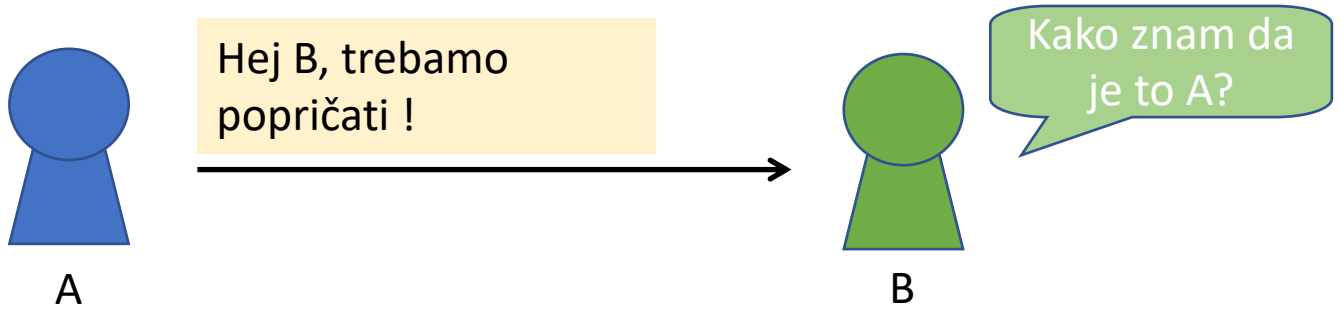
Otvoreno računarstvo

9. Osnove sigurnosti

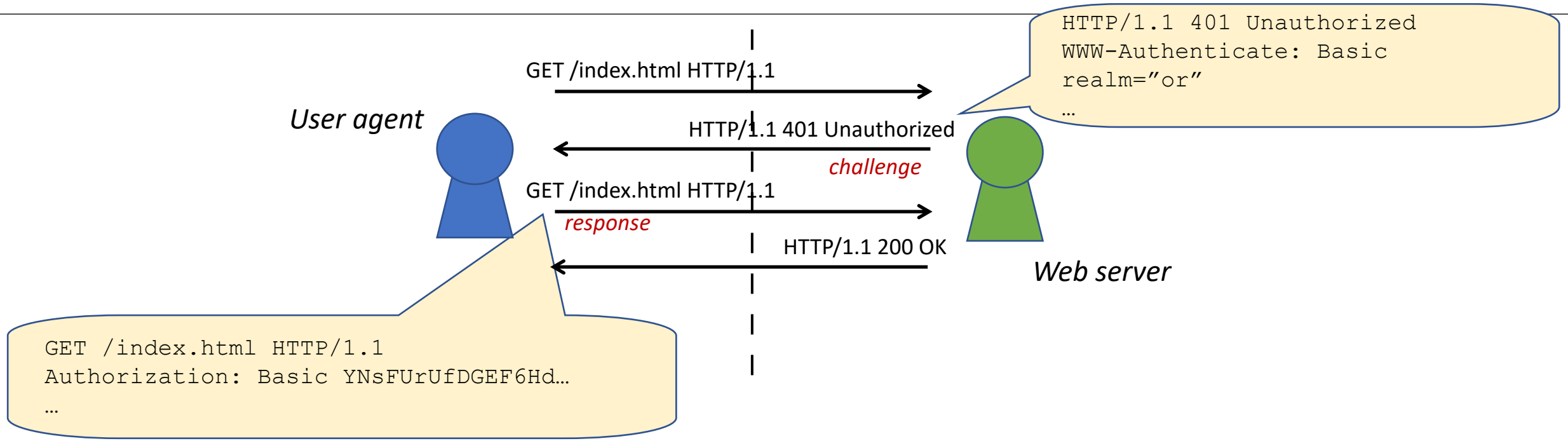
- Osnovi pojmovi
- Osnovni algoritmi
- Složeniji algoritmi i postupci
- Sigurnost u mrežnoj komunikaciji

Protokoli *challenge – response* (I)



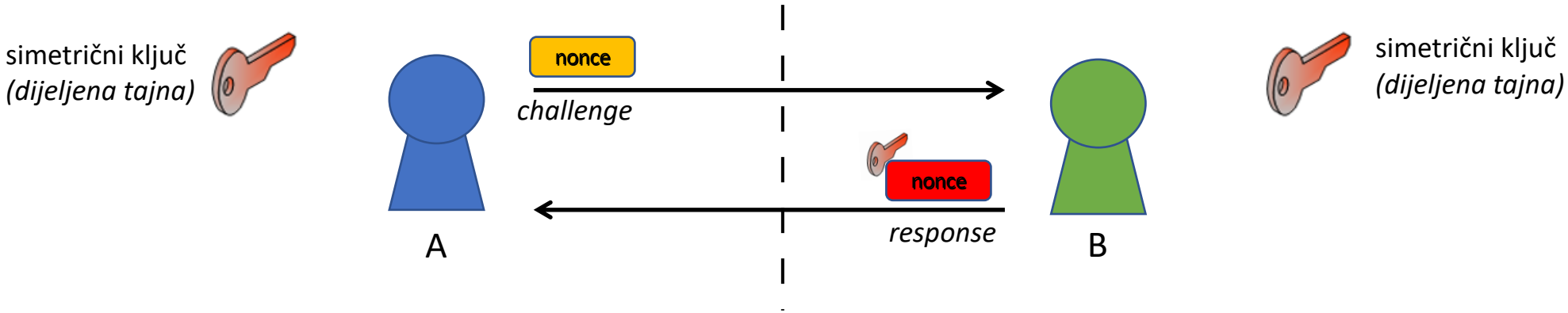
- Dva entiteta u komunikaciji – dokaz identiteta?
- Pretpostavimo da oba entiteta dijele tajnu – tijekom uspostave komunikacije jedan ili oba entiteta trebaju drugoj strani dokazati da znaju tu dijeljenu tajnu (engl. shared secret)
  - One-way challenge-response – samo klijent ili samo poslužitelj dokazuju identitet
  - Two-way challenge-response – obje strane u komunikaciji dokazuju identitet
- Tajna može biti *par korisničko ime - lozinka*, *simetrični ključ* …
- Prenošenje tajne komunikacijskim kanalom:
  - Korišteno - problem presretanja, utjelovljenja druge strane u komunikaciji
  - Nije korišteno – znanje tajne nedvosmisleno se dokazuje drugoj strani u komunikaciji korištenjem kriptografskih metoda

