

# Kriptozaštita ( šifriranje podataka)

Anela Bocor i Vojislav Đuračković

27. travnja 2009.

## Uvod

Julije Cezar nije vjerovao glasnicima kada je slao poruke svojim generalima.

Zato je on u porukama svako slovo sa A zamijenio s D, svako slovo B sa E, ...

Samo ona osoba koja je znala pravilo “pomaka za tri” mogla je razumijeti sadržaj poruke.

- ▶ Šifriranjem se postiže visok stupanje zaštite podataka koji se spremaju na računalima i podataka koji se posredstvom računalne mreže razmjenjuju između korisnika i računala
- ▶ npr. zaštita financijskih podataka koji se prenose mrežom
- ▶ Sadržaje podataka koji su pohranjeni na računalu moguće je “uhvatiti” korištenjem analizatora protokola ili nekog *sniffer* programa

- ▶ Šifriranjem se postiže visok stupanje zaštite podataka koji se spremaju na računalima i podataka koji se posredstvom računalne mreže razmjenjuju između korisnika i računala
- ▶ npr. zaštita financijskih podataka koji se prenose mrežom
- ▶ Sadržaje podataka koji su pohranjeni na računalu moguće je “uhvatiti” korištenjem analizatora protokola ili nekog *sniffer* programa

- ▶ Šifriranjem se postiže visok stupanje zaštite podataka koji se spremaju na računalima i podataka koji se posredstvom računalne mreže razmjenjuju između korisnika i računala
- ▶ npr. zaštita financijskih podataka koji se prenose mrežom
- ▶ Sadržaje podataka koji su pohranjeni na računalu moguće je “uhvatiti” korištenjem analizatora protokola ili nekog *sniffer* programa

## Terminologija u kriptografiji

Kriptografija je znanost koja se oslanjajući na matematiku bavi proučavanjem i pronalaženjem metoda za šifriranje\ dešifriranje podataka. Kriptoanaliza je znanost o “razbijanju” šifri.

Kriptologija je nauka koja objedinjuje kriptografiju i kriptoanalizu.

- ▶ *plain (clear) text* → otvoren tekst
- ▶ *šifriranje ( encryption)* → metoda skrivanja sadržaja
- ▶ *ciphertext (cipher)* → šifrirani tekst
- ▶ *dešifriranje (decryption)*

## Terminologija u kriptografiji

Kriptografija je znanost koja se oslanjajući na matematiku bavi proučavanjem i pronalaženjem metoda za šifriranje\ dešifriranje podataka. Kriptoanaliza je znanost o “razbijanju” šifri.

Kriptologija je nauka koja objedinjuje kriptografiju i kriptoanalizu.

- ▶ *plain (clear) text* → otvoren tekst
- ▶ *šifriranje ( encryption)* → metoda skrivanja sadržaja
- ▶ *ciphertext (cipher)* → šifrirani tekst
- ▶ *dešifriranje (decryption)*

## Terminologija u kriptografiji

Kriptografija je znanost koja se oslanjajući na matematiku bavi proučavanjem i pronalaženjem metoda za šifriranje \ dešifriranje podataka. Kriptoanaliza je znanost o “razbijanju” šifri.

Kriptologija je nauka koja objedinjuje kriptografiju i kriptoanalizu.

- ▶ *plain (clear) text* → otvoren tekst
- ▶ *šifriranje ( encryption)* → metoda skrivanja sadržaja
- ▶ *ciphertext (cipher)* → šifrirani tekst
- ▶ *dešifriranje (decryption)*

## Terminologija u kriptografiji

Kriptografija je znanost koja se oslanjajući na matematiku bavi proučavanjem i pronalaženjem metoda za šifriranje\ dešifriranje podataka. Kriptoanaliza je znanost o “razbijanju” šifri.

Kriptologija je nauka koja objedinjuje kriptografiju i kriptoanalizu.

