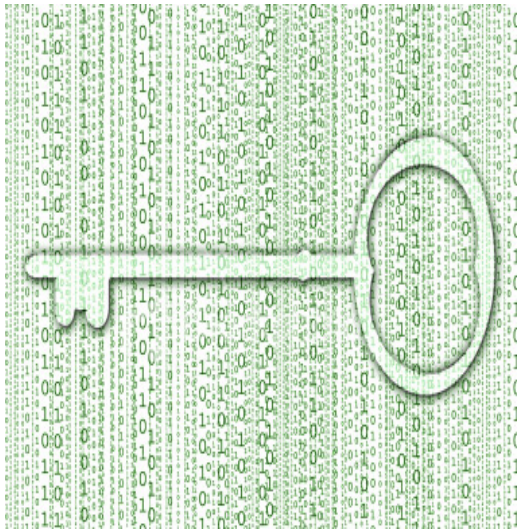
Bezbednost Aplikacija
Osnove Bezbednosti Podataka

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



1. AUTENTIFIKACIJA (Authentication)

Provera identiteta

Šta znači?

Sistem mora da proveri ko pokušava da pristupi sistemu i da li je korisnik zaista osoba za koju se predstavlja.

Primeri:

- Korisničko ime i lozinka
- Otisak prsta
- Face ID
- Smart kartice
- OTP kodovi

SUŠTINA:

„Dokaži da si ti zaista ti.“

2. POVERLJIVOST PODATAKA (Data Confidentiality)

Kripcija podataka

Šta znači?

Podatke mogu da čitaju samo ovlašćeni korisnici. Napadač koji presretne komunikaciju ne može da razume sadržaj.

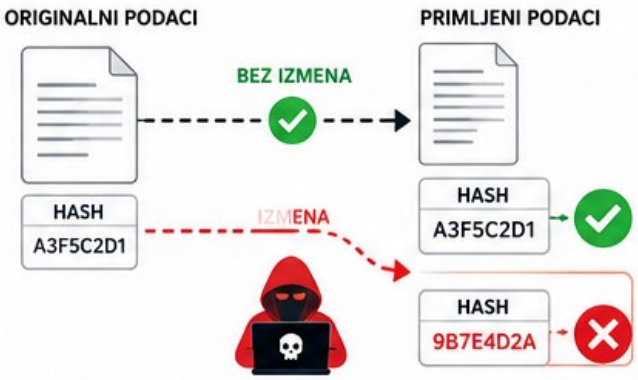
Kako se postiže?

- Enkripcija (AES, RSA)
- VPN tuneli
- HTTPS / TLS protokoli

SUŠTINA:
„Samo ovlašćeni smeju da vide podatke."

3. INTEGRITET PODATAKA (Data Integrity)

Zaštita od modifikacije tokom prenosa



Šta znači?

Podaci nisu promenjeni tokom prenosa ili skladištenja. Primalac dobija potpuno iste podatke koje je pošiljalac poslao.

Kako se postiže?

- Hash funkcije
- Digitalni potpisi
- Checksum mehanizmi
- MAC kodovi

SUŠTINA:

„Podaci moraju ostati nepromenjeni.“

PRIMER:

Ako preuzimate instalaciju programa i hash vrednost nije ista kao originalna, znači da je fajl možda izmenjen ili oštećen.

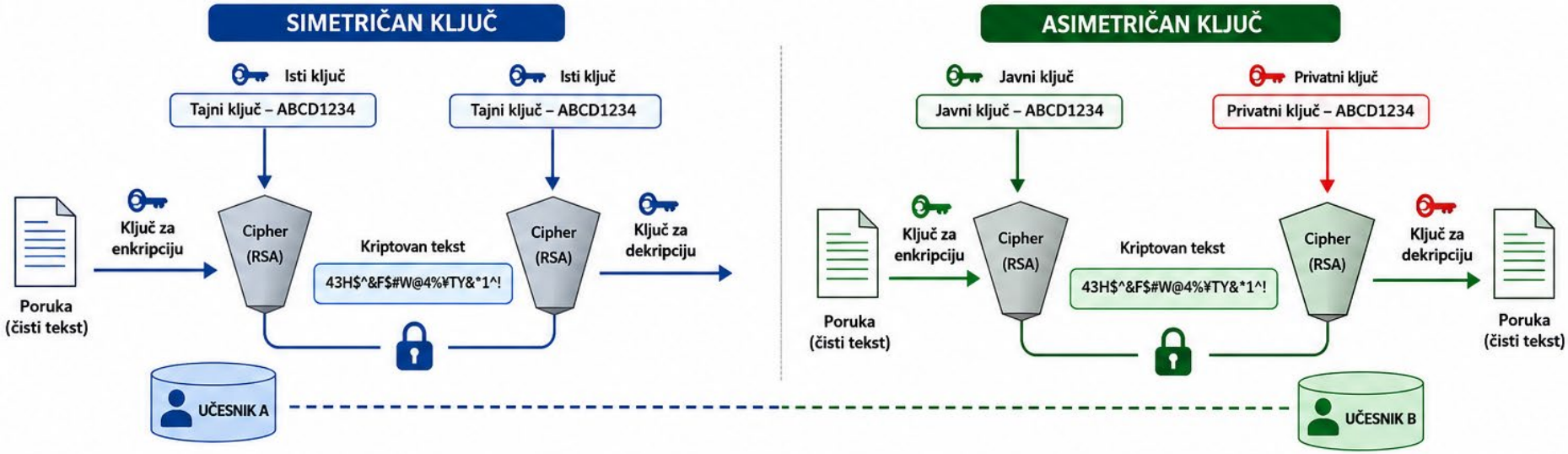
OSNOVI KRIPTOGRAFIJE - TERMINI

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)



OSNOVI KRIPTOGRAFIJE - TERMINI

Moderne tehnike kriptografije predstavljaju algoritmi koji pomoću matematičkih transformacija razumljivu poruku predstavljaju kao dugi niz karaktera čineći je nerazumljivom sve do krajnjeg korisnika

Prilikom šifrovanja, pored čistog teksta, koristi se nezavisna vrednost koja se naziva ključ šifrovanja, a na prijemnoj strani ključ dešifrovanja.

