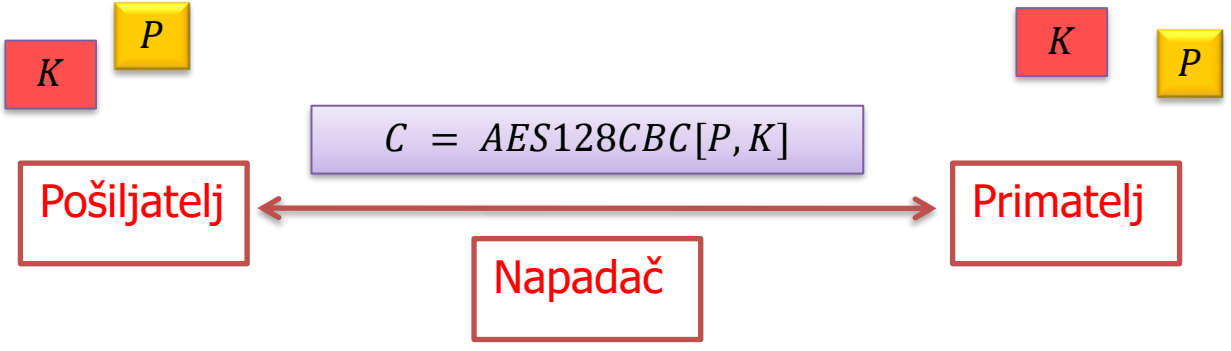
6.
Asimetrični kriptosustavi

Digitalni potpis zasnovan na RSA

Digitalni potpis zasnovan na diskretnom logaritmu

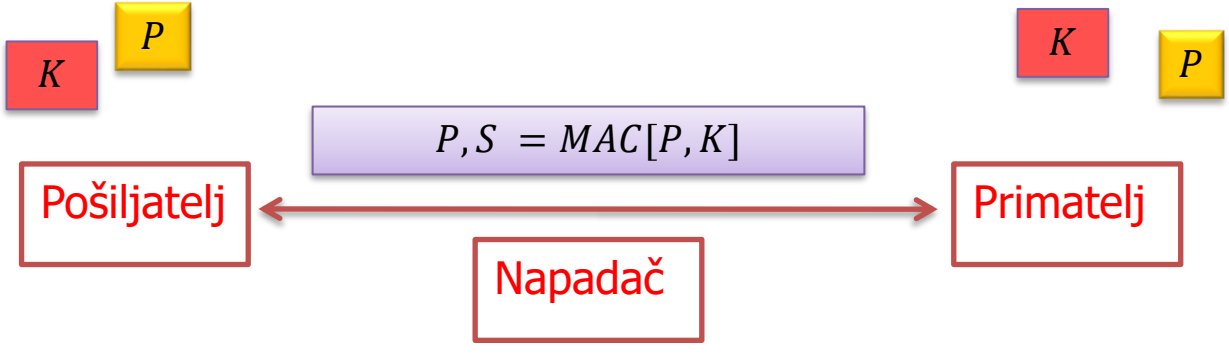
Enkripcija ne rješava sve probleme!



