Virtuelne Privatne Mreže

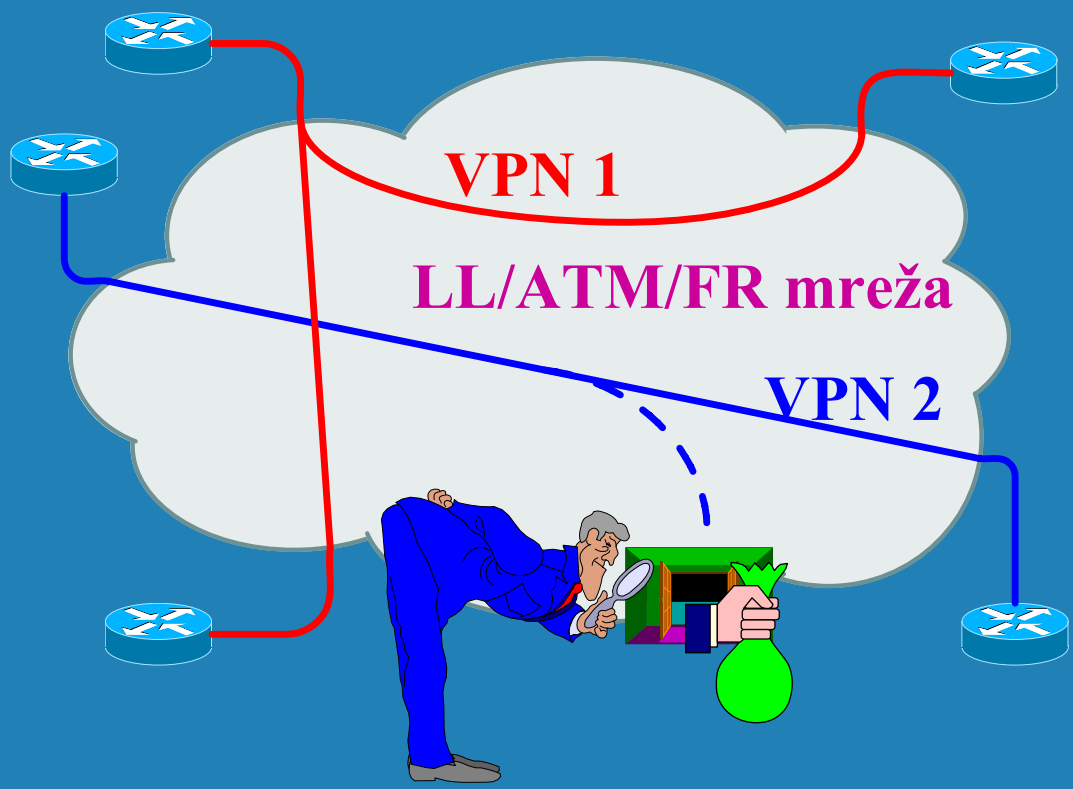
Kripto zaštita

Mr Nenad Krajnović, dipl. inž.
e-mail: krajko@etf.bg.ac.yu

VPN - kripto zaštita

- prethodno opisane metode su obezbeđivale ***virtuelne mreže***
- pošto se podaci prenose u čitljivom obliku privatnost se ne može garantovati, posebno ako se za realizaciju koristi neka javna mreža za prenos podataka tipa Interneta