Broj simbola koji predstavlja ključ naziva se **dužina ključa**.

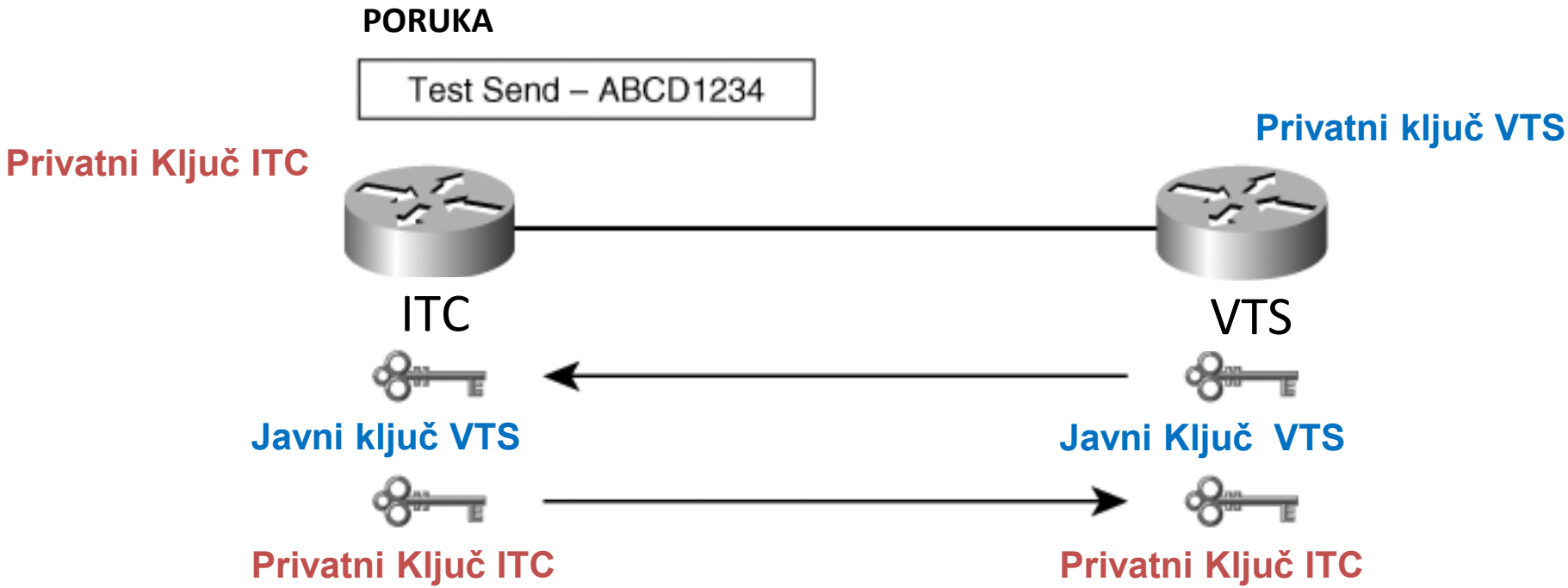
Duže dužine ključa zavise od sistema šifrovanja i jedan su od parametara sigurnosti tog sistema.

ASIMETRIČNA KRIPTOGRAFIJA

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

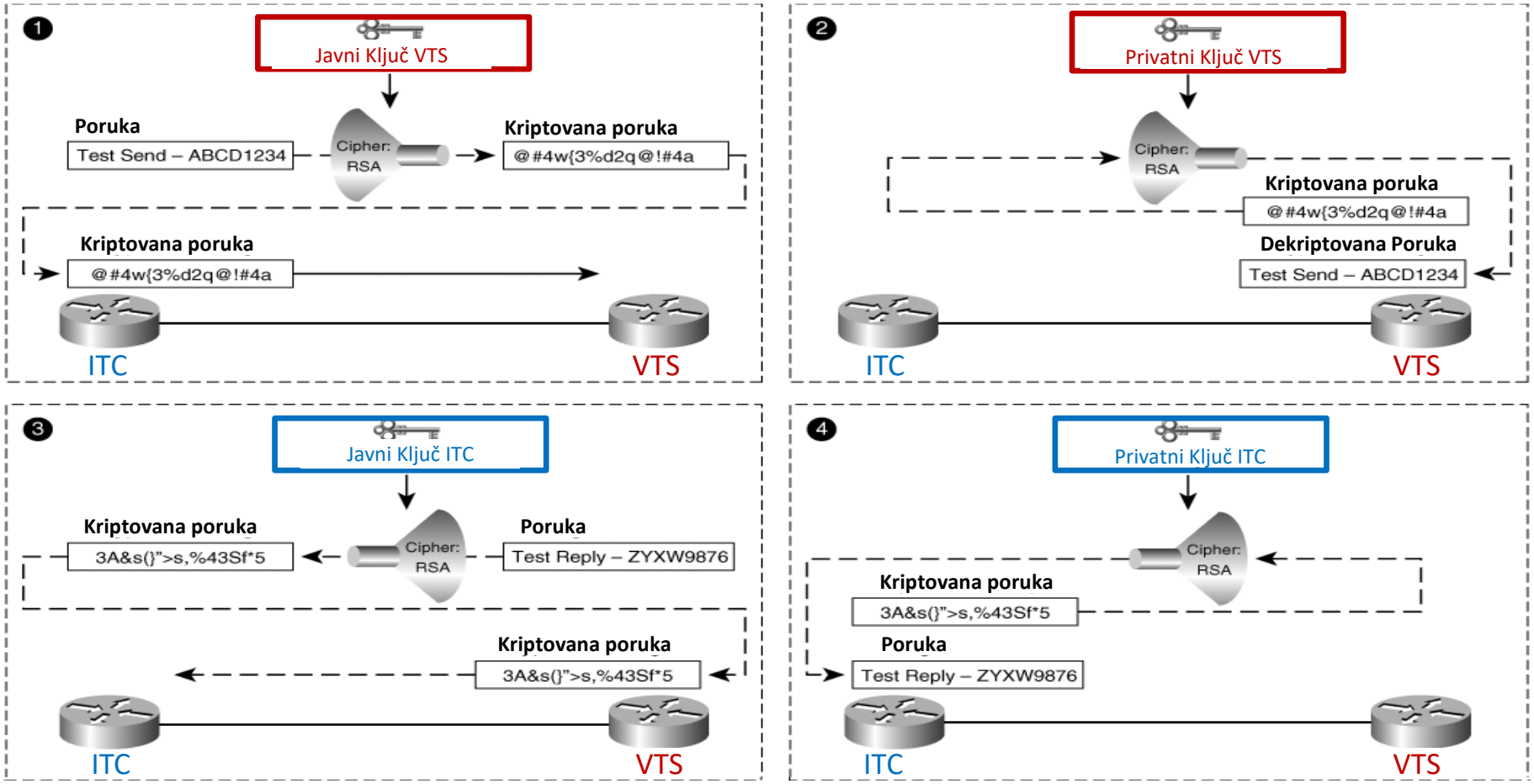
Privatni ključevi (dekriptuju podatke) – ne prosleđuju se učesnicima u komunikaciji.