Challenge-response u protokolu HTTP



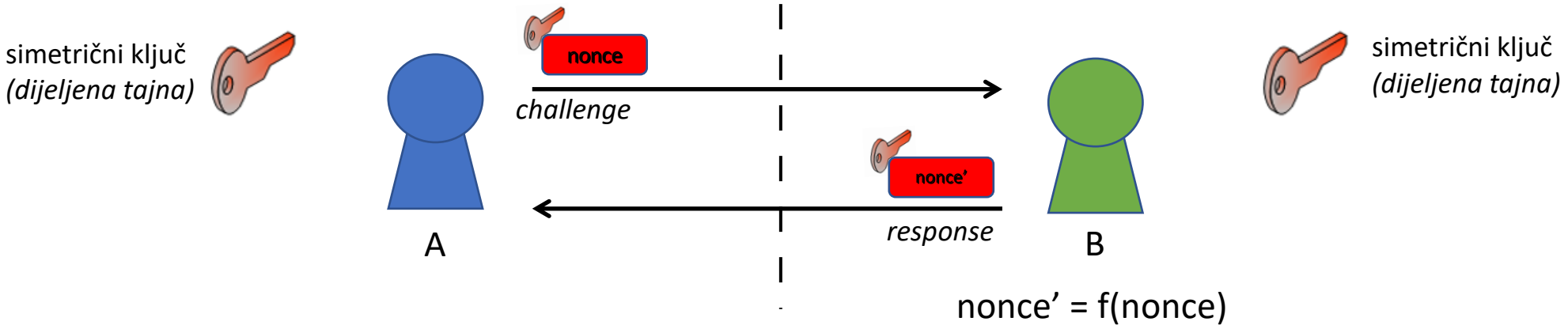
- Zahtjev za štićenim resursom
  - Poslužitelj odbija zahtjev i pruža upute o traženoj metodi autorizacije (Basic)
  - Klijent otvara *username-password* dijalog korisniku preglednika
  - Klijent ponovno šalje zahtjev s uključenim autorizacijskim podacima
    - HTTP – protokol bez čuvanja stanja
    - Base64 kodirani niz znakova *username:password* -> vrlo nesigurno preko HTTP kanala (HTTPS je prihvatljiv)
    - Par *username-password* je dijeljena tajna između korisnika i poslužitelja

Protokoli *challenge – response* (II)



- Naivna implementacija protokola *challenge-response*
  - Oba entiteta imaju dijeljenu tajnu – simetrični ključ
  - Entitet koji inicira dokazivanje identiteta druge strane u komunikaciji pošalje jednokratni, slučajno generirani podatak (engl. nonce)
  - Entitet koji dokazuje identitet vraća nonce šifriran simetričnim ključem
  - Entitet koji je inicirao dokazivanje uspoređuje primljeni šifrirani nonce sa svojim šifriranim nonce
- U čemu je problem?

Protokoli *challenge – response* (III)

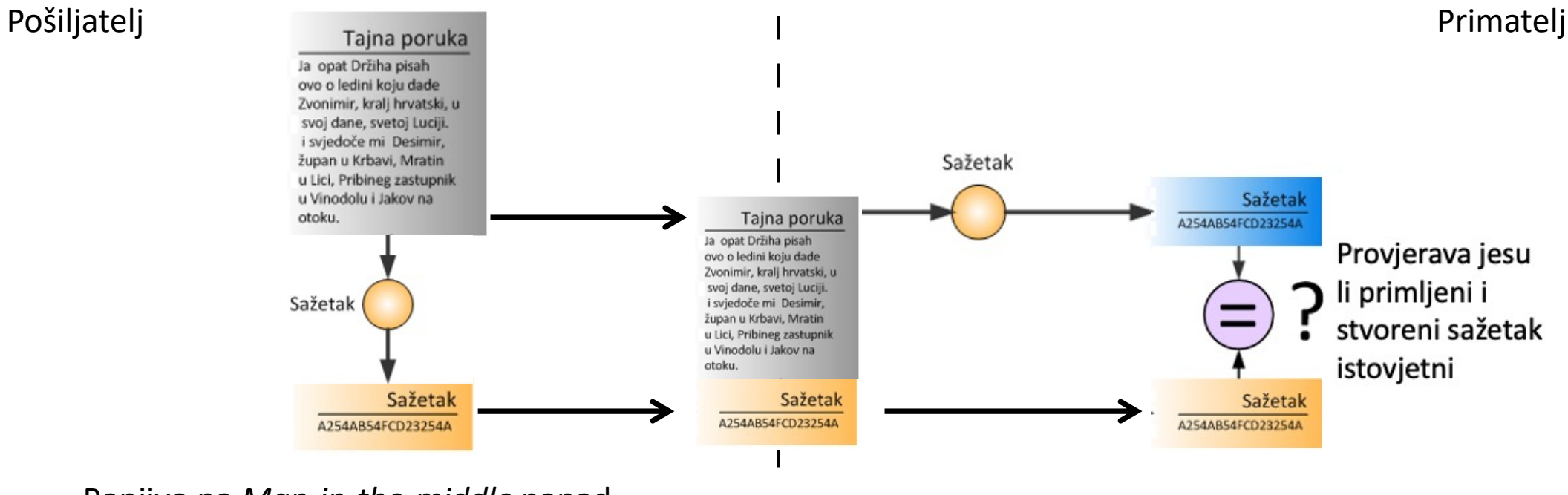


- Uobičajena implementacija protokola *challenge-response*
  - Oba entiteta imaju dijeljenu tajnu – simetrični ključ
  - Entitet koji inicira dokazivanje identiteta druge strane u komunikaciji pošalje jednokratni, slučajno generirani podatak (engl. nonce) šifriran simetričnim ključem
  - Entitet koji dokazuje identitet vraća f(nonce) šifriran simetričnim ključem
  - Entitet koji je inicirao dokazivanje uspoređuje primljeni šifrirani f(nonce) sa svojim šifriranim f(nonce)

- Primjeri funkcija transformacije *challenge informacije*
  - funkcija sažetka (md5, sha256 …)
  - KERBEROS: nonce – slučajno stvoren broj n, f(nonce) = nonce + 1

Message Authentication Code – MAC (I)