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

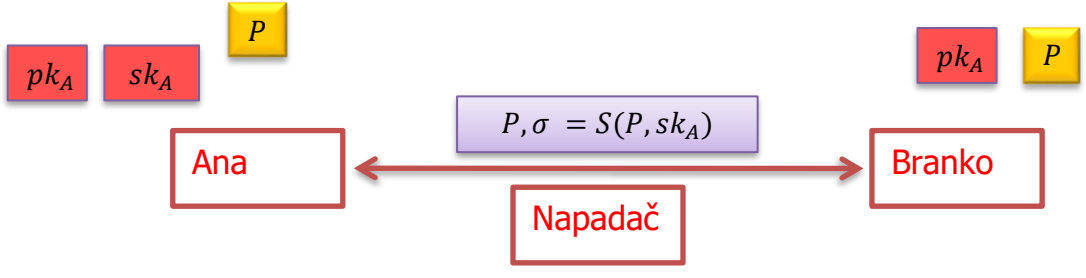
MAC / Autentificirana enkripcija

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

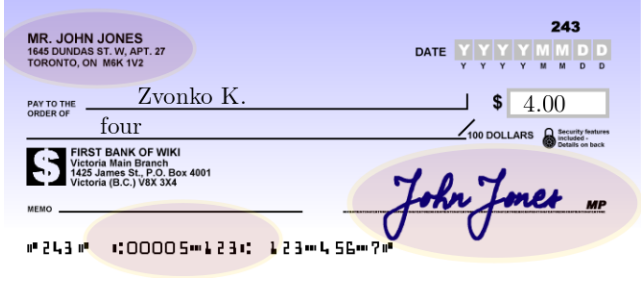


Javni i tajni ključevi

- 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



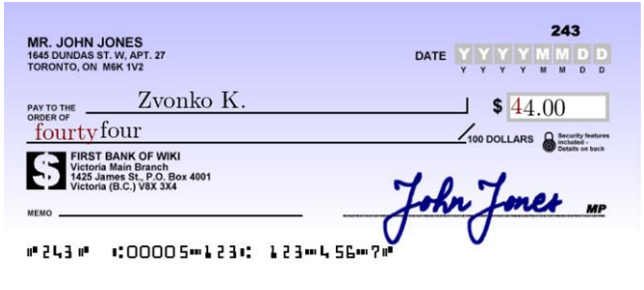
Digitalni vs analogni potpis – autentičnost



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?

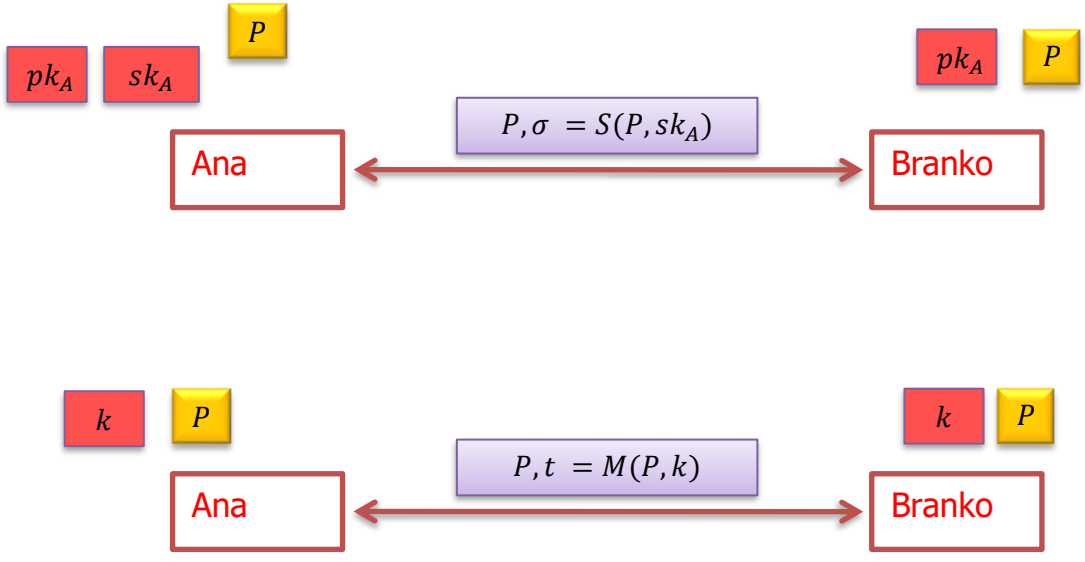
Digitalni vs analogni potpis – integritet



Izvor: wikipedia.org

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

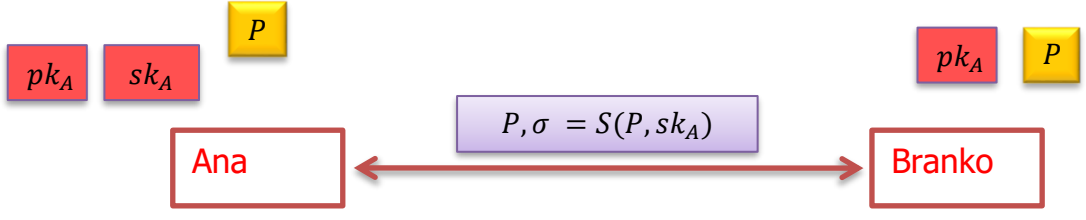
Digitalni potpis vs MAC – neporecivost (non-repudiation)