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

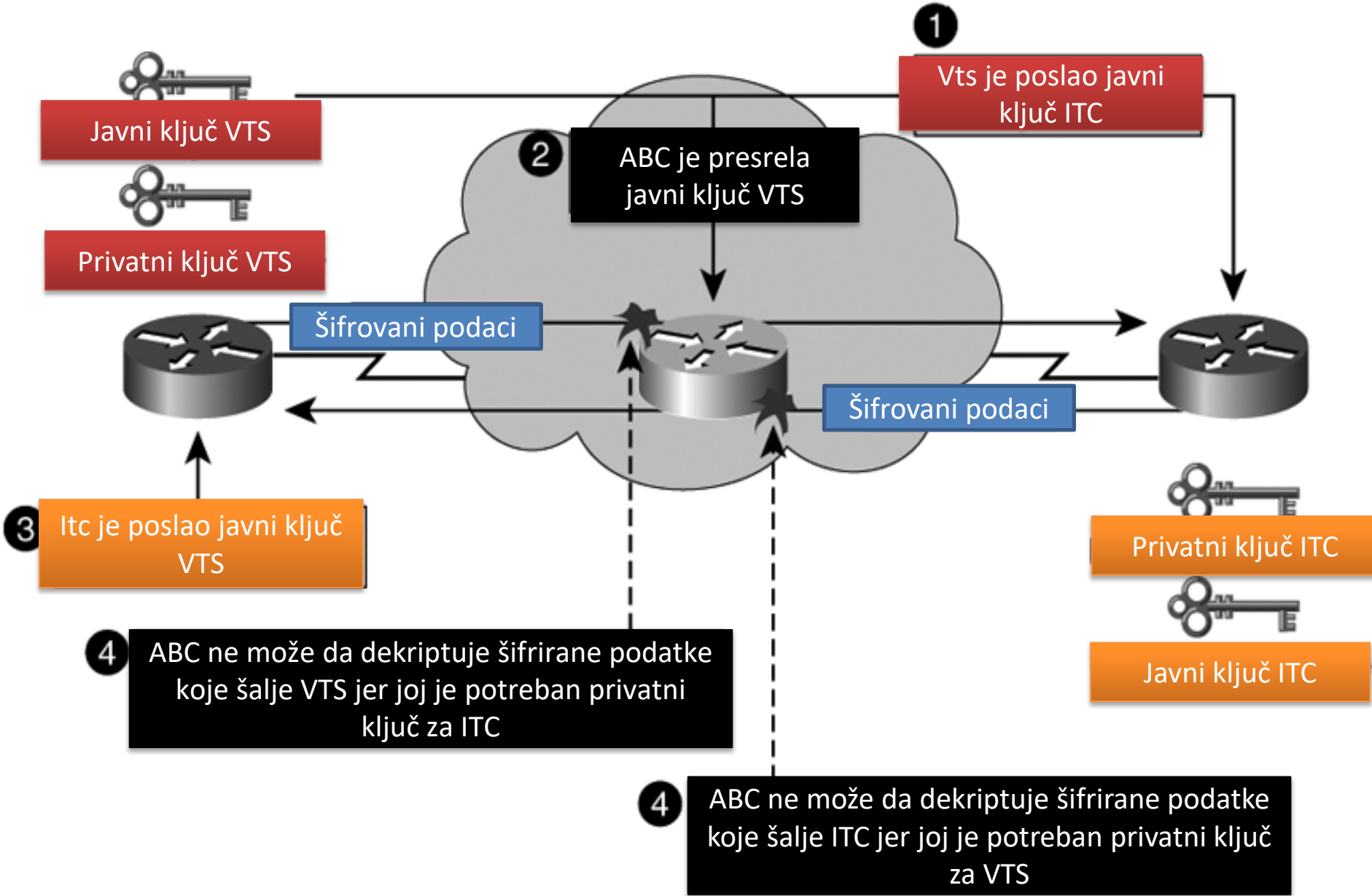


ASIMETRIČNA KRIPTOGRAFIJA – JAVNI / PRIVATNI KLJUČEVI

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



SIMETRIČNA KRIPTOGRAFIJA

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

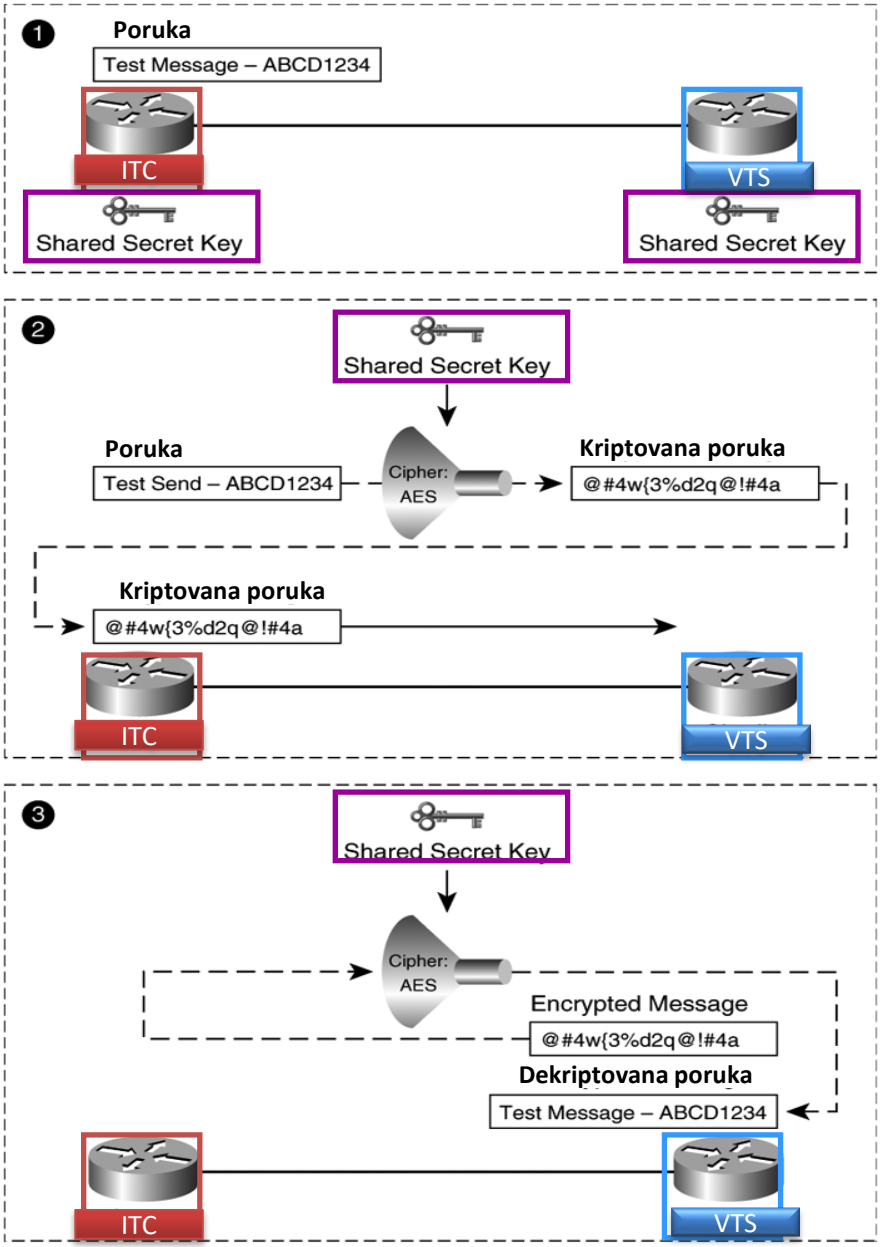