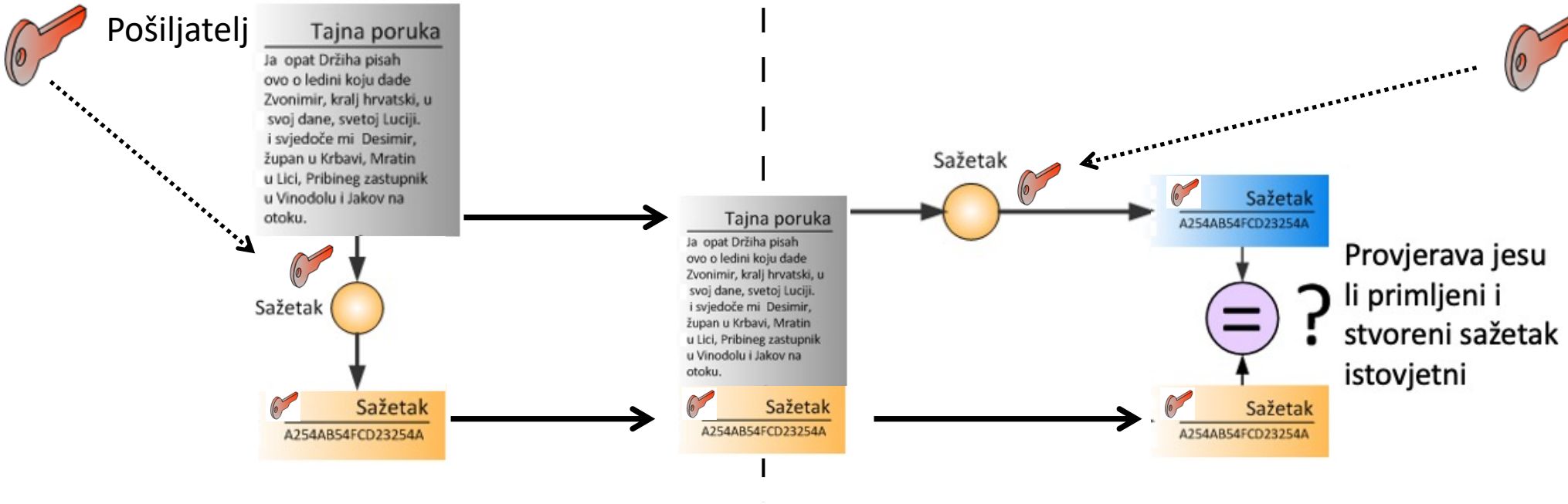
- Pošiljatelj treba poslati poruku primatelju, cjelovitost i integritet poruke moraju biti očuvani tijekom prijenosa
- Primjer 1 – gdje je tu problem (?)?:
  - pošiljatelj generira sažetak poruke D = d(P), šalje sažetak D i poruku P primatelju
  - primatelj prima sažetak D' i poruku P', generira D'' = d(P') i provjerava D' == D''



Ranjivo na *Man-in-the-middle* napad

Message Authentication Code – MAC (II)

- Pošiljatelj treba poslati poruku primatelju, cjelovitost i integritet poruke moraju biti očuvani tijekom prijenosa
- I pošiljatelji i primatelj imaju zajedničku tajnu (npr. simetrični ključ)
- Primjer 2 – gdje je tu problem (?)?:
  - osoba A generira sažetak poruke D = d(P + tajna), šalje sažetak D i poruku P osobi B
  - osoba B prima sažetak D' i poruku P', generira D'' = d(P' + tajna) i provjerava D' == D''



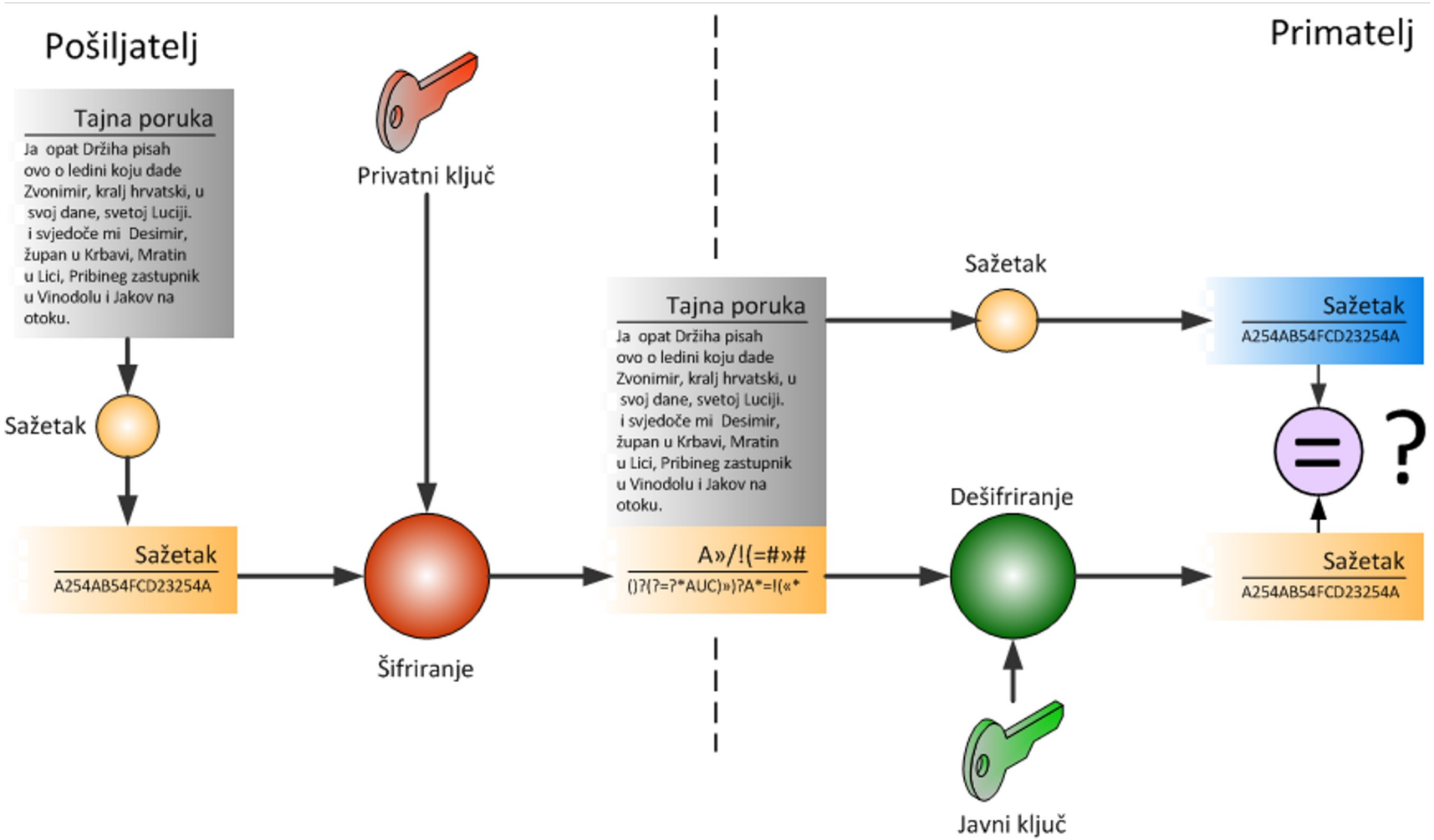
Štiti od *Man-in-the-middle* napada, jamči integritet, ali ne i neporecivost (npr. osoba A može tvrditi da je poruku stvorila osoba B jer i ona ima ključ)