- ▶ *plain (clear) text* → otvoren tekst
- ▶ *šifriranje ( encryption)* → metoda skrivanja sadržaja
- ▶ *ciphertext (cipher)* → šifrirani tekst
- ▶ *dešifriranje (decryption)*

## Terminologija u kriptografiji

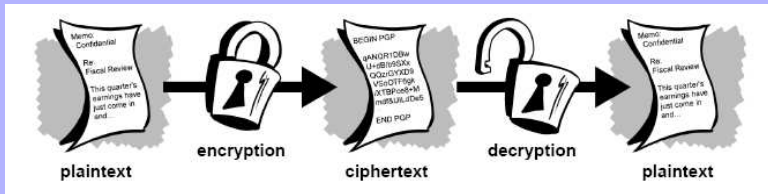
Kriptografija je znanost koja se oslanjajući na matematiku bavi proučavanjem i pronalaženjem metoda za šifriranje \ dešifriranje podataka. Kriptoanaliza je znanost o “razbijanju” šifri.

Kriptologija je nauka koja objedinjuje kriptografiju i kriptoanalizu.

- ▶ *plain (clear) text* → otvoren tekst
- ▶ *šifriranje ( encryption)* → metoda skrivanja sadržaja
- ▶ *ciphertext (cipher)* → šifrirani tekst
- ▶ *dešifriranje (decryption)*

## Šifre i kriptosustavi

Šifra ili kriptografski algoritam je matematička funkcija koja se koristi u procesu šifriranja i dešifriranja. Kriptografski algoritam radi u kombinaciji sa ključem (riječ, broj ili fraza) da bi se moglo izvršiti šifriranje poruke, odnosno, dešifriranje šifriranih tekstova.



## Kriptosustavi

Kriptografski algoritam zajedno sa ključem i protokolima koji omogućuju njegov rad, čine kriptosustav.

- ▶ Postoji veliki broj kriptosustava za šifriranje podataka koji se klacificiraju u dvije grupe:
  - ▶ simetrični → koristi se jedan ključ
  - ▶ asimetrični → postoje dva ključa

## Kriptosustavi

Kriptografski algoritam zajedno sa ključem i protokolima koji omogućuju njegov rad, čine kriptosustav.

- ▶ Postoji veliki broj kriptosustava za šifriranje podataka koji se klacificiraju u dvije grupe:
  - ▶ simetrični → koristi se jedan ključ
  - ▶ asimetrični → postoje dva ključa

## Kriptosustavi

Kriptografski algoritam zajedno sa ključem i protokolima koji omogućuju njegov rad, čine kriptosustav.

- ▶ Postoji veliki broj kriptosustava za šifriranje podataka koji se klacificiraju u dvije grupe:
  - ▶ simetrični → koristi se jedan ključ
  - ▶ asimetrični → postoje dva ključa

Dva osnovna zahtjeva koja se postavljaju pred kriptosustave pri njihovoj primjeni na zaštiti podataka u računalnim mrežama su:

- ▶ jednostavnost za upotrebu tako da ih korisnici mogu lakše koristiti
- ▶ zaštita podataka zavisi od tajnosti ključa, a ne od primjenjenog kriptografskog algoritma

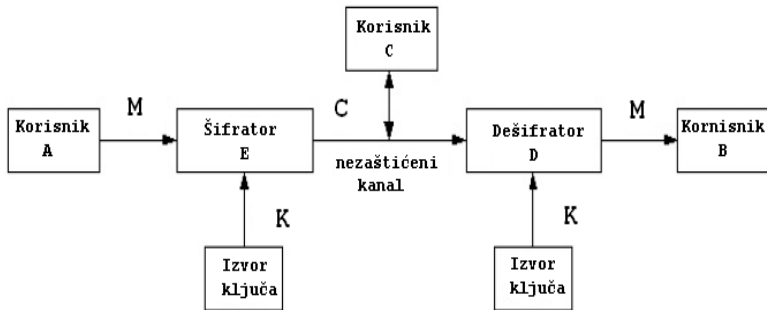
Dva osnovna zahtjeva koja se postavljaju pred kriptosustave pri njihovoj primjeni na zaštiti podataka u računalnim mrežama su:

- ▶ jednostavnost za upotrebu tako da ih korisnici mogu lakše koristiti
- ▶ zaštita podataka zavisi od tajnosti ključa, a ne od primjenjenog kriptografskog algoritma

## Simetrični kriptosustavi

Osnovna osobina simetričnih kriptosustava sa jednim ključem *Single-Key Cryptosystems* je da se isti ključ koristi i za šifriranje i za dešifriranje.

