

Otvoreno računarstvo

9. Osnove sigurnosti

- Osnovi pojmovi
- Osnovni algoritmi
- Složeniji algoritmi i postupci
- Sigurnost u mrežnoj komunikaciji

Creative Commons



[Otvoreno računarstvo 2022/23](#) by Ivana Bosnić & Igor Čavrak, FER
is licensed under [CC BY-NC-SA 4.0](#)

Attribution-NonCommercial-ShareAlike 4.0 International (CC BY-NC-SA 4.0)

This license requires that reusers give credit to the creator.

It allows reusers to distribute, remix, adapt, and build upon the material in any medium or format, for noncommercial purposes only.

If others modify or adapt the material, they must license the modified material under identical terms.

BY: Credit must be given to you, the creator.

NC: Only noncommercial use of your work is permitted.

SA: Adaptations must be shared under the same terms.

Otvoreno računarstvo

9. Osnove sigurnosti

- Osnovi pojmovi
- Osnovni algoritmi
- Složeniji algoritmi i postupci
- Sigurnost u mrežnoj komunikaciji

Uvod - Sigurnost (*Security*)

- Široko dostupne računalne mreže
 - javne informacije - privatne informacije, javne usluge – privatne usluge
 - kako ih odvojiti i zaštititi, kako kontrolirati (ne)dostupnost?
- Sigurnosni zahtjevi - ciljevi:
 - povjerljivost, tajnost (*confidentiality, secrecy*)
 - cjelovitost, očuvanost (*integrity*)
 - izvornost, ovjera (*authenticity*)
 - neporicljivost (*nonrepudiation*)
 - dostupnost (*availability*)
 - kontrola pristupa (*access control*)

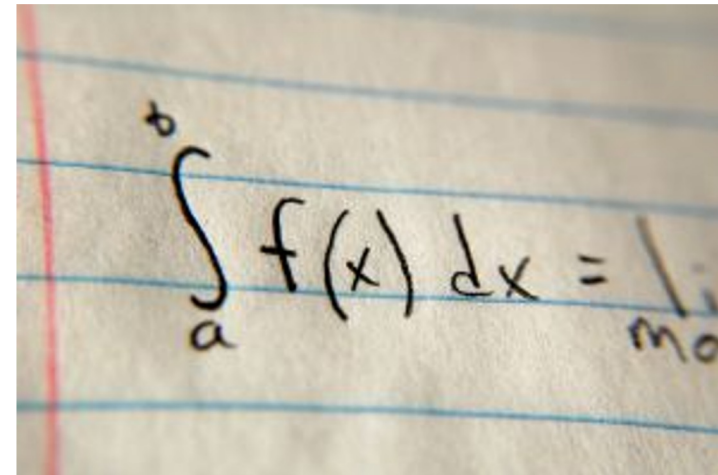
Ciljevi – povjerljivost

- Povjerljivost, tajnost (*confidentiality, secrecy*)
 - očuvanje tajnosti poruke
 - treba biti razumljiva samo pošiljatelju i namjeravanom primatelju



Ciljevi – cjelovitost

- Cjelovitost, očuvanost (*integrity*)
 - sadržaj poruke ne smije se mijenjati prilikom prijenosa
 - zbog grješaka u prijenosu
 - namjernom promjenom – napadom
 - svaku promjenu poruke treba moći primijetiti



A photograph of a handwritten mathematical formula on lined paper. The formula is the definite integral of a function f(x) from a to b, which is equal to the limit of a Riemann sum as the number of subintervals n approaches infinity. The handwriting is in black ink, and the paper has blue horizontal lines and a red vertical margin line on the left.

$$\int_a^b f(x) dx = \lim_{n \rightarrow \infty} \sum_{i=1}^n f(x_i) \Delta x$$

Ciljevi – izvornost

- Izvornost, ovjera (*authenticity*)

- sposobnost određivanja izvornosti (autentičnosti, ovjere) partnera u komunikaciji
- mogućnost otkrivanja promjene sugovornika



Ciljevi – neporicljivost

- Neporicljivost (*nonrepudiation*)
 - nemogućnost poricanja slanja poslano poruke
 - za svaku poslanu poruku moguće je utvrditi autora ili izvor



Ciljevi – dostupnost

- Dostupnost (*availability*)
 - osiguranje dostupnosti usluge aktivnim sprječavanjem napada