Digitalni potpis (I)

- Pošiljatelj generira sažetak poruke S
- Pošiljatelj šifrira sažetak ključem Pk (privatni ključ pošiljatelja)
  - ključ (Pk) ostaje u posjedu pošiljatelja
- Pošiljatelj dodaje šifrirani sažetak na poruku

- Primatelj ključem Jk (Javni ključ pošiljatelja) dešifrira sažetak S
  - ovjera (autentičnost)
  - neporicljivost
- Primatelj generira sažetak primljene poruke S'
  - ako je S = S', primljena poruka je istovjetna originalu
  - očuvanost (integritet)

Digitalni potpis (II)

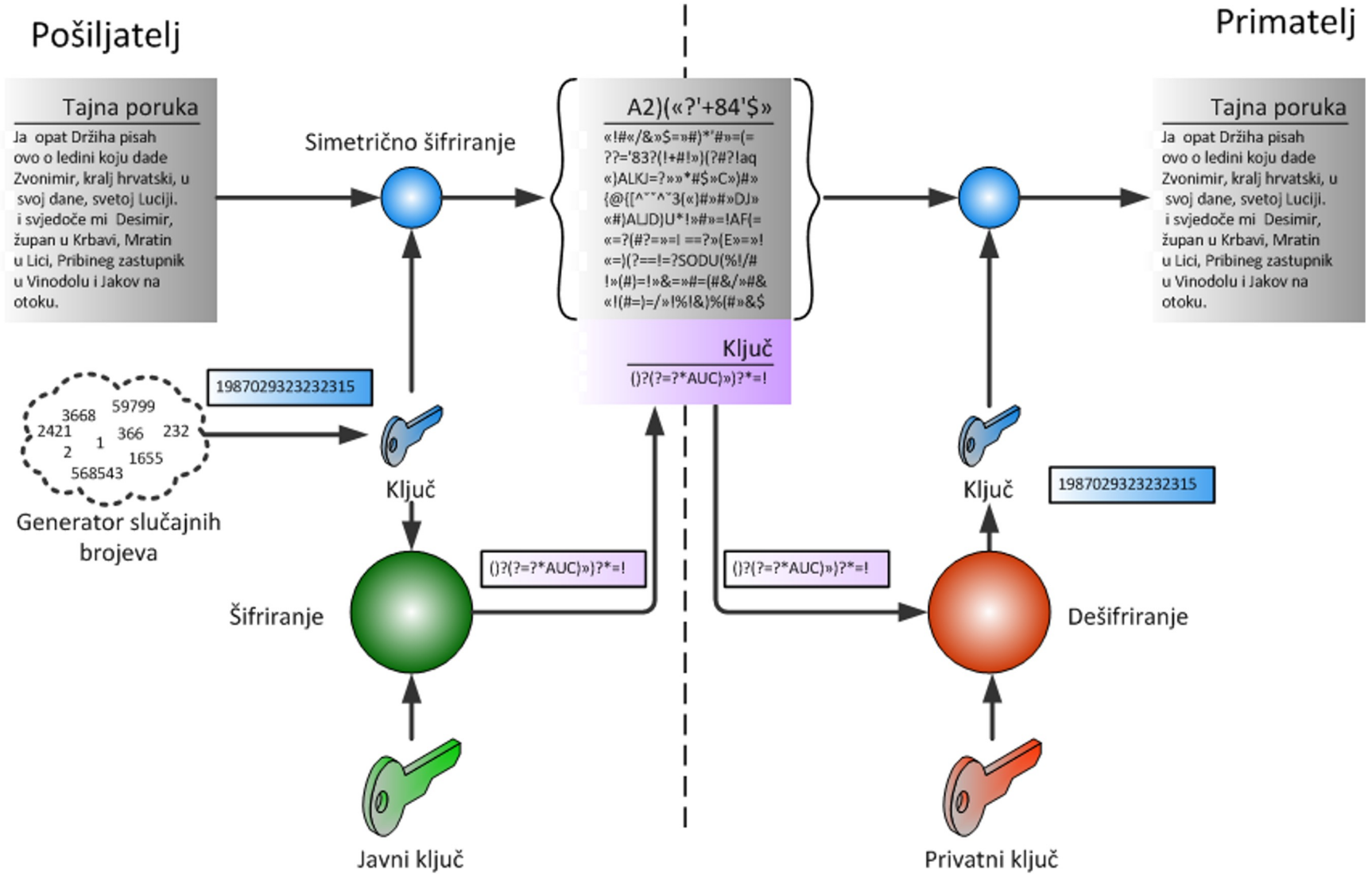


Provjerava jesu li primljeni i stvoreni sažetak istovjetni