Slijedeća slika prikazuje princip rada jednog kriptosustava



Osnovni problemi kod simetričnih kriptosustava:

- ▶ distribucija ključeva
- ▶ zamjena postojećih ključeva novim ključevima

Najpoznatiji algoritmi simetričnih kriptosustava su:

- ▶ DES (Data Encryption Standard) s ključem dužine 56 bita
- ▶ 3DES s dva ključa od po 112 bita
- ▶ RC2 i RC4 (Ron's Ciphers) s ključevima od 40 i 128 bita

Osnovni problemi kod simetričnih kriptosustava:

- ▶ distribucija ključeva
- ▶ zamjena postojećih ključeva novim ključevima

Najpoznatiji algoritmi simetričnih kriptosustava su:

- ▶ DES (Data Encryption Standard) s ključem dužine 56 bita
- ▶ 3DES s dva ključa od po 112 bita
- ▶ RC2 i RC4 (Ron's Ciphers) s ključevima od 40 i 128 bita

Osnovni problemi kod simetričnih kriptosustava:

- ▶ distribucija ključeva
- ▶ zamjena postojećih ključeva novim ključevima

Najpoznatiji algoritmi simetričnih kriptosustava su:

- ▶ DES (Data Encryption Standard) s ključem dužine 56 bita
- ▶ 3DES s dva ključa od po 112 bita
- ▶ RC2 i RC4 (Ron's Ciphers) s ključevima od 40 i 128 bita

Osnovni problemi kod simetričnih kriptosustava:

- ▶ distribucija ključeva
- ▶ zamjena postojećih ključeva novim ključevima

Najpoznatiji algoritmi simetričnih kriptosustava su:

- ▶ DES (Data Encryption Standard) s ključem dužine 56 bita
- ▶ 3DES s dva ključa od po 112 bita
- ▶ RC2 i RC4 (Ron's Ciphers) s ključevima od 40 i 128 bita

Osnovni problemi kod simetričnih kriptosustava:

- ▶ distribucija ključeva
- ▶ zamjena postojećih ključeva novim ključevima

Najpoznatiji algoritmi simetričnih kriptosustava su:

- ▶ DES (Data Encryption Standard) s ključem dužine 56 bita
- ▶ 3DES s dva ključa od po 112 bita
- ▶ RC2 i RC4 (Ron's Ciphers) s ključevima od 40 i 128 bita

## Asimetrični kriptosustavi

Kao rješenje problema distribucije ključeva koji postoji kod simetričnih kriptosustava, Whitfield Diffie i Martin Hellman su 1975. godine prodložili asimetrične kriptosustave.

Mogućnosti koje pružaju ti kriptosustavi koriste državne institucije, vojska, policija i dr.

Asimetrični kriptosustavi ili kriptosustavi sa javnim ključem (Public-Key Cryptosystems) se baziraju na radu s dva ključa:

1. javni ključ (Public Key), kojim se vrši šifriranje
2. tajni ili privatni ključ (Secret Key), koji se koristi za dešifriranje.

## Asimetrični kriptosustavi

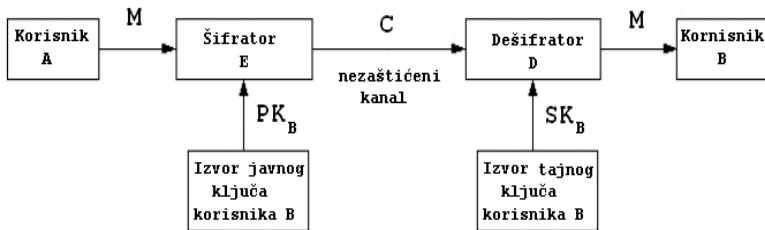
Kao rješenje problema distribucije ključeva koji postoji kod simetričnih kriptosustava, Whitfield Diffie i Martin Hellman su 1975. godine prodložili asimetrične kriptosustave.

Mogućnosti koje pružaju ti kriptosustavi koriste državne institucije, vojska, policija i dr.

Asimetrični kriptosustavi ili kriptosustavi sa javnim ključem (Public-Key Cryptosystems) se baziraju na radu s dva ključa:

1. javni ključ (Public Key), kojim se vrši šifriranje
2. tajni ili privatni ključ (Secret Key), koji se koristi za dešifriranje.