VPN - kripto zaštita



VPN - kripto zaštita

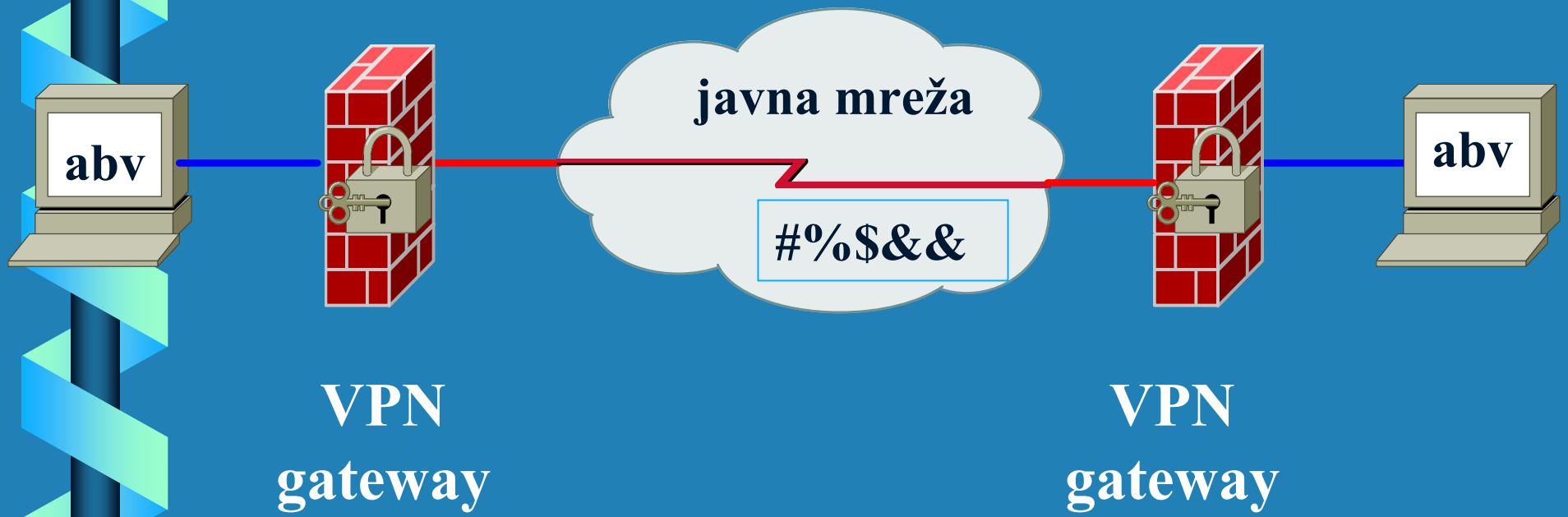
Zahtevi koji se postavljaju pred VPN mreže su:

1. sigurnost
2. pouzdanost
3. performanse

VPN - kripto zaštita

- koristi se u kombinaciji sa tunelovanjem podataka pri čemu se tunel definiše važnošću primenjene šifre
- u kombinaciji sa *firewall*-om obezbeđuje zaštitu lokalne mreže

