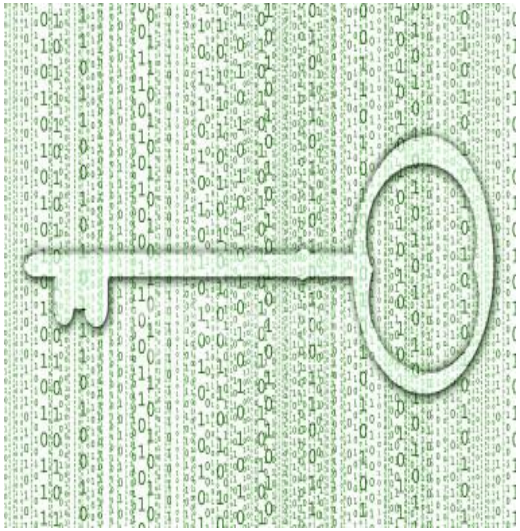
Bezbednost Aplikacija
Osnove Bezbednosti Podataka

Predmet: Bezbednost Aplikacija

Predavač: dr Dušan Stefanović

KLJUČNI ELEMENTI BEZBEDNOSTI

- Autentifikacija (Authentication)
  - Provera identiteta
- Poverljivost podataka (Data Confidentiality)
  - Kripcija podataka
- Integritet podataka (Data Integrity)
  - Zaštita od modifikacije podataka tokom prenosa



AUTENTIFIKACIJA

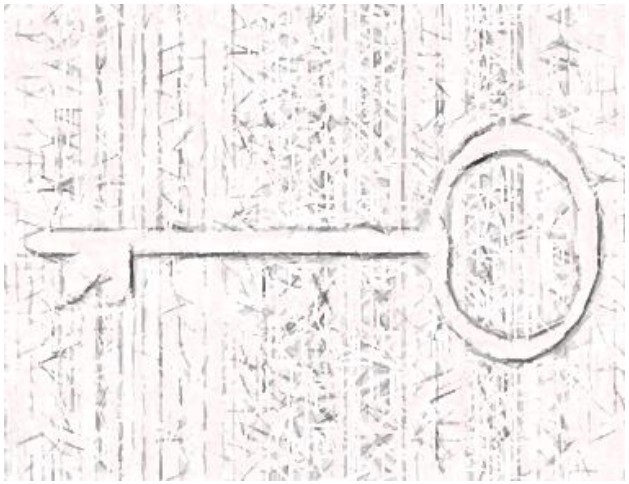
Obezbeđuje da je poruka stigla od izvora koji je autentifikovan.

- Koristi se nekoliko metoda za proveru identiteta učesnika u komunikaciji.
  - Lozinke
  - Digitalni sertifikati
  - Smart kartice
  - Biometrija

POVERLJIVOST PODATAKA

Sprečava da se vidi sadržaj presretnutih(eavesdropp) podataka od neautorizovanog izvora

Poverljivost podataka se postiže šifrovanjem (kripcijom)



INTEGRITET PODATAKA

Uvek postoji opasnost da neautorizovan korisnik promeni sadržaj poruke

Algoritmi koji se koriste za proveru integriteta podataka garantuju da između izvora i odredišta nije bilo modifikacije podataka.

- Za integritet podataka koristi se jadna od tri tehnologije:
  - one-way hash funkcije
  - message authentication codes (MAC)
  - digital signatures

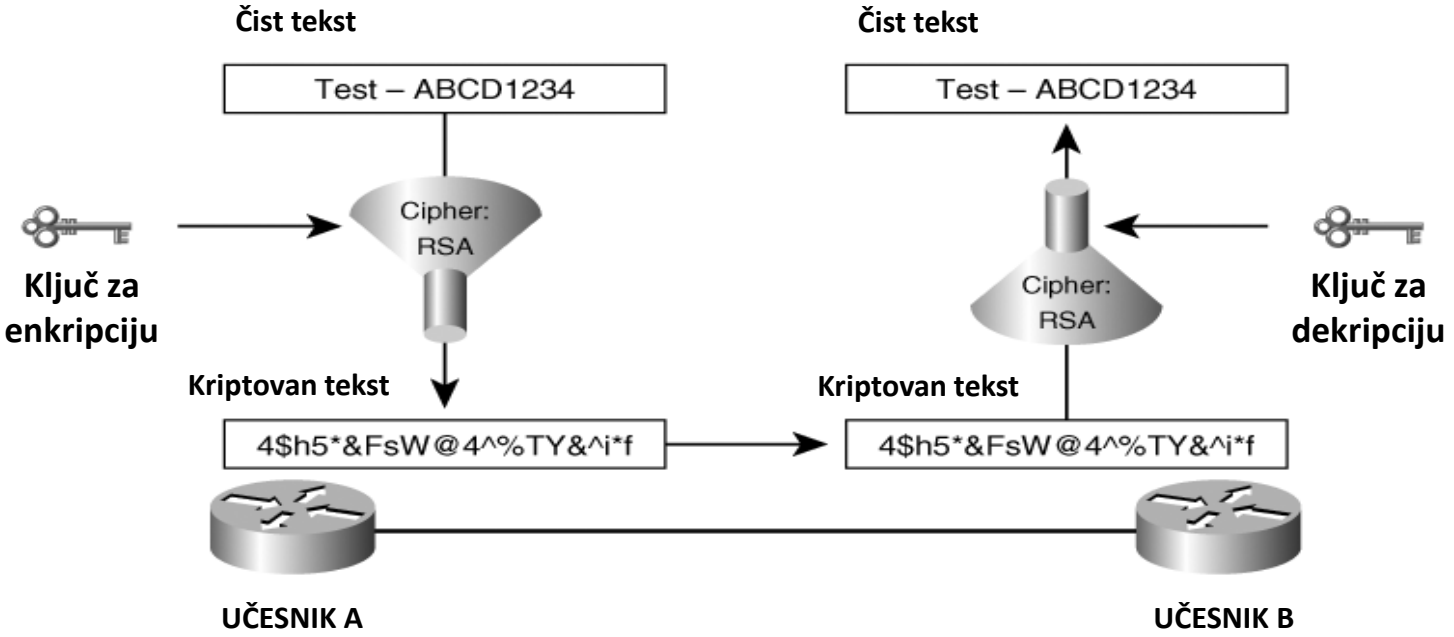
OSNOVI KRIPTOGRAFIJE - TERMINI

Kriptografija se zasniva na tri ključne komponente:

1. Ključ
2. Matamatička funkcija (cipher)
3. Poruka koja se enkriptuje ili dekriptuje

U nekim slučajevima ključ za kripciju i dekripciju je isti (simetričan)

U nekim slučajevima ključ za kripciju i dekripciju je različit (asimetričan)

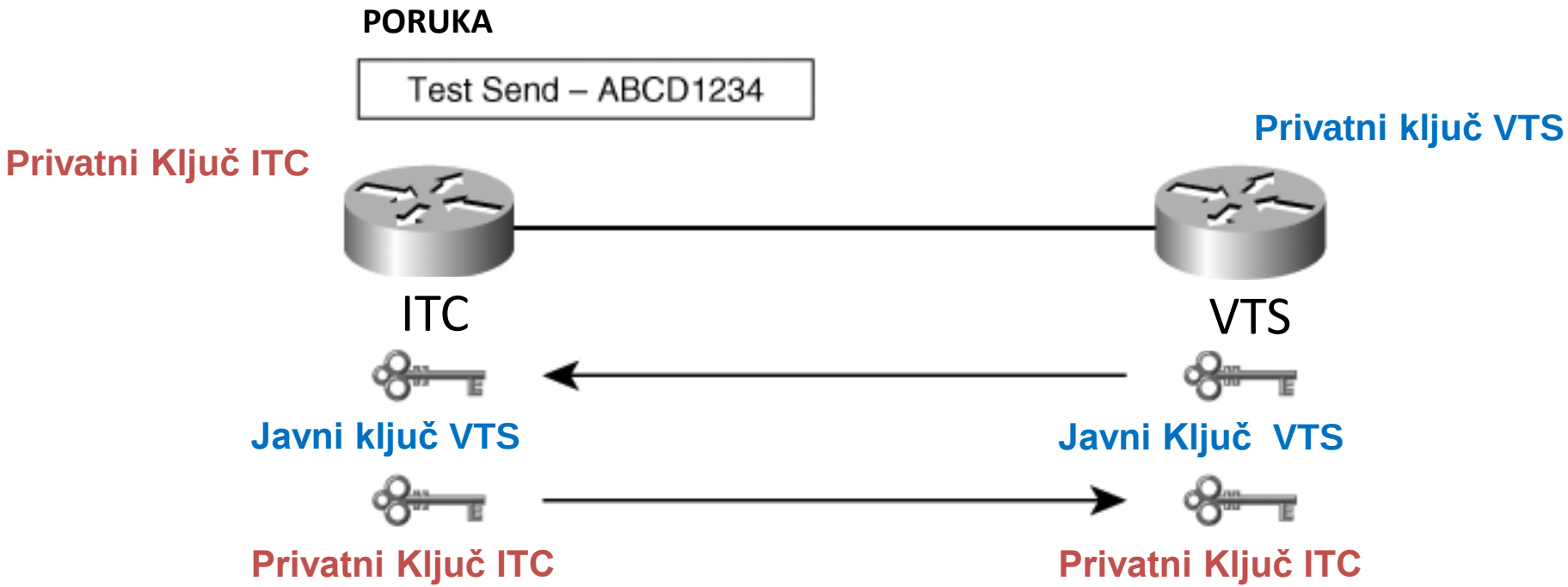


ASIMETRIČNA KRIPTOGRAFIJA

Javni ključevi (kriptuju podatke) - prosleđuju se učesnicima u komunikaciji (kroz mrežu).