Ciljevi – kontrola pristupa

- Kontrola pristupa (*access control*)
 - sposobnost dodjele ili zabrane prava pristupa i korištenja resursa na pouzdan način



Osnovni pojmovi

- Kriptologija (*Cryptology*)
 - kriptografija (*cryptography*) – umijeće čuvanja tajnih informacija
 - što znači *iu9o5gfmxcv[grs* ?
 - umjetnost pretvaranja razumljivog u nerazumljivo, svima osim nekolicini (i obratno)
 - nešto što malo ljudi potpuno razumije, ali svi možemo koristiti
 - kriptanaliza (*cryptanalysis*) – umijeće otkrivanja (tuđih) tajnih informacija
- Izvorni tekst (*clear-text, plain-text*)
- Šifrirani, kriptirani tekst (*cypher-text, cipher-text*)
- Šifriranje, kriptiranje, zakrivanje, dešifriranje, dekriptiranje, otkrivanje (*encryption/decryption*)

Osnovni pojmovi

- Ključ (*key*)
 - informacija koja se koristi u postupku kriptiranja i/ili dekriptiranja i jednoznačno određuje postupak kriptiranja i/ili dekriptiranja
- Šifra (*cypher, cipher*)
 - par algoritama koji se koriste za pretvorbu iz izvornog u kriptirani oblik i natrag
 - katkad može imati značenje ključa
- Kôd (*code*)
 - zamjena jedinice izvornog teksta kodnom riječi
 - bilo koja metoda skrivanja izvornog značenja

Pasivni napadi

- Prisluškivanje – *eavesdropping, tapping*
- Pogađanje ključeva ili lozinki
 - napad grubom silom – *brute force*
 - napad rječnikom – *dictionary attack*
 - napad odabranim porukama – *chosen cipher-/plain-text*
 - kriptanaliza, statističke metode



Aktivni napadi

- Lažno predstavljanje
 - korisnika – *impersonation*
 - usluge – *phishing*
- Ubacivanje u komunikaciju – *man in the middle*
- Uskraćivanje usluge – *denial of service* (DOS/DDOS)
- Napad lažnim porukama
 - ponavljanjem poruka – *replay attack*
 - zamjenom poruka – *substitution attack*



Metode zaštite

- **Zaštita na više razina**
 - **sustav**
 - arhitektura mreže (demilitarizirane zone, DMZ)
 - vatrozid (*firewall*)
 - antivirusna zaštita
 - sigurnosni alati
 - **komunikacijski kanal**
 - Secure Sockets Layer (SSL)
 - IPSEC
 - kriptiranje komunikacije (sklopovsko)
 - **poruke**
 - digitalni potpis
 - digitalna omotnica

Primjer: telnet

- Protokol telnet ne koristi zaštitu prilikom prijenosa osjetljivih informacija
 - korisničko ime

```
login: mario
```

```
TELNET:  ----- TELNET:  -----
```

```
TELNET:
```

```
TELNET:  "mario"
```

```
TELNET:
```

```
 0:0800 200e 1a39 0060 9795 628d 0800 4500 .. ..9.`..b...E.
```

```
16:0029 1e00 4000 8006 13fe a135 4364 a135 .) ..@.....5Cd.5
```

```
32:4302 0404 0017 0023 17fa 3ac5 4bf6 5018 C.....#...:K.P.
```

```
48:21cf b537 0000 6d61 7269 6f !..7..mario
```

```
...
```


Primjer: telnet

- Protokol telnet ne koristi zaštitu prilikom prijenosa osjetljivih informacija
 - lozinka

```
Password: xxxxxx
```

```
TELNET:  ----- TELNET:  -----
```

```
TELNET:
```

```
TELNET:  "123456"
```

```
TELNET:
```

```
 0:0800 200e 1a39 0060 9795 628d 0800 4500 .. ..9.`..b...E.
```

```
16:0029 2b00 4000 8006 06fe a135 4364 a135 .)+.@.....5Cd.5
```

```
32:4302 0404 0017 0023 1801 3ac5 4c07 5018 C.....#...:L.P.
```

```
48:21be b530 0000 3132 3334 3536 !..0..123456
```

```
...
```

Primjer: HTTP Basic autentikacija

GET /sigurno/ HTTP/1.1

Host: www.fer.unizg.hr

...