- 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 $V(p, S(p, sk), pk) = 1$

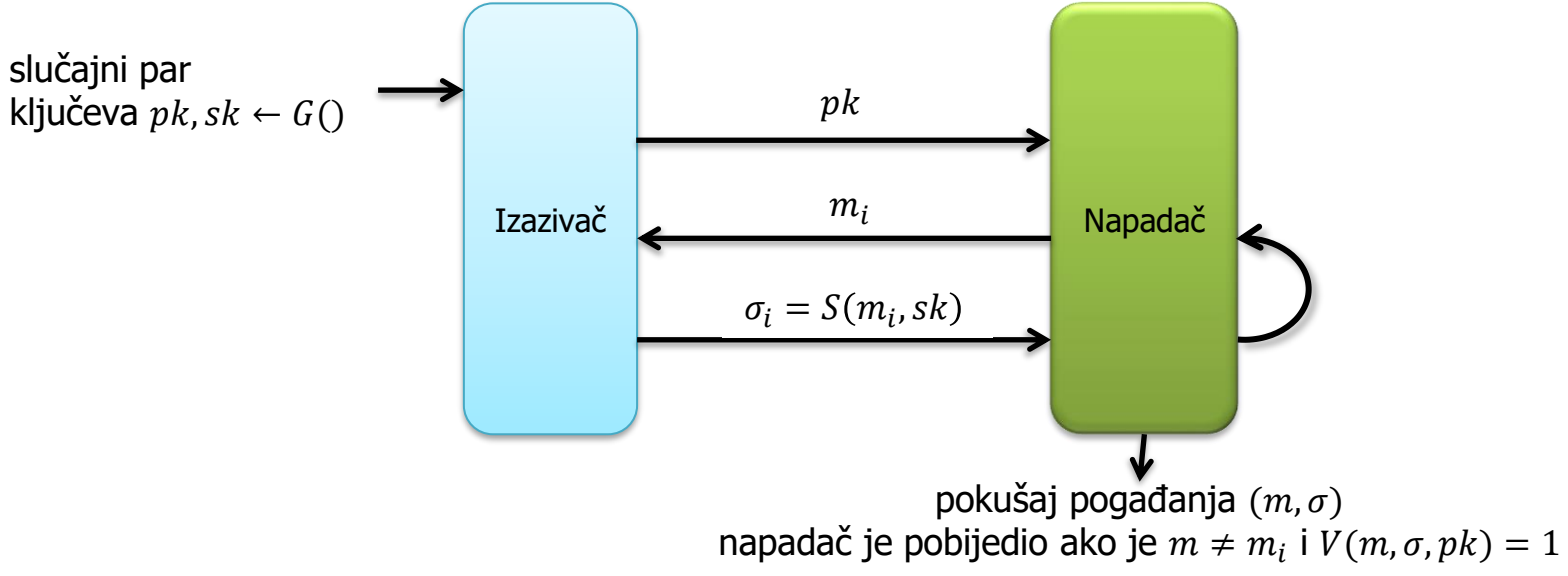


Sustav digitalnog potpisa – sigurnost

- 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

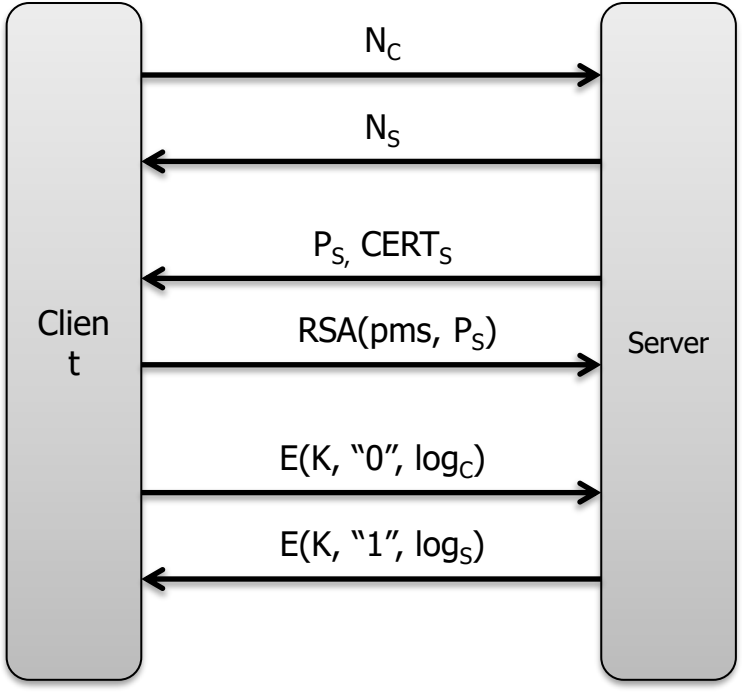
Nemogućnost krivotvorenja potpisa bilo kakve poruke pod napadom odabranom porukom (*existential unforgeability under chosen message attack):* Mti jedan algoritam koji koristi razumne resurse ne može pobijediti u sljedećoj igri s vjerojatnošću nezanemarivo većom od nule.

