Elektronsko poslovanje

Problemi zastite i sigurnosti
(drugi dio)

Kriptografija i vrste algoritama

- Osnovni element koji se koristi u kriptografiji naziva se **šifarski sistem** ili **algoritam šifriranja**

- Svaki šifarski sistem obuhvata par transformacija podataka, koje se nazivaju **šifriranje** i **dešifriranje**.

- **Šifriranje** je procedura koja transformiše originalnu informaciju u šifrirane podatke (šifrat)

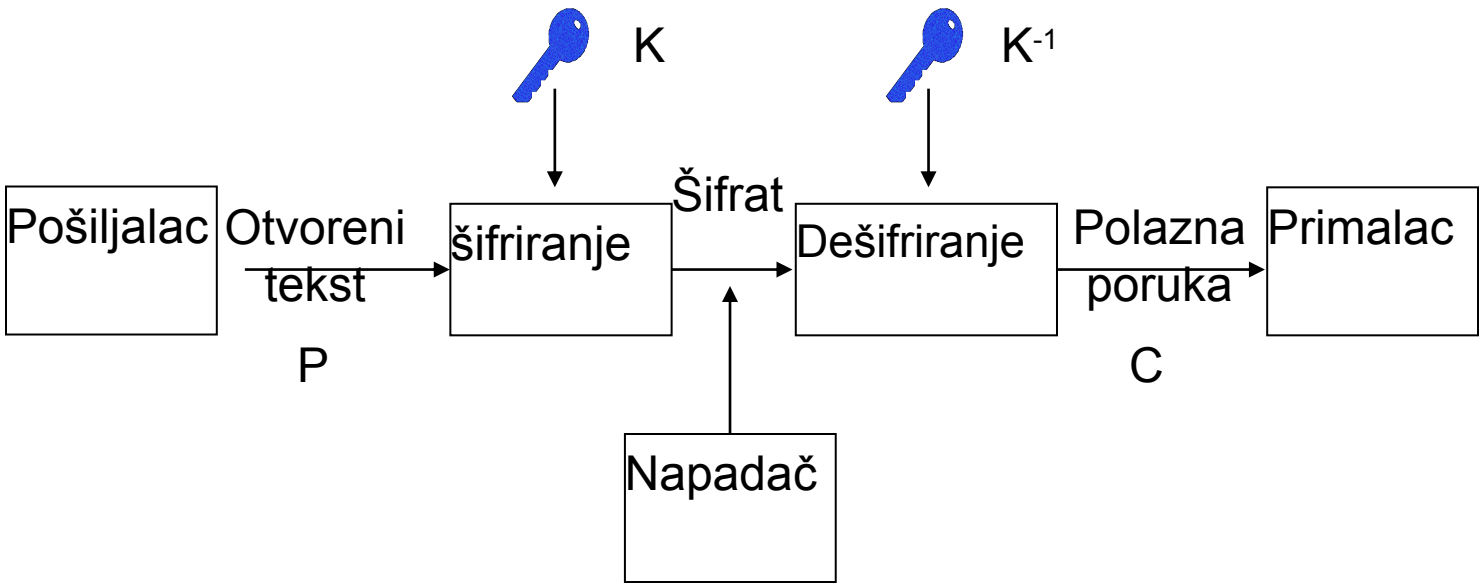
- **Dešifriranje**, rekonstruiše originalnu informaciju na osnovu šifrata

- U šifarskoj transformaciji se koristi jedna nezavisna vrijednost koja se naziva **ključ** šifriranja

Šema šifriranja ima 5 komponenti:

1) Tekst koji se šifruje (plaintext)
2) Algoritam šifriranja
3) Tajni ključ
4) Šifrirani tekst (ciphertext)
5) Algoritam dešifriranja

Šematski prikaz kriptovanja (Encryption) i dekriptovanja (Decryption)



- Kriptografski algoritmi zasnovani su na matematičkoj funkciji koja se koristi za šifriranje i dešifriranje.

- Razlikuju se dvije vrste algoritama:

  A) **Ograničeni algoritmi**: bezbjednost se zasniva na tajnosti algoritma (istorijski interesantni)

- B) **Algoritmi zasnovani na ključu**: bezbjednost se zasniva na ključevima, a ne na detaljima algoritma koji se može publikovati i analizirati (algoritam je javno poznat, a ključ se čuva tajnim).