Neznatno jednostavnija operacija i znatno brža od asimetrične kriptografije .

Simetrična kriptografija je pogodna kod prenosa velike količine podataka.

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

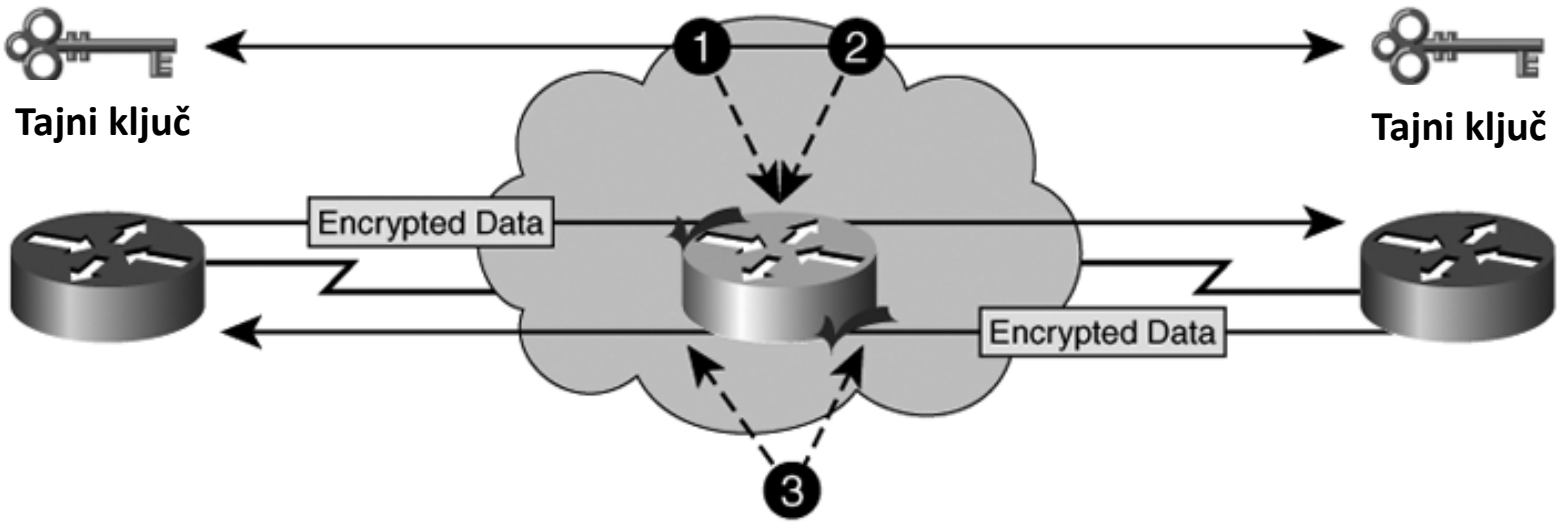
Simetrični algoritmi koji se najčešće koriste (DES,3DES ili AES)

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.