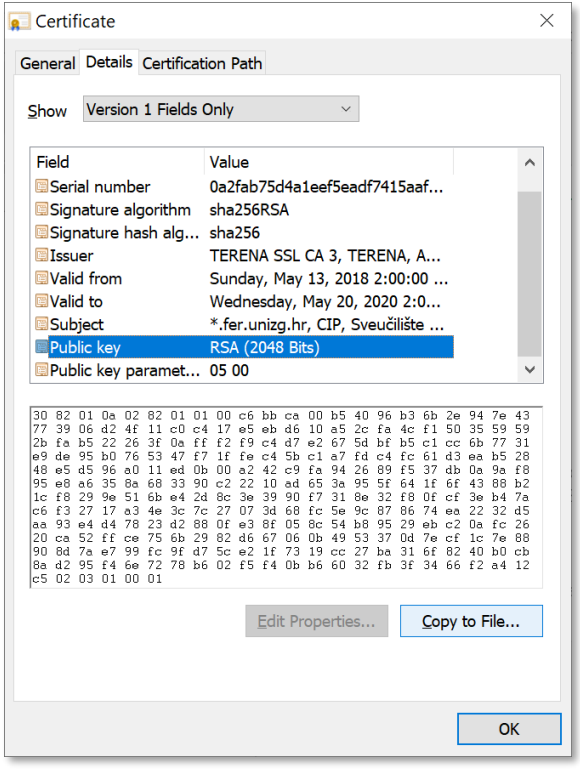


Digitalni potpis – primjene

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

Primjena – TLS protokol

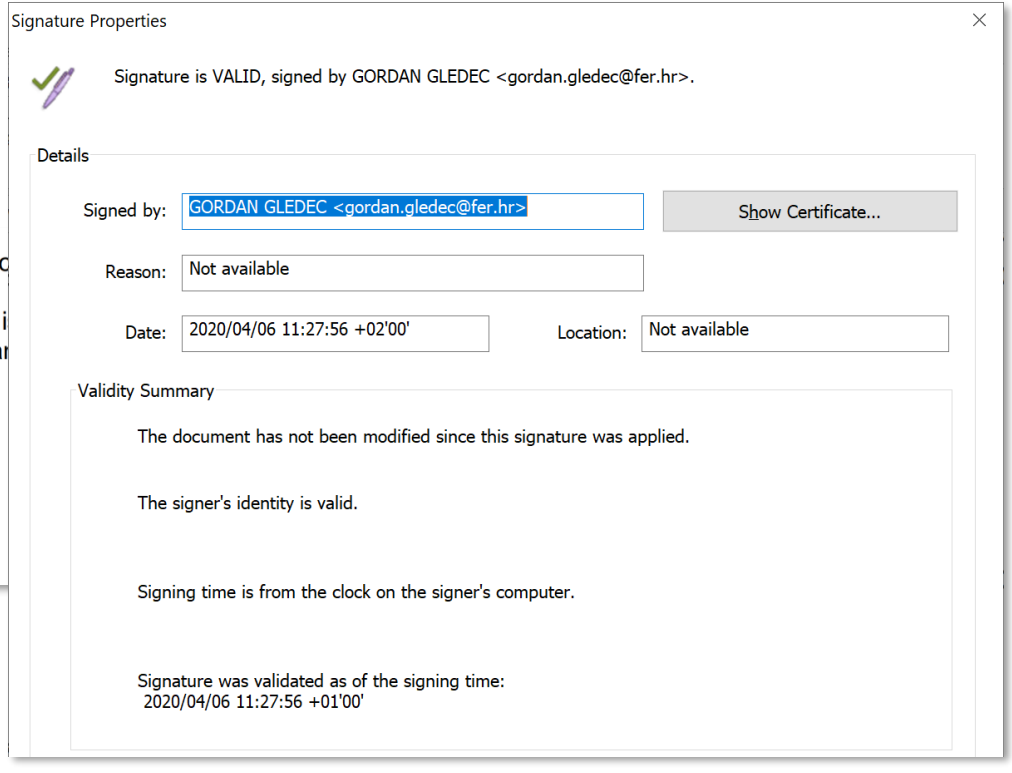




Primjena – e-Dokumenti

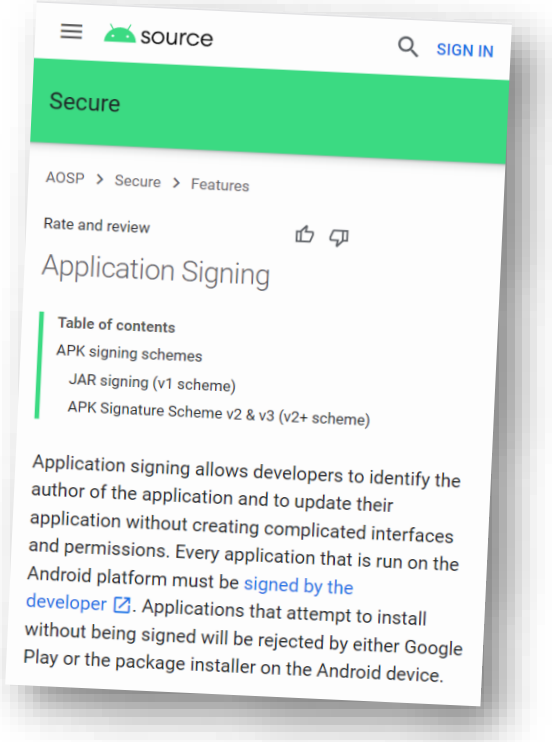
- ovisno o razvoju situacije, razmotrit će se uvo

II. Ova odluka je privremenog karaktera, donosi se i
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.



