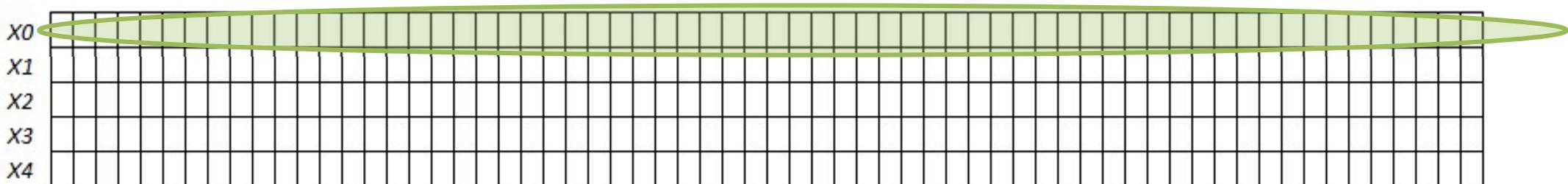
ASCON – permutacija p - supstitucija

- djeluje nad svih 64 stupaca stanja
- umjesto supstitucijske tablice, može se prikazati slikom:
 - slika je preuzeta sa službenih stranica algoritma
<https://ascon.iaik.tugraz.at/specification.html>



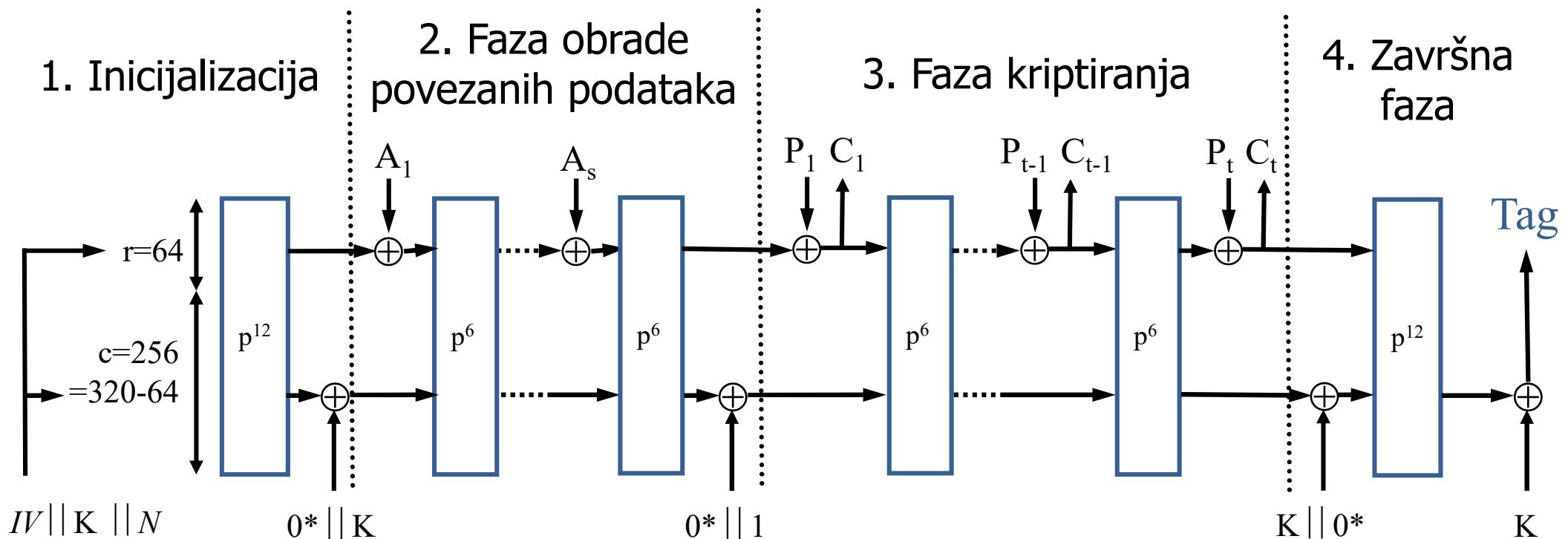
ASCON – permutacija p - difuzija

- djeluje nad svih 5 redaka stanja
- koristi se rotacija, oznaka $<<<$
- zbrajaju se tri varijante svakog retka:
 - $X_0 = X_0 \oplus (X_0 <<< 19) \oplus (X_0 <<< 28)$
 - $X_1 = X_1 \oplus (X_1 <<< 61) \oplus (X_1 <<< 39)$
 - $X_2 = X_2 \oplus (X_2 <<< 1) \oplus (X_2 <<< 6)$
 - $X_3 = X_3 \oplus (X_3 <<< 10) \oplus (X_3 <<< 17)$
 - $X_4 = X_4 \oplus (X_4 <<< 7) \oplus (X_4 <<< 41)$