Privatni ključevi (dekriptuju podatke) – ne prosleđuju se učesnicima u komunikaciji.

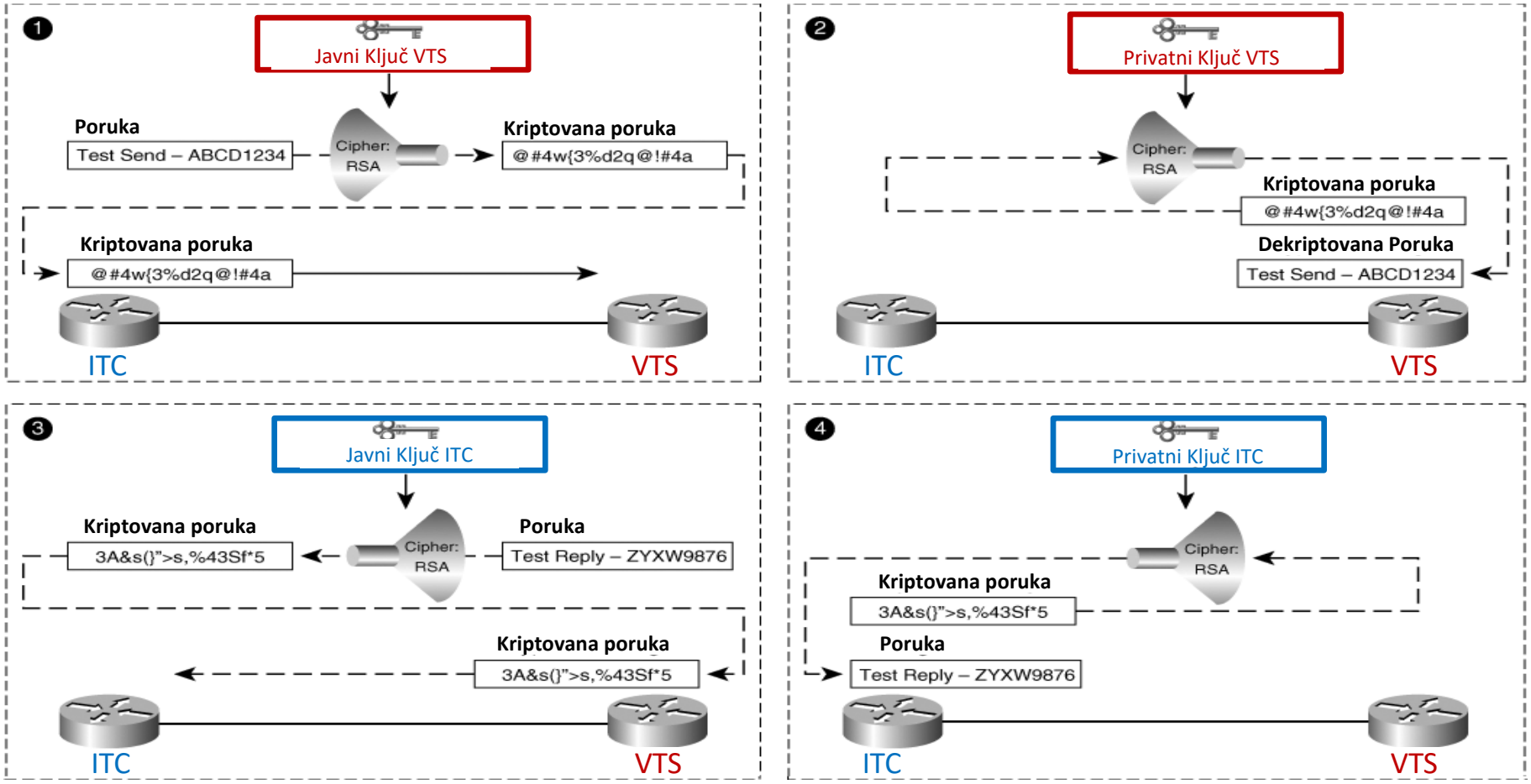
- Javne ključeve je potrebno razmeniti bezbedno između strana koje učestvuju u komunikaciji.
- Postoje algoritmi koji garantuju pouzdanu razmenu ključeva kroz nebezbedni medijum



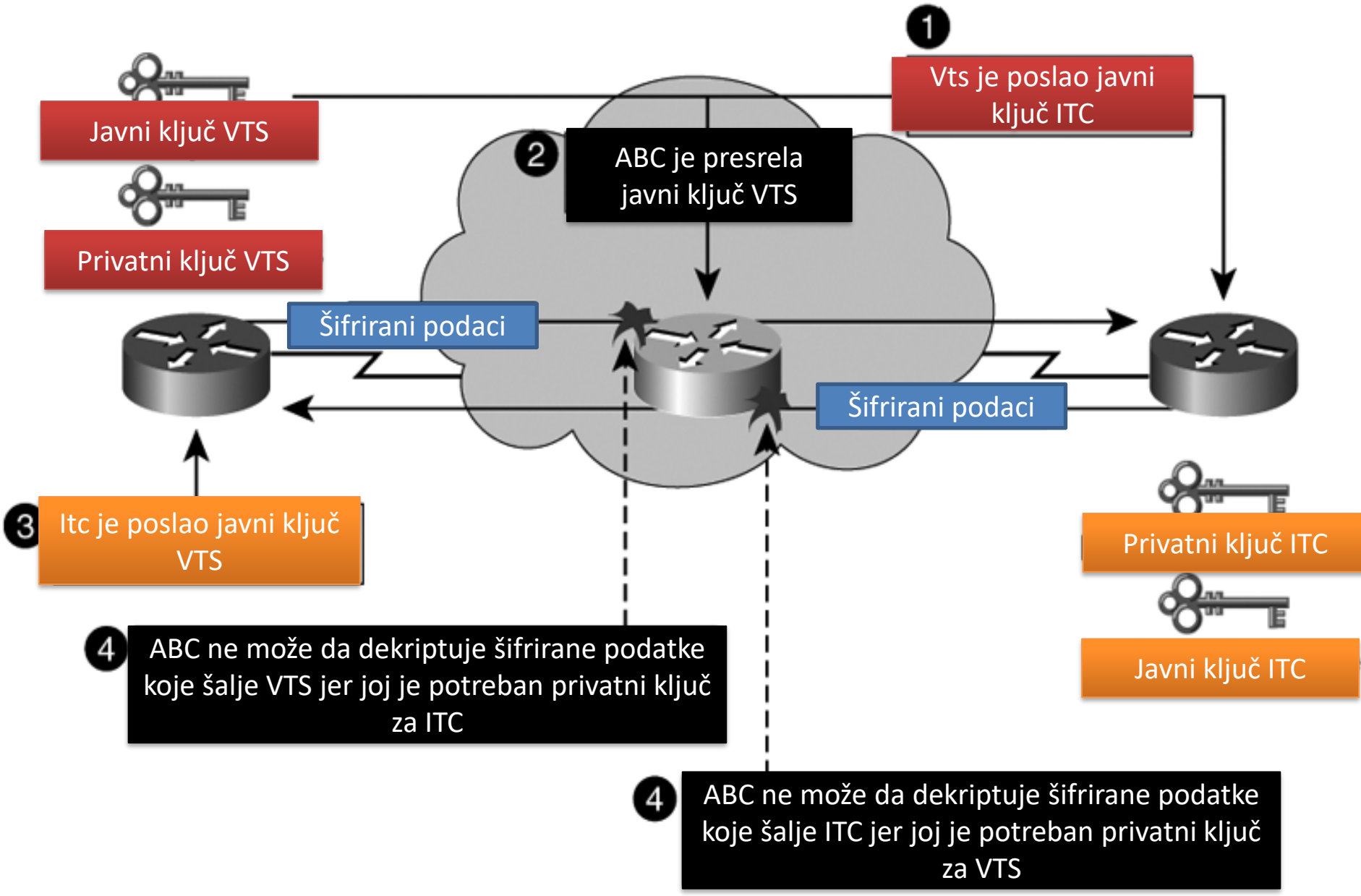
ASIMETRIČNA KRIPTOGRAFIJA – JAVNI / PRIVATNI KLJUČEVI

Originalna poruka se ne šalje kroz prenosni medijum ne kriptovana.

Posredni uređaji između dve strane koje učestvuju u komunikaciji ne mogu da vide originalnu poruku jer ne poseduju privatni ključ za dekripciju podataka.