HTTP/1.1 401 Access Denied

WWW-Authenticate: Basic realm="FER"

GET /sigurno/ HTTP/1.1

Host: www.fer.unizg.hr

Authorization: Basic aHR0cHdhbGNoOmY=

...

HTTP/1.1 200 OK

...

Otvoreno računarstvo

8. Osnove sigurnosti

- Osnovi pojmovi
- Osnovni algoritmi
- Složeniji algoritmi i postupci
- Sigurnost u mrežnoj komunikaciji

Algoritmi

- Tajni algoritmi
 - neprikladni za ozbiljnu primjenu (što kad se otkriju?)
- Javni algoritmi
 - algoritmi sažetka (*digest, hash*)
 - digitalni otisak prsta (*fingerprinting*)
 - algoritmi s ključem
 - tajni ključ (*secret key*) – simetrični algoritmi
 - šifriranje blokova (*block cipher*)
 - šifriranje toka (*stream cipher*)
 - javni ključ (*public key*) – asimetrični algoritmi
 - steganografija
 - digitalni vodeni žig (*watermarking*)



Svojstva algoritama

- Algoritmi sažetka (*digest, hash*)
 - cjelovitost
 - (izvornost)
- Algoritmi šifriranja ključem
 - povjerljivost
 - (cjelovitost)
 - (izvornost)
- Steganografija
 - povjerljivost



Algoritmi sažetka (*hash*)

- Prevode sadržaj poruke u jedinstveni sažetak
- Funkcija generiranja sažetka
 - **jednosmjerna** (gubitak informacija)
 - prevodi izvorni tekst u sažetak **fiksne** duljine
 - različiti izvorni tekstovi **mogu** imati iste sažetke
 - **nije moguće** odrediti koje dvije poruke imaju isti sažetak
 - generirani sažetak treba sličiti **slučajno generiranim** podacima
 - minimalna promjena ulaza → velika promjena izlaza
- Sažetak poruke odgovara digitalnom **otisku prsta** poruke
- Algoritmi: MD5, SHA-1, SHA-3

Algoritmi s tajnim ključem

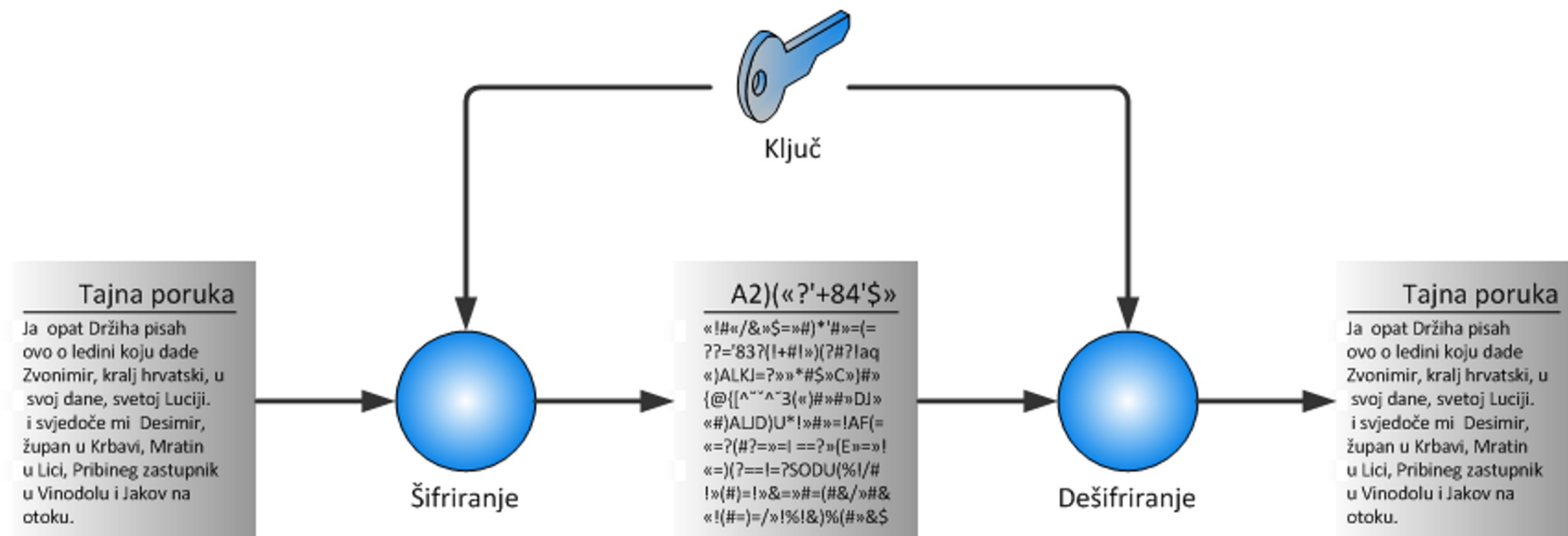
- **Isti ključ** za kriptiranje i dekriptiranje – **simetrični**
 - tajni ključ, dijeljeni ključ
- Sigurnost ovisi o:
 - ključu (duljini ključa)
 - mehanizmu dogovora ključa među sugovornicima
- Osnovne grupe
 - **blokovske** šifre – najčešće
 - ulaz u funkciju – blok podataka stalne duljine
 - šifre **tôka**
 - ulaz u funkciju – bit po bit iz tôka podataka koji se šifrira
- Gradivni blokovi
 - S (supstitucijske) i P (permutacijske) kutije
 - sklopovske implementacije – **brzina!**