Dvostruka spužvasta konstrukcija algoritma ASCON-128

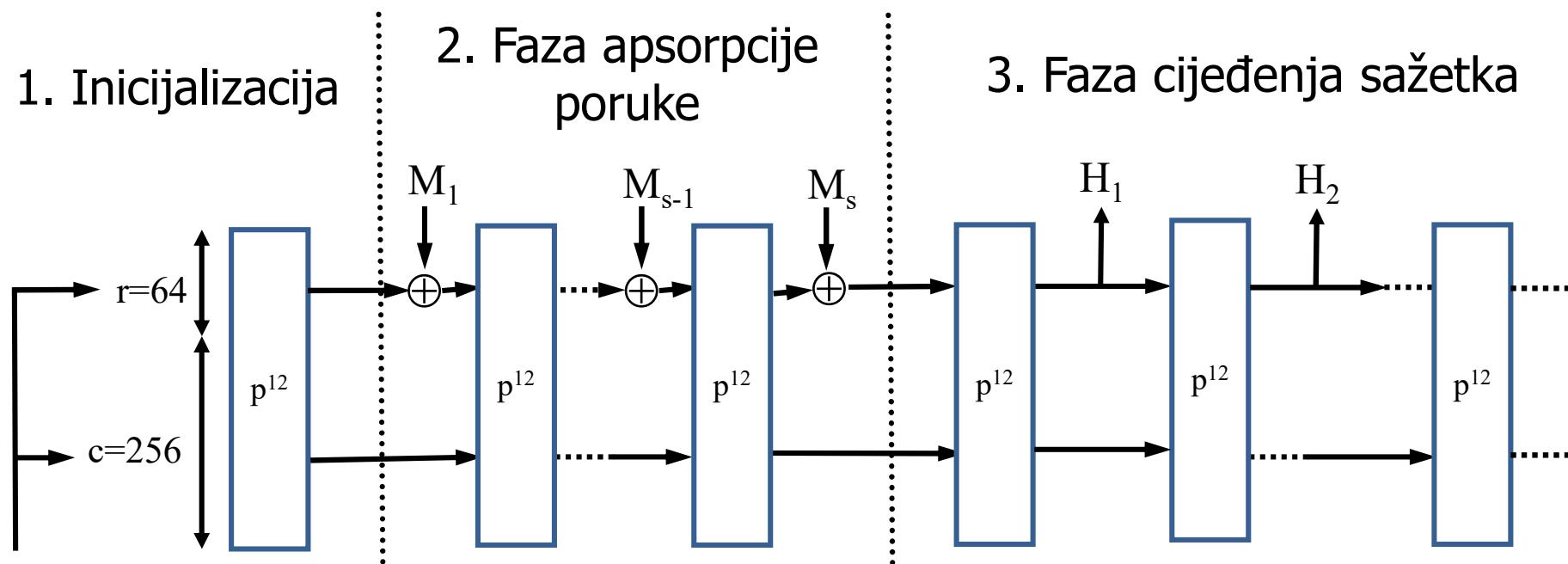
- odvija se u 4 faze
- permutacije se obavljaju ili u 12 ili u 6 rundi
- permutacije kod algoritma **ASCON-128a** se obavljaju ili u 12 ili u **8** rundi



IV je unaprijed određen i iznosi 80400c0600000000

Izračunavanje sažetka uz pomoć algoritma ASCON-HASH

- odvija se u 3 faze
- veličina sažetka najmanje 256 bita
- ima više varijanti, a u ovoj osnovnoj se sve permutacije obavljaju u 12 rundi
- varijanta algoritma ASCON-XOF je jednaka ASCON-HASH, ali sažetak može biti proizvoljne duljine

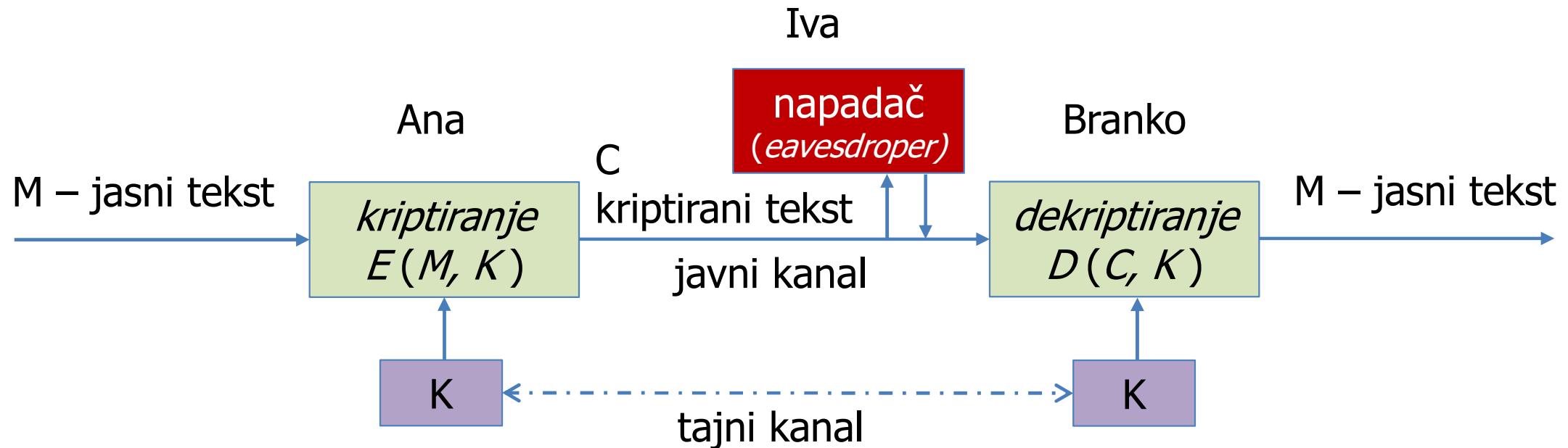


8. Kvantna i postkvantna kriptografija

Kvantna kriptografija

- danas se računalna sigurnost zasniva na nedokazanoj činjenici da **ne postoji djelotvoran algoritam** za faktorizaciju velikih brojeva te za izračun diskretnog logaritma
- Shor, 1994.: kvantni algoritam (može se ostvariti na kvantnom računalu) za brzu faktorizaciju brojeva
- moguće rješenje: protokol QKD
- prvi takav protokol: BB84
 - predložili su ga Charles H.Bennett (IBM) i Gilles Brassard
 - koristi dva kanala: javni i kvantni (optički kabel)

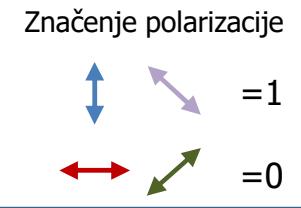
Protokol BB84



4 moguće polarizacije foton-a:

- baza \oplus : foton je ili vertikalno (90°) ili horizontalno (0°) polariziran
- baza \otimes : foton je dijagonalno polariziran (45° ili 135°)