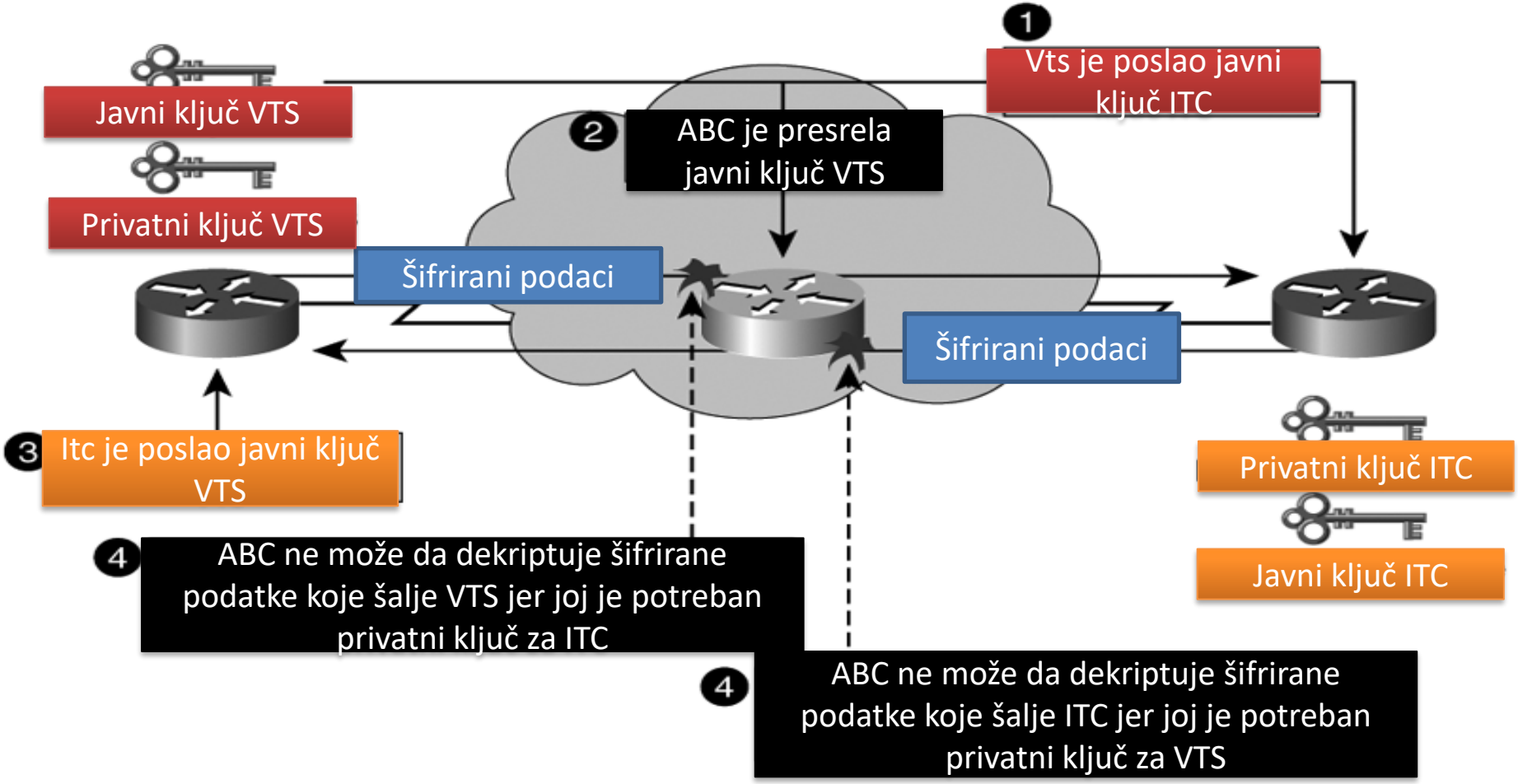
ASIMETRIČNA KRIPTOGRAFIJA – PRESRETANJE KLJUČEVA



ASIMETRIČNA KRIPTOGRAFIJA – PRESRETANJE KLJUČEVA

Da bi ABC uspešno sprovela napad potrebno je da:

- Uveri VTS da je ona ustvari ITC a ne ABC kako bi dobila javni ključ VTS



SIMETRIČNA KRIPTOGRAFIJA

ITC i VTS koriste isti secret key za kripciju i dekripciju podataka

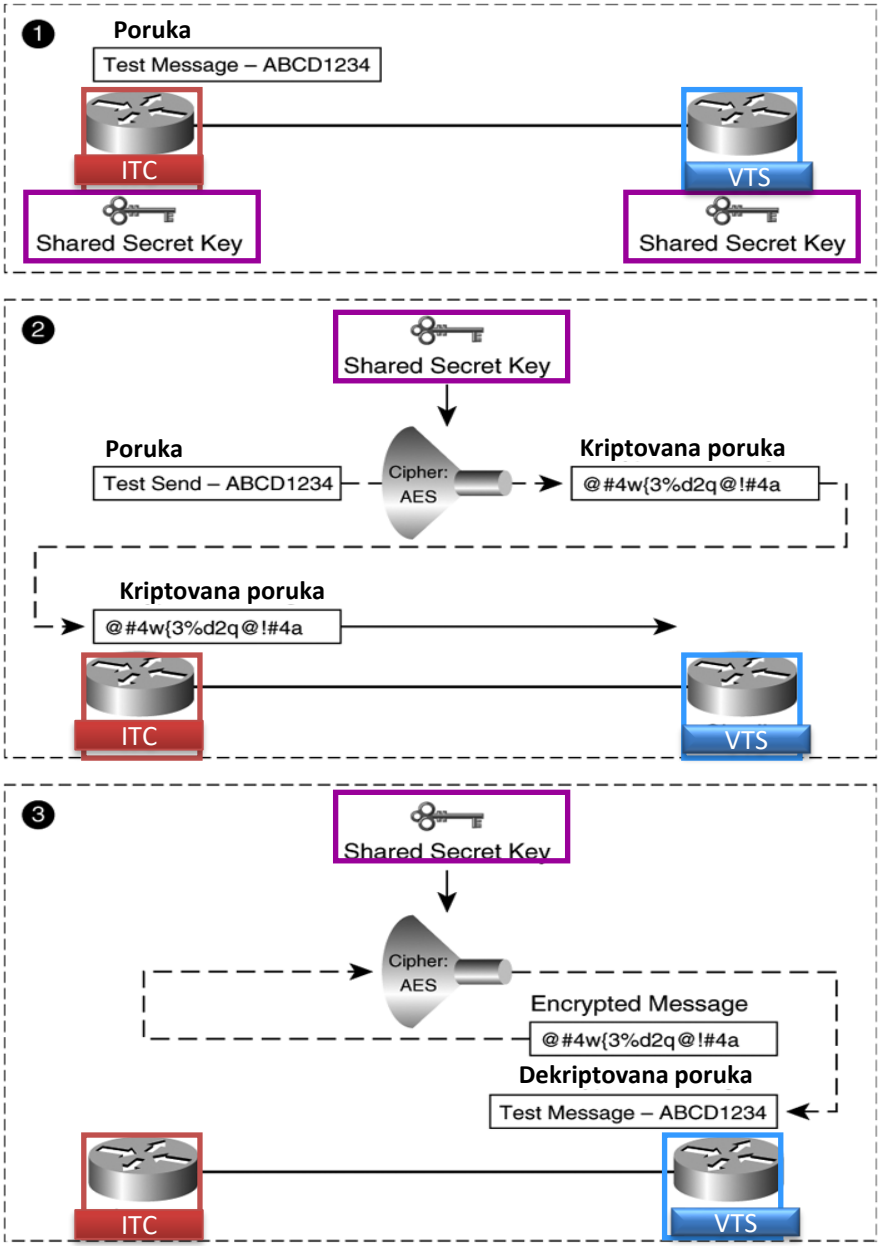
Neznatno jednostavnija operacija i znatno brža od asimetrične kriptografije .

Simetrična kriptografija je pogodna kod prenosa velike količine podataka.

Razmena tajnog ključa(shared secret key) može biti ručna ili dinamička.

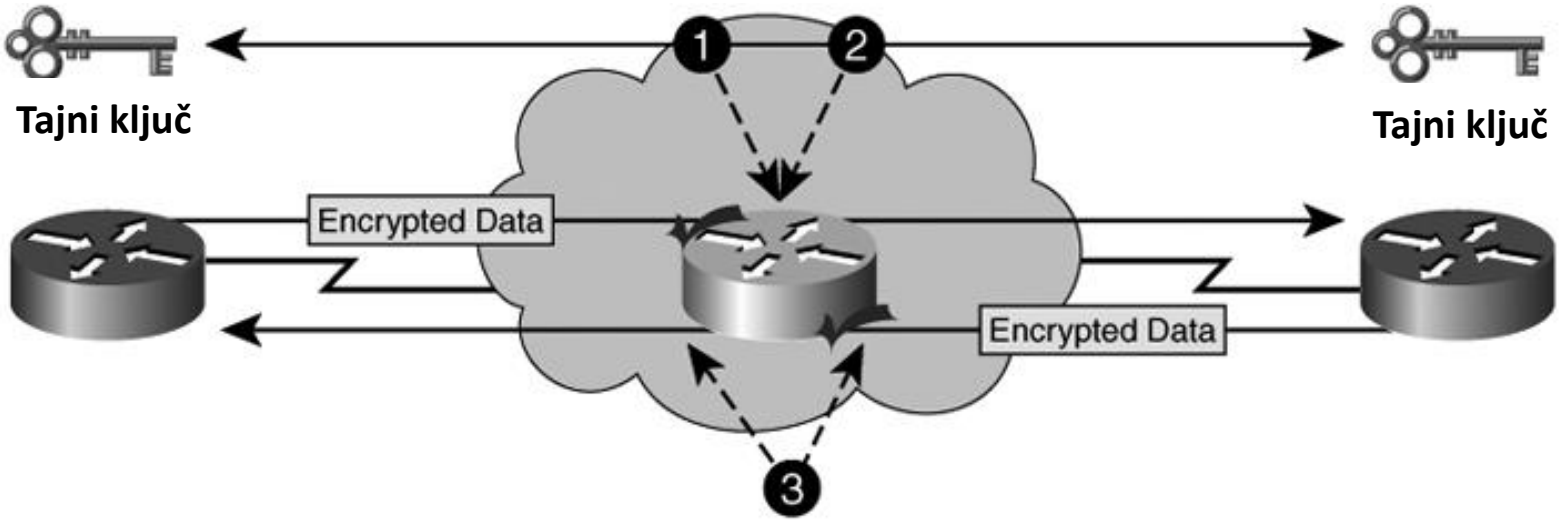
Simetrični algoritmi koji se najčešće koriste (DES,3DES ili AES)

Sigurnost podataka je u dužini ključa



PRESRETANJE TAJNOG KLJUČA

ABC ukoliko sazna simetrični ključ koji koriste ITC i VTS za kripciju i dekripciju podataka, moći će da prisluškuje komunikaciju.