- šifriranje je, pojednostavljeno, matematička funkcija čiji izlaz zavisi od dva ulazna parametra :
  1. originalna poruka koja se šifrira P (Plaintext)
  2. ključ K

Rezultat je niz naizgled nepovezanih brojeva koji se mogu, bez straha od mogućnosti da poruka dođe u neželjene ruke, prenositi do osobe kojoj je namijenjena.

Da bi šifriranu poruku druga osoba mogla da koristi potrebno je sprovesti obrnuti postupak od šifriranja, dešifriranje.

- Dešifriranje je, pojednostavljeno, matematička funkcija čiji izlaz zavisi od dva ulazna parametra:
    1. šifrirana poruka C (Chipertext)
    2. ključ K^{-l}

- kao rezultat funkcije dobija se originalna poruka

- Minimalna i potrebna informacija koju dvije osobe moraju da dijele, ako žele da razmjenjuju podatke na siguran način, skup ključeva (K, K^{-l})

- Prema odnosu ključeva K i K^{-l} kriptografske sisteme dijelimo na simetrične i asimetrične.

Zaštita ključa

(zaštita zavisi od zaštite ključa a ne od zaštite algoritma)

Kirkohov (Kerckhoff) princip: Važan kriterijum za ocjenjivanje kriptografskih algoritama; napadač poznaje kriptosistem ili algoritme, koje upotrijebljavamo, ali ne i ključeve koji nam obezbjeđuju sigurnost.

Sigurnost kriptovanog algoritma

- Vrijeme potrebno za “razbijanje” algoritma mora da bude duže od vremena u kome podaci moraju da ostanu tajni.

- Takođe, potrebno je da bude zadovoljen i uslov da broj podataka šifriranih jednim ključem bude manji od broja potrebnih podataka da se dati algoritam “razbije”.

Cijena “razbijanja” algoritma mora da bude veća od cene šifriranih podataka

Dužina ključa (bit)	Broj alternativnih ključeva	Potrebno vrijeme pri 10^6 dekriptovanja/μs
32	$2^{32} = 4.3 \times 10^9$	2.15 milisekundi
56	$2^{56} = 7.2 \times 10^{16}$	10 sati
128	$2^{128} = 3.4 \times 10^{38}$	5.4×10^{18} godina
168	$2^{168} = 3.7 \times 10^{50}$	5.9×10^{30} godina

Simetrično šifriranje

- Simetrično šifriranje je šifriranje tajnim ključem, pri čemu je ključ za šifriranje identičan ključu za dešifriranje:

$$K = K^{-1}$$

- u slučaju simetričnog šifriranja pošiljalac i primalac poruke koriste isti tajni ključ

Poznati simetrični algoritmi su:

- DES (Data Encryption Standard) – ključ je dužine 56 bita
- Triple DES, DESX, GDES, RDES – ključ je dužine 168 bita
- (Rivest) RC2, RC4, RC5, RC6 – promenljiva dužina ključa
- IDEA – osnovni algoritam za PGP – ključ je dužine 128 bita
- Blowfish – promenljiva dužina ključa do 448 bita
- AES (Advanced Encryption Standard) - radi sa blokovima od po 128 bita i koristi ključeve dužine 128, 192 i 256 bita

Sledeća tri algoritma koja imaju široku upotrebu u komercijalnim sistemima su:

- RC2 – je 64-bitna blok šifra
- RC4 – je niz šifra (radi sa nizom bitova, umjesto sa blokovima bitova)

- RC5 – koristi promjenljive ključeve (32/64/128 bita) koje primjenjuje na promenljive blokove podataka i uključuje pomjenljive operacije
- RC6 – naslednik RC5, 128-bitna blok šifra, finalista na AES konkursu

Data Encryption Standard (DES)

- DES je simetričan algoritam koji je IBM predstavio 1975
- Razvijan je od strane brojnih organizacija za kriptovanje poruka i podataka pa je postao najrasprostranjeniji komercijalni algoritam
- Des je blok šifra što znači da algoritam kriptuje podatke u 64-bitna bloka i koristi 64-bitni ključ
- U realnosti, samo 56 bitova se koristi za kriptovanje/dekriptovanje podataka gde preostalih 8 bitova rade kao analogni
- Upotreba 56 bita omogućavala je, za to vrijeme, veliki broj ključeva
- 2^{56} potencijalnih mogućnosti za ključ su, za to vrijeme, napede grubom silom (brute force) činile veoma teškim