Na slici je prikazan princip rada kod asimetričnih kriptosustava kada korisnik A šalje poruku korisniku B.



- ▶ Najveća prednost asimetričnih kriptosustava u odnosu na simetrične je u pogledu distribucije ključeva.
- ▶ Samo korisnik koji ima odgovarajući tajni ključ može dešifrirati poruku.
- ▶ Matematički je praktički nemoguće odrediti tajni ključ ukoliko se poznaje javni, jer se primjenjuju funkcije, čiji je inverz veoma teško naći, primjerice:
  - ▶ logaritmiranje po modulu nekog velikog cijelog broja
  - ▶ pronalaženje prostih faktora velikih cijelih brojeva

- ▶ Najveća prednost asimetričnih kriptosustava u odnosu na simetrične je u pogledu distribucije ključeva.
- ▶ Samo korisnik koji ima odgovarajući tajni ključ može dešifrirati poruku.
- ▶ Matematički je praktički nemoguće odrediti tajni ključ ukoliko se poznaje javni, jer se primjenjuju funkcije, čiji je inverz veoma teško naći, primjerice:
  - ▶ logaritmiranje po modulu nekog velikog cijelog broja
  - ▶ pronalaženje prostih faktora velikih cijelih brojeva

- ▶ Najveća prednost asimetričnih kriptosustava u odnosu na simetrične je u pogledu distribucije ključeva.
- ▶ Samo korisnik koji ima odgovarajući tajni ključ može dešifrirati poruku.
- ▶ Matematički je praktički nemoguće odrediti tajni ključ ukoliko se poznaje javni, jer se primjenjuju funkcije, čiji je inverz veoma teško naći, primjerice:
  - ▶ logaritmiranje po modulu nekog velikog cijelog broja
  - ▶ pronalaženje prostih faktora velikih cijelih brojeva

- ▶ Najveća prednost asimetričnih kriptosustava u odnosu na simetrične je u pogledu distribucije ključeva.
- ▶ Samo korisnik koji ima odgovarajući tajni ključ može dešifrirati poruku.
- ▶ Matematički je praktički nemoguće odrediti tajni ključ ukoliko se poznaje javni, jer se primjenjuju funkcije, čiji je inverz veoma teško naći, primjerice:
  - ▶ logaritmiranje po modulu nekog velikog cijelog broja
  - ▶ pronalaženje prostih faktora velikih cijelih brojeva

- ▶ Najveća prednost asimetričnih kriptosustava u odnosu na simetrične je u pogledu distribucije ključeva.
- ▶ Samo korisnik koji ima odgovarajući tajni ključ može dešifrirati poruku.
- ▶ Matematički je praktički nemoguće odrediti tajni ključ ukoliko se poznaje javni, jer se primjenjuju funkcije, čiji je inverz veoma teško naći, primjerice:
  - ▶ logaritmiranje po modulu nekog velikog cijelog broja
  - ▶ pronalaženje prostih faktora velikih cijelih brojeva

- ▶ Najpoznatiji algoritmi koji se primjenjuju kod asimetričnih kriptosustava su: Diffie–Hellmanov, RSA, ElGamal, Rabin, Eliptic Curves i dr.
- ▶ RSA (Rivest–Shamir–Adleman) algoritam, jedan je od najkorištenijih asimetričnih algoritama danas.
- ▶ U RSA algoritmu ključnu ulogu imaju veliki prosti brojevi.

- ▶ Najpoznatiji algoritmi koji se primjenjuju kod asimetričnih kriptosustava su: Diffie–Hellmanov, RSA, ElGamal, Rabin, Eliptic Curves i dr.
- ▶ RSA (Rivest–Shamir–Adleman) algoritam, jedan je od najkorištenijih asimetričnih algoritama danas.
- ▶ U RSA algoritmu ključnu ulogu imaju veliki prosti brojevi.

- ▶ Najpoznatiji algoritmi koji se primjenjuju kod asimetričnih kriptosustava su: Diffie–Hellmanov, RSA, ElGamal, Rabin, Eliptic Curves i dr.
- ▶ RSA (Rivest–Shamir–Adleman) algoritam, jedan je od najkorištenijih asimetričnih algoritama danas.
- ▶ U RSA algoritmu ključnu ulogu imaju veliki prosti brojevi.