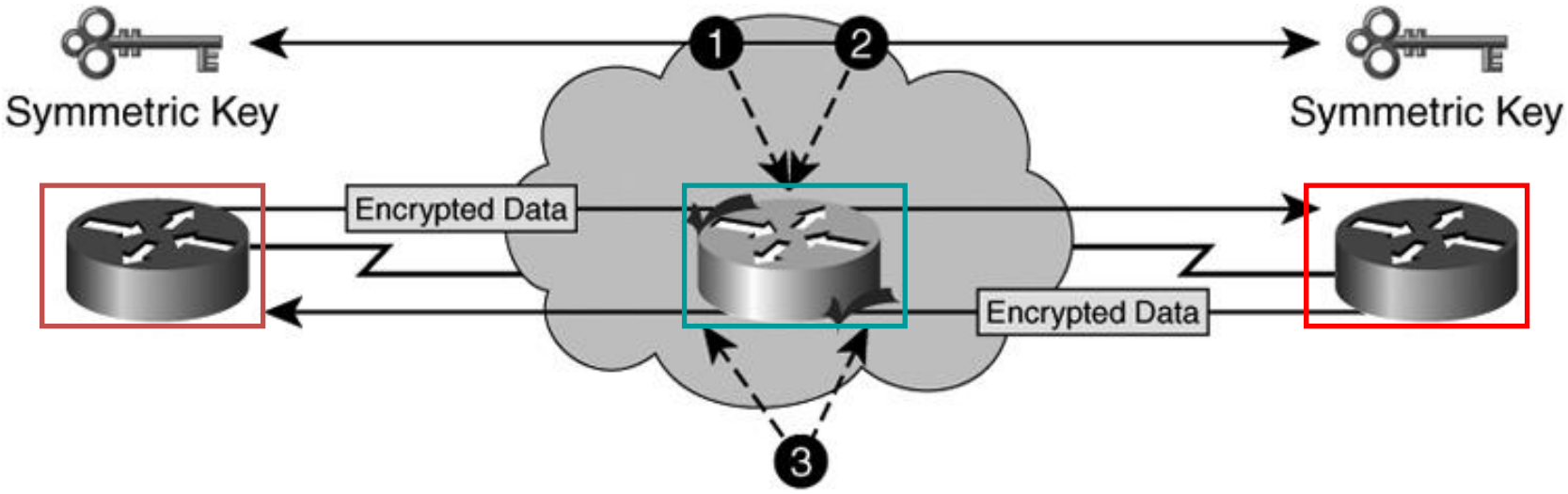


PRESRETANJE TAJNOG KLJUČA

Zaštita simetričnim algoritmom je osetljivija na napade ukoliko je simetričan ključ kompromitovan.

Iz tog razloga, simetrični ključevi se obično ne razmenjuju preko javne mreže već se isporučuju preko bezbednog medijuma.

Najčešće se koristi **Diffie-Hellman algoritam** za isporuku shared secret key (tajni ključ) kod simetrične kriptografije.



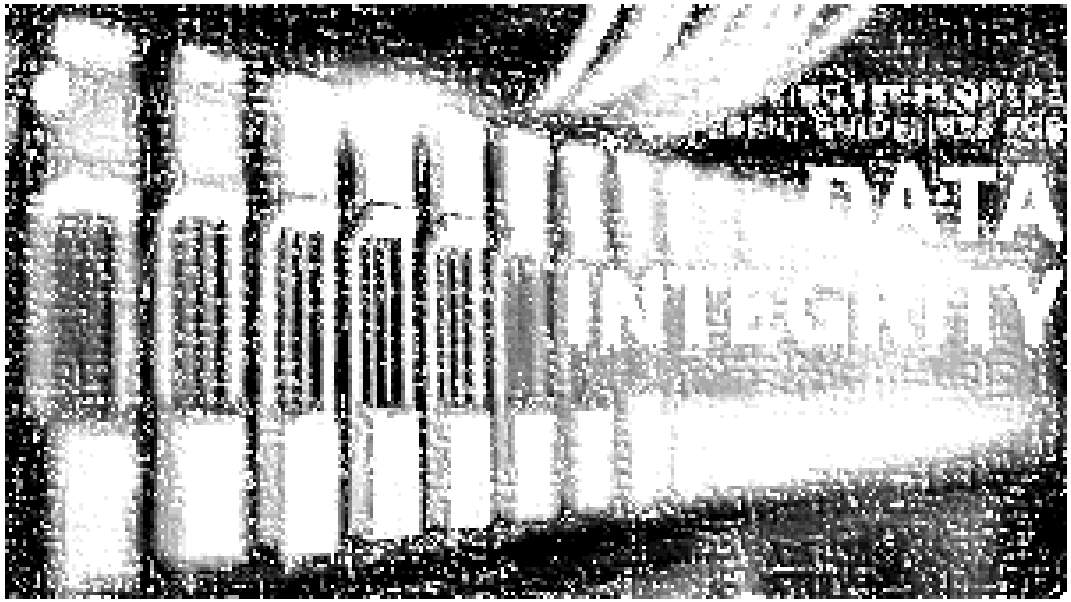
AUTENTIFIKACIJA I INTEGRITET PODATAKA

Bezbedni protokolski stek (TLS, IPSec, ...) posduje funkcije koje obezbeđuju:

- Autentičnost poruke
- Integritet podataka
- Autentifikaciju pošiljaoca

Gore navedene funkcije se oslanjaju na:

- Hashing poruke
- Digest poruke
- Digitalni potpis



INTEGRITET PODATAKA
MESSAGE DIGEST

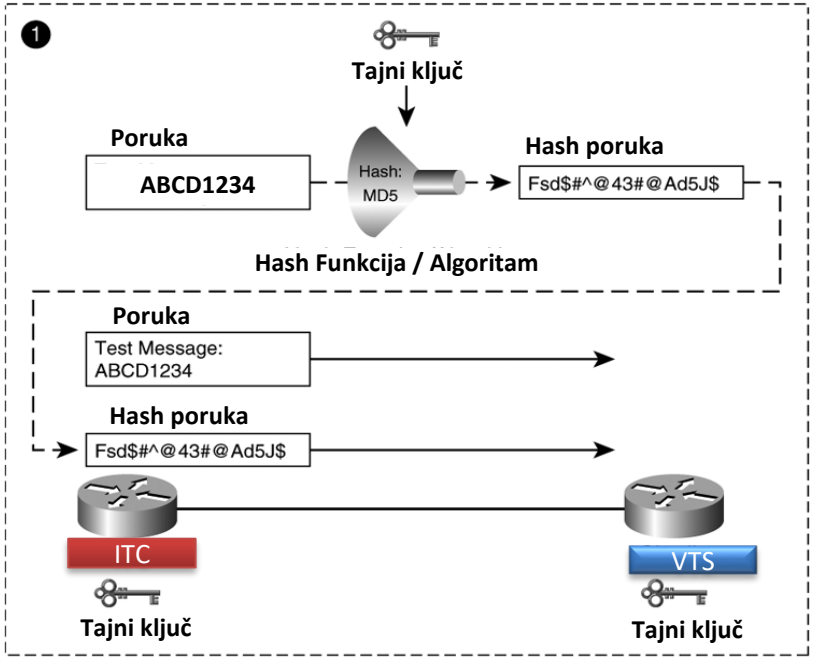
Integritet podataka proverava da li je poruka promenjena tokom prenosa.

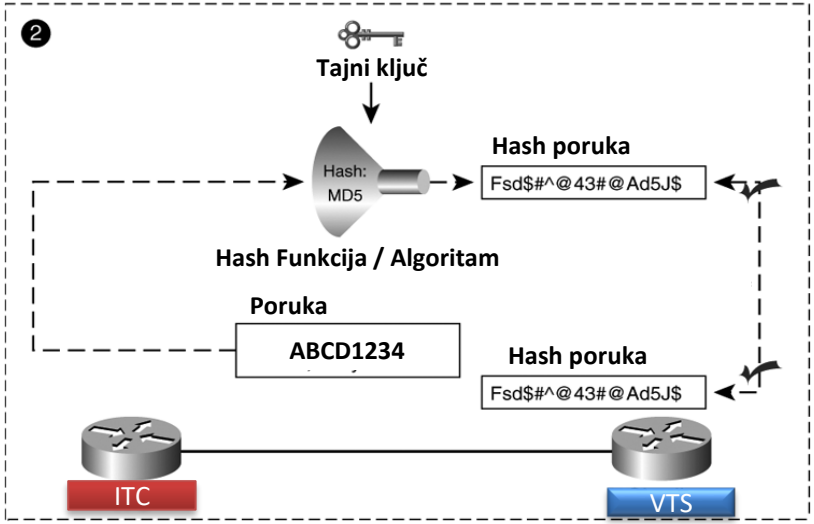
Hash obezbeđuje integritet podataka.