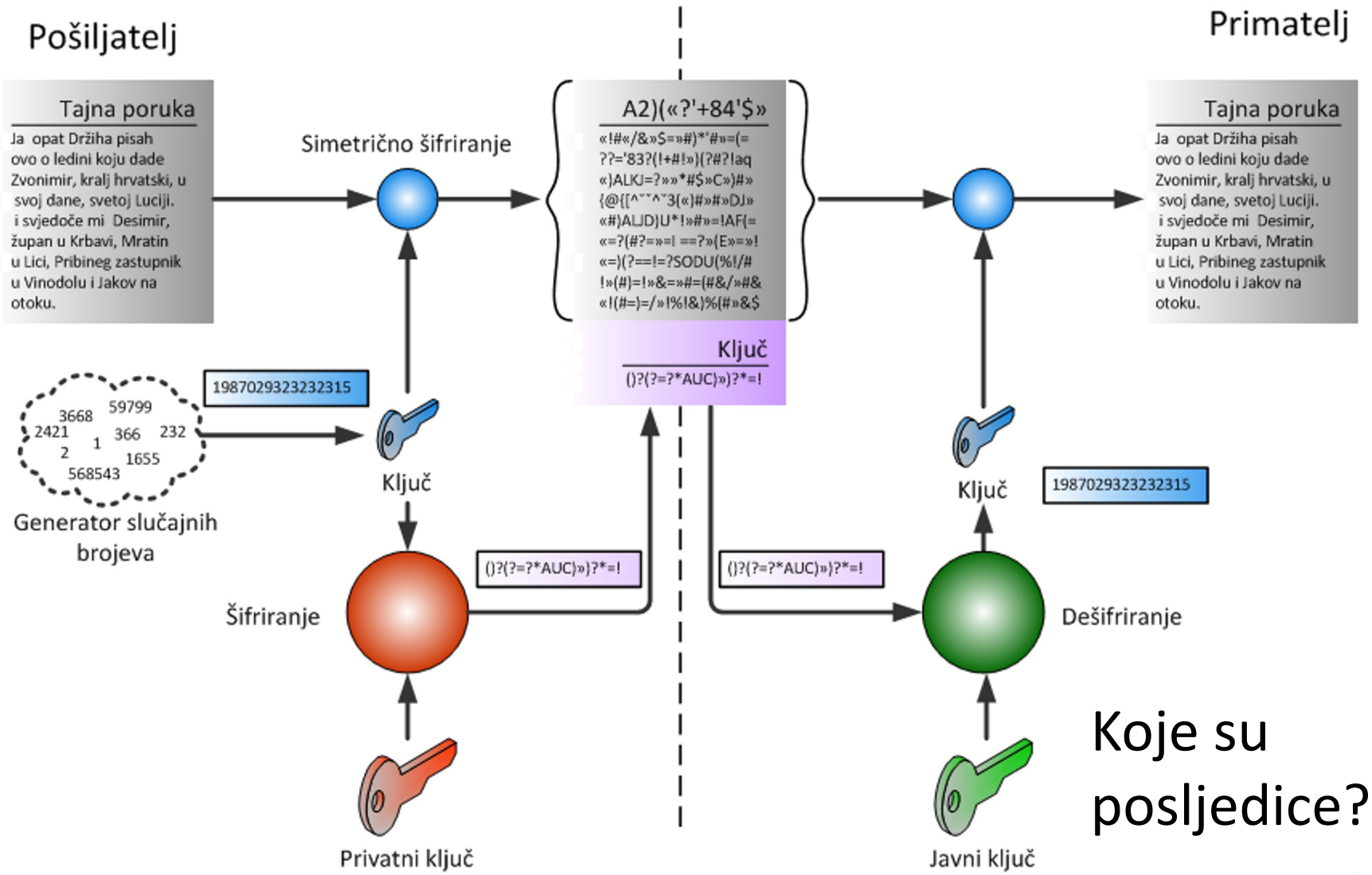
Digitalna omotnica (I)

- Pošiljatelj šifrira poruku simetričnim algoritmom ključem K
  - ključ K je generiran slučajno od strane pošiljatelja
  - Brzina
- Pošiljatelj šifrira ključ K asimetričnim algoritmom
  - javnim ključem Jk primatelja (Pk je kod vlasnika ključa – primatelja)
  - nema problema distribucije ključeva
- Primatelj svojim ključem Pk dešifrira simetrični ključ K
- Primatelj simetričnim ključem K dešifrira poruku
  - tajnost

Digitalna omotnica (II)



Pitanje: Je li ovo ispravno???

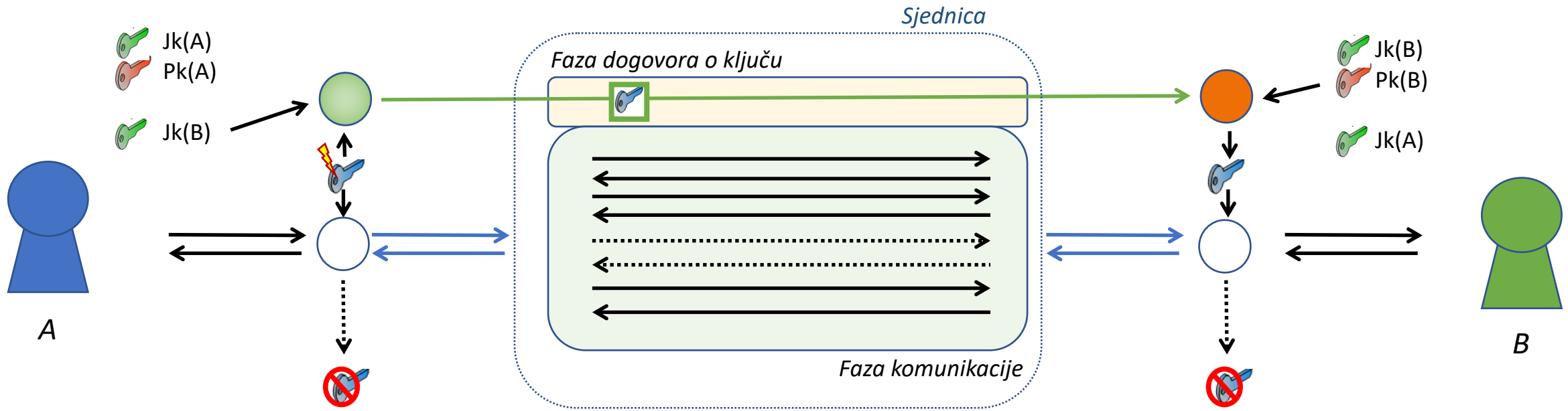


Koje su posljedice?