Simetrični algoritmi

- Tajni (dijeljeni) ključ
 - početni problem sigurnog prenošenja poruke (veća količina podataka) prevodimo u problem sigurnog prenošenja ključa (mala količina podataka)
- Dogovor o ključu
 - dogovor dviju strana o zajedničkom (dijeljenom) ključu putem (ne)sigurnog kanala

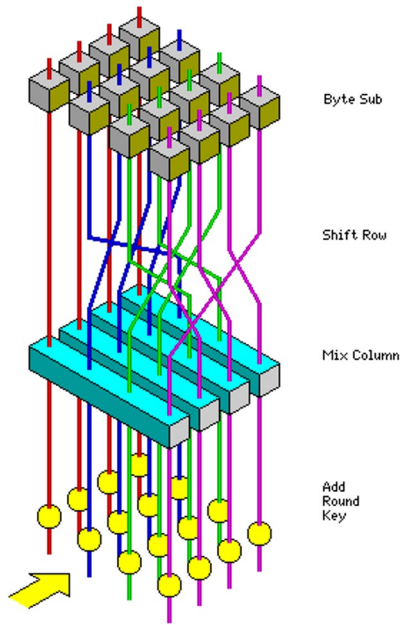


Simetrični algoritmi

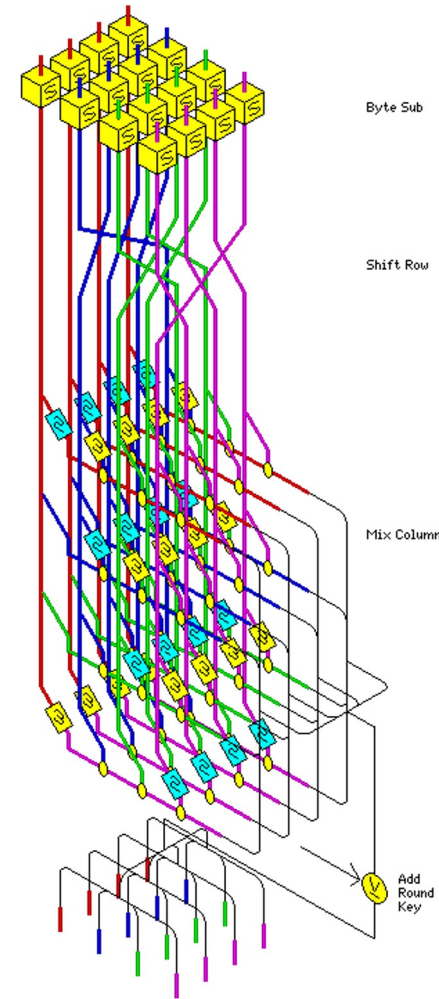


Simetrični algoritmi

- AES (Rijndael)
- Serpent
- Twofish
- Blowfish
- IDEA
- 3DES
- DES



Ilustracija AES/Rijndael algoritma, John Savard



Primjer: probijanje ključa (DES) sirovom snagom

Napadač	Proračun	Alat	Vrijeme i troškovi za svaki ključ		Duljina ključa koja jamči sigurnost	
			40 bita	56 bita	1996.	2015. (predviđanje)
Haker vulgaris	Mali	PC	1 tjedan	Nepraktično	45	59
	\$400	FPGA	5 sati \$0,08	38 godina \$5.000	50	64
Malo poduzeće	\$10.000	FPGA	12 minuta \$0,08	556 dana \$5.000	55	69