Na ulaz u **Hash** generator se dovodi poruka promenjive dužine.

Izlaz iz **Hash** generatora je kod fiksne dužine

- Dobijeni kod se dodaje originalnoj poruci koja se zatim šalje kroz kanal.
- Osnovna **hash funkcija** sastoji se iz:
  - algoritma
  - ključa koji je poznat prijemniku i predajniku





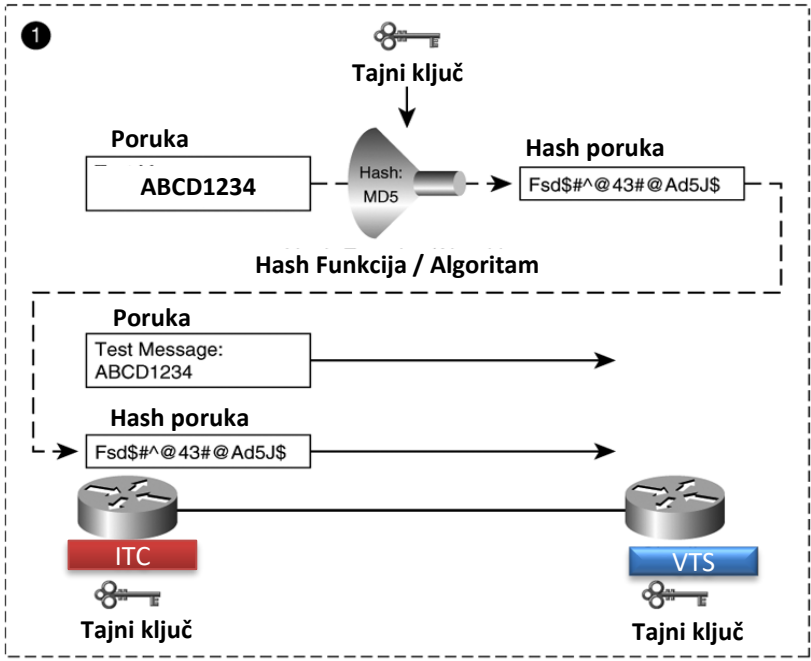
INTEGRITET PODATAKA
MESSAGE DIGEST

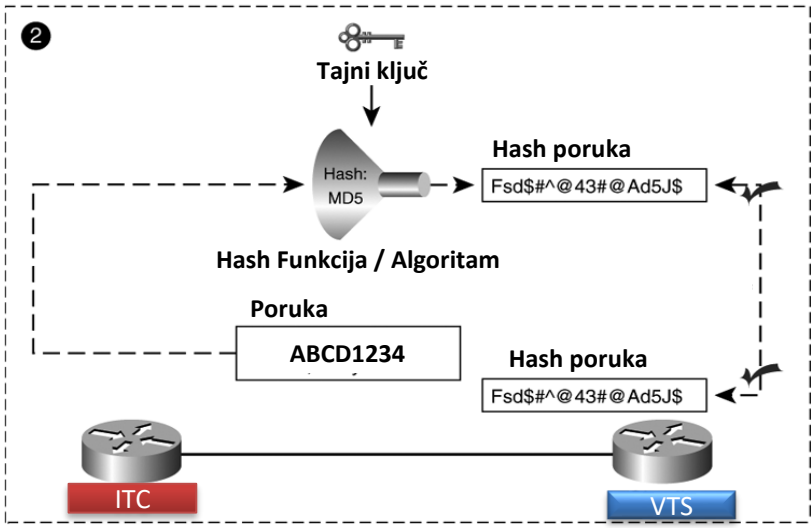
1.

- ITC izvršava matematičku operaciju (hash funkcija) na originalnoj poruci.
- Izlaz iz matematičke funkcije je hash vrednost (message digest)
- Hash vrednost se dodaje originalnoj poruci pre nego što se pošalje VTS.

2.

- VTS primljenu poruku, bez hash vrednosti, vodi na svoj hash generator.
- Upoređuje svoju dobijenu hash vrednost sa dobijenim hash-om od ITC.
- Ukoliko se dve hash vrednosti podudaraju očuvan je integritet poruke.



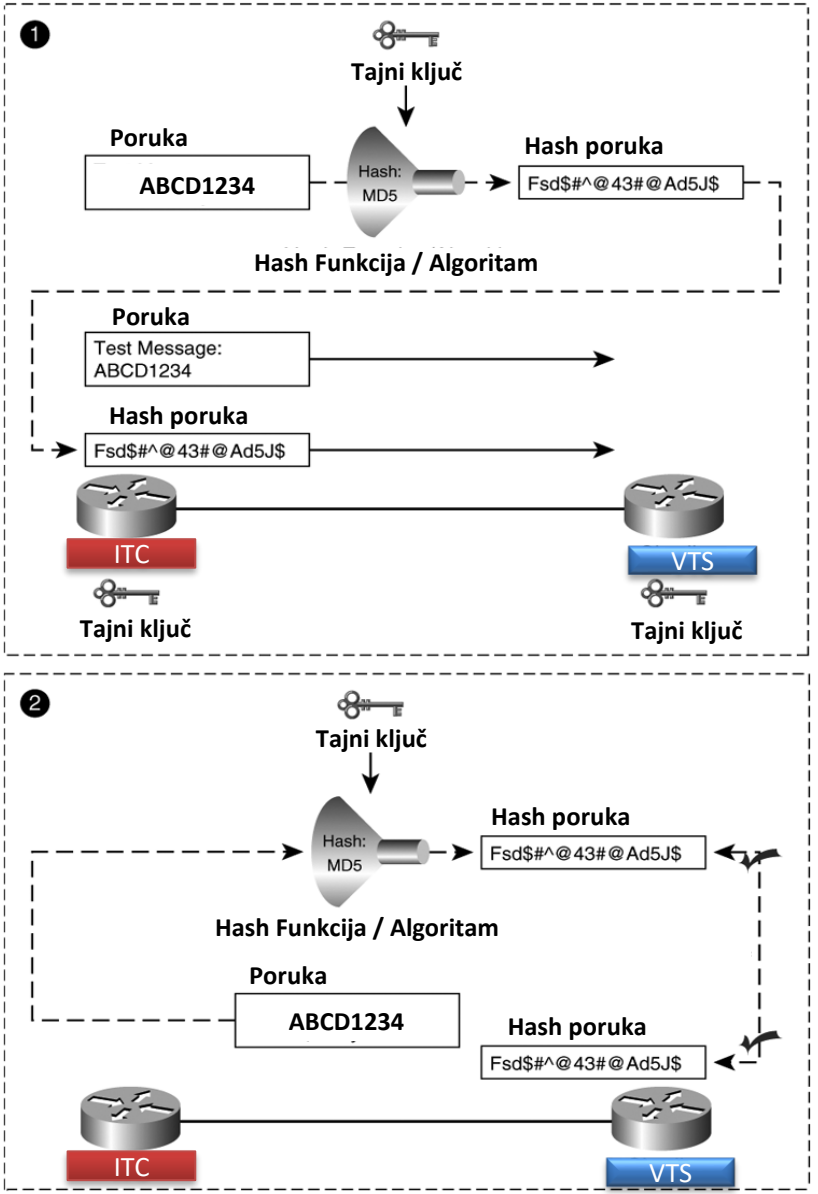


INTEGRITET PODATAKA

Message digest:

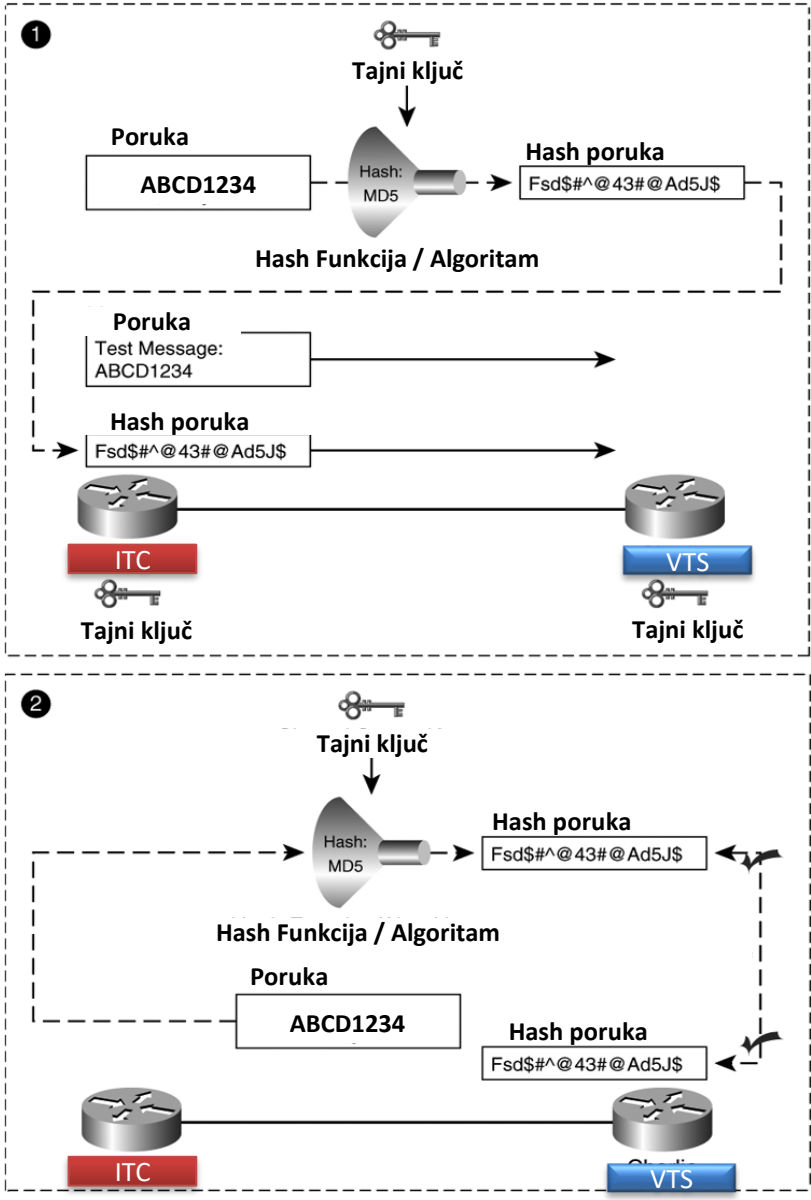
- Obezbeđuje integritet podataka
- Ne obezbeđuje autentifikaciju,
  - Osim ako se od originalne poruke kreirao hash sa zajedničkim ključem (secret key) koji se koristi između dva endpoint-a (HMAC).