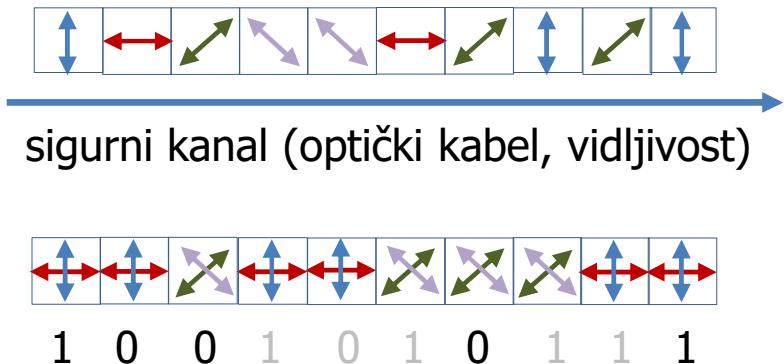
Protokol BB84



- 1 Ana nasumično bira slučajni niz bitova i polarizacija i šalje Branku

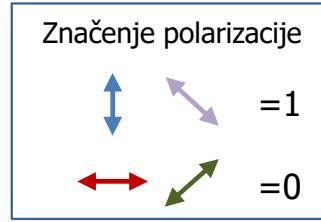


ANA



BRANKO

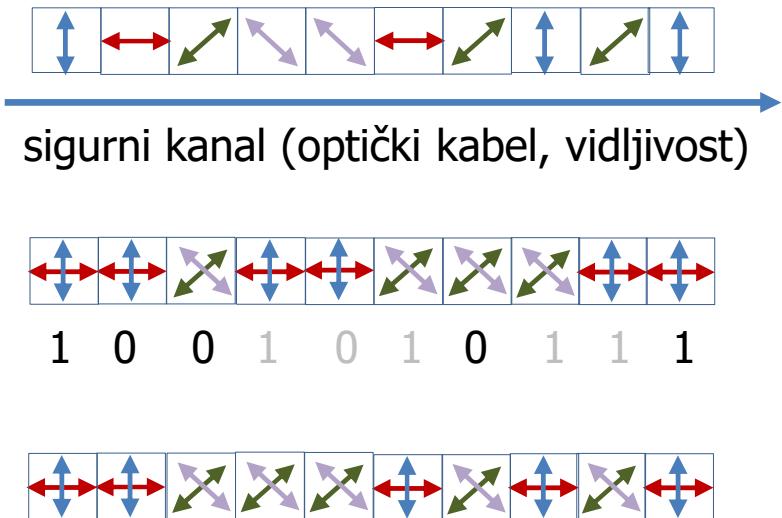
Protokol BB84



- 1 Ana nasumično bira slučajni niz bitova i polarizacija i šalje Branku



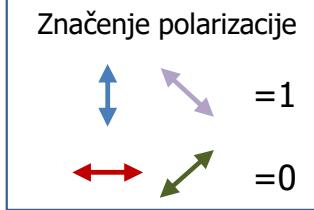
ANA



BRANKO

- 2 Branko primajući fotone nasumično bira polarizaciju i kada pogriješi dobit će kao rezultat s jednakom vjerojatnošću 0 ili 1

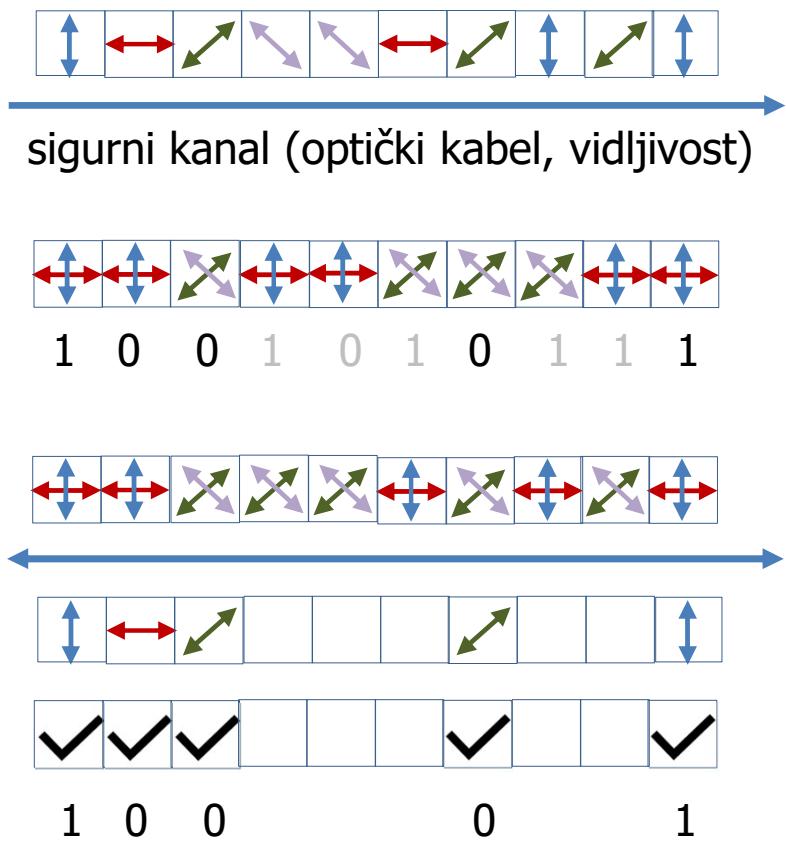
Protokol BB84



- 1 Ana nasumično bira slučajni niz bitova i polarizacija i šalje Branku



ANA



BRANKO

- 2 Branko primajući fotone nasumično bira polarizaciju i kada pogriješi dobit će kao rezultat s jednakom vjerojatnošću 0 ili 1



- 3 Branko koristeći javni kanal (primjerice telefon ili Internet) javi Ani koje je polarizacije koristio, a Ana mu odgovara koje su bile ispravno odabране

- 4 Kada god su Ana i Branko odavrali jednake baze, ti bitovi su zajednički i čine tajni ključ

Prednosti i nedostaci protokola BB84

- sigurnost protokola temelji se na
 - nemogućnosti kloniranja fotona
 - Heisenbergovom principu neodređenosti
- puls polariziranog svjetla s *jednim* fotonom
- mora se ugraditi kod za ispravku pogrešaka koje se javljaju tijekom prijenosa
- duži kabel ili veća udaljenost – veća vjerojatnost pogreške
 - 2004. g.: - max. dužina kabla 60 km
 - max. udaljenost oko 2 km
 - brzina prijenosa ~ 1 kb/s
(a treba 1 Mb/s)
 - 2015.g.: 10 kb/s na udaljenosti od 50 km

- Prvi komercijalni produkt 2002. g



Main features

- First commercial quantum key distribution system
- Key distribution distance: up to 60 km
- Key distribution rate: up to 1000 bits/s
- Compact and reliable