VPN - kripto zaštita

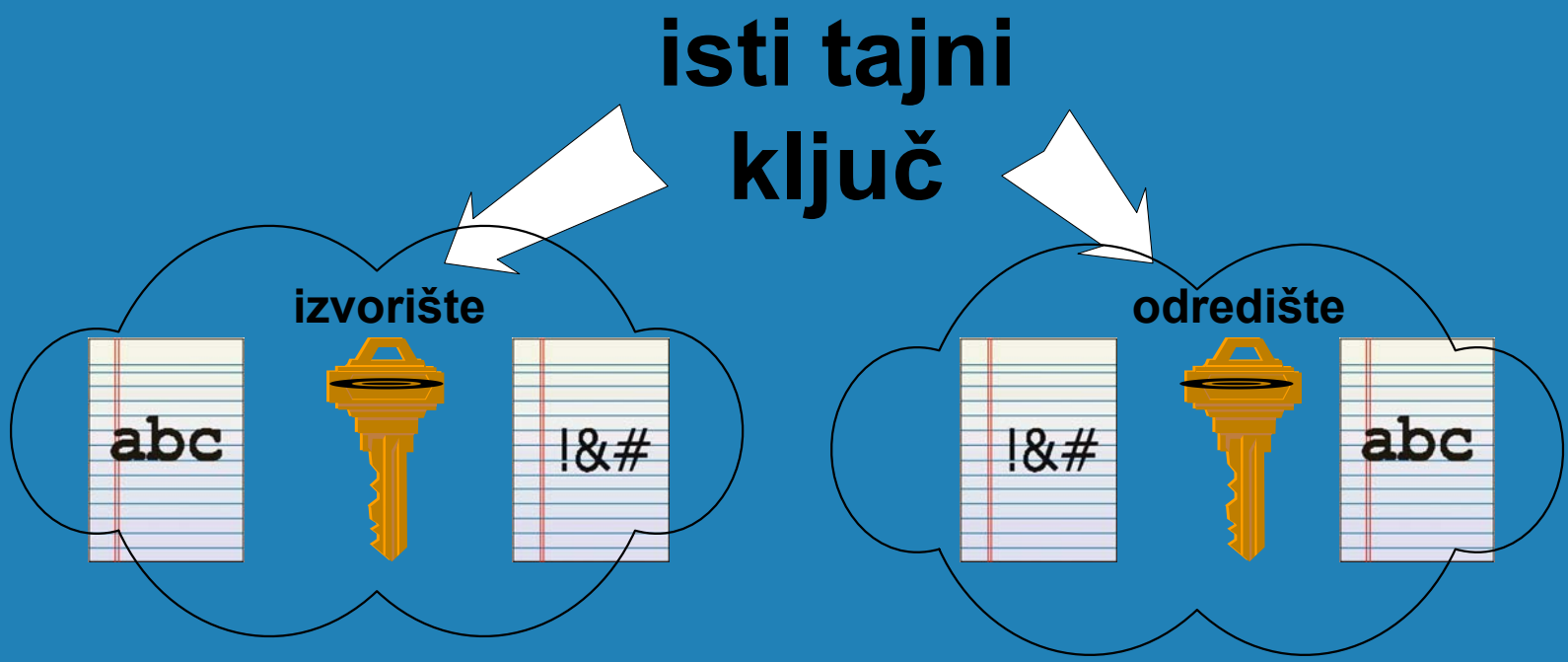


VPN - tipovi kripto zaštite

Dva osnovna sistema kripto zaštite:

- sistem sa simetričnim ključem - isti tajni ključ se koristi i za šifrovanje i za dešifrovanje podataka
- sistem sa asimetričnim ključem - postoje dva ključa, javni i tajni

VPN - sistem sa simetričnim ključem



VPN-sistem sa simetričnim ključem

- tajnost ključa utiče na sigurnost celog sistema
- brz sistem što je veoma dobro sa stanovišta performansi VPN *gateway*-a
- najčešće se koriste AES, RC-4, DES, TripleDES i FWZ-1 algoritmi
- dužina ključa utiče na kvalitet kripto zaštite (današnji ključevi su 56-bitni i više)

Dužina ključa (menja se sa napretkom računara)

Tip informacije	*Životni vek tajne*	*Minimalna veličina ključa*
Vojne taktičke informacije	Min/sati	Min 64 bita
Berzanski podaci, razvoj proiz.	Dani/nedelje	80
Biznis razvojni planovi	Godine	112
Recept Coca Cole	Decenije	Min 112
Identiteti špijuna	>50 god.	128
Strogo čuvane državne tajne	100 god	192

Vreme potrebno za razbijanje šifre (podaci iz 2003. godine)

Napadač	*Sredstva*	*Vreme potrebno za probijanje*			
		56 bita	64 bita	80 bita	128 bita
Pojedinac	**~$400 mreža PC ili FPGA**	**1 god**	**Neizvodivo**	**Neizvodivo**	**Neizvodivo**
korporacija	**$300K ASIC**	**10 min**	**2 dana**	**300 god**	**Neizvodivo**
Multinacionalna kompanija	**$10 mil**	**14 sec**	**2 sata**	**7 god**	**Neizvodivo**
Država	**$300 mil**	**Realno vreme**	**4 min**	**90 dana**	**Neizvodivo**