- Hashed Message Authentication Codes (HMACs) se najčešće koristi kod autentifikacije



OSOBINE HASH FUNKCIJE

- **Hash** :
- Ista poruka na ulazu u hash generator uvek daje istu hash vrednost.
- Dužina ulazne poruke može da varira,dok dužina izlazne hash poruke je uvek ista.
- Izlaz iz hash generatora mora biti slučajna vrednost.
- Hash funkcija je ireverzibilna tj. nije povratna (one way):
- Na osnovu hash vrednosti nije moguće odrediti originalnu poruku.
- Svaka jednoznačna ulazna poruka daje jedinstvenu izlaznu vrednost.
- **hash algoritmi**:
  - Secure Hash Algoritam (SHA)
  - Message Digest 5 algoritam (MD5)



AUTENTIFIKACIJA UČESNIKA

Digitalni potpis predstavlja tehniku koja se bavi autentičnošću dokumenata i korisnika.

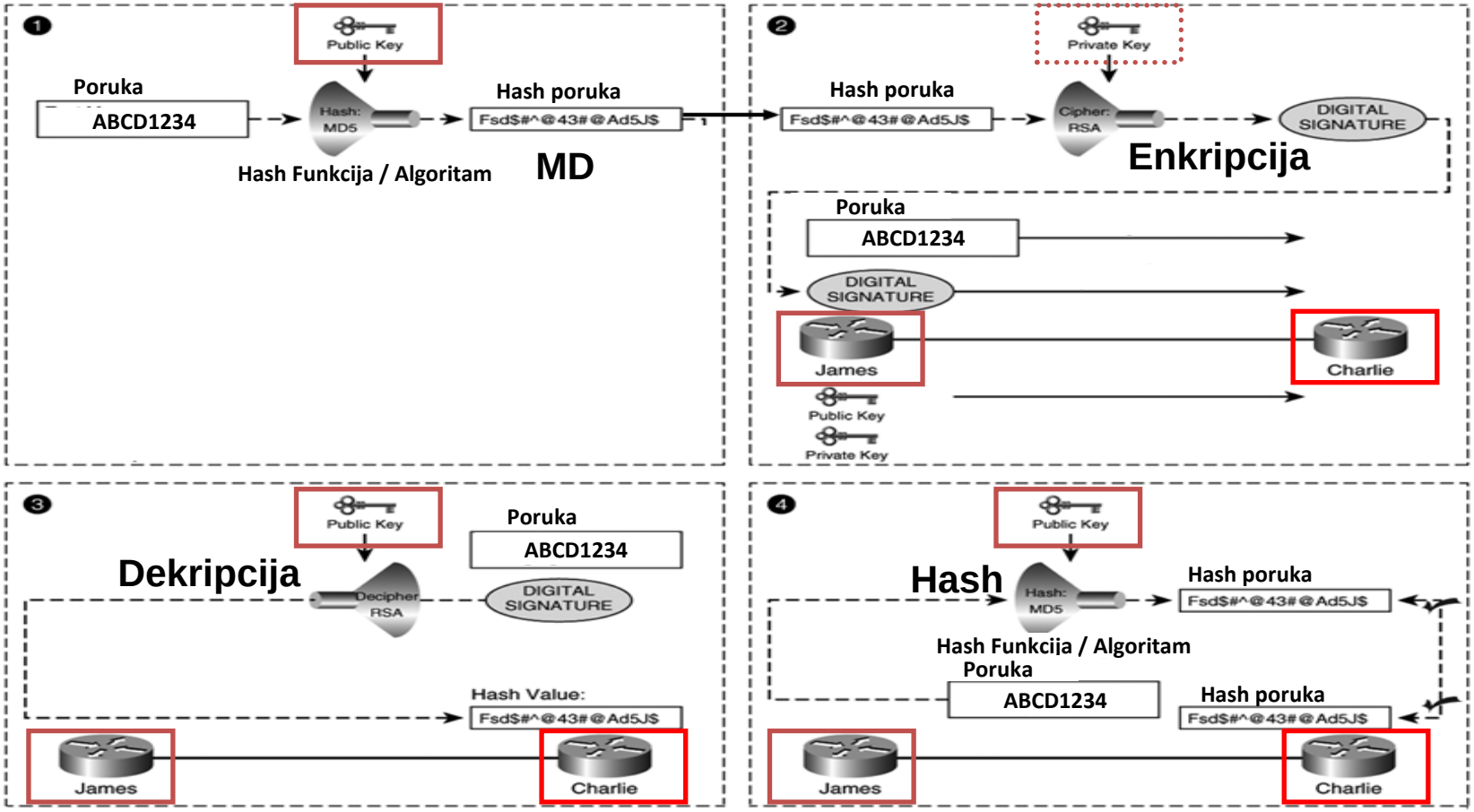
- Predstavlja skup podataka u elektronskom obliku koji je logički povezan drugim podacima koji služe za identifikaciju korisnika i autentifikaciju dokumenata.
- Životni ciklus digitalnog potpisa se odvija unutar infrastrukture javnog ključa (PKI) čije se uverenje izdaje od strane trećeg poverljivog lica od koga bezbednost javnog ključa:
  - Autoriteta za izdavanje sertifikata (CA)
  - Autoriteta za registraciju (RA)
  - Autoriteta za validaciju (VA)

DIGITALNI POTPIS

Digitalni potpis: Autentifikacija i Hash (Integrity)

Data autentifikacija proverava identitet uređaja koji je poslao poruku.

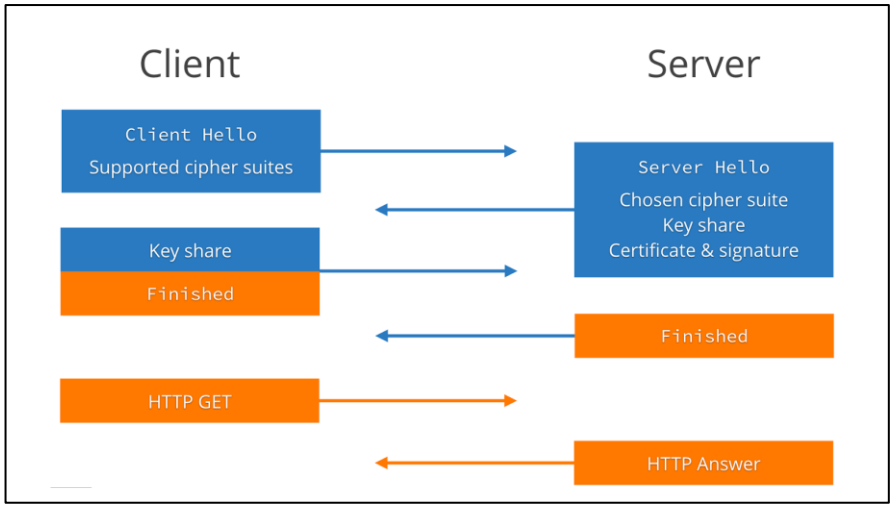
Digital Signatures koristi kombinaciju hash i asimetrične enkripcije da bi se obezbedii integritet i autentifikacija podataka.