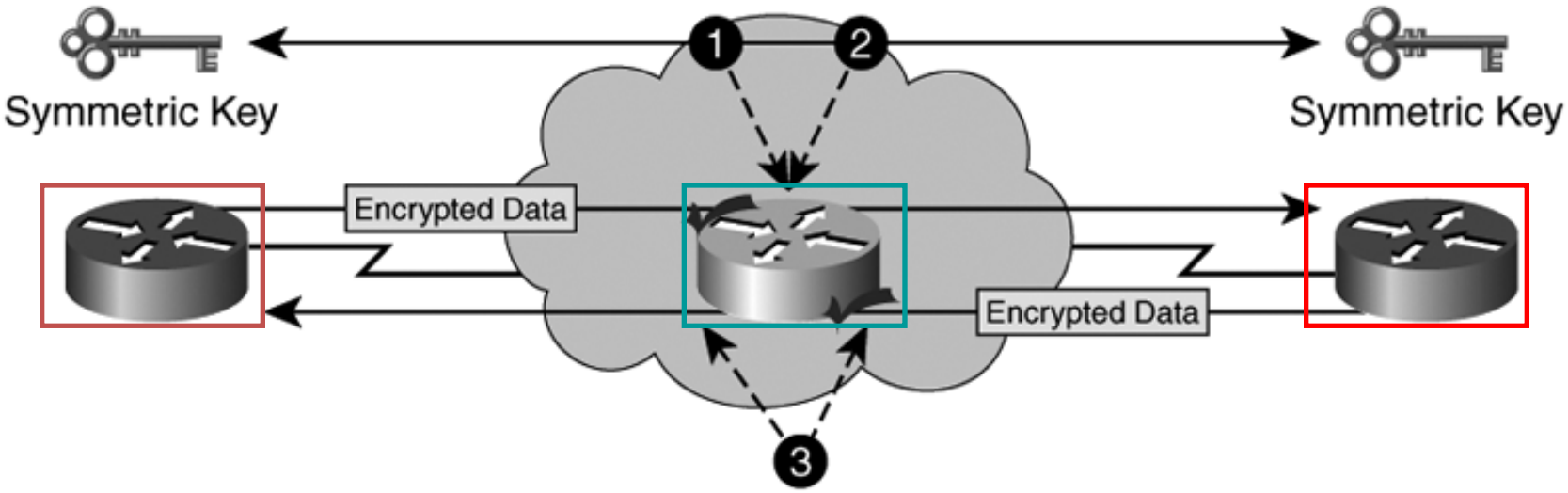


PRESRETANJE TAJNOG KLJUČA

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.



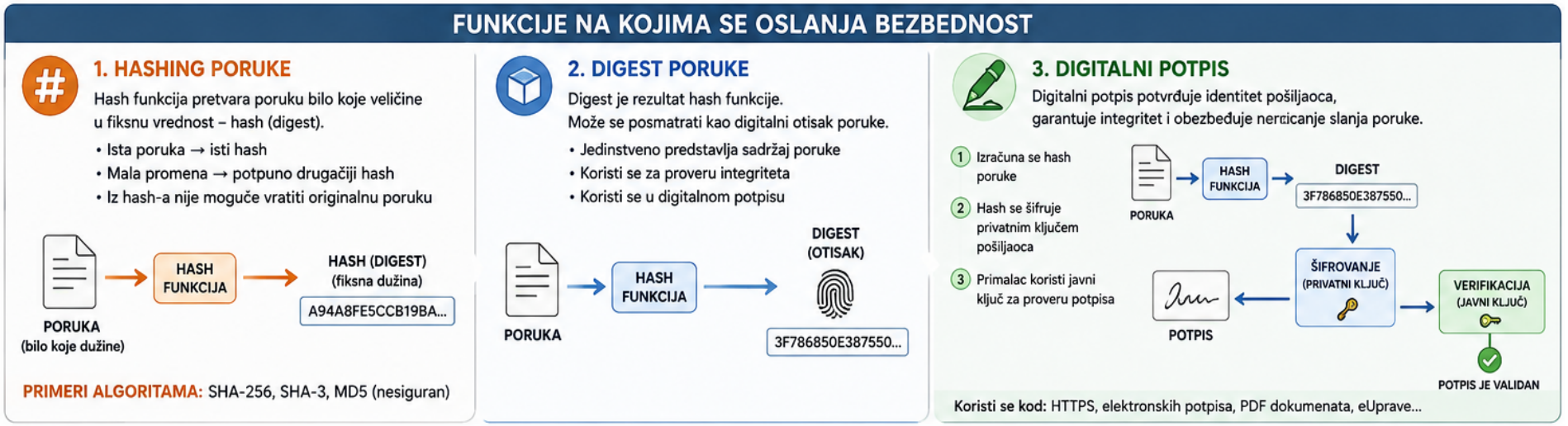
SIMETRIČNA ENKRIPCIJA Vs ASIMETRIČNE ENKRIPCIJE

Karakteristika	Simetrična kriptografija	Asimetrična kriptografija

AUTENTIFIKACIJA I INTEGRITET PODATAKA

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

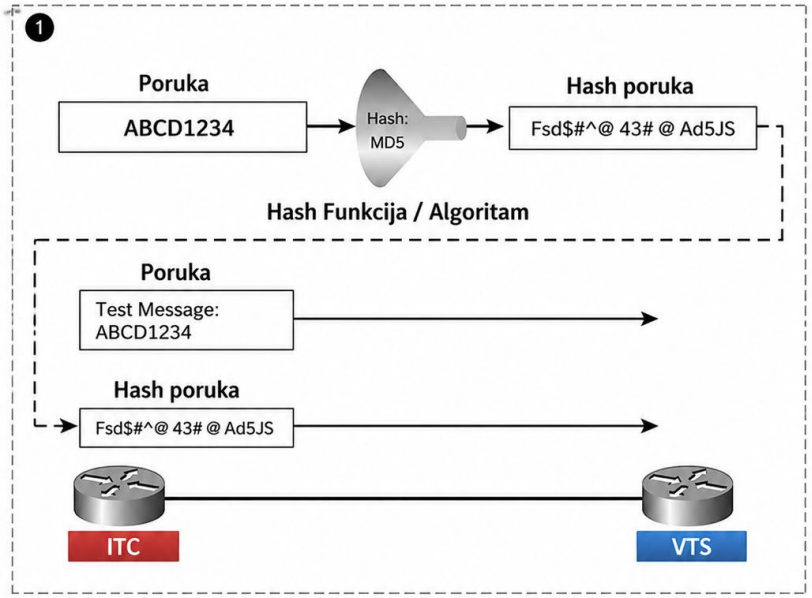
- Autentičnost poruke
- Integritet podataka
- Autentifikaciju pošiljaoca