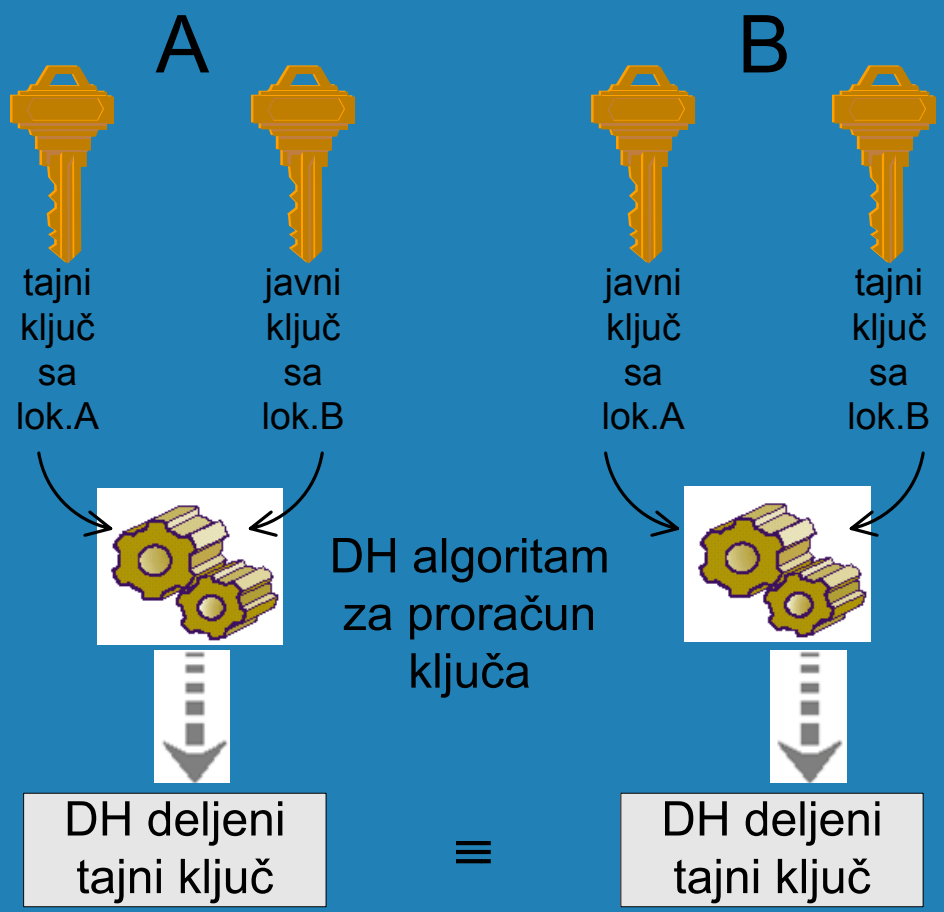
VPN-sistem sa asimetričnim ključem

- problem tajnosti ključa u sistemu sa simetričnim ključem razrešen je u sistemu sa asimetričnim ključem
- ovde se koriste dva ključa, javni i tajni
- javni ključ se slobodno distribuira dok je tajni poznat samo vlasniku
- kombinacijom javnog i tajnog ključa dobija se novi ključ koji se koristi za šifrovanje