- 2004. g., prva sigurna transakcija između banaka koju je ostvarila grupa prof. Antona Zeilingera na Bečkom sveučilištu primjenivši protokol QKD

Problemi s QKD

- obavezna ili optička vidljivost (koja je nepouzdana) ili optički kabel (bez prekida)
- zahtjeva specijalno sklopolje
- mala brzina, ograničena skalabilnost
- teško integrirati s postojećim kriptografskim sklopoljem
- visoka cijena
- još uvijek u eksperimentalnoj fazi

Post-quantum kriptografija javnog ključa

ili

Asimetrična kriptografija otporna na napade kvantnim računalom

Public-Key Post-Quantum Cryptography

Natječaj

- <https://csrc.nist.gov/Projects/post-quantum-cryptography>
- Na NIST-ovoj radionici 2.4.2015. "Workshop on Cybersecurity in a Post-Quantum World" iskazuje se potreba za novim kriptografskim algoritmima koji su otporni na napade kvantnim računalom.
- Motiv:
 - posljednjih se godina mnogo istražuje u području kvantnih računala
 - ako se ikad izgradi kvantno računalo s velikim brojem q-bitova klasična asimetrična kriptografija će biti kompromitirana (RSA, DSA i ECC)
- NIST raspisuje natječaj 20.12.2016. rok je 30.11.2017.
- predloženi algoritmi moraju zadovoljavati određene uvjete

Tijek natječaja

21.12.2017. NIST objavljuje 69 kandidata koji zadovoljavaju uvjete natječaja

30.1.2019. objavljeno 26 kandidata za drugi krug natječaja

- 17 algoritama za kriptografsku zaštitu javnim ključem i za razmjenu ključeva (*Public-key Encryption and Key-establishment Algorithms*)
- 9 algoritama za digitalni potpis (*Digital Signature Algorithms*)

22.7.2020. objavljeno 15 algoritama za 3. krug

- 4 finalista i 5 zamjenskih kandidata algoritama za kriptografsku zaštitu javnim ključem i za razmjenu ključeva
- 3 finalista i 3 zamjenska kandidata algoritama za digitalni potpis

5.7.2022. objavljeno 4 algoritma koji se šalju u standardizacijski postupak

- 1 algoritam za kriptografsku zaštitu javnim ključem i za razmjenu ključeva i 3 algoritma za digitalni potpis (6.9.2022. raspisuje se natječaj za dodatne alg. DSA), a 4 algoritma za uspostavu ključeva (*Key-establishment Algorithm*) idu u 4. krug

11.3.2025. proglašen pobjednik natječaja za algoritam za uspostavu ključeva

Uvjeti natječaja 1/2

- sigurnost predloženog algoritma se ne smije temeljiti na:
 - nemogućnosti faktorizacije velikih brojeva
 - nemogućnosti izračunavanja inverza diskretnog logaritma
- moguće funkcionalnosti predloženog algoritma su:
 - asimterična kriptografija (*publickey encryption*) i/ili
 - razmjena ključeva (*key exchange, KEM*) i/ili
 - kao i asimetrična kriptografija, služi za razmjenu simetričnog ključa najmanje duljine 256 bita
 - digitalni potpis (*digital signature*)
 - najveća duljina poruke koja se potpisuje je 2^{63} bitova

Uvjeti natječaja 2/2

- pretpostavlja se da napadač nema više od 2^{64} parova (M,C) i napada s odabranim čistim ili kriptiranim tekstrom
- u analizi složenosti napada na predloženi algoritam, sigurnost algoritma će se uspoređivati s napadima na
 - AES128, AES192, AES256
 - SHA256, SHA384, SHA512 odnosno
 - SHA3-256, SHA3-384, SHA3-512

21.12.2017. objavljeno 69 kandidata za prvi krug natječaja

| BIG QUAKE12 | BIKE | CFPKM | Classic McEliece | Compact LWE | CRYSTALS-DILITHIUM | CRYSTALS-KYBER | DAGS |
|-------------------|-----------------------------|----------------------------|------------------|-------------|---------------------|-----------------|-------------|
| Ding Key Exchange | DME | DRS | DualModeMS | Edon-K | EMBLEM and R.EMBLEM | FALCON | FrodoKEM |
| GeMSS | Giophantus | Gravity-SPHINCS | Guess Again | Gui | HILA5 | HiMQ-3 | HK17 |
| HQC | KCL | KINDI | LAC | LAKE | LEDAkem | LEDApkc | Lepton |
| LIMA | Lizard | LOCKER | LOTUS | LUOV | McNie | Mersenne-756839 | MQDSS |
| NewHope | NTRUEncrypt | pqNTRUSign | NTRU-HRSS-KEM | NTRU Prime | NTS-KEM | Odd Manhattan | Ouroboros-R |
| Picnic | Post-quantum RSA-Encryption | Post-quantum RSA-Signature | pqsigRM | QC-MDPC KEM | qTESLA | RaCoSS | Rainbow |
| Ramstake | RankSign | RLCE-KEM | Round2 | RQC | RVB | SABER | SIKE |
| SPHINCS+ | SRTPI | Three Bears | Titanium | WalnutDSA | | | |

Prije drugog kruga autori 5 algoritama su povukli svoje prijave, ostaje 64 kandidata

| BIG QUAKE12 | BIKE | CFPKM | Classic McEliece | Compact LWE | CRYSTALS-DILITHIUM | CRYSTALS-KYBER | DAGS |
|-------------------|-----------------------------|----------------------------|------------------|-------------|---------------------|-----------------|-------------|
| Ding Key Exchange | DME | DRS | DualModeMS | Edon-K | EMBLEM and R.EMBLEM | FALCON | FrodoKEM |
| GeMSS | Giophantus | Gravity-SPHINCS | Guess Again | Gui | HILA5 | HiMQ-3 | HK17 |
| HQC | KCL | KINDI | LAC | LAKE | LEDAkem | LEDApkc | Lepton |
| LIMA | Lizard | LOCKER | LOTUS | LUOV | McNie | Mersenne-756839 | MQDSS |
| NewHope | NTRUEncrypt | pqNTRUSign | NTRU-HRSS-KEM | NTRU Prime | NTS-KEM | Odd Manhattan | Ouroboros-R |
| Picnic | Post-quantum RSA-Encryption | Post-quantum RSA-Signature | pqsigRM | QC-MDPC KEM | qTESLA | RaCoSS | Rainbow |
| Ramstake | RankSign | RLCE-KEM | Round2 | RQC | RVB | SABER | SIKE |
| SPHINCS+ | SRTPI | Three Bears | Titanium | WalnutDSA | | | |