Korporacijski odjel	\$300.000	FPGA	24 sekunde \$0,08	19 dana \$5.000	60	74
		ASIC	0,18 sekundi \$0,001	3 sata \$38	60	74
Velika kompanija	\$10.000.000	FPGA	0,7 sekundi \$0,08	13 sati \$5.000	70	84
		ASIC	0,005 sek. \$0,001	6 minuta \$38	70	84
Obavještajna agencija	\$300.000.000	ASIC	0,0002 sek. \$0,001	12 sekundi \$38	75	89

Algoritmi s javnim ključem

- **Različiti ključevi** za šifriranje i dešifriranje - **asimetrični**
 - tajni ključ – šifriranje / dešifriranje
 - javni ključ – šifriranje / dešifriranje
- Temeljeni na NP-teškim matematičkim problemima
 - nema poznatog algoritma polinomne (P) složenosti za poznate NP-teške probleme i vjeruje se da takvi algoritmi ne postoje
- Sigurnost ovisi o:
 - odabranom problemu
 - ključu (duljini ključa)
 - **zaštiti tajnog ključa**



Asimetrični algoritmi

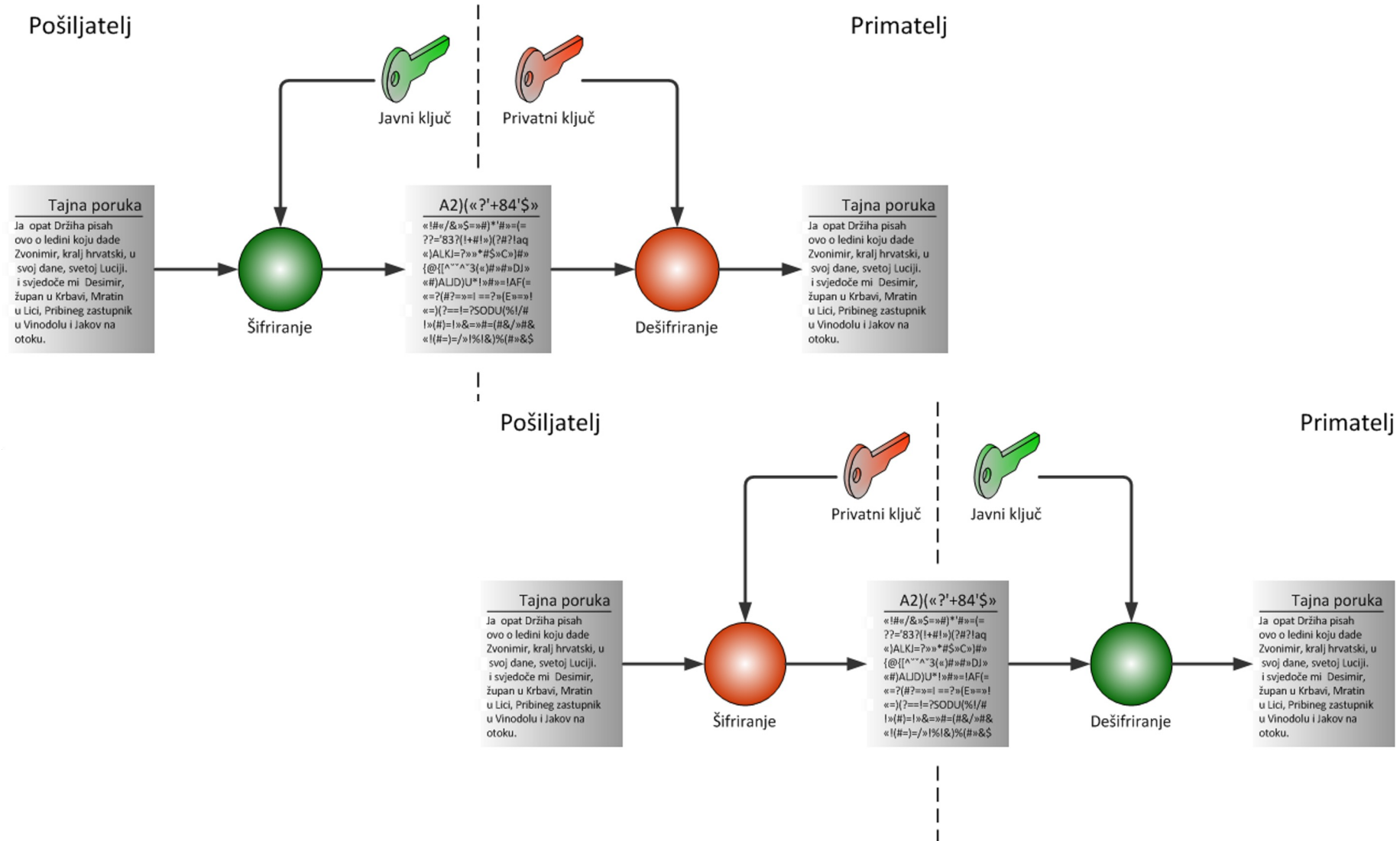
- Kako izgraditi algoritam?