Sjednice

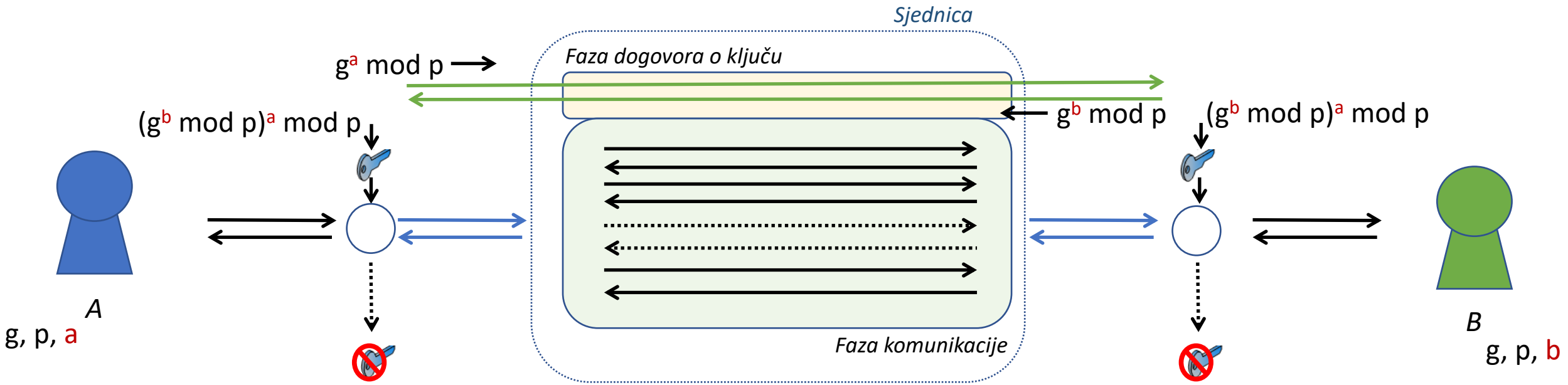
- Niz transakcija korištenjem sigurnog komunikacijskog kanala
  - Pretpostavka je da oba entiteta u komunikaciji imaju javni ključ drugog entiteta
  - Šifriranje poruka prosljeđivanih kroz kanal jednokratnim simetričnim sjedničkim ključem (engl. session key)
    - Sprječava napade temeljene na prikupljanju veće količine podataka šifrirane istim ključem
    - Efikasnije kodiranje podataka od asimetričnih algoritama
  - Problem inicijalnog dogovora o sjedničkom ključu između dva entiteta u komunikaciji
  - Faze sjednice:
    - Faza dogovora o sjedničkom ključu
    - Faza komunikacije kriptirane sjedničkim ključem
  - Dva osnovna načina dogovora o sjedničkom ključu
    - Jedan entitet generira sjednički ključ i prosljeđuje ga drugom entitetu (key exchange protocol)
    - Entiteti zajednički stvaraju sjednički ključ (key agreement protocol)

Razmjena sjedničkog ključa



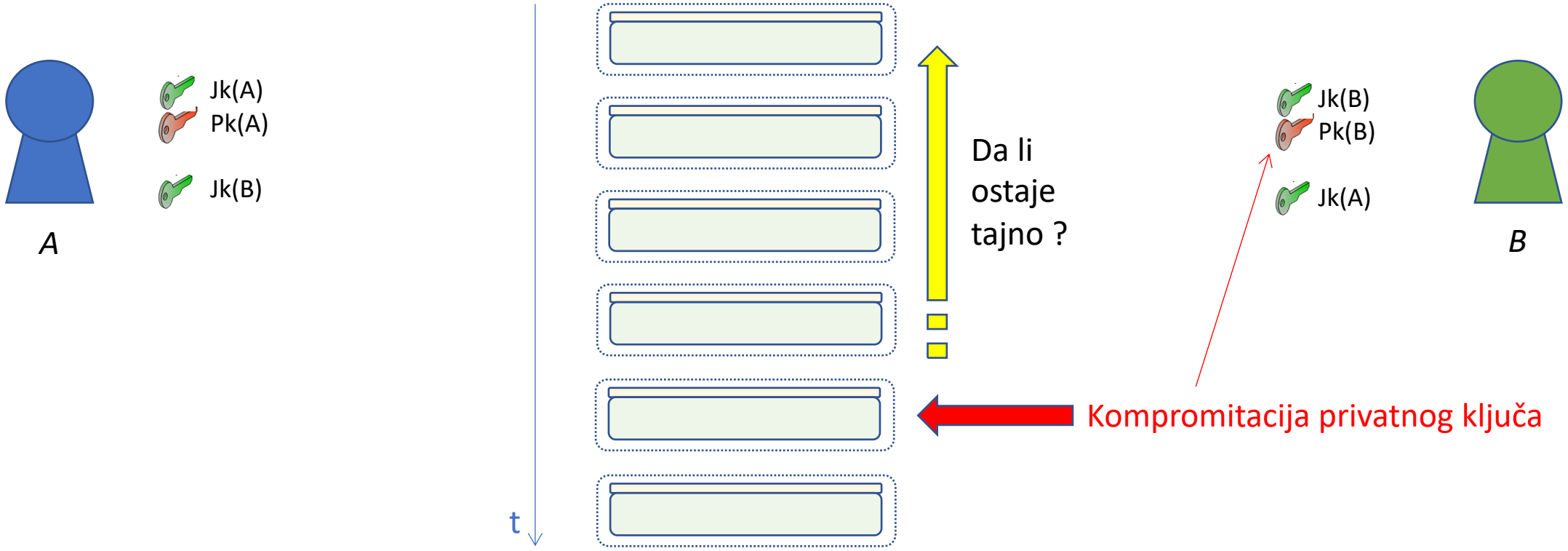
- Protokol razmjene sjedničkog ključa (engl. key exchange protocol)
  - Entitet (najčešće inicijator sjednice) generira slučajni sjednički ključ ili broj kao podlogu za generiranje ključa na strani oba entiteta
    - Kvaliteta generatora slučajnih brojeva od iznimne važnosti
  - Ključ se šifrira javnim ključem primatelja i šalje drugom entitetu
    - Primatelj dešifrira sjednički ključ svojim tajnim ključem
  - Sva daljnja komunikacija se šifrira/dešifrira sjedničkim ključem
  - Po završteku sjednice ključ se uništava

Protokol dogovora o ključu



- Obje strane sudjeluju u dogovoru o sjedničkom ključu
  - Sjednički ključ se stvara iz dijeljenih podataka dvaju entiteta i slučajno generiranih podataka
  - Diffie-Helman key exchange
    - Prenošenje parametara neštićenim kanalom – nije sigurnosni rizik (ali identitet sugovornika je!)
    - Zasniva se na problemu teškog računanja diskretnog logaritma
  - Sjednički ključ se nikada ne prenosi komunikacijskim kanalom

Forward secrecy



- Sva komunikacija između osobe A i B je snimljena i pohranjena
- U slučaju „proboja” privatnog ključa osobe B:
  - Ako je sjednički ključ bio prenošen u fazi dogovora o ključu (*key exchange* protokoli) – sve snimljene sjednice se mogu naknadno dešifrirati
  - Ako sjednički ključ nije bio prenošen u fazi dogovora o ključu (*key agreement* protokoli) - nema kompromitacije prošle komunikacije !
- Forward secrecy – povijest šifrirane komunikacije ostaje nedostupna napadaču