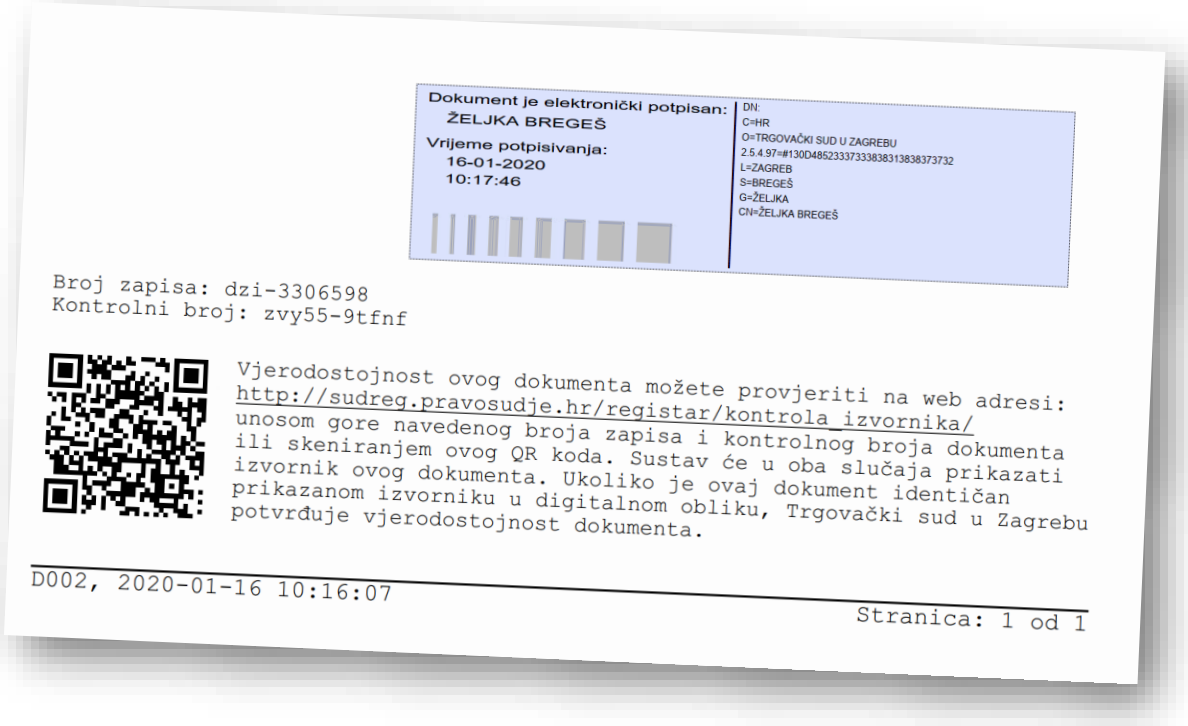
Izvor: source.android.com

Primjena – COVID potvrde

Izvor: Interoperability of health certificates Trust framework

Što sve *nije* digitalni potpis?

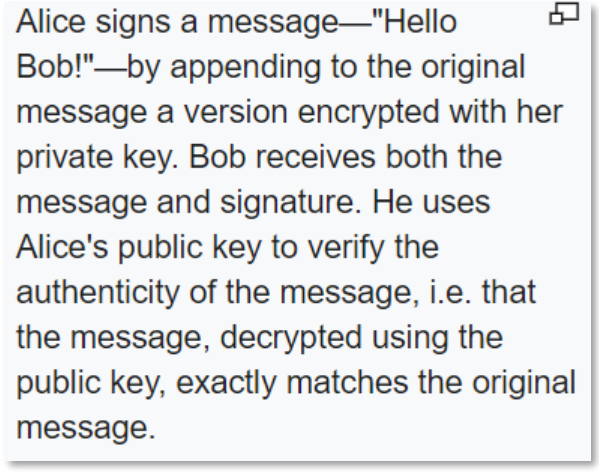
- Tekst koji kaže da je dokument digitalno potpisan.
- Broj koji omogućuje dohvaćanje originalnog dokumenta online.
- QR kod.
- Slika analognog potpisa.
- …