- uzeti težak problem (NP-težak) s posebnim slučajem koji se može riješiti u P (polinomne složenosti)
- **šifriranje** – pretvoriti poruku u poseban slučaj problema, zatim javnim ključem pretvoriti jednostavan problem u težak
- **dešifriranje** – korištenjem privatnog ključa pretvoriti težak problem u jednostavan i riješiti ga

- Primjeri problema

- faktORIZACIJA brojeva (**RSA**, Rabin)
- diskretni logaritmi (**Diffie-Hellman**, DSS, **El-Gamal**)
- eliptičke krivulje (LUC, XTR)

Asimetrični algoritmi (svojstvo)



Steganografija

- **Skrivanje** poruke
 - nitko osim pošiljatelja i primatelja nije svjestan postojanja poruke
- **Primjer**
 - skrivanje tajne slike u niže bitove kamuflažne slike



Najniža 2 bita svakog piksela



Izvor: Wikipedia: Steganography

- Primjena: *vodeni žig* u multimedijalnim sadržajima (©, DRM)

Usporedba svojstva algoritama - simetrični

- Prednosti

- **velika raznolikost** algoritama
- **brzina**
 - manja računska složenost
 - *jednostavna* sklopovska implementacija



- Mane

- **distribucija** ključeva
 - razgovor N sugovornika zahtijeva $n \cdot (n-1)/2$ ključeva
 - problem razmjene ključa

Usporedba svojstava algoritama - asimetrični

- Mane

- **sporost**

- velika računska složenost
 - složena implementacija

- Prednosti

- **distribucija** ključeva

- javni ključ se može slobodno dijeliti

- Idealni algoritam imao bi dobra svojstva obje grupe

- brzinu simetričnih
 - rukovanje ključevima asimetričnih



Primjena algoritama

- Šifriranje podataka (npr. na disku)
 - cjelovitost
 - tajnost
- Digitalni potpis
 - ovjera izvornosti
 - cjelovitost
 - neporicljivost
- Digitalna omotnica
 - ovjera izvornosti
 - cjelovitost
 - neporicljivost
 - tajnost



Ključevi

- Što sve može biti ključ?
- Vrste ključeva
 - kratki (pamtljivi)
 - alfanumerički
 - lozinke
 - OTP (*one-time password*, ključ za jednokratnu uporabu)
 - token – sklopovska izvedba OTP-a
 - Dugi
 - sažetak
 - certifikat
 - pametna kartica
 - Biometrijski
 - otisak prsta ili dlana
 - uzorak šarenice ili lica
 - glas, DNA ...



Važnost ključa

- Sigurnost ovisi o kvaliteti ključa
 - idealan ključ – slučajni broj velike duljine
- Ključevi za simetrične kriptosustave
 - (pseudo)slučajni brojevi
 - bitna kvaliteta generatora slučajnih brojeva
 - predvidivost generatora = predvidivost ključa
- Ključevi za asimetrične sustave
 - posebna svojstva
 - npr. umnožak dva velika prosta broja (RSA)
 - potrebna veća duljina ključa za istu razinu sigurnosti

Pohrana ključeva

- Tajni ključ (simetrični i asimetrični algoritmi)
 - sigurnosne norme zahtijevaju pohranu unutar uređaja
 - pametne kartice (ključ, certifikat)
 - kriptouređaji (ključ, certifikat)
 - ključ **ne može** (ne smije) napustiti uređaj
 - pokušaj otvaranja uređaja rezultira uništenjem ključa
- Slično je i s biometrijskim ključevima :)