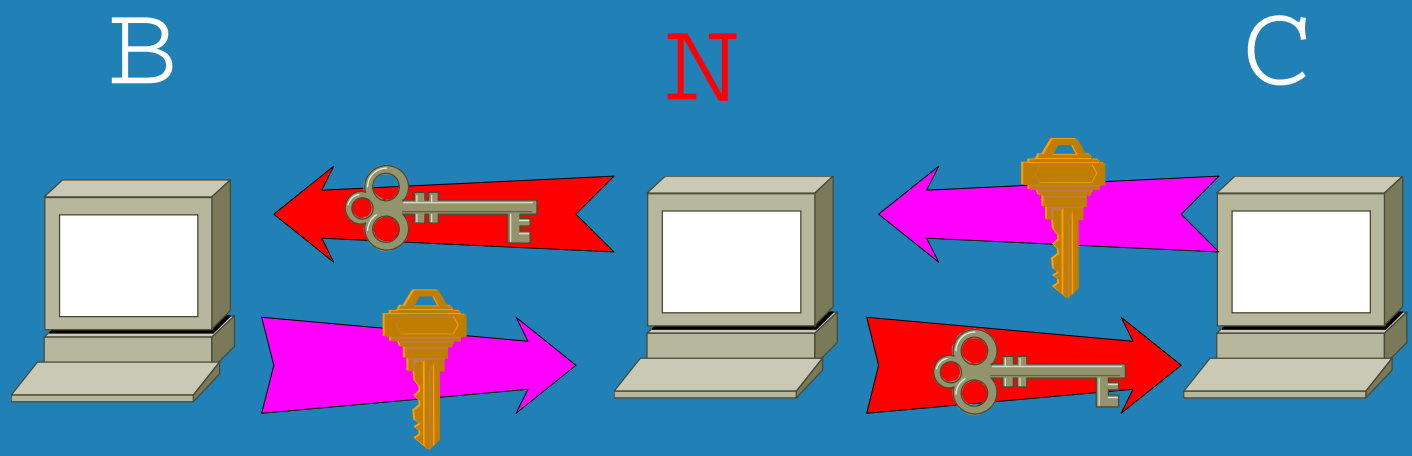
VPN-sistem sa asimetričnim ključem

- novodobijeni ključ se koristi za šifrovanje kao i kod sistema sa simetričnim ključem
- najčešće se koriste dva algoritma Diffie-Hellman (DH) i Rivest-Shamir-Adlemen (RSA)
- problem ako se neko ubaci u prenos javnih ključeva (*man-in-the-middle*)