Primjeri sustava digitalnog potpisa

- RSA (1978)
  - teorija brojeva, sigurnost povezana s problemom faktorizacije
- McEliece (1978)
  - teorija kodiranja, sigurnost povezana s problemom dekodiranja općenitog linearnog 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



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

- 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

„Obični RSA” digitalni potpis

Algoritam S:

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

Algoritam V:

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

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?

- $m_1, \sigma_1 = m_1^d$ u $\mathbb{Z}_N$
- $m_2, \sigma_2 = m_2^d$ u $\mathbb{Z}_N$
- $\sigma_1 \cdot \sigma_2 = m_1^d \cdot m_2^d = (m_1 \cdot m_2)^d$ 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 konkretne poruke m po njegovom izboru.

RSA digitalni potpis

H – kriptografska funkcija sažetka
Pad – funkcija nadopunjavanja

Algoritam S:

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

Algoritam V:

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

Zadatak: Obični RSA potpis 3

- Zašto isti napad više ne radi?

RSA digitalni potpis – Padding

- Hash poruke se uvijek nadopunjuje na zadanu 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.

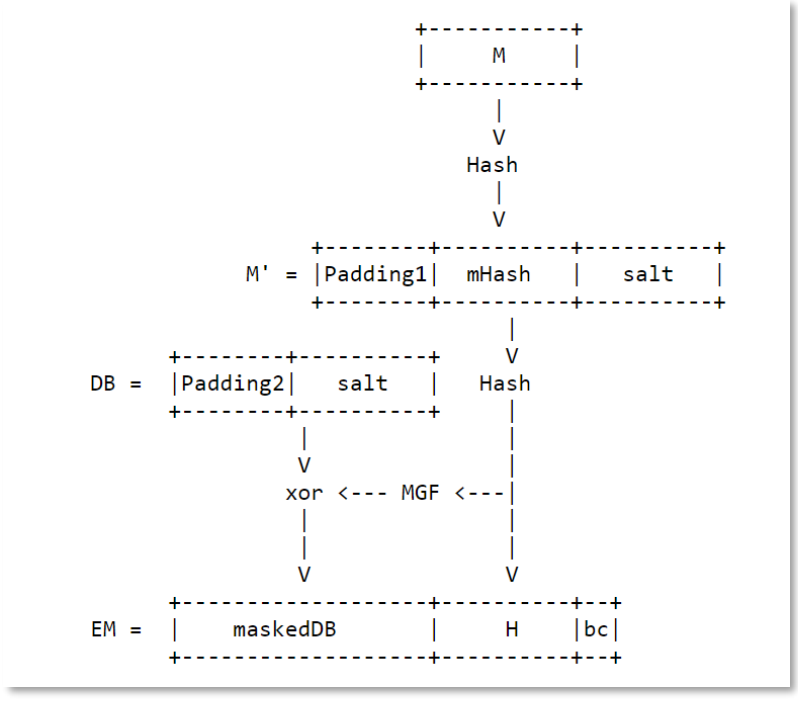
5. Concatenate PS, the DER encoding T, and other padding to form the encoded message EM as

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

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

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)*



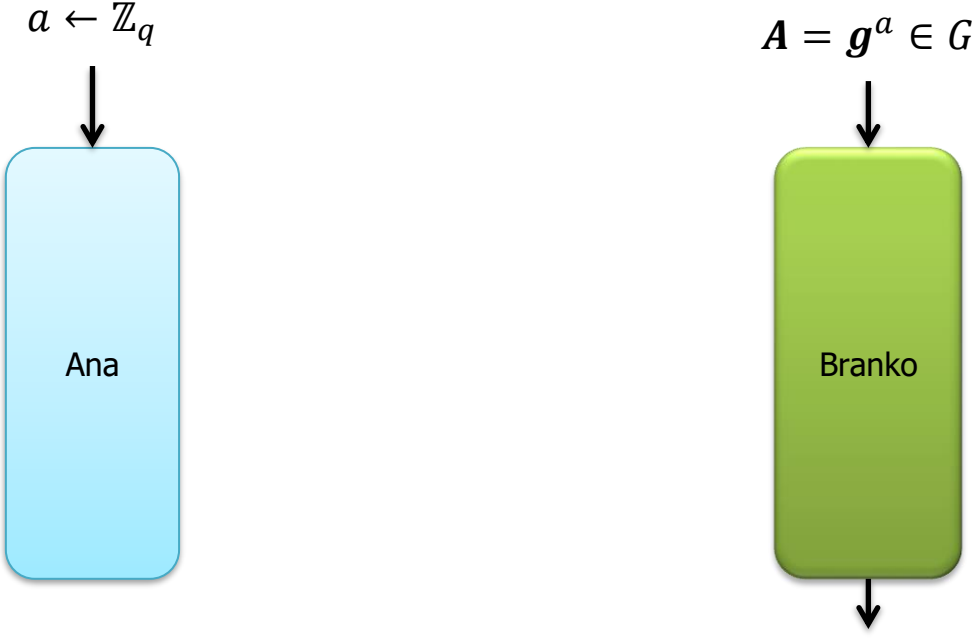
Izvor: https://datatracker.ietf.org/doc/html/rfc8017