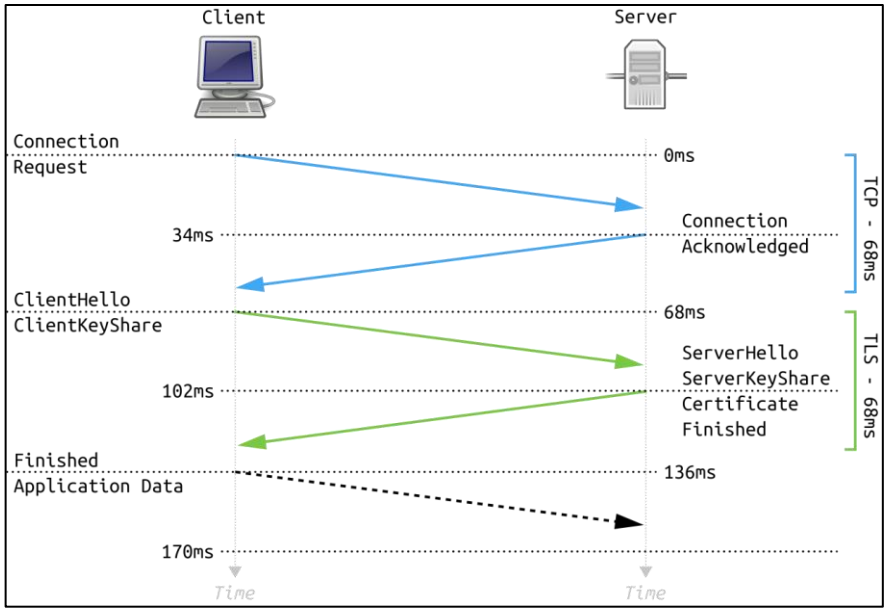


TLSv1.3 HANDSHAKE PROCEDURA

TLSv1.3 je efikasnija od svojih prthodnika u pogledu uspostavljnja bezbedne komunikacije

- Klijent šalje Hello poruku koja uključuje podržane verzije i podržane kriptografske parametre (algoritmi za šifrovanje, algoritmi za razmenu ključeva i predložene ključeve (share key) za svaku od podržanih verzija koji se koristi za dobijanje simetričnog ključa.
- Server dobija sve neophodne informacije, bira najveću zajedničku podržanu verziju i algoritme, generiše svoj ključ (share key) koji u kombinaciji sa ključem klijenta se koristi za dobijanje simetričnog ključa.
- Server na osnovu ovih parametara generiše sertifikat koji se šalje kriptovano i koristi se za autentifikaciju.
- Klijent ima sve informacije da kreira simetrični ključ na osnovu kojeg dekriptuje sertifikat.





TLS HANDSHAKE PROCEDURA

Cilj je kreiranje bezbedne komunikacije između klijenta i servera.

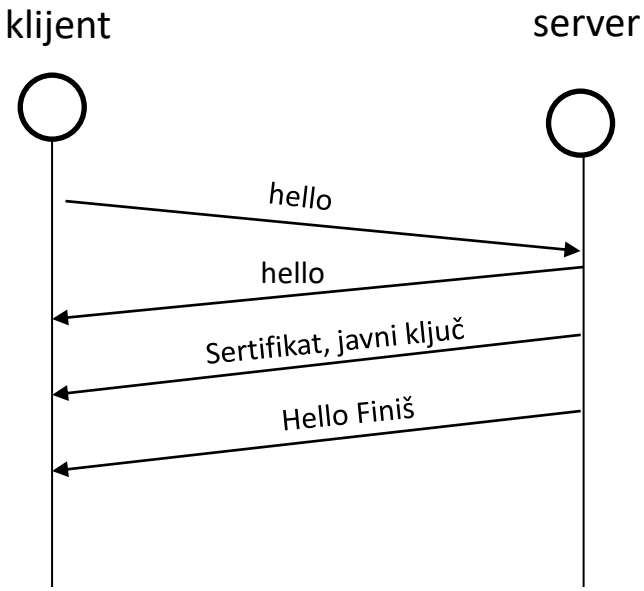
Bezbedna komunikacija se postiže ugovaranjem ključa (secret key) između klijenta i servera koji se koristi za kriptovanje i dekriptovanje poruka

TLS Handshake procedura treba da obezbedi bezbedno ugovaranje zajedničkog simetričnog ključa.

Hello poruka koju šalje klijent uključuje podržane verzije protokola i podržane algoritme za kriptovanje podataka, autentifikaciju i integritet podataka (cipher suites).

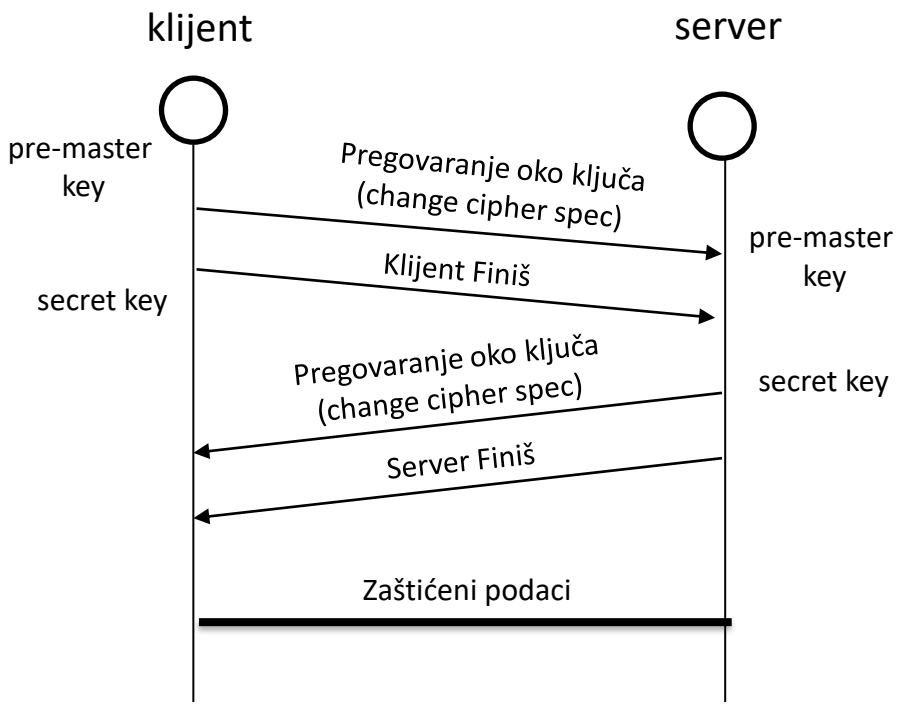
Hello poruka koju šalje server kao odgovor na hello poruku klijenta sadrži cipher suite (algoritamski paket) koji podržavaju obe strane i koji će da se koristi za uspostavljanje bezbedne komunikacije

Server šalje sertifikat koji sadrži javni ključ koji koristi klijent nakon provere autentičnosti sertifikata za kripciju podataka a u cilju bezbedne razmene simetričnog ključa



TLS HANDSHAKE PROCEDURA

- Na kraju razmene Hello poruka, klijent dobija javni ključ na osnovu kojeg zajedno sa parametrima iz sertifikata kreira pre-master ključ.
- Klijent kriptuje master key na osnovu javnog ključa dobijenog od servera koji zatim šalje serveru, change cipher spec faza.
- Server dekriptuje dobijenu poruku na osnovu svog privatnog ključa i saznaje pre-master ključ vrednost dobijenu od klijenta.
- Na osnovu pre-master ključa obe strane generišu secret (simetrični) ključ.



TLS CIPHER SUITS

- TLS (cipher suits) je protoklski stek koji sadrži protokole i algoritme koji se koriste za kreiranje bezbednog komunikacionog kanala između klijentske i serverske strane aplikacije.
- Klijent sadrži listu podržanih bezbedonosnih parametara (cipher suits) a server je taj koji odlučuje koji protokolski stek će se koristiti na osnovu podržanih od strane klijenta.
- Protokoli koji su deo protokolskog steka (cipher suits) su:
  - TLS 1.3, TLS 1.2, TLS 1.1, TLS 1.0, SSLv3 i SSLv2
- Algoritmi koji se koriste za razmenu ključeva su:
  - DH (Diffie Helman) i RSA (Ron Rivest, Adi Shamir and Leonard Adleman)
  - DH varijanta koja se koriste u TLS su ECDHE (Elliptic Curve Diffie-Hellman Ephemeral)
  - EC se koristi jer omogućava znatno manje dužine ključa a postiže isti stepen bezbednosti

Primer Chipher Suit parametara

TLS CIPHER SUITS

- Algoritmi koji se koriste za autentifikaciju:
  - RSA i ECDSA (Eliptic Curve Digital Signature Algorithm)
  - Zadužen je za proveru identiteta servera
  - Zasniva se na sertifikatu
- Simetrični algoritmi za šifrovanje (kriptovanje):
  - AES sa dodatnim modovima GCM ili CBC , Camellia, DES i RC4
- Algoritmi za proveru integriteta podataka MAC (Message Authentication Code):
  - SHA (Secure Hash Algorithm) ili MD5
  - HASH funkcija omogućava da se odradi promena tj. smanjenje veličine poruke

Primer Chipher Suit parametara koristi heksa prezentaciju

DIGITALNI SERTIFIKATI

Struktura podataka koja za cilj ima pouzdano povezivanje javnog ključa sa podacima o njegovom nosiocu, obezbeđujući na taj način proveru identiteta

- Da bi se uspostavila bezbedna komunikacija između web browser-a (klijent) i web servera potrebno je da klijent od web servera dobije sertifikat tokom faze inicijalizacije bezbedne konekcije (handshake faza)
- Podaci koji se nalaze u sertifikatu su bitni za uspostavljanje bezbedne komunikacije između klijenta i servera.
- Osnovni parametri svakog sertifikata su:
  - ***Verzija sertifikata*** npr *version 3* koja opisuje po standardu (X.509) šta sve treba da sadrži od parametara.
  - ***Serijski broj*** *je* jedinstven broj koji se zadaje konkretnom sertifikatu i izdaje se od strane sertifikacionog tela (CA)