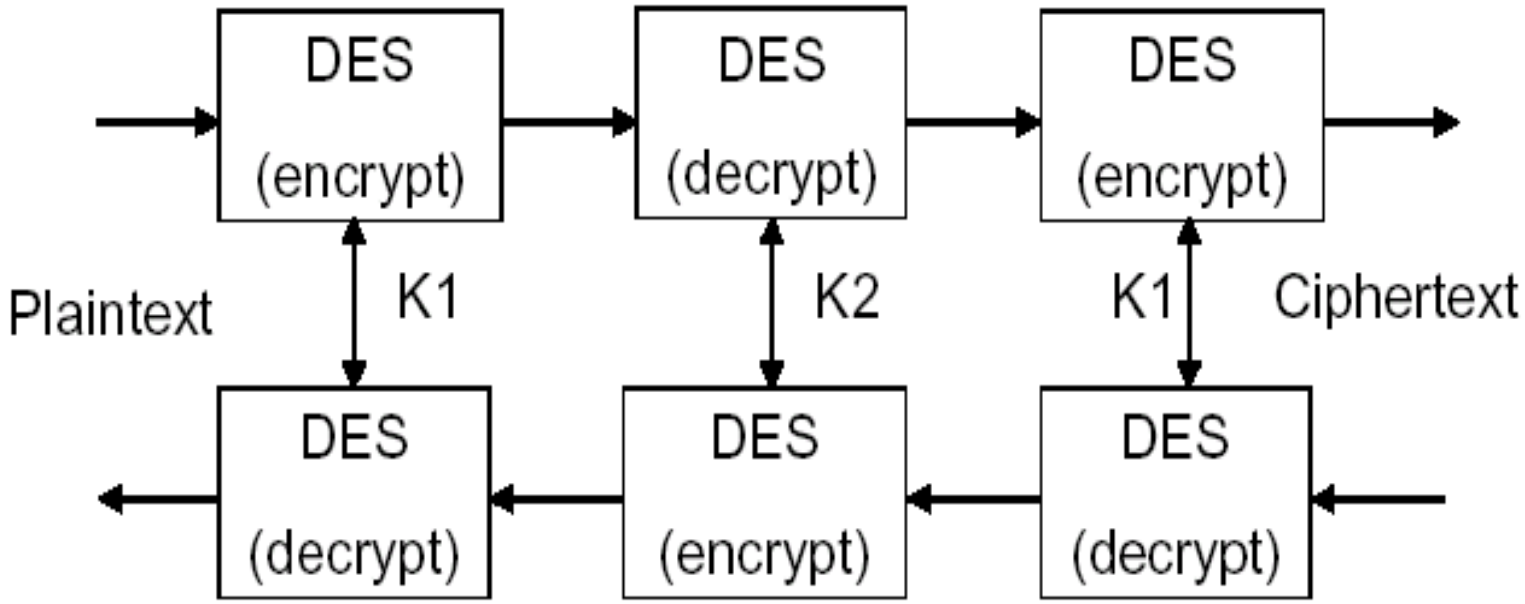
Triple DES algoritam

- Sredinom devedestih godina prošlog vijeka, povećanjem snage računara, DES pokazuje slabosti na napade grubom silom, pa se moralo pribjeći drugim rešenjima.
- Kako DES više nije priznat kao standard, a zbog velikog broja hardverskih implementacija DES-a, mnoge organizacije prešle su na Triple DES algoritam

- Tripl DES koristi tri ključa za kriptovanje podataka, što povećava veličinu ključa na 168 bita
- Postoji više metoda Triple DES algoritma
    I. Prvi metod: podaci se kriptuju tri puta sa tri odvojena ključa
    II. Drugi metod: podaci se kriptuju sa prvim ključem, dekriptuju sa drugim, i ponovo se kriptuje trećim ključem
    III. Treći metod: sličan je sa prethodna dva, sa tim što se isti ključ koristi u prvoj i trećoj operaciji.