INTEGRITET PODATAKA
MESSAGE DIGEST

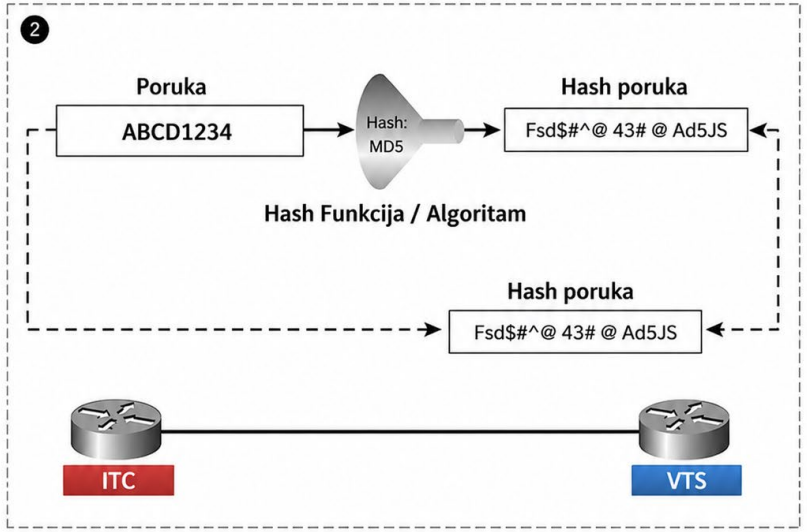
1.

- 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.

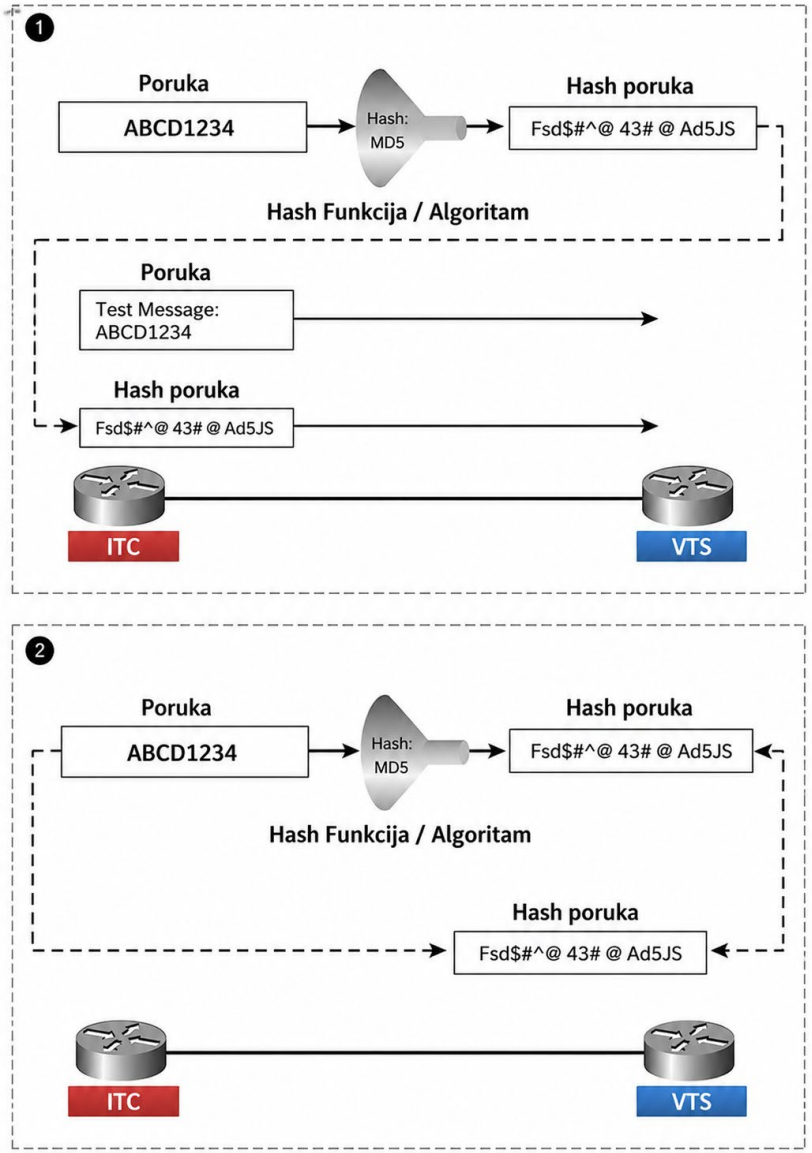
- VTS primljenu poruku, bez hash vrednosti, vodi na svoj hash generator.
- Upoređuje svoju dobijenu hash vrednost sa dobijenim hash-om od ITC.
- Ukoliko se dve hash vrednosti podudaraju očuvan je integritet poruke.