Primer sertifikata

```
Certificate:
   Data:
      Version: 1 (0x0)
      Serial Number: 7829 (0x1e95)
      Signature Algorithm: md5WithRSAEncryption
      Issuer: C=ZA, ST=Western Cape, L=Cape Town,
              O=Thawte Consulting cc,
         OU=Certification Services Division,
         CN=Thawte Server CA/Email=server-certs@thawte.com
      Validity
         Not Before: Jul  9 16:04:02 1998 GMT
         Not After : Jul  9 16:04:02 1999 GMT
      Subject: C=US, ST=Maryland, L=Pasadena, O=Brent Baccala,
         OU=FreeSoft, CN=www.freesoft.org/
         Email=baccala@freesoft.org
      Subject Public Key Info:
         Public Key Algorithm: rsaEncryption
         RSA Public Key: (1024 bit)
            Modulus (1024 bit):
               00:b4:31:98:0a:c4:bc:62:c1:88:aa:dc:b0:c8:bb:
               33:35:19:d5:0c:64:b9:3d:41:b2:96:fc:f3:31:e1:
               ...
            Exponent: 65537 (0x10001)
   Signature Algorithm: md5WithRSAEncryption
      93:5f:8f:5f:c5:af:bf:0a:ab:a5:6d:fb:24:5f:b6:59:5d:9d:
      92:2e:4a:1b:8b:ac:7d:99:17:5d:cd:19:f6:ad:ef:63:2f:92:
      ...
```

DIGITALNI SERTIFIKATI

- **Signature Algorithm** ili algoritam za hešovanje koji sertifikaciono telo koristi da potpiše sertifikat kao npr SHA 256 ili RSA
- **Signature Hash Algorithm** je algoritam koji se koristi za potpisivanje hash-a tj. Izlaza iz hash generatora. Obično je SHA 256.
- **Issuer (Izdavač)** je ovlašćeno sertifikaciono telo
- **Valid dates** (vreme važenja) sertifikata
- **Subject informacije** o nosiocu kao što su zemlja, grad, ime,...
- **Public key** ili javni ključ npr RSA 2048 koji klijent koristi da bezbedno pošalje podatke serveru
- **AIA** sadrži URL adresu gde browser može da proveri validnost sertifikata (Online Cestificate Status protocol) da nije kompromitovan

Primer sertifikata

```
Certificate:
   Data:
      Version: 1 (0x0)
      Serial Number: 7829 (0x1e95)
      Signature Algorithm: md5WithRSAEncryption
      Issuer: C=ZA, ST=Western Cape, L=Cape Town,
              O=Thawte Consulting cc,
         OU=Certification Services Division,
         CN=Thawte Server CA/Email=server-certs@thawte.com
      Validity
         Not Before: Jul  9 16:04:02 1998 GMT
         Not After : Jul  9 16:04:02 1999 GMT
      Subject: C=US, ST=Maryland, L=Pasadena, O=Brent Baccala,
         OU=FreeSoft, CN=www.freesoft.org/
         Email=baccala@freesoft.org
      Subject Public Key Info:
         Public Key Algorithm: rsaEncryption
         RSA Public Key: (1024 bit)
            Modulus (1024 bit):
               00:b4:31:98:0a:c4:bc:62:c1:88:aa:dc:b0:c8:bb:
               33:35:19:d5:0c:64:b9:3d:41:b2:96:fc:f3:31:e1:
               ...
            Exponent: 65537 (0x10001)
   Signature Algorithm: md5WithRSAEncryption
      93:5f:8f:5f:c5:af:bf:0a:ab:a5:6d:fb:24:5f:b6:59:5d:9d:
      92:2e:4a:1b:8b:ac:7d:99:17:5d:cd:19:f6:ad:ef:63:2f:92:
      ...
```

SERTIFIKACIONO TELO

- **S**ertifikaciono telo (CA) je entitet koji digitalno potpisuje primljene zahteve za digitalne sertifikate. Ono je neophodno u procesu izdavanja digitalnih sertifikata, jer predstavlja instituciju kojoj se veruje.

- Poverenje u CA se sprovodi tako što je na vrhu vrhovno državno sertifikaciono telo (Root CA – kao da je u korenu stabla). Ono je dobro čuvano, kako fizički tako i elektronski, i ima skup strogih pravila po kojima radi.

- Za razliku od ostalih, Root CA telo samo sebi potpisuje digitalni sertifikat.

- U našoj zemlji ono je pod upravom Ministarstva za nauku.

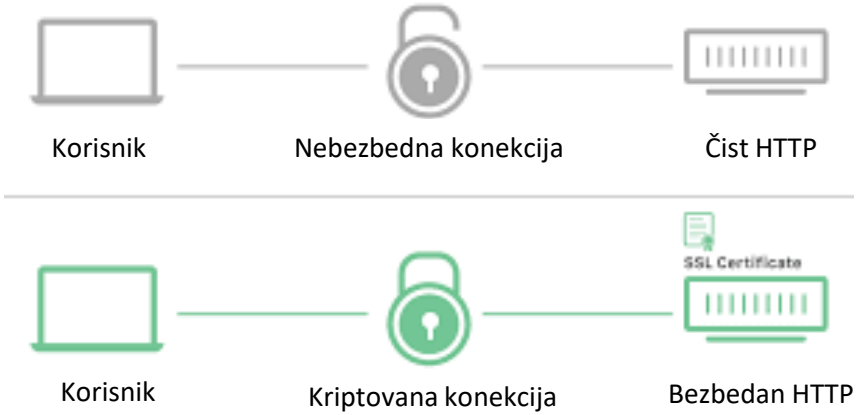
- Od ovog tela se ne može kupiti digitalni sertifikat.

- Root CA ih izdaje samo tzv. među-CA telima (Intermediate CA, kratko ICA), koja komercijalno izdaju sertifikate.

- Korisnici mogu kupiti kvalifikovani digitalni sertifikat samo od ICA tela, kojih će u Srbiji biti nekoliko. Root CA nije univerzalno telo, već se koriste različita za elektronske pasoše, lične karte...

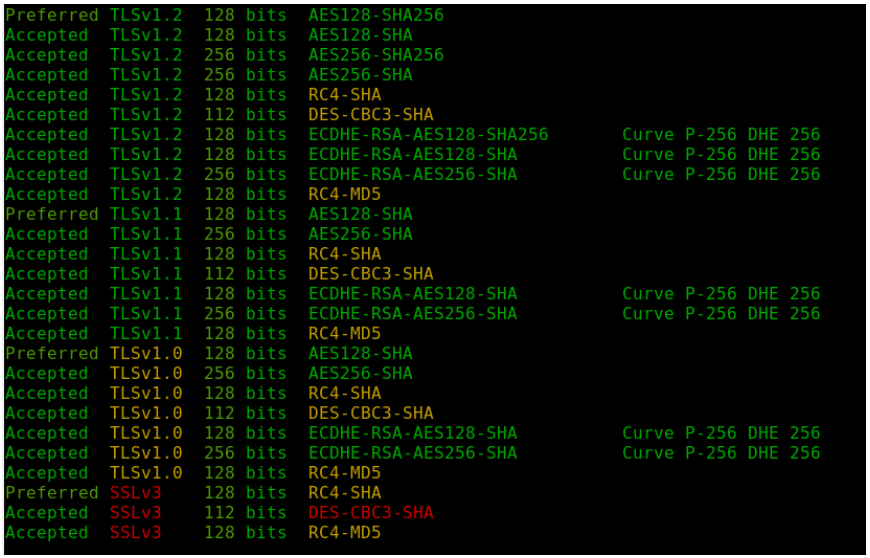
HTTPS

- HTTP je kreiran kao čist tekstualni protokol koji ne uključuje mehanizme za zaštitu podataka između klijenta i servera
- HTTPS je implementacija zaštićenog HTTP protokola
- HTTPS obezbeđuje formiranje zaštićenog kanala za prenos HTTP paketa između klijenta i servera zasnovan na TLS (Transport Layer Security) protokolu, ranije na SSL (Secure Socket Layer).
- SSL je zastareo i 2014 je zamenjen TLS standardom
  - Postoje web sajtovi koji koriste SSLv3 zbog loše konfiguracije ili kompatibilnosti sa starim verzijama.
  - Kriptoanalitičari bez velikog napora mogu da probiju pakete koji su zaštićeni nekom od starijih SSL verzija koristeći snagu računara koja je danas dostupna



ALATI ZA DETEKCIJU RANJIVIH SSL/TLS KONFIGURACIJA

- OPEN SSL KLIJENT
  - SSL/TLS klijent koji uključuje funkcionalnosti za pokretanje osnovnih testova na HTTPS serveru
  - Prikazuje opširnije informacije o parametrima konekcije i razmenu sertifikata
  - Sadrži opcije za testiranje samo željene verzije protokola
  - Danas se sve SSL verzije i TLS 1.0 smatra nepouzdanim
- SSLScan
  - Alat koji vraća listu protokola i paketa za kripciju koje SSL/TLS server prihvata



ALATI ZA DETEKCIJU RANJIVIH SSL/TLS KONFIGURACIJA

- SSLyze
  - Slična je po načinu rada sa SSLScan alatom
  - Može više hostova da skenira istovremeno da testira performasne i da upotrebi sertifikat klijenta za proveru identiteta
- Nmap
  - Uključuje skript *ssl – enum – ciphers* koji može da identifikuje koje pakete za kripciju podržava server i da ih ocenjuje na osnovu kriptografske jačine