- Vlada U.S razvija različite algoritme koji će postati AES (Advanced Encryption Standard) standardi

Tripl DES koristi tri ključa za kriptovanje podataka



Asimetrično šifriranje

- Asimetrično šifriranje je šifriranje javnim ključem
- Svaki učesnik u komunikaciji koristi dva ključa
- Jedan ključ je javni i koristi se za šifriranje, dok je drugi tajni i koristi se za dešifriranje
- Tajni ključ je dostupan samo vlasniku

Ideja javnih ključeva

- zasnivaju se na funkcijama čiju je inverznu funkciju gotovo nemoguće odrediti
- kriptografisanje pomoću javnih ključeva je vrlo sporo
- Diffie i Hellman 1976. razvili metodu zasnovanu na ireverzibilnim funkcijama sa ključevima od 128, 256 i 512 bita

Princip javnih ključeva

- uzmite telefonski imenik velikog grada:
  - pronađite telefonski broj određene osobe
  - pronađite osobu koja ima određeni telefonski broj
- koji ćete postupak sprovesti lako, a od kojeg ćete odustati?

- Javni ključ je svima dostupan.
- Kad šaljemo podatke nekoj osobi, šifriramo ih javnim ključem
- Kada osoba primi podatke, dešifrira ih svojim privatnim ključem, koji samo ta osoba posjeduje.

- Oba ključa su vezana za entitet (računar ili korisnika) koji treba da

dokaže svoj identitet, elektronski potpiše ili šifrira podatke

RSA

- tvorci Ronald Rivest, Adi Shamir i Leonard Adleman
- ključevi dužine 1024 bita
- dva izuzetno velika prosta broja (sa približno po 100 cifara) je lako pomnožiti, ali gotovo nemoguće rastaviti na faktore
- proizvod – osnova za kriptografisanje, a faktori – za dešifriranje

RSA Public Key Standard

- RSA Public Key je asimetrični algoritam šifriranja koji koristi javni i privatni ključ za kriptovanje i dekriptovanje podataka

- RSA sistem je zasnovan na odgovarajućim matematičkim operacijama razvijen je na pretpostavci da je teško razložiti na činioce velike brojeve koji su proizvod dva prosta broja.

- RSA sistem sa javnim ključem i DES (ili neki drugi sistem sa simetričnim ključem) se obično koriste zajedno.

  Razlog: RSA je relativno spor za kriptovanje velikih blokova podataka, dok je DES pogodan za to.
- Sistemi koriste RSA da bi razmijenili DES ključeve međusobno, a zatim koriste DES algoritam da kriptuju blokove podataka. Ovakav protokol prepoznaje dvije strane i omogućava sigurnu razmjenu ključeva