U prvom krugu otpala 33 algoritma

| BIG QUAKE12 | BIKE | CFPKM | Classic McEliece | Compact LWE | CRYSTALS-DILITHIUM | CRYSTALS-KYBER | DAGS |
|--------------------------|------------------------------------|-----------------------------------|-------------------------|--------------------|----------------------------|------------------------|--------------------|
| Ding Key Exchange | DME | DRS | DualModeMS | Edon-K | EMBLEM and R.EMBLEM | FALCON | FrodoKEM |
| GeMSS | Giophantus | Gravity-SPHINCS | Guess Again | Gui | HILA5 | HiMQ-3 | HK17 |
| HQC | KCL | KINDI | LAC | LAKE | LEDAkem | LEDApkc | Lepton |
| LIMA | Lizard | LOCKER | LOTUS | LUOV | McNie | Mersenne-756839 | MQDSS |
| NewHope | NTRUEncrypt | pqNTRUSign | NTRU-HRSS-KEM | NTRU Prime | NTS-KEM | Odd Manhattan | Ouroboros-R |
| Picnic | Post-quantum RSA-Encryption | Post-quantum RSA-Signature | pqsigRM | QC-MDPC KEM | qTESLA | RaCoSS | Rainbow |
| Ramstake | RankSign | RLCE-KEM | Round2 | RQC | RVB | SABER | SIKE |
| SPHINCS+ | SRTPI | Three Bears | Titanium | WalnutDSA | | | |

... a neki su se udružili

- LEDAcrypt = LEDAkem + LEDApkc
- NTRU = NTRUEncrypt + NTRU-HRSS-KEM
- ROLLO = LAKE + LOCKER + Ouroboros-R
- Round5 = HILA5 + Round2

| BIG QUAKE12 | BIKE | CFPKM | Classic McEliece | Compact LWE | CRYSTALS-DILITHIUM | CRYSTALS-KYBER | DAGS |
|-------------------|-----------------------------|----------------------------|------------------|-------------|---------------------|-----------------|-------------|
| Ding Key Exchange | DME | DRS | DualModeMS | Edon-K | EMBLEM and R.EMBLEM | FALCON | FrodoKEM |
| GeMSS | Giophantus | Gravity-SPHINCS | Guess Again | Gui | HILA5 | HiMQ-3 | HK17 |
| HQC | KCL | KINDI | LAC | LAKE | LEDAkem | LEDApkc | Lepton |
| LIMA | Lizard | LOCKER | LOTUS | LUOV | McNie | Mersenne-756839 | MQDSS |
| NewHope | NTRUEncrypt | pqNTRUSign | NTRU-HRSS-KEM | NTRU Prime | NTS-KEM | Odd Manhattan | Ouroboros-R |
| Picnic | Post-quantum RSA-Encryption | Post-quantum RSA-Signature | pqsigRM | QC-MDPC KEM | qTESLA | RaCoSS | Rainbow |
| Ramstake | RankSign | RLCE-KEM | Round2 | RQC | RVB | SABER | SIKE |
| SPHINCS+ | SRTPI | Three Bears | Titanium | WalnutDSA | | | |

30.1.2019. objavljeno 26 kandidata za drugi krug natječaja

| BIG QUAKE12 | BIKE | CFPKM | Classic McEliece | Compact LWE | CRYSTALS-DILITHIUM | CRYSTALS-KYBER | DAGS |
|-------------------|-----------------------------|----------------------------|------------------|-------------|---------------------|-----------------|-------------|
| Ding Key Exchange | DME | DRS | DualModeMS | Edon-K | EMBLEM and R.EMBLEM | FALCON | FrodoKEM |
| GeMSS | Giophantus | Gravity-SPHINCS | Guess Again | Gui | HILA5 | HiMQ-3 | HK17 |
| HQC | KCL | KINDI | LAC | LAKE | LEDAkem | LEDApkc | Lepton |
| LIMA | Lizard | LOCKER | LOTUS | LUOV | McNie | Mersenne-756839 | MQDSS |
| NewHope | NTRUEncrypt | pqNTRUSign | NTRU-HRSS-KEM | NTRU Prime | NTS-KEM | Odd Manhattan | Ouroboros-R |
| Picnic | Post-quantum RSA-Encryption | Post-quantum RSA-Signature | pqsigRM | QC-MDPC KEM | qTESLA | RaCoSS | Rainbow |
| Ramstake | RankSign | RLCE-KEM | Round2 | RQC | RVB | SABER | SIKE |
| SPHINCS+ | SRTPI | Three Bears | Titanium | WalnutDSA | | | |

26 algoritama za 2. krug je podijeljeno u dvije skupine

Algoritmi za razmjenu ključeva (17)

Public-key Encryption and Key-establishment Algorithms

| | | | | | | | |
|-------------|------------------|----------------|----------|--------|-----|-----------|---------|
| BIKE | Classic McEliece | CRYSTALS-KYBER | FrodoKEM | HQC | LAC | LEDAcrypt | NewHope |
| NTRU | NTRU Prime | NTS-KEM | ROLO | Round5 | RQC | SABER | SIKE |
| Three Bears | | | | | | | |

Algoritmi za digitalni potpis (9)

Digital Signature Algorithms

| | | | | | | | |
|--------------------|--------|-------|------|-------|--------|--------|---------|
| CRYSTALS-DILITHIUM | FALCON | GeMSS | LUOV | MQDSS | Picnic | qTESLA | Rainbow |
| SPHINCS+ | | | | | | | |

22.7.2020. objavljeno 15 algoritama za 3. krug

Algoritmi za kriptografsku zaštitu javnim ključem i za razmjenu ključeva
(4 finalista i 5 zamjenskih kandidata)

Public-key Encryption and Key-establishment Algorithms

| | | | | | | | |
|---------------------------|--|--------------------------------------|----------|--------|-----|-----------|---------|
| BIKE | Classic McEliece Bernstein, ... | CRYSTALS-KYBER Peter Schwabe, ... | FrodoKEM | HQC | LAC | LEDAcrypt | NewHope |
| NTRU ... Peter Schwabe | NTRU Prime Bernstein, Tanja Lange, ... | NTS-KEM | ROLO | Round5 | RQC | SABER | SIKE |
| Three Bears | | | | | | | |

Algoritmi za digitalni potpis (3 finalista i 3 zamjenska kandidata)
Digital Signature Algorithms

| | | | | | | | |
|---|--------|-------|------|-------|--------|--------|---------|
| CRYSTALS-DILITHIUM ... Peter Schwabe | FALCON | GeMSS | LUOV | MQDSS | Picnic | qTESLA | Rainbow |
| SPHINCS+ Bernstein, T. Lange, P. Schwabe, ... | | | | | | | |

5.7.2022. objavljeno 4 algoritma koji se šalju u standardizacijski postupak i ...

