

BEZBJEDNOST E-POSLOVANJA

Kod e-poslovanja informacije se prenose putem *elektronske pošte* (e-mail), *sistema EDI* (Electronic Data Interchange) ili *preko servisa WWW* (World Wide Web) Interneta.

Posledice otkaza ili zloupotrebe Internet tehnologije su:

- direktni finansijski gubici kao posledica prevare,
- gubljenje vrijednih i poverljivih informacija,
- gubljenje poslova zbog nedostupnosti servisa,
- neovlašćena upotreba resursa,
- gubljenje poslovnog ugleda i povjerenja klijenata,
- troškovi izazvani neizvjesnim uslovima poslovanja

ZAŠTITA e-poslovanja

Bezbjednosni servisi

Skup pravila koja se odnose na sve aktivnosti organizacije u vezi sa bezbjednošću - politika bezbjednosti

- Bezbjednosni servisi - djelovi sistema koji realizuju aktivnosti koje pariraju bezbjednosnim prijetnjama.

Kriptografske osnove elektronske trgovine

Neophodna je upotreba kriptoloških tehnologija, kao na primer šifre sa javnim i privatnim “ključevima” i digitalni potpis. .

ZAŠTITA e-poslovanja

Ciljevi mjera bezbjednosti u informacionim sistemima su:

- * ***Povjerljivost*** – obezbedjuje nedostupnost informacija neovlašćenim licima
- * ***Integritet*** – obezbedjuje konzistentnost podataka, sprečavajući neovlašćeno generisanje, promjenu i uništenje podataka
- * ***Dostupnost*** – obezbedjuje da ovlašćeni korisnici uvijek mogu da koriste servise i da pristupe informacijama.
- * ***Upotreba sistema isključivo od strane ovlašćenih korisnika*** – obezbedjuje da se resursi sistema ne mogu koristiti od strane neovlašćenih osoba niti na neovlašćen način.

Komponente bezbjednosti IS-a

Informacijska sigurnost se realizuje kroz tri komponente:

- ljudstvo,
- tehnologija i
- procesi.

Nivoi rizika i bezbjednosti

- ◆ I nivo – individualni korisnici i male kompanije (manje cilj, a više posrednici)
- ◆ II nivo – velike kompanije (najčešći cilj)
- ◆ III nivo – kritični sektori/infrastruktura (lideri bezbjednosti)
- ◆ IV nivo – nacionalni nivo (zakonski okvir i inicijativa)
- ◆ V nivo – globalni nivo – Internet (fenomen rizika i saradnje na polju bezbjednosti)

Tipovi napada na IS i zaštita

- Napadi se mogu podijeliti na
 - **netehničke** i
 - **tehničke.**

Netehnički napadi su usmjereni na ljudski faktor, koji je najvažniji ali i najslabiji element u lancu bezbjednosti IS-a (Socijalni inženjering)