- RSA sistem javnog ključa se koristi za kriptovanje i digitalni potpis

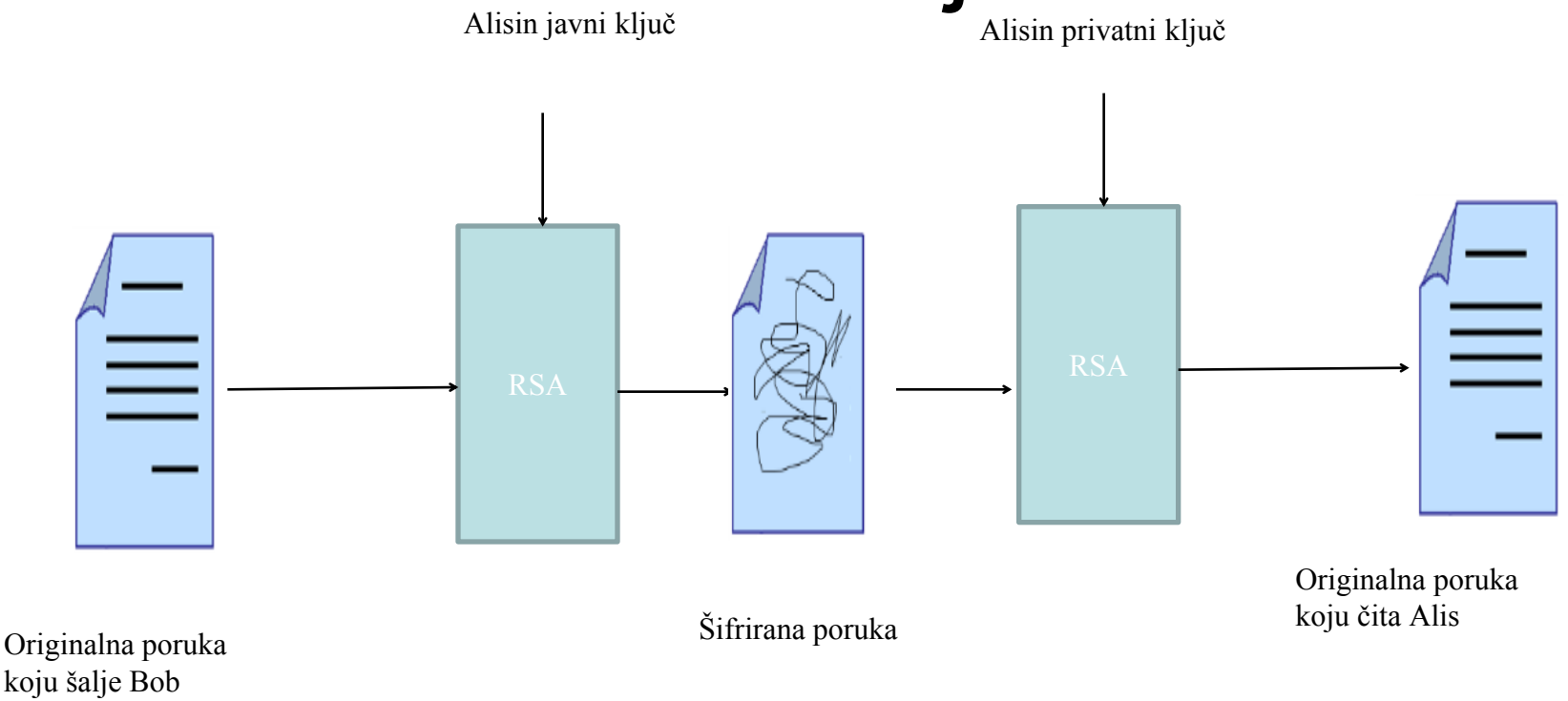
KRIPTOVANJE

- **Primjer 1**: Bob hoće da pošalje kriptovanu poruku Ani. On kriptuje poruku Aninim javnim ključem i šalje je. Pošto Ana ima privatan ključ (odgovarajući Aninom javnom ključu) koji dekriptuje podatke, podaci ostaju povjerljivi u toku tranzicije.

DIGITALNI POTPIS - prepoznaje pošiljaoca poruke.