DH algoritam



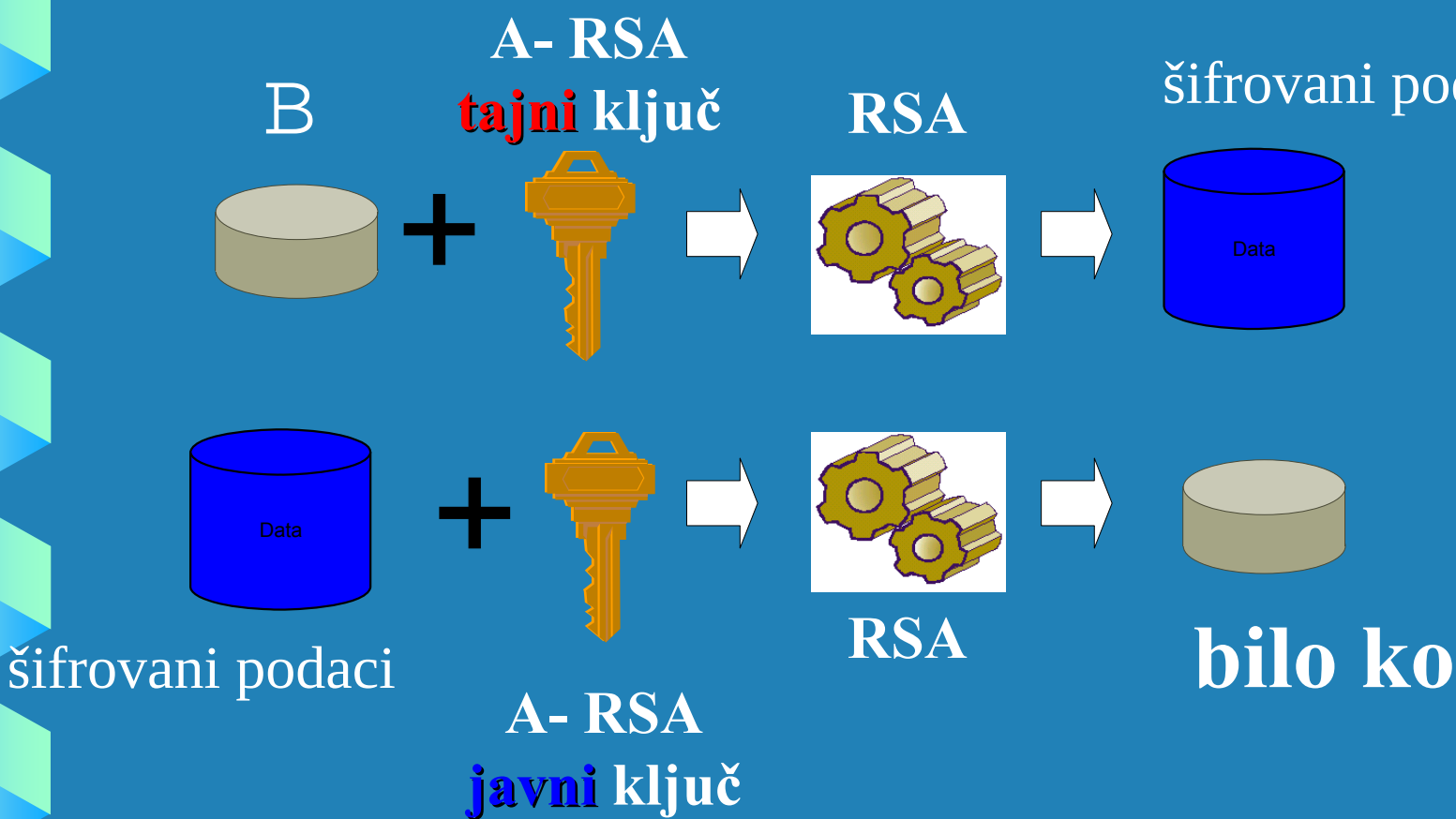
DH - *man-in-the-middle*



VPN - RSA algoritam

- problem trećeg u komunikaciji prevaziđen je korišćenjem RSA algoritma i uvođenjem digitalnog potpisa
- podaci šifrovani RSA tajnim ključem mogu biti dešifrovani **SAMO** RSA javnim ključem