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



INTEGRITET PODATAKA + AUTH

Hashed Message Authentication Codes

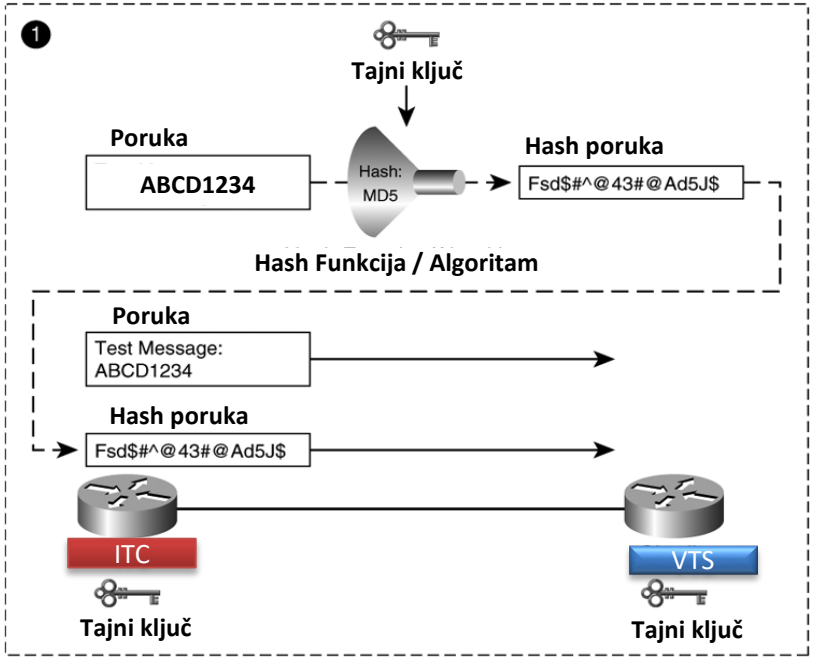
Integritet podataka proverava da li je poruka promenjena tokom prenosa.

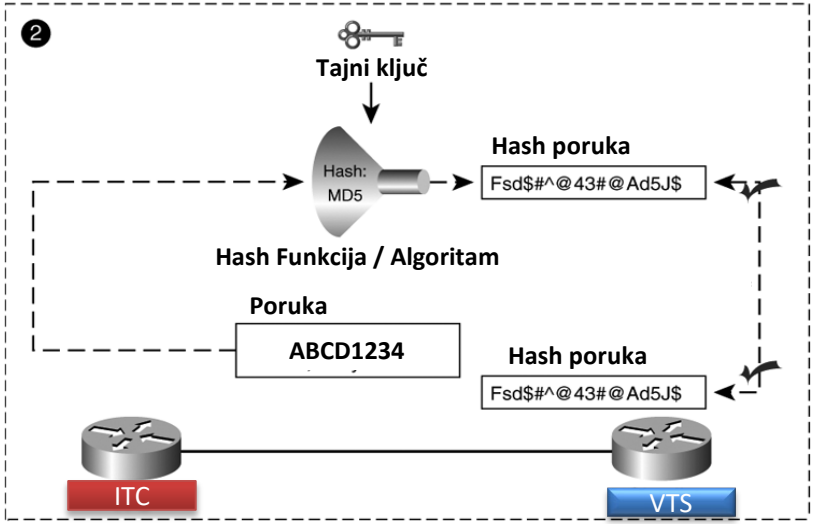
Hash obezbeđuje integritet podataka.

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





OSOBINE HASH FUNKCIJE

Osobina hash funkcije	Objašnjenje	Primer / Značenje

AUTENTIFIKACIJA UČESNIKA

Digitalni potpis je „elektronski dokaz” da je:

- poruku ili dokument poslala određena osoba
- i da dokument nije menjan

Digitalni potpis obezbeđuje 3 važne stvari:

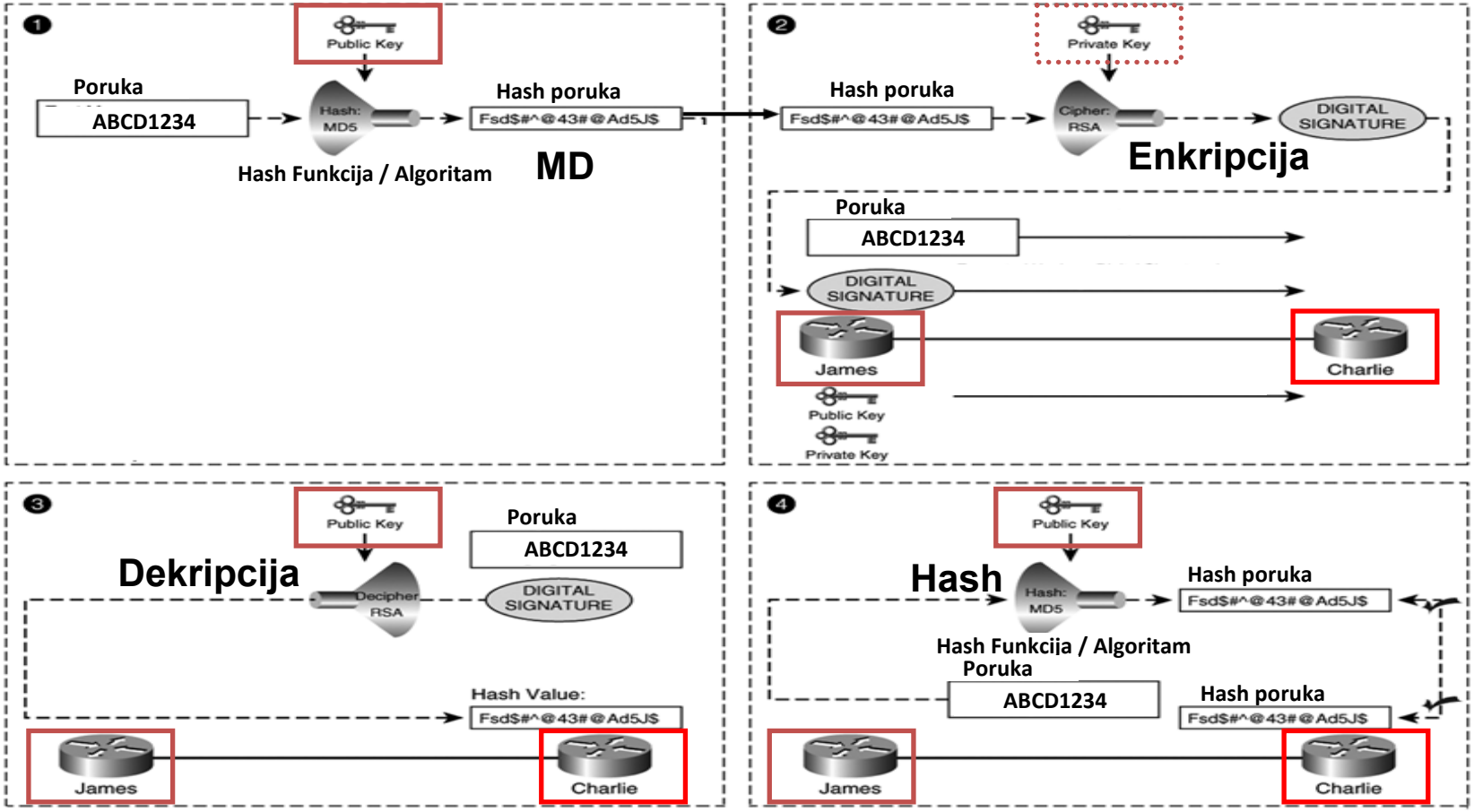
Funkcija	Šta znači
Autentifikacija	Znamo ko je poslao dokument
Integritet	Dokument nije menjan
Nericanje	Pošiljalac ne može da kaže „nisam ja poslao”