Jedan algoritam algoritma za kriptografsku zaštitu javnim ključem (*Public-key Encryption*) i

| BIKE | Classic McEliece | CRYSTALS-KYBER | FrodoKEM | HQC | LAC | LEDAcrypt | NewHope |
|-------------|---|----------------|----------|--------|-----|-----------|---------|
| NTRU | NTRU Prime | NTS-KEM | ROLO | Round5 | RQC | SABER | SIKE |
| Three Bears | CRYSTALS-Kyber is Lattice-based; NP problem: Learning with Errors | | | | | | |

tri algoritma za digitalni potpis (*Digital Signature Algorithms*)

| CRYSTALS-DILITHIUM | FALCON | GeMSS | LUOV | MQDSS | Picnic | qTESLA | Rainbow |
|--------------------|---|-------|------|-------|--------|--------|---------|
| SPHINCS+ | CRYSTALS-Dilithium and Falcon are Lattice-based; NP problem: Short Integer Solution SPHINCS+ is Hash-based - relies on collision resistance and pre-image resistance of cryptographic hash functions | | | | | | |

... i 4 algoritma za razmjenu, odnosno uspostavu ključeva (*Key-establishment Algorithm*) idu u 4. krug natječaja

| BIKE | Classic McEliece | CRYSTALS-KYBER | FrodoKEM | HQC | LAC | LEDAcrypt | NewHope |
|-------------|------------------|----------------|----------|--------|-----|-----------|---------|
| NTRU | NTRU Prime | NTS-KEM | ROLO | Round5 | RQC | SABER | SIKE |
| Three Bears | | | | | | | |

2023. autori W. Castryck i T. Decru u radu "An efficient key recovery attack on sidh," su pokazali uspješan napad na SIKEp434 u svega 10 min na samo jednoj jezgri

11.3.2025. proglašen pobjednik 4. krug natječaja za algoritam uspostave tajnog ključa *(Key-establishment Algorithm)*

| BIKE | Classic McEliece | CRYSTALS-KYBER | FrodoKEM | HQC | LAC | LEDAcrypt | NewHope |
|-------------|------------------|----------------|----------|--------|-----|-----------|---------|
| NTRU | NTRU Prime | NTS-KEM | ROLO | Round5 | RQC | SABER | SIKE |
| Three Bears | | | | | | | |

CRYSTALS-KYBER – 5.7.2022. odabran algoritam za kriptografsku zaštitu javnim ključem

HQC – 11.3.2025. odabran algoritam uspostave tajnog ključa

6.9.2022. NIST raspisuje natječaj za dodatne algoritme za digitalni potpis uz 3 PQ-DSA algoritma koji su poslani na standardizaciju

| | | | | | | | |
|--------------------|--------|-------|------|-------|--------|--------|---------|
| CRYSTALS-DILITHIUM | FALCON | GeMSS | LUOV | MQDSS | Picnic | qTESLA | Rainbow |
| SPHINCS+ | | | | | | | |

rok za dostavu algoritama bio je 1.6.2023.

40 prispjelih kandidata je razvrstan u 7 kategorija:

- **Code-based Signatures** (Based on decoding random linear codes, considered infeasible for both classical and quantum computers.)
- **Isogeny Signatures** (Difficulty in computing isogenies between elliptic curves, even for quantum computers.)
- **Lattice-based Signatures** (Hardness of finding short vectors in lattices; enables security against quantum attacks.)
- **MPC-in-the-Head Signatures**
- **Multivariate Polynomials** (Hard to solve systems of multivariate quadratic equations over finite fields.)
- **Symmetric-based Signatures**
- **Ostali**

17.6.2023. objavljeno 40 kandidata za PQ DSA za 1. krug natječaja

<https://csrc.nist.gov/Projects/pqc-dig-sig/round-1-additional-signatures>

| CROSS | Enhanced pqsigRM | FuLeeca | LESS | MEDS | Wave | SQIsign | EagleSign |
|-----------------|------------------|---------------|-------|--------------|-----------|----------|----------------|
| EHTv3 and EHTv4 | HAETAE | HAWK | HuFu | Raccoon | SQUIRRELS | Biscuit | MIRA |
| MiRitH | MQOM | PERK | RYDE | SDiTH | 3WISE | DME-Sign | HPPC |
| MAYO | PROV | QR-UOV | SNOVA | TUOV | UOV | VOX | AIMer |
| Ascon-Sign | FAEST | SPHINCS-alpha | ALTEQ | eMLE-Sig 2.0 | KAZ-SIGN | Preon | Xifrat1-Sign.I |

Code-based Signatures (6)

Isogeny Signatures (1)

Lattice-based Signatures (7)

MPC-in-the-Head Signatures (7)

Multivariate Signatures (10)

Symmetric-based Signatures (4)

Ostali (5)

29.8.2024. objavljeno 12 kandidata za PQ DSA za 2. krug natječaja

<https://csrc.nist.gov/Projects/pqc-dig-sig/round-2-additional-signatures>

| CROSS | Enhanced pqsigRM | FuLeeca | LESS | MEDS | Wave | SQIsign | EagleSign |
|-----------------|------------------|---------------|-------|--------------|-----------|----------|----------------|
| EHTv3 and EHTv4 | HAETAE | HAWK | HuFu | Raccoon | SQUIRRELS | Biscuit | MIRA |
| MiRitH | MQOM | PERK | RYDE | SDiTH | 3WISE | DME-Sign | HPPC |
| MAYO | PROV | QR-UOV | SNOVA | TUOV | UOV | VOX | AIMer |
| Ascon-Sign | FAEST | SPHINCS-alpha | ALTEQ | eMLE-Sig 2.0 | KAZ-SIGN | Preon | Xifrat1-Sign.I |