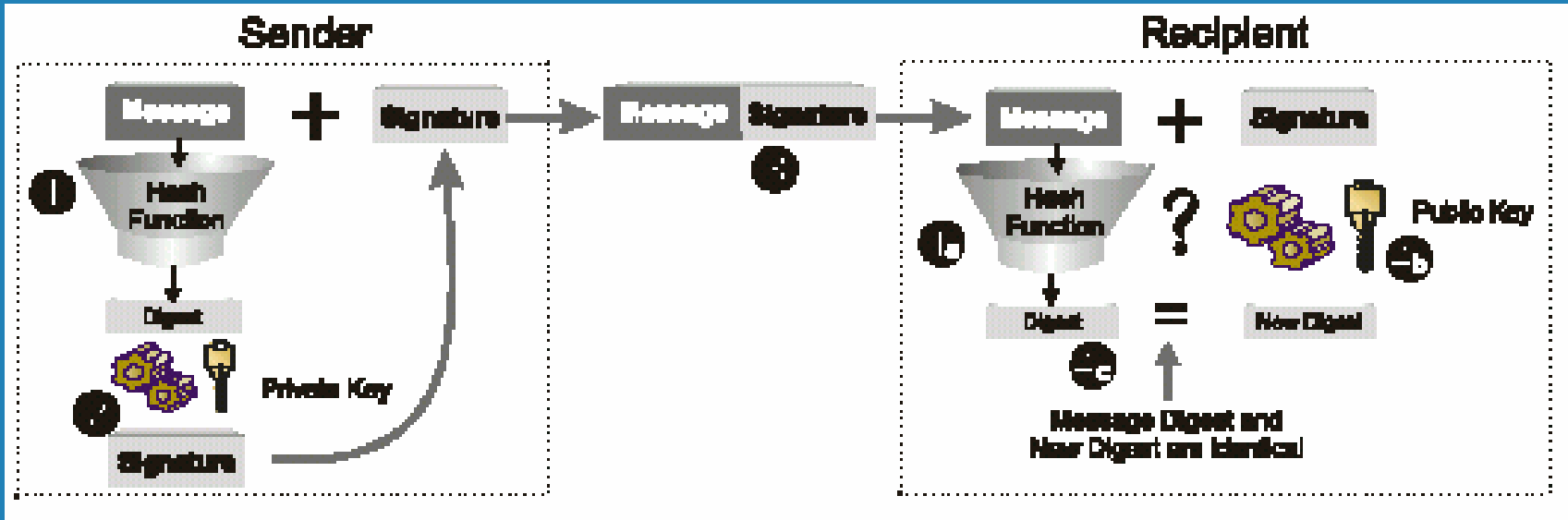
VPN - RSA algoritam



RSA - digitalni potpis

- RSA algoritam se može koristiti za kriptovanje podataka ili za ditalni potpis
- obezbeđuje sigurnost u poreklo poruke jer se samo sa odgovarajućim javnim ključem može dešifrovati poruka