Prijetnje e-poslovanju

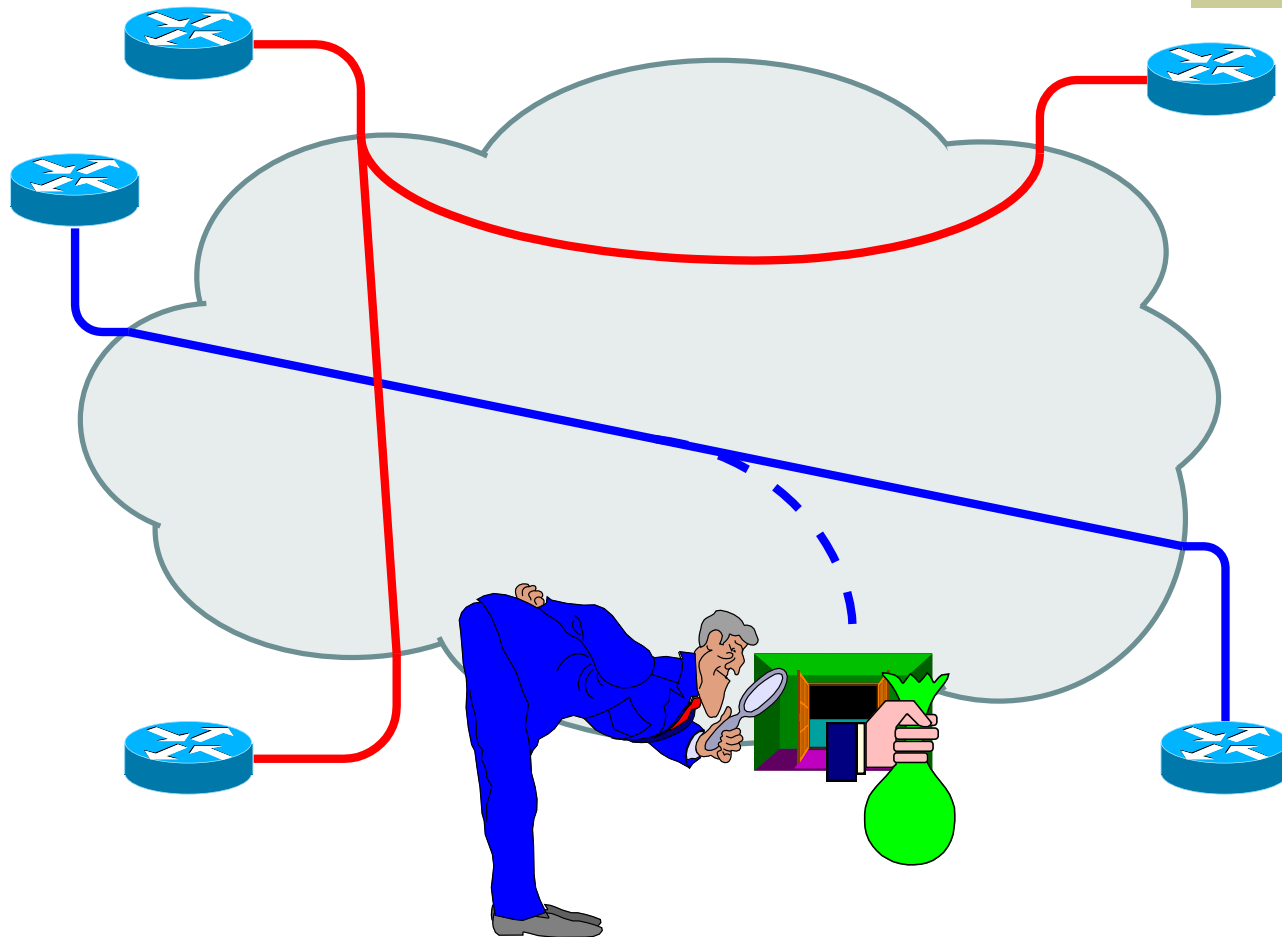
Najčešći upadi u sistem e-poslovanja su od:

- **48%** Autorizovani zaposleni
- **24%** Neautorizovani zaposleni
- **13%** Spoljni saradnici (zaposleni ukupno: 85%)
- **12%** Hakeri, Teroristi
- **3%** Ostali

TRI NIVOVA ZAŠTITE RAČUNARSKIH SISTEMA

- **Zaštita korporacijske mreže (firewall-i)**
- **Zaštita servera i radnih stanica**
- **Zaštita aplikacija**

Kripto zaštita



Kriptovanje



Tipovi kriptozastite

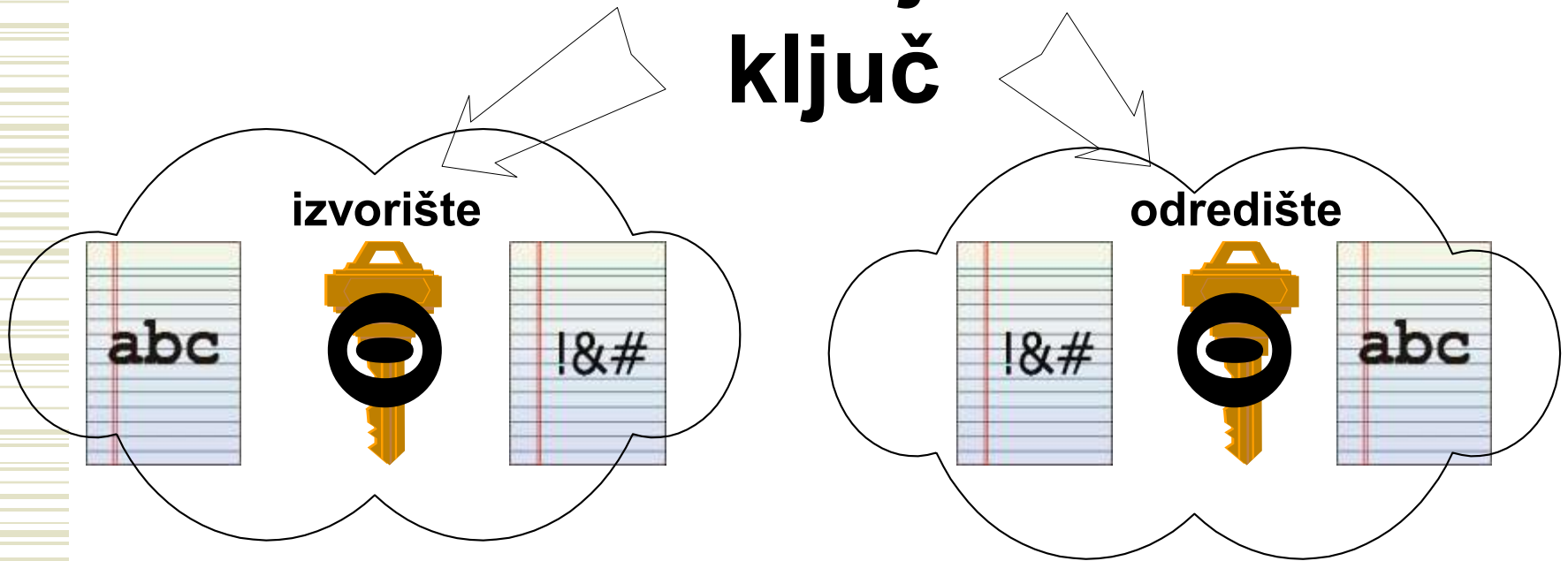
Dva osnovna sistema kriptozastite:

 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 (privatni)

Sistem sa simetričnim ključem

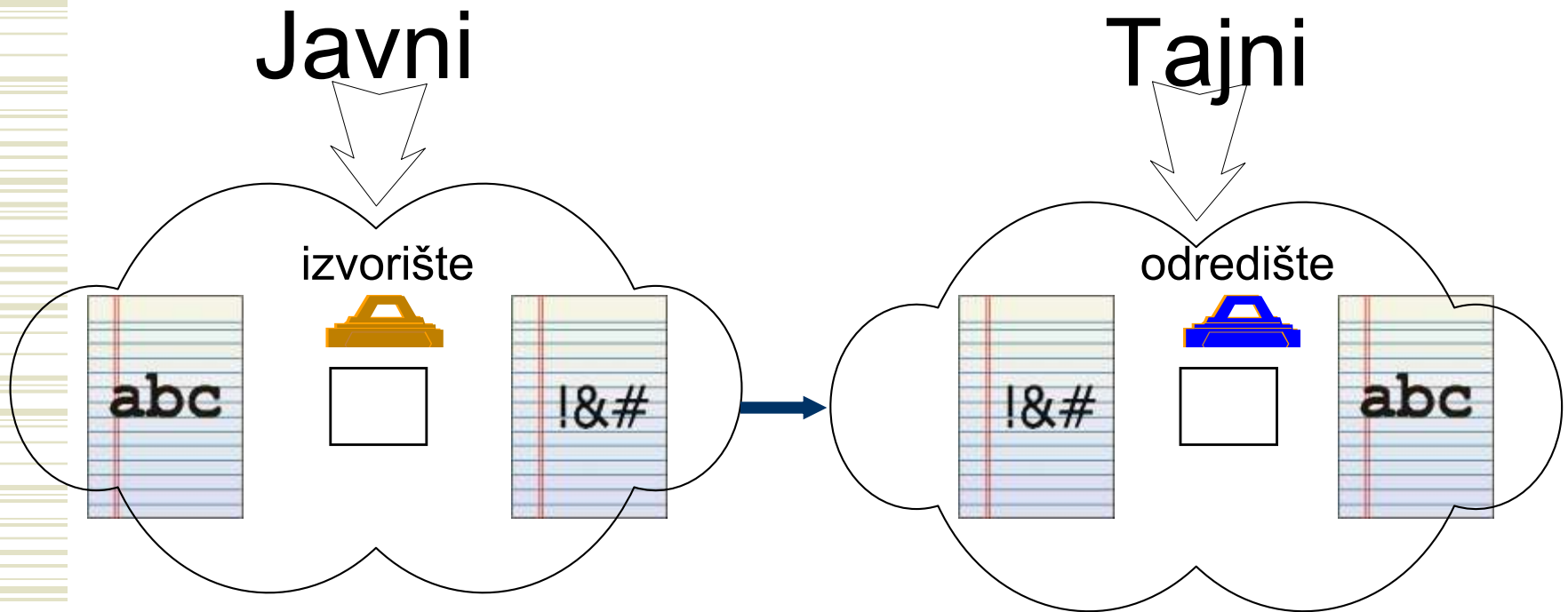
isti tajni
ključ



Sistem sa *asimetričnim* ključem

- ◆ problem tajnosti ključa u sistemu sa simetričnim ključem razriješen je u sistemu sa asimetričnim ključem
- ◆ ovde se koriste dva ključa, **javni i tajni (privatni)**
- ◆ 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

Sistem sa simetričnim ključem



DIGITALNI POTPIS

Digitalni potpis predstavlja prvi stepen u identifikaciji stranaka koje razmjenjuju poruke.