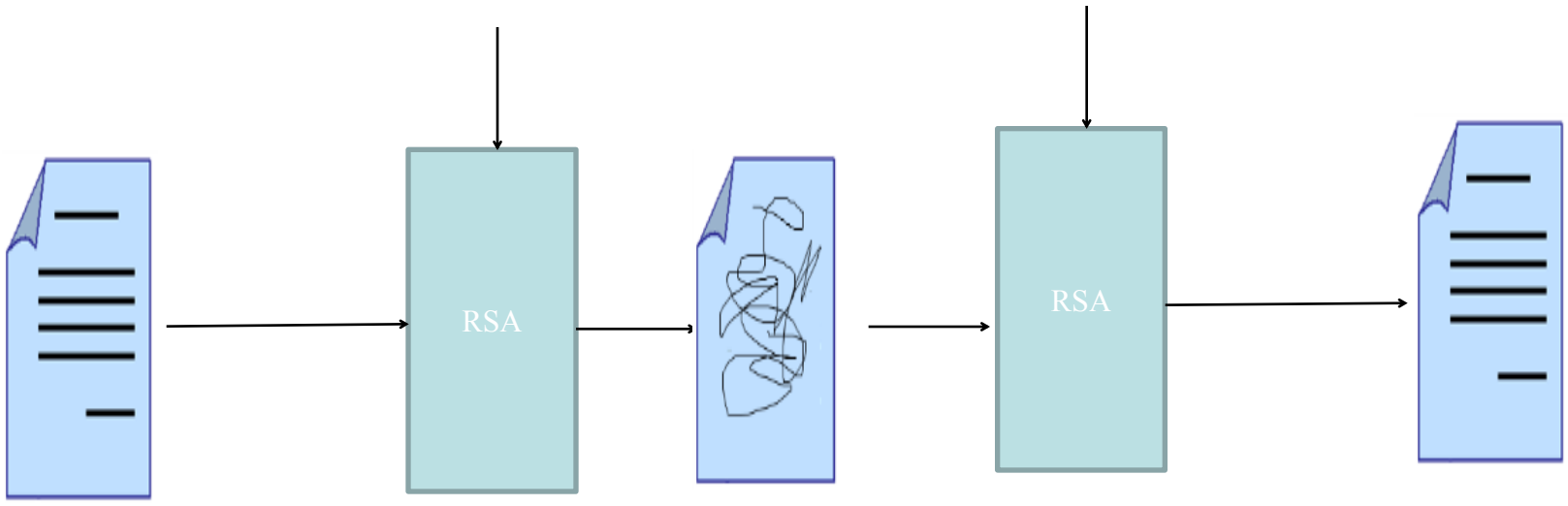
- **Primjer 2**: Da bi se identifikovao, Bob šalje Ani poruku kriptovanu svojim privatnim ključem. Kada Ana dobije poruku, dekriptuje je upotrebom Bobovog javnog ključa. Uspješno dekriptovanje potvrđuje da je Bob pošiljalac, zato što je poruka kriptovana Bobovim privatnim ključem koji samo on ima u svom vlasništvu.

Režim rada asimetričnog šifriranja



- Pošto svako ima Alisin javni ključ, to Bob može „zaključati“ poruku i poslati je Alisi. Samo ona ima privatni ključ, pa je samo ona može „otključati“

Režim rada autentifikacije



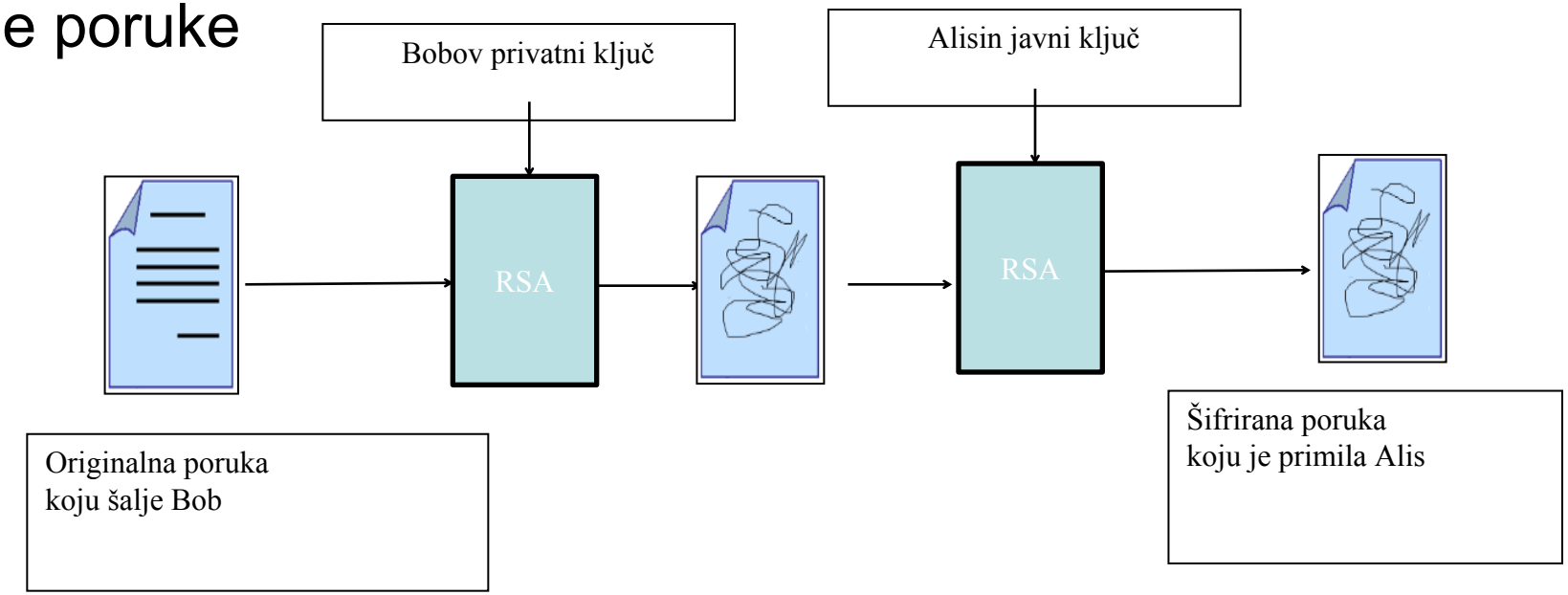
Pošto svako ima Bobov javni ključ, to svako može „otključati“ poruku koju je Bob poslao Alisi. Ali samo Bob ima svoj privatni ključ, pa je samo on mogao „zaključati“