Elektronički potpis

- Elektronički potpis
  - *Skup podataka u elektroničkom obliku koji su pridruženi ili su logički povezani s drugim podacima u elektroničkom obliku i koji služe za identifikaciju potpisnika i vjerodostojnosti potpisanoga elektroničkog dokumenta*
- HR zakon o elektroničkom potpisu, 2002.
- Našom terminologijom
  - ovjera (identifikacija potpisnika)
  - očuvanost (vjerodostojnost)

Zakonodavstvo

- Napredan elektronički potpis
  - *Elektronički potpis koji pouzdano jamči identitet potpisnika i koji*
    - je povezan isključivo s potpisnikom
    - nedvojbeno identificira potpisnika
    - nastaje korištenjem sredstava kojima potpisnik može samostalno upravljati i koja su isključivo pod nadzorom potpisnika
    - sadržava izravnu povezanost s podacima na koje se odnosi i to na način koji nedvojbeno omogućava uvid u bilo koju izmjenu izvornih podataka
  - neporicljivost (povezan isključivo s potpisnikom)
  - ovjera (identificira potpisnika)
  - očuvanost (vjerodostojnost)

Izvedba elektroničkog potpisa (I)

- Potpis dijeljenim (simetričnim) ključem
  - potreba za središnjim autoritetom koji ovjerava naš potpis simetričnim ključem
  - komunikacija sa središnjim autoritetom zaštićena je simetričnom kriptografijom
  - autoritet označava vrijeme primitka poruka
    - zaštita od napada ponavljanjem poruka
- Problem:
  - ključevi za komunikaciju sa središnjim autoritetom
    - moraju biti tajni
    - velika količina tajnih informacija koja se čuva u središnjem autoritetu i kod svakog sugovornika
  - središnji autoritet može čitati sve poruke
  - središnji autoritet ovjerava svaku poruku

Izvedba elektroničkog potpisa (II)

- Potpis javnim (asimetričnim) ključem
  - poruku potpisujemo našim tajnim ključem
  - sugovornik provjerava potpis našim javnim ključem
    - nužno da su operacije šifriranja (potpisa) i dešifriranja (provjere) međusobno inverzne

- Nema potrebe za središnjim autoritetom koji ovjerava svaku poruku

- Problem: kako vjerovati da je javni ključ sugovornika baš njegov?
  - središnji autoritet jamči ispravnost ključa
  - potvrda o valjanosti ključa = certifikat

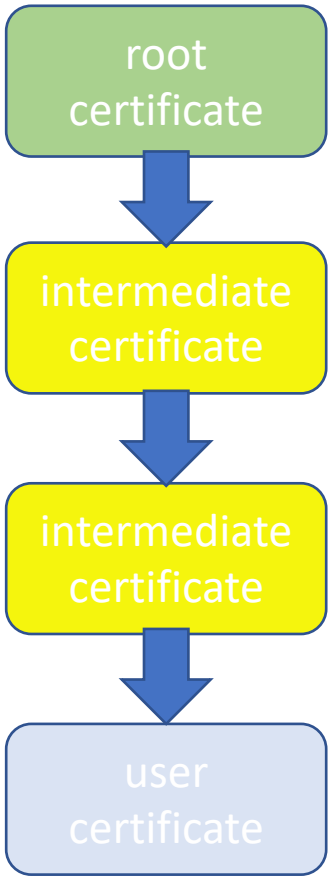
Certifikati

- Zakon: *certifikat je potvrda u elektroničkom obliku koja povezuje podatke za verificiranje elektroničkog potpisa s nekom osobom i potvrđuje identitet te osobe*
- Certifikat
  - potvrda o vezi između identiteta i javnog ključa
  - javan
    - norma za certifikate ITU X.509 v3
  - sadrži
    - identifikaciju izdavatelja i subjekta
    - oznaku algoritma potpisa i javni ključ
    - razdoblje važenja
    - potpis

Izdavatelj certifikata

- Davatelj usluga certificiranja
  - pravna ili fizička osobu koja izdaje certifikate ili daje druge usluge povezane s elektroničkim potpisima
- CA – *Certificate Authority*
  - izdaje certifikate
  - moguće ostvarenje hijerarhije CA
    - lanac povjerenja, staza certificiranja
      - stablo certifikata od korijenskog CA do našeg certifikata
    - ne postoji jedinstvena hijerarhija
      - Internet – niz CA
        - GTE CyberTrust Global Root
          - CyberTrust Educational CA
            - ahyco.fer.hr

C=HR/S=Zagreb/L=Zagreb/O=FER/OU=ZPR/CN=ahyco.fer.hr



Povlačenje certifikata

- Certifikat potvrđuje vezu između javnog ključa i osobe
  - javni ključ nećemo izgubiti, ne može biti ukraden
  - što ako izgubimo privatni ključ ili je ukraden?

- Certifikat sadrži razdoblje valjanosti
  - što kad to razdoblje istekne?

- CA održava mehanizme provjere valjanosti certifikata
  - provjera potpisa
  - održavanje popisa povučenih certifikata (CRL)

Zakonodavstvo

- Potpisnik
  - *koji izgubi ili mu je otuđeno sredstvo za izradu elektroničkog potpisa te u slučajevima kada mu je onemogućen pristup podacima za izradu elektroničkog potpisa, dužan je o tome odmah obavijestiti davatelja usluga certificiranja*

- Davatelj usluga certificiranja
  - *koji je zaprimio obavijest ... provodi uvid u postupak opoziva izdatog certifikata i dalje postupa po utvrđenim pravilima opozivanja izdatih certifikata*

Popis povučenih certifikata

- CRL – Certificate Revocation List
- Popis povučenih certifikata
  - ne uključuje certifikate kojima je automatski istekla valjanost
- Provjera valjanosti certifikata
  - provjera digitalnih potpisa certifikata
  - provjera razdoblja valjanosti certifikata
  - provjera popisa povučenih certifikata
    - adresa CRL upisana u certifikat
    - certifikat može biti označen kao nekritičan (*non-critical*)
      - ako pristup popisu (CRL) nije moguć, smatramo da je sigurnost dovoljna
        - npr. nedostupna mrežna veza ...