Digitalni potpisi zasnovani na problemu diskretnog logartima

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

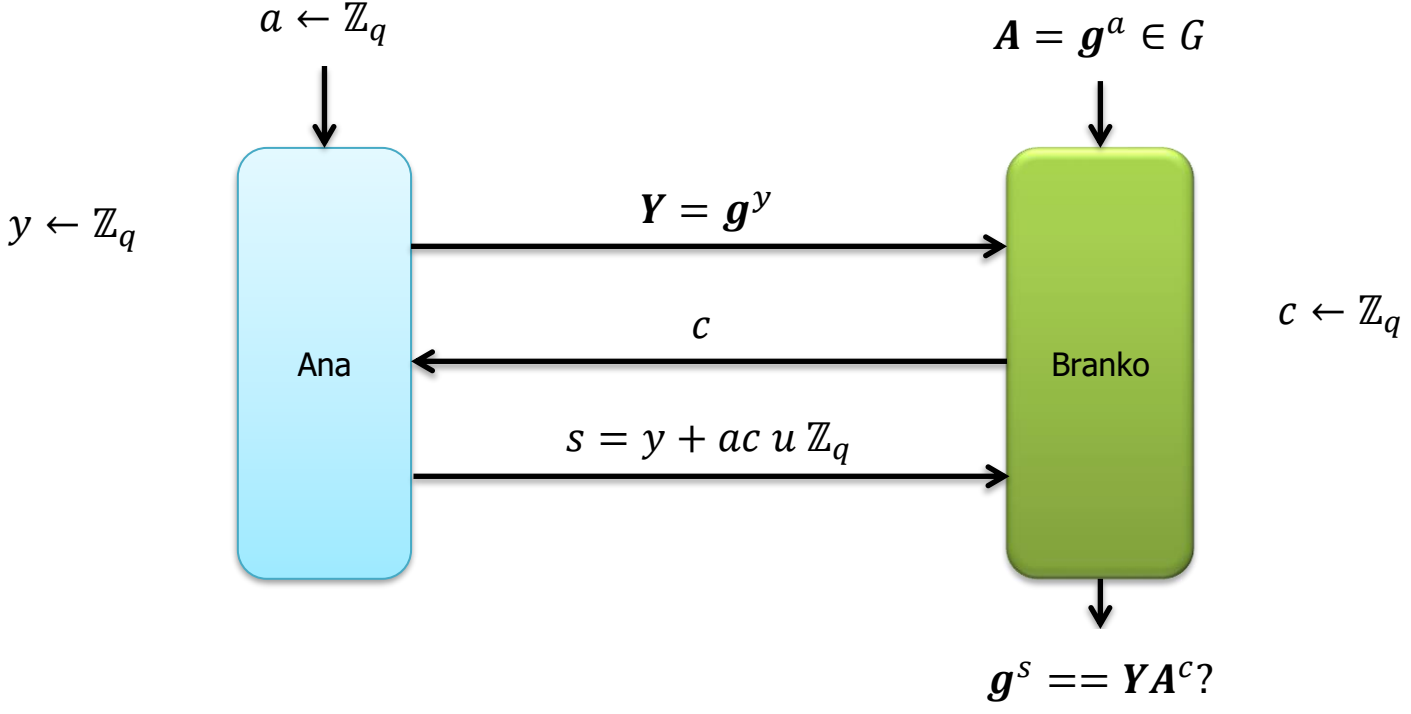
Schnorrov identifikacijski protokol

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

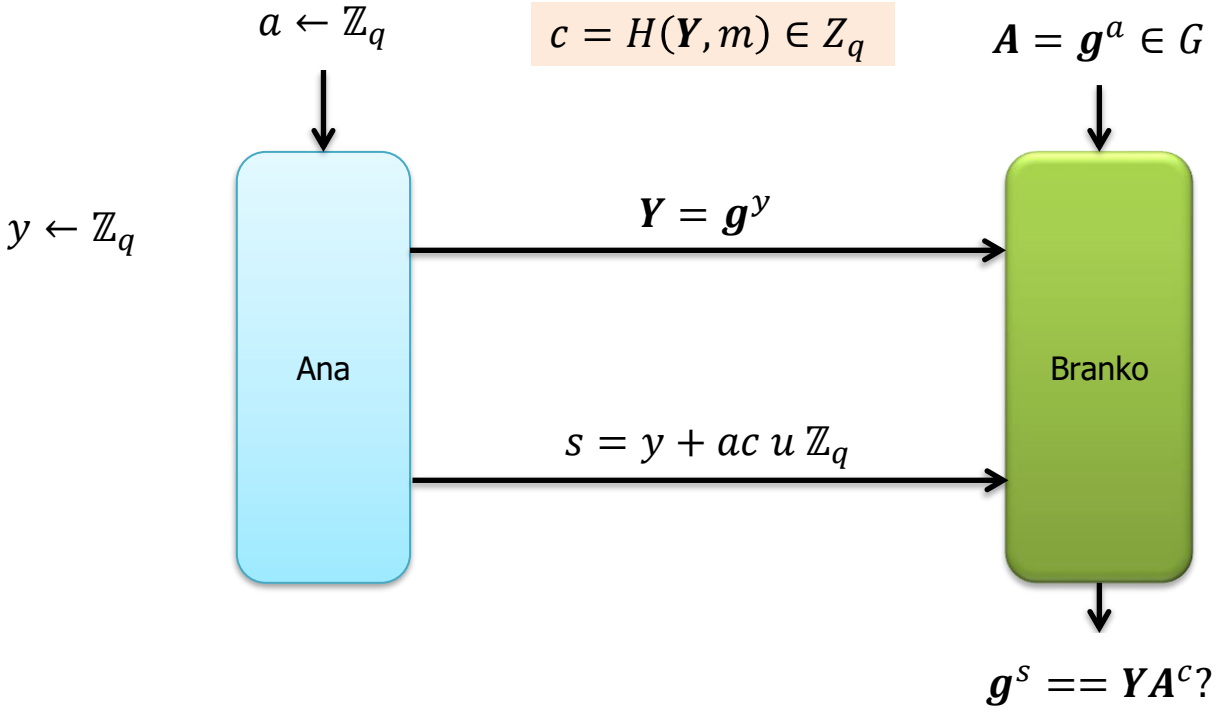


Schnorrov identifikacijski protokol

Kako Ana može dokazati Branku da posjeduje privatni ključ $a \in \mathbb{Z}_q$ koji odgovara javnom ključu $\boldsymbol{A} = \boldsymbol{g}^a \in G$, 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 $\boldsymbol{A} = \boldsymbol{g}^a$
3. Javni ključ je $\boldsymbol{A} \in G$
4. Privatni ključ je $a \in Z_q$

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 $\boldsymbol{Y} = \boldsymbol{g}^y$
3. Izračunam $c = H(\boldsymbol{Y}, m)$
4. Izračunam $s = y + a\,c$ u $\mathbb{Z}_q$

Potpis je par $(\boldsymbol{Y}, s)$

Algoritam V:

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

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

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.

Izvor: Digital Signature Standard (DSS) (FIPS 186-5), draft, 2019.

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 $\boldsymbol{A} = \boldsymbol{g}^a$
3. Javni ključ je $\boldsymbol{A} \in G$
4. Privatni ključ je $a \in Z_q$

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 $\boldsymbol{Y} = \boldsymbol{g}^y$
3. Izračunam $r = F(\boldsymbol{Y})$
4. Izračunam $s = y^{-1}(H(m) + ar)$ u $\mathbb{Z}_q$
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 $\boldsymbol{A}$

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

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 $s \equiv (SHA(x) + d \cdot r)\, {k_E}^{-1} \bmod q$.

Izvor: Christof Paar, Jan Pelzl, Understanding Cryptography

DSA na Z_p^*

- *Prime-order subgroup*
  - Računamo u $(\mathrm{Z}_\mathrm{p}^*,*)$ 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 bizova)

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 $F((x, y)) = x \bmod \mathrm{q}$.

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 $s \equiv (h(x) + d \cdot r)\, {k_E}^{-1} \bmod q$.