Samo ona ima privatni ključ, pa je samo ona može ovu poruku, pa je Alis sigurna da je on poslao.

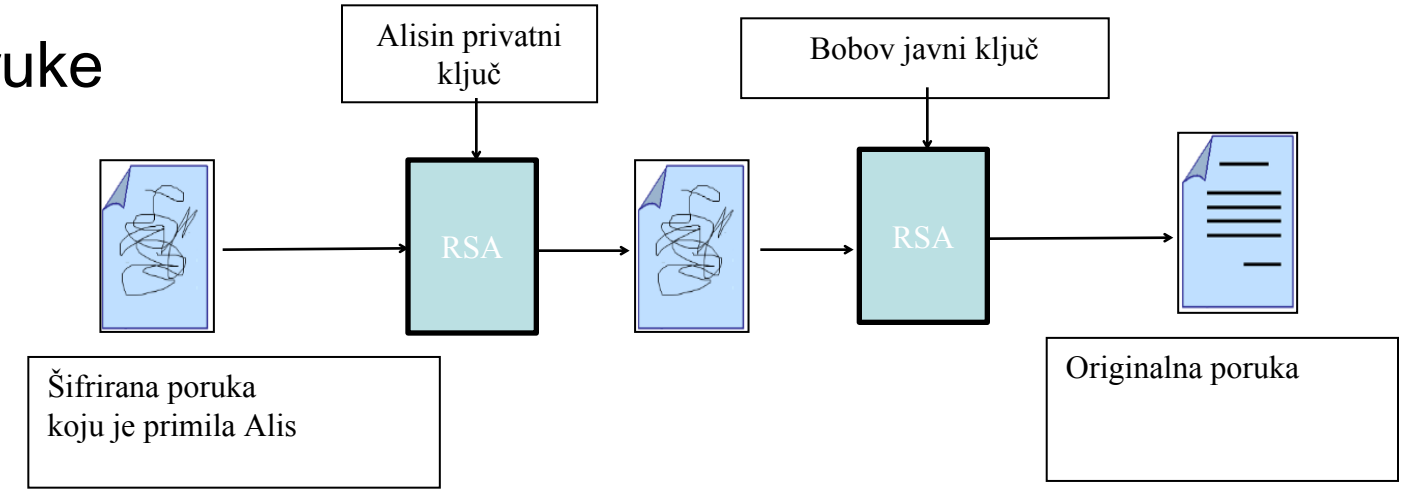
To je elektronski potpis!

- U prvom slučaju svako može poslati Alisi poruku (i lažno se predstaviti)
- U drugom slučaju svako može pročitati poruku koju je Bob poslao (iako smo sigurni da je on poslao)
- Kako riješiti i prvi i drugi problem?
- **Kombinacija**!

Slanje poruke



Primanje poruke



Novi kriptografski sistem – Eliptičke krive (Elliptic Curves)

- Sistem je građen na drugačijoj matematičkoj osnovi
- Ovi algoritmi koriste kraće ključeve i ispoljavaju bolje performanse za pojedine operacije
- U poređenju sa RSA, u nekim slučajevima ovi algoritmi pokazuju bolje performanse za operacije dekripcije i potpisivanja
- RSA se pokazao boljim za operacije kriptovanja i verifikacije potpisa
- Algoritam eliptičkih krivih se pokazao ograničen za komercijalnu upotrebu