Pogledajmo na primjeru kako se pomoću RSA algoritma generiraju javni i tajni ključ

- ▶ Prosti brojevi ( $P$  i  $Q$ ) u RSA algoritmu služe za generiranje javnog i tajnog ključa preko sljedećih formula
  - ▶  $K_{\text{javni}} = P \times Q$
  - ▶  $K_{\text{tajni}} = \frac{2 \times (P-1) \times (Q-1) + 1}{3}$
- ▶ Algoritam šifriranja i dešifriranja sastoji se iz dvije formule
  - ▶ Šifriranje:  $M_{\text{šifrirano}} = (M_{\text{izvorno}}^3) \bmod K_{\text{javni}}$
  - ▶ Dešifriranje:  $M_{\text{izvorno}} = (M_{\text{šifrirano}}^{K_{\text{tajni}}}) \bmod K_{\text{javni}}$

Pogledajmo na primjeru kako se pomoću RSA algoritma generiraju javni i tajni ključ

- ▶ Prosti brojevi ( $P$  i  $Q$ ) u RSA algoritmu služe za generiranje javnog i tajnog ključa preko sljedećih formula
  - ▶  $K_{\text{javni}} = P \times Q$
  - ▶  $K_{\text{tajni}} = \frac{2 \times (P-1) \times (Q-1) + 1}{3}$
- ▶ Algoritam šifriranja i dešifriranja sastoji se iz dvije formule
  - ▶ Šifriranje:  $M_{\text{šifrirano}} = (M_{\text{izvorno}}^3) \bmod K_{\text{javni}}$
  - ▶ Dešifriranje:  $M_{\text{izvorno}} = (M_{\text{šifrirano}}^{K_{\text{tajni}}}) \bmod K_{\text{javni}}$

Pogledajmo na primjeru kako se pomoću RSA algoritma generiraju javni i tajni ključ

- ▶ Prosti brojevi ( $P$  i  $Q$ ) u RSA algoritmu služe za generiranje javnog i tajnog ključa preko sljedećih formula
  - ▶  $K_{\text{javni}} = P \times Q$
  - ▶  $K_{\text{tajni}} = \frac{2 \times (P-1) \times (Q-1) + 1}{3}$
- ▶ Algoritam šifriranja i dešifriranja sastoji se iz dvije formule
  - ▶ Šifriranje:  $M_{\text{šifrirano}} = (M_{\text{izvorno}}^3) \bmod K_{\text{javni}}$
  - ▶ Dešifriranje:  $M_{\text{izvorno}} = (M_{\text{šifrirano}}^{K_{\text{tajni}}}) \bmod K_{\text{javni}}$

Pogledajmo na primjeru kako se pomoću RSA algoritma generiraju javni i tajni ključ

- ▶ Prosti brojevi ( $P$  i  $Q$ ) u RSA algoritmu služe za generiranje javnog i tajnog ključa preko sljedećih formula
  - ▶  $K_{\text{javni}} = P \times Q$
  - ▶  $K_{\text{tajni}} = \frac{2 \times (P-1) \times (Q-1) + 1}{3}$
- ▶ Algoritam šifriranja i dešifriranja sastoji se iz dvije formule
  - ▶ Šifriranje:  $M_{\text{šifrirano}} = (M_{\text{izvorno}}^3) \bmod K_{\text{javni}}$
  - ▶ Dešifriranje:  $M_{\text{izvorno}} = (M_{\text{šifrirano}}^{K_{\text{tajni}}}) \bmod K_{\text{javni}}$

Pogledajmo na primjeru kako se pomoću RSA algoritma generiraju javni i tajni ključ

- ▶ Prosti brojevi ( $P$  i  $Q$ ) u RSA algoritmu služe za generiranje javnog i tajnog ključa preko sljedećih formula
  - ▶  $K_{\text{javni}} = P \times Q$
  - ▶  $K_{\text{tajni}} = \frac{2 \times (P-1) \times (Q-1) + 1}{3}$
- ▶ Algoritam šifriranja i dešifriranja sastoji se iz dvije formule
  - ▶ Šifriranje:  $M_{\text{šifrirano}} = (M_{\text{izvorno}}^3) \bmod K_{\text{javni}}$
  - ▶ Dešifriranje:  $M_{\text{izvorno}} = (M_{\text{šifrirano}}^{K_{\text{tajni}}}) \bmod K_{\text{javni}}$