Code-based Signatures (2)

Isogeny Signatures (1)

Lattice-based Signatures (1)

MPC-in-the-Head Signatures (5)

Multivariate Signatures (4)

Symmetric-based Signatures (1)

Ostali (0)

Napadi na PQC

- 2023. autori W. Castryck i T. Decru u radu “An efficient key recovery attack on sidh,” su pokazali uspješan napad na SIKEp434 u svega 10 min na samo jednoj jezgri
- 10. mj 2025. danski znanstvenici postigli znatan pomak u kriptoanalizi PQ kriptosustava zasnovanih na rešetkama*

* Lynn Engelberts, Yanlin Chen, Amin Shiraz Gilani, Maya-Iggy van Hoof, Stacey Jeffery, Ronald de Wolf; [An Improved Quantum Algorithm for 3-Tuple Lattice Sieving](#), dostupno na <https://arxiv.org/pdf/2510.08473>

Problemi s implementacijom algoritama PQC

Računalno su zahtjevni

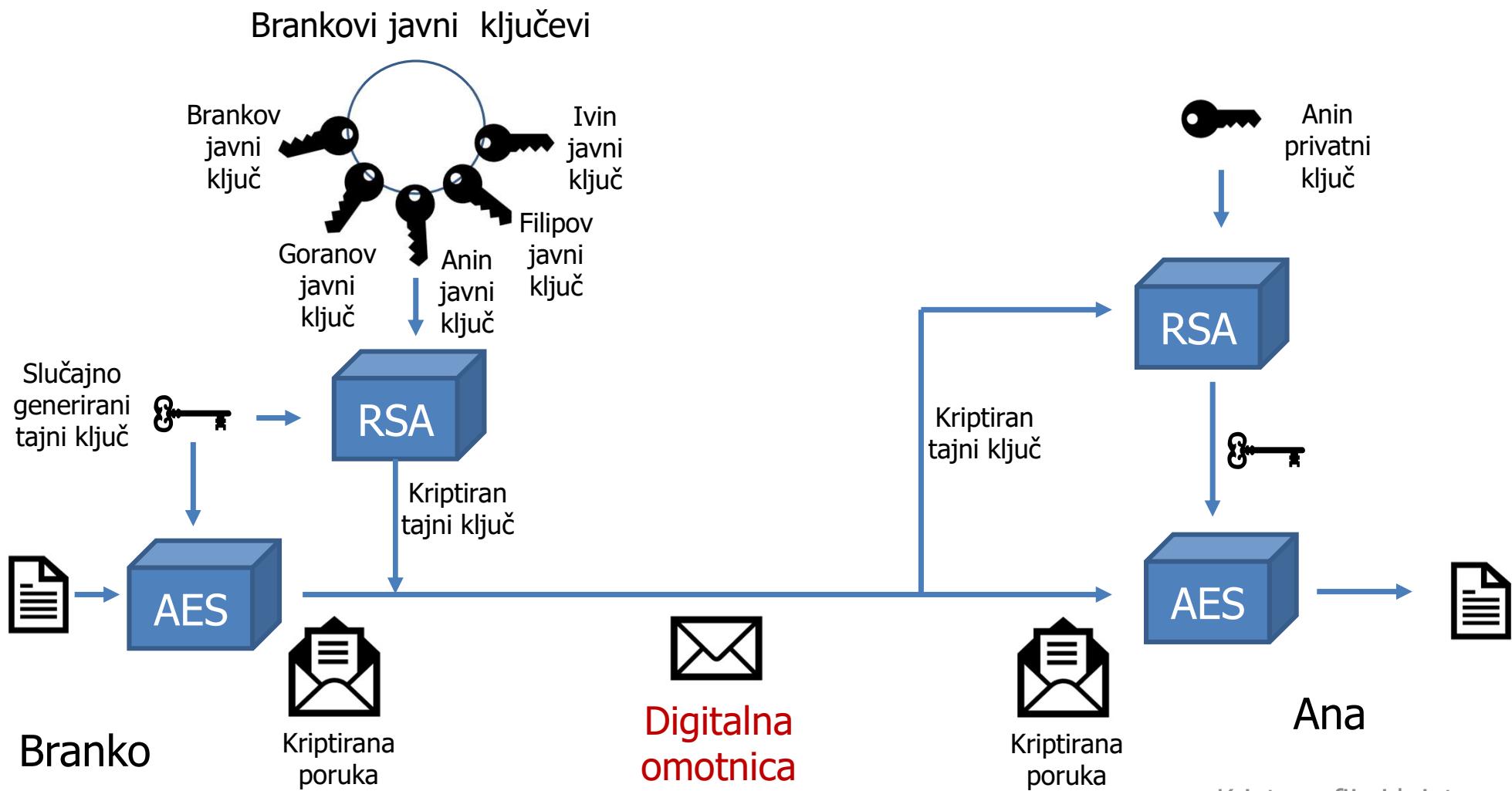
- veliki ključevi
- CPU zahtjevni
 - = > teško ostvarivi sigurnosni sklopovali moduli
(engl. *Hardware Security Module, HSM*) odgovarajućih performansi

Digitalna omotnica

- osigurava tajnost
- pošiljatelj kriptira poruku *proizvoljnim* ključem K simetričnim algoritmom kriptiranja
- simetrični (sjednički) ključ K se kriptira javnim ključem primatelja P_B
- kriptirana poruka i kriptirani ključ čine digitalnu omotnicu