DIGITALNI POTPIS

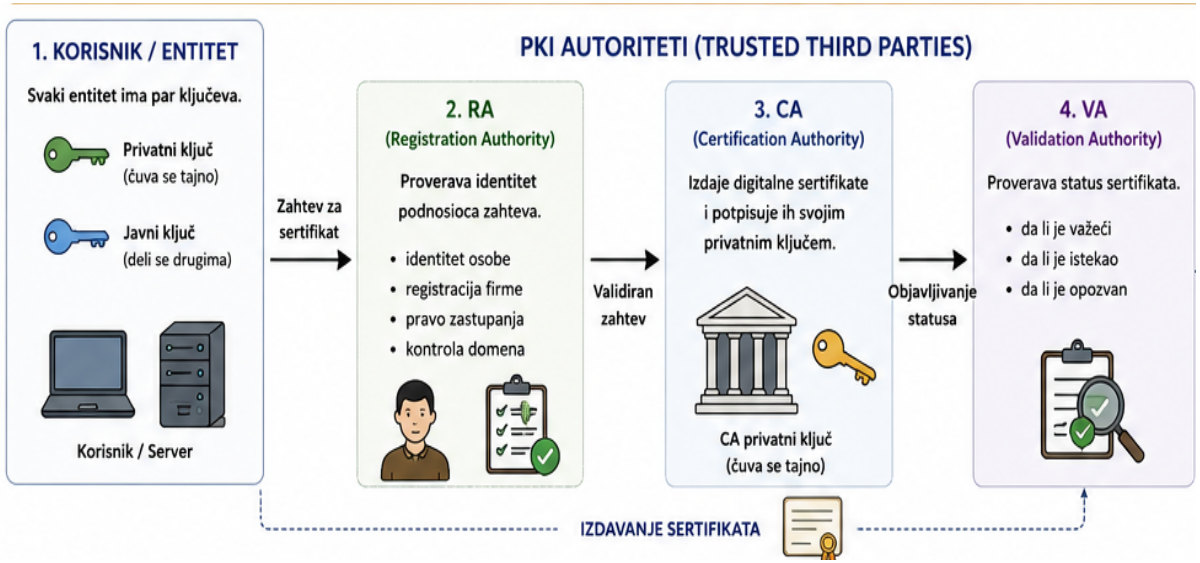
Digitalni potpis: Autentifikacija i Hash (Integrity)

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.



PKI INFRASTRUKTURA



Korisnik:
- šalje zahtev za sertifikat
- koristi sertifikat za autentifikaciju i digitalni potpis.

Registration Auth:
- proverava identitet korisnika
- proverava firmu ili domen
- proverava pravo pristupa.

CA (Sertifikacioni Autoritet):
- izdaje sertifikate
- digitalno ih potpisuje
- garantuje da javni ključ pripada određenom identitetu.

DIGITALNI SERTIFIKAT

Digitalni sertifikat povezuje:

👤 identitet + 🔓 javni ključ.

Sadrži:

ime vlasnika

javni ključ

Izdavaoca

rok važenja

serijski broj

digitalni potpis CA.

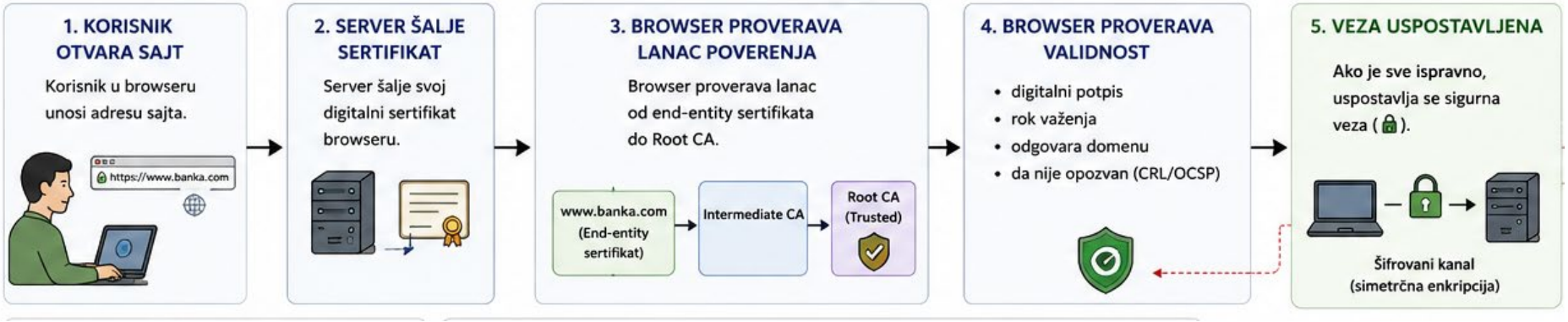
📌 Sertifikat omogućava:

✅ autentifikaciju

✅ poverenje

✅ sigurnu komunikaciju

USPOSTAVLJANJE SIGURNE VEZE PUTEM SERTIFIKATA



Korak	Uspostava sigurne veze
1	Korisnik otvara HTTPS sajt
2	Server šalje sertifikat
3	Browser proverava chain of trust
4	Browser proverava validnost sertifikata
5	TLS uspostavlja šifrovani kanal
6	Počinje sigurna HTTPS komunikacija