RSA - digitalni potpis

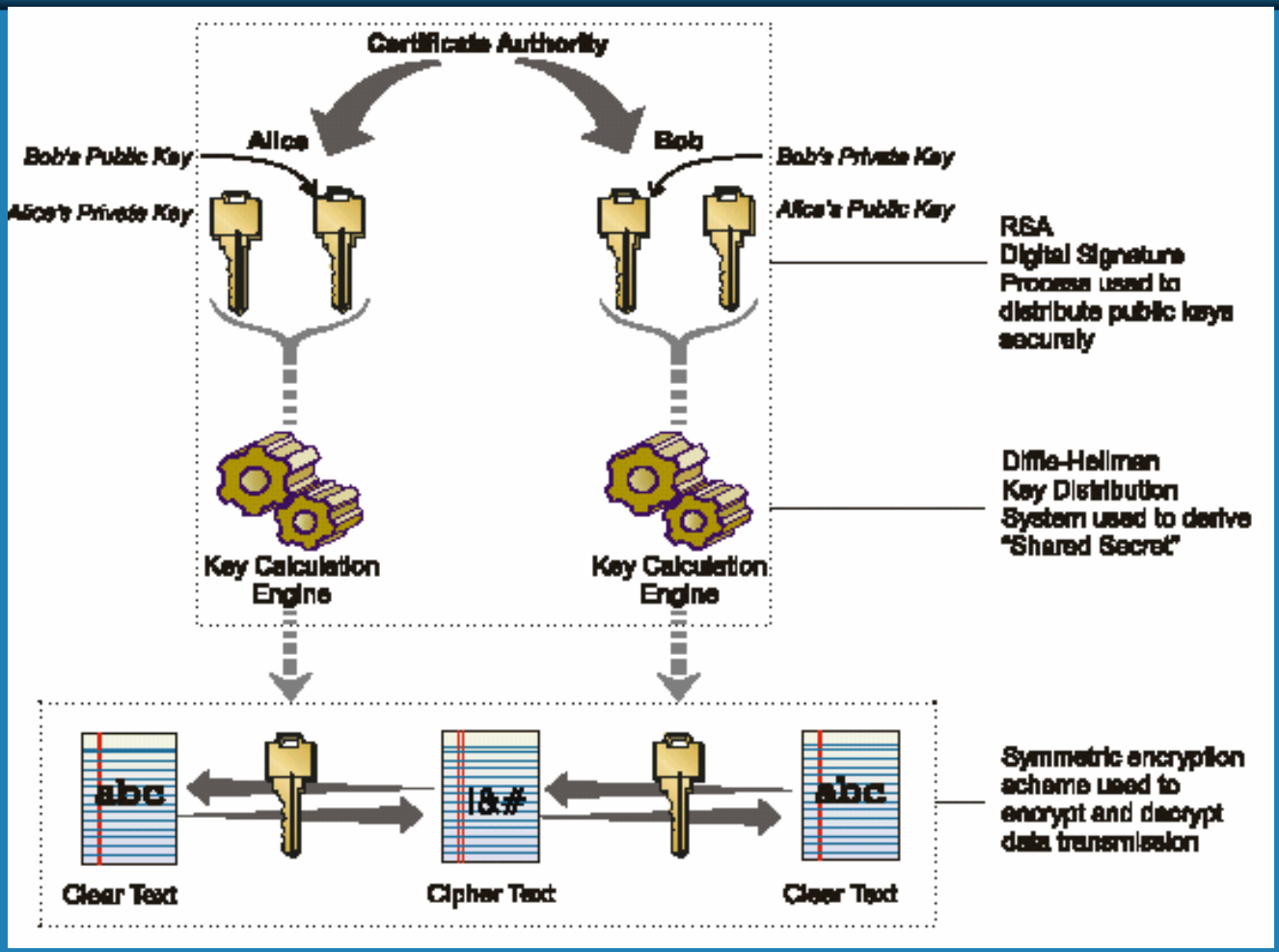


hash funkcije koje se danas koriste: MD4, MD5, SHA-1, CBC-DES-MAC

VPN - distribucija ključeva

- Da bi se obezbedila kriptovana komunikacija između proizvoljnih partnera potrebno je obezbediti distribuciju ključeva između njih.
- To je zadatak posebnih servera koji se zovu *Certificate Authority* (CA)
- CA čuva javne ključeve svih zainteresovanih i distribuira ih po želji

VPN - tipična komunikacija



VPN - generisanje ključeva

- celokupni sistem kripto zaštite zavisi od generisanja, čuvanja i distribucije ključeva
- ceo sistem rada sa ključevima zasniva se na javno definisanim pravilima koja čine *Public Key Infrastructure* (PKI)

VPN - implementacija (IP mreža)

Prethodno navedena pravila i načini kriptovanja podataka mogu biti različito implementirani.

U zavisnosti od toga šta se kriptuje, razlikujemo:

- *In place transmission mode*
- *Transport mode*
- *Encrypted tunnel mode*

In place transmission mode

- šifruje se samo korisnički deo IP datagrama
- ne menja se dužina IP datagrama
- zadržava se originalno IP zaglavlje što omogućava da se vidi ko su partneri u komunikaciji

Transport mode

- kriptuju se samo korisnički podaci iz IP datagrama
- postojećem datagramu se dodaje još jedno zaglavlje koje sadrži informacije o primenjenoj metodi kripto zaštite, što dovodi do produženja datagrama
- originalno IP zaglavlje ostaje ne promenjeno što omogućava uvid u partnere u komunikaciji

Encrypted tunnel mode

- kompletan IP datagram, uključivši i zaglavlje, se kriptuje, dodaje se novo IP zaglavlje i novodobijeni datagram se šalje kroz mrežu
- obezbeđuje potpunu privatnost jer se ne može videti čak ni ko komunicira

VPN - standardizacija

- prvobitne realizacije VPN uređaja koristile su razna *proprietery* rešenja
- da bi se obezbedila interoperabilnost uređaja raznih proizvođača, pristupilo se definisanju standarda iz ove oblasti
- IETF formirao *IP Security* (IPSEC) radnu grupu čiji je zadatak da definiše standarde za VPN oblast

Rezultati IPSEC radne grupe

- definisana su dva protokola zaštićenog prenosa koji definišu *Authentication Header* (AH) i *Encapsulating Security Payload* (EPS)
- definisan način komunikacije uvođenjem pojma *Security Associations* (SA)
- definisan je način razmene ključeva posredstvom Interneta, *Internet Key Exchange* (IKE)

Rezultati IPSEC radne grupe

- Za IPv6 definisan je ISAKMP/Oakley (*Internet Security Association and Key Management*) protokol pri čemu je SKIP (*Simple Key management for IP*) definisan kao opcija.

QoS u VPN mrežama

- problem garantovanja QoS u VPN mrežama je izražen u situacijama kada se kompletan saobraćaj kriptuje
- VPN *gateway* uređaj mora da obezbedi što bolje poštovanje željenog kvaliteta servisa
- zavisi i od izabrane mreže za komunikaciju

Zaključak

- potrebno je znati od koga se štitimo
- potrebno je znati koji su to podaci koji se štite
- problem generisanja i razmene ključeva
- velike mogućnosti primene u elektronskom poslovanju

HVALA!