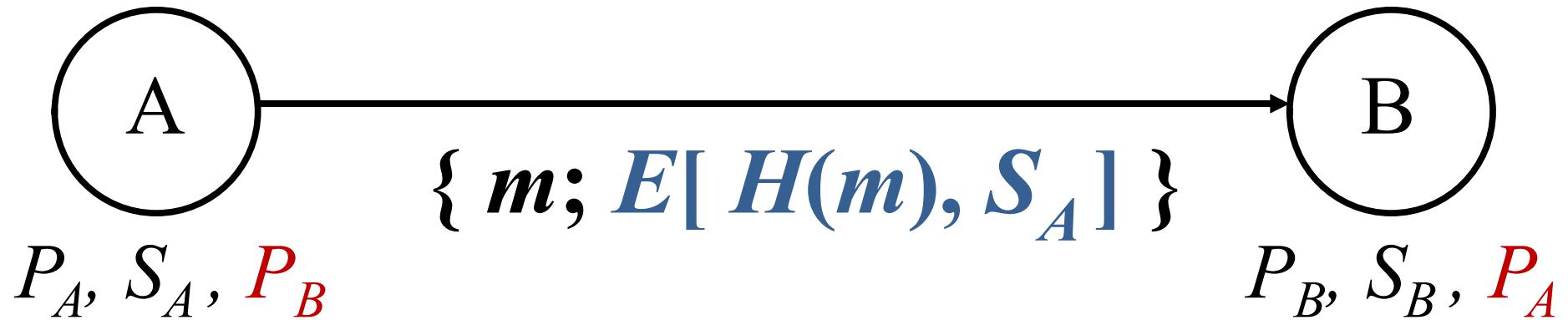


Kako osigurati tajnost?

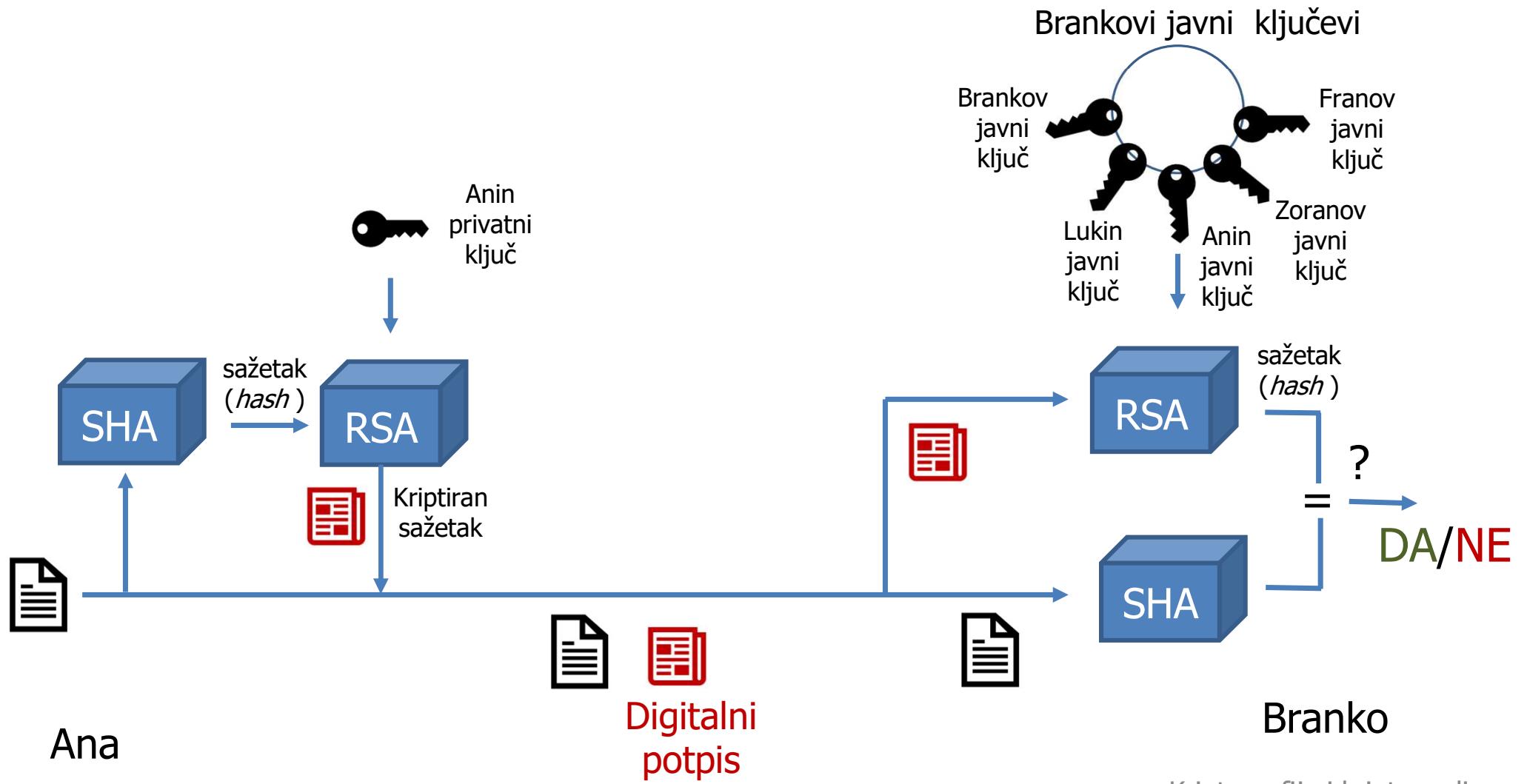


Digitalni potpis

- dodatak poruci koji služi za
 - utvrđivanje bespriječnosti informacije (integritet i neporecivost) i za
 - identifikaciju pošiljatelja (autentičnost)
- ne osigurava tajnost!



Kako osigurati integritet, autentičnost i neporecivost?



Digitalni pečat (1/2)

- digitalni pečat osigurava sva četiri sigurnosna zahtijeva:
 - tajnost
 - autentičnost
 - integritet i
 - neporecivost
- digitalni pečat je digitalno potpisana digitalna omotnica

$$\{ E(m,K); E(K,P_B) \}; E\{ H [E(m,K); E(K,P_B)], S_A \}$$

Digitalni pečat (2/2)

- češće se koristi obrnuti postupak:
 1. digitalno se potpiše poruka
 2. poruka s potpisom se kriptira slučajno generiranim tajnim ključem K
 3. na kraju se dodaje kriptirani ključ javnim ključem primatelja
- digitalna omotnica s digitalno potpisanim porukom:

$$E\{ [m; \underbrace{E(H(m), S_A)}_{\text{digitalni potpis}}], K \}; E(K, P_B)$$