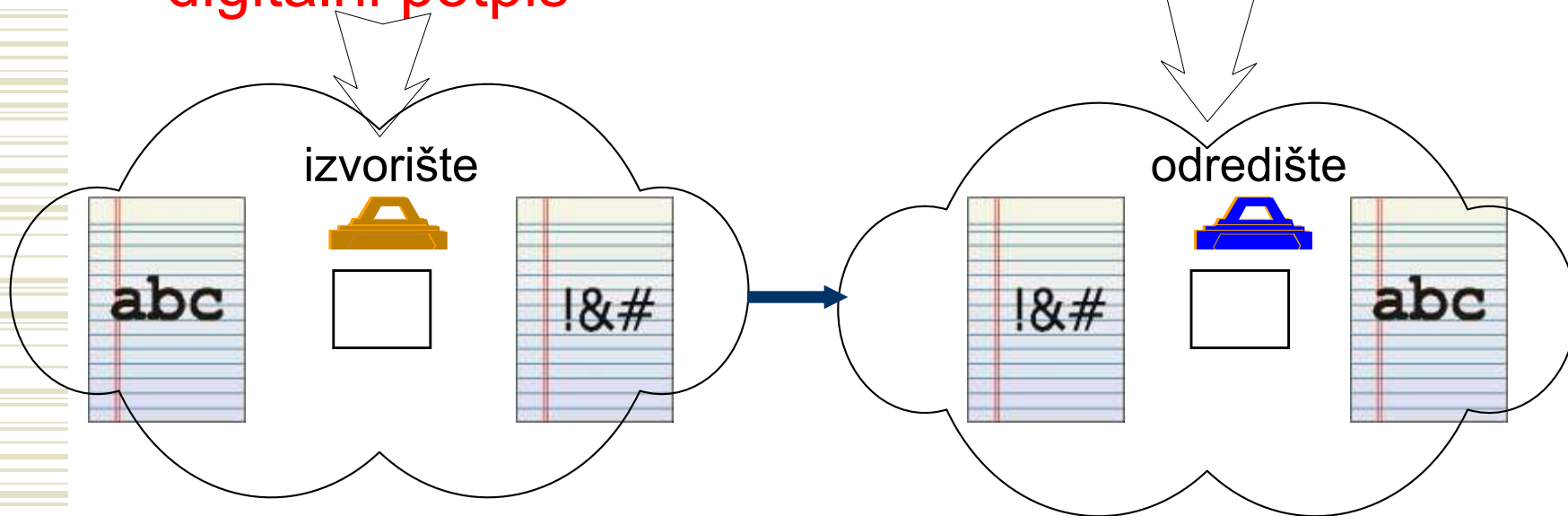
Jedan način implementacije digitalnog potpisa je korištenje inverznog postupka asinhronog ključa.

Privatni ključ koristi pošiljaoc kako bi potpisao poruku (**digitalni potpis**) dok primatelj koristi javni ključ pošiljaoca da dekriptira poruku.

Digitalni potpis

Tajni / privatni –
digitalni potpis

Javni



DIGITALNI POTPIS

Ipak u stvarnosti, samo se sažetak poruke (*message digest*) potpisuje korištenjem privatnog ključa.

Tako generišete sažetak poruke i potpisuje ga sa svojim privatnim ključem. Zatim šaljete nekriptovanu poruku zajedno sa potpisanim sažetkom poruke.

Kada dekriptuje potpisani sažetak poruke sa javnim ključem i uporedi sažetak poruke iz originalne poruke, primalac može biti siguran da je poruka original.

NAPOMENA: Digitalni potpisi ne pružaju enkripciju poruka, tako da enkripcijske tehnike moraju biti korištene zajedno sa digitalnim potpisom ukoliko trebate očuvati tajnost poruka.

Domaći br. 5

1. Šta je M-banking?
2. Da li se **digitalnim potpisom** enkriptuju (šifruju) poruke?

**Odgovore poslati na mail bozok@ac.me
najkasnije do 19.04. u 24,00!**