Značaj CA

- CA
  - ovjerava certifikate
  - održava popise povučenih certifikata

- Kompromitirani CA unosi veliku štetu
  - cijela hijerarhija od tog CA na niže postaje nevažeća
  - sigurna komunikacija s članovima hijerarhije nije moguća
    - uskraćivanje usluge - DOS

Norme

- Public Key Cryptography Standards (PKCS)
  - RSA Security definirao niz normi
    - PKCS #1 – *RSA Cryptography Standard*
    - PKCS #3 – *Diffie-Hellman Key Agreement Standard*
    - PKCS #7 – *Cryptographic Message Syntax Standard*
    - PKCS #8 – *Private-Key Information Syntax Standard*
    - PKCS #10 – *Certification Request Standard*
    - PKCS #11 – *Cryptographic Token Interface (programsko sučelje)*
    - PKCS #12 – *Personal Information Exchange Syntax Standard*
- X.509
  - ITU-T - norme za ostvarenje PKI
  - oblik certifikata

Norme

- FIPS – Federal Information Processing Standards
  - između ostalog – DES i AES
- W3C
  - struktura XML-a s digitalnim potpisom
  - XML DSig, XML AdES
- Problem
  - XML istog značenja može biti zapisan na više načina
    - razmaci u oznakama elemenata
    - redoslijed atributa, elemenata ...

```
<SignatureValue>C7di9  ....  ligw+o=</SignatureValue>
<X509SubjectName>Ivo Ivić #BrojCertifikata</X509SubjectName>
<X509Certificate>
   MIIEazCCA  .... iG9w0BA
</X509Certificate>
```

Otvoreno računarstvo

9. Osnove sigurnosti

- Osnovi pojmovi
- Osnovni algoritmi
- Složeniji algoritmi i postupci
- Sigurnost u mrežnoj komunikaciji

Sigurnost na Internetu (I)

- Internet je u načelu nesiguran
  - niz raznih mogućnosti napada, koje se u praksi kombiniraju
- Praćenje mrežnog prometa (čitanje) je izuzetno lako
  - prisluškivanje (*eavesdropping*, *interception*)
    - ako podaci nisu kriptirani, kao da stojite na ulici i slušate što drugi govore (*ako znate koga treba slušati*)

- Lažno predstavljanje korisnika
  - utjelovljivanje korisnika (*impersonation*)
    - probijanje sigurnosne tehnologije
    - krađa autentikacijskih uređaja/podataka (kartice, tokena, lozinke, identiteta) – na razne načine
    - pogađanje lozinki (korisničkih) – napad grubom silom i ostali napadi

Sigurnost na Internetu (II)

- Lažno predstavljanje poslužitelja ili klijenta
  - utjelovljivanje usluge ili računala (*impersonation*)
  - lažno predstavljanje lažiranjem IP (ili MAC) adrese
  - napad "čovjeka u sredini" (*man-in-the middle attack*, MITM)
    - presretanje originalnih podataka (paketa) i mijenjanje te slanje dalje kao da je originalan
  - pogađanje ključeva ili certifikata
    - napad grubom silom (*brute force atack*)
    - napad poznatim šifriranim tekstom (*chosen-ciphertext attack*, CCA)
    - napad poznatim čistim tekstom (*chosen-plaintext attack*, CPA)

Sigurnost na Internetu (III)

- Lažno predstavljanje usluge ili sjedišta Weba
  - napad lažnim predstavljanjem usluge (*phishing*)
- Onesposobljavanje usluge preopterećenjem
  - napad generiranjem velike količine prometa ili poziva
  - uskraćivanje usluge (*denial-of-service*)
- Namjerno odugovlačenje ili ponavljanje poruke ili podataka
  - napad reprodukcijom (*replay attack*)
- Promjena dijela poruke drugim podacima
  - napad zamjenom dijela poruke (*substitution attack*)

Sigurnosna zaštita

- Na svaki od ovih sigurnosnih problema se mora adekvatno odgovoriti
- Razine zaštite su onoliko visoke (jake, skupe), koliko je ono što se čuva vrijedno (bitno)
- Zaštite se obično rade na nekoliko razina kako bi se povećala sigurnost
- U načelu se štite:
  - sustavi
  - aplikacije
  - komunikacija

Sigurnost sustava

- Zaštita sustava
  - onemogućavanje upada u mrežu
    - uporaba vatrozida (*firewall*)
    - postavljanje demilitariziranih zona (DMZ)
  - onemogućavanje stražnjih vrata (*backdoor*)
    - zaštita i kontrola bežičnih mrežnih (WLAN) konekcija
    - zabrana korištenja modemskih priključaka
    - kontrola uporabe mrežnih (LAN) priključaka
  - praćenje neuobičajenih i potencijalno štetnih mrežnih aktivnosti
    - uporaba antivirusnih alata
    - uporaba posebnih sigurnosnih alata

Sigurnost aplikacija Weba

- Zaštita aplikacije
  - onemogućavanje stražnjih vrata (*backdoor*)
    - zaštita javnih servisa
    - provjera sigurnosti svih dijelova aplikacije
    - otvaranje sučelja samo prema poznatim klijentima
    - autentikacija svih klijenata
  - praćenje neuobičajenih i štetnih aktivnosti
    - zapis svih aktivnosti (log)
  - sigurnosna testiranja aplikacije
    - simulacije namjernih napada
    - bolje spriječiti nego liječiti

Sigurnost komunikacije

- Autentikacija korisnika
  - princip ključ-brava – dokazivanje identiteta
  - korištenje raznih metoda (lozinke, tokeni, certifikati)

- Autorizacija korisnika za skup akcija
  - provjera da li korisnik ima odgovarajuća prava
- Zaštita poruka od čitanja i mijenjanja
  - kriptiranje poruka
- Zaštita pristupa komunikacijskom kanalu i zaštita od čitanja podataka s komunikacijskog kanala
  - kriptiranje komunikacije na kanalu

Sigurnosne tehnologije aplikacija Weba

- Najčešće sigurnosne tehnologije aplikacija Weba – podskup navedenih tehnologija/tehnika/metoda:
  - zaštita komunikacijskog kanala kriptiranjem
    - protokol HTTPS
  - autentikacija korisnika
    - lozinka
    - token
    - certifikat (npr. na pametnim karticama u sklopu PKI sustava)
  - autentikacija klijenta (npr. preglednika)
    - certifikat na strani klijenta
  - autentikacija poslužitelja
    - certifikat na strani poslužitelja

HTTPS

- https je URI shema
  - sintaksa identična http protokolu
  - inicijalna postavka vrata 443 (umjesto 80)

- Enkripcija/autentikacija između HTTP i TCP sloja temeljena na poznatim kriptografskim protokolima
  - SSL (Secure Socket Layer) – službeno TLS (Transport Layer Security)
- Korištenje certifikata
  - problematika potpisivanja/vjerovanja certifikatu
- Onemogućava niz napada raznih tipova