Pogledajmo na primjeru kako se pomoću RSA algoritma generiraju javni i tajni ključ

- ▶ Prosti brojevi ( $P$  i  $Q$ ) u RSA algoritmu služe za generiranje javnog i tajnog ključa preko sljedećih formula
  - ▶  $K_{\text{javni}} = P \times Q$
  - ▶  $K_{\text{tajni}} = \frac{2 \times (P-1) \times (Q-1) + 1}{3}$
- ▶ Algoritam šifriranja i dešifriranja sastoji se iz dvije formule
  - ▶ Šifriranje:  $M_{\text{šifrirano}} = (M_{\text{izvorno}}^3) \bmod K_{\text{javni}}$
  - ▶ Dešifriranje:  $M_{\text{izvorno}} = (M_{\text{šifrirano}}^{K_{\text{tajni}}}) \bmod K_{\text{javni}}$

Na primjer hoćemo kodirati riječ “MAJA”, koja ima ASCII kod oblika: 77 65 74 65

Za proste brojeve možemo uzeti  $P = 9839$  i  $Q = 22391$ . U tom slučaju ključevi koji će se koristiti glase:

Kjavni: 220305049

Ktajni: 146848547

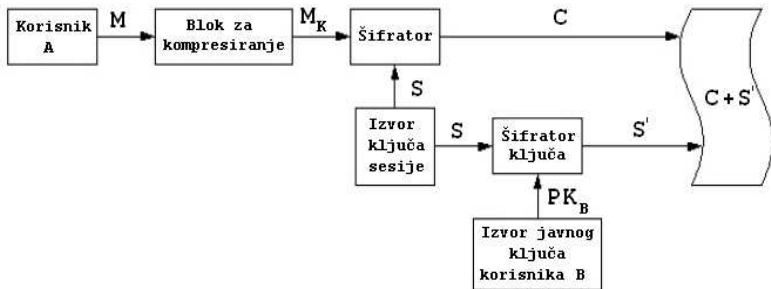
Primjenimo formule i imamo:

$$(77657465^3) \bmod 220305049 = 162621874$$

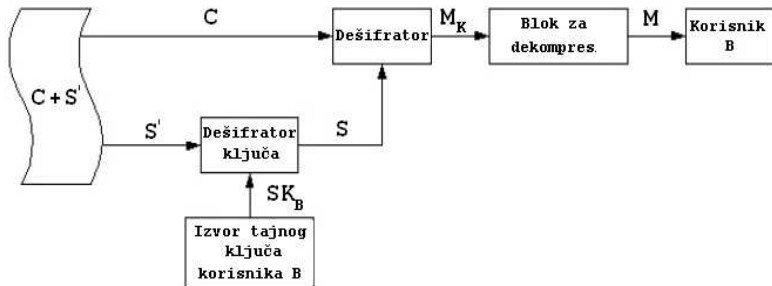
$$(162621874^{146848547}) \bmod 220305049 = 77657465$$

## Hibridni kriptosustav PGP

PGP ( *Pretty Good Privacy* ) je hibridni kriptosustav jer kombinira najbolje osobine simetričnih i asimetričnih kriptosustava. Princip rada PGP kriptosustava prikazan je sljedećim dvijema slikama, prva prikazuje postupak šifriranja, a druga dešifriranja.



PGP šifriranje



PGP dešifriranje

## Digitalni potpis

Tehnologija digitalnog potpisa također koristi tehniku asimetričnog kriptiranja.

Svrha digitalnog potpisa je potvrditi autentičnost sadržaja poruke ili integritet podataka.

Osnovu digitalnog potpisa čini sadržaj same poruke.

Pošiljatelj primjenom određenih kriptografskih algoritama, prvo od svoje poruke koja je proizvoljne dužine stvara zapis fiksne dužine, koji u potpunosti oslikava sadržaj poruke. Ovako dobiven zapis se dalje šifrira tajnim ključem te se tako formirani digitalni potpis šalje zajedno s porukom.

