

SIGURNOST RAČUNARSKIH MREŽA (SRM)

Tema 3: Kriptografija

URLs:

2

- Zvanična Web strana: www.viser.edu.rs/predmeti.php?id=122

- Dodatni resursi: www.conwex.info/draganp/teaching.html

- Knjige:
www.conwex.info/draganp/books.html

- Teme za seminarske radove:
www.conwex.info/draganp/SRM_seminarski_radovi.html

Napomena

3

- **Ovo je skraćena verzija prezentacije / predavanja na temu “Kriptografija”**
 - ▣ Podrazumeva se da je oblast kriptografije detaljnije obrađena u prethodno slušanom predmetu
 - ▣ Za demonstraciju se koriste alati CryptTool i Animal

Kriptografija

4

- Sadržaj poglavlja i predavanja:
 - 3.1 Matematičke osnove (neophodne za izučavanje kriptografije)
 - 3.2 Osnovni kriptografski pojmovi i klasična kriptografija
 - 3.3 Simetrični blokovski algoritmi
 - 3.4 Pseudoslučajne sekvence i protočno šifrovanje
 - 3.5 Heš funkcije
 - 3.6 Kriptografija s javnim ključevima
 - 3.7 Sertifikati i infrastruktura javnih ključeva
 - 3.8 Kriptografski softver
 - 3.9 Vežbe za programere

"It seems very simple."

"It is very simple. But if you don't know what the key is it's virtually indecipherable."

—Talking to Strange Men, Ruth Rendell

Kriptografija

6

- Na predavanjima će samo delimično biti pomenuto:
 - ▣ Matematičke osnove (neophodne za izučavanje kriptografije)
 - ▣ Kriptografski softver
 - ▣ Vežbe za programere

Potrebna predznanja

7

- Matematika
- Programiranje
- Materija predmeta “Sigurnost informacionih sistema”

- Za primenu:
 - ▣ Računarske mreže i protokoli
 - ▣ Baze podataka
 - ▣ Operativni sistemi
 - ▣ Internet

CrypTool

8

- www.cryptool.org
eLearning Program for Cryptology
- Binarna verzija i otvoreni izvorni kod (engl. *open source*)
raspoloživi za besplatno preuzimanje (GPL licenca)
- Raspoloživa obimna dokumentacija
- Raspoloživo na nekoliko jezika, uključujući i srpski
- Možete se uključiti i učestvovati u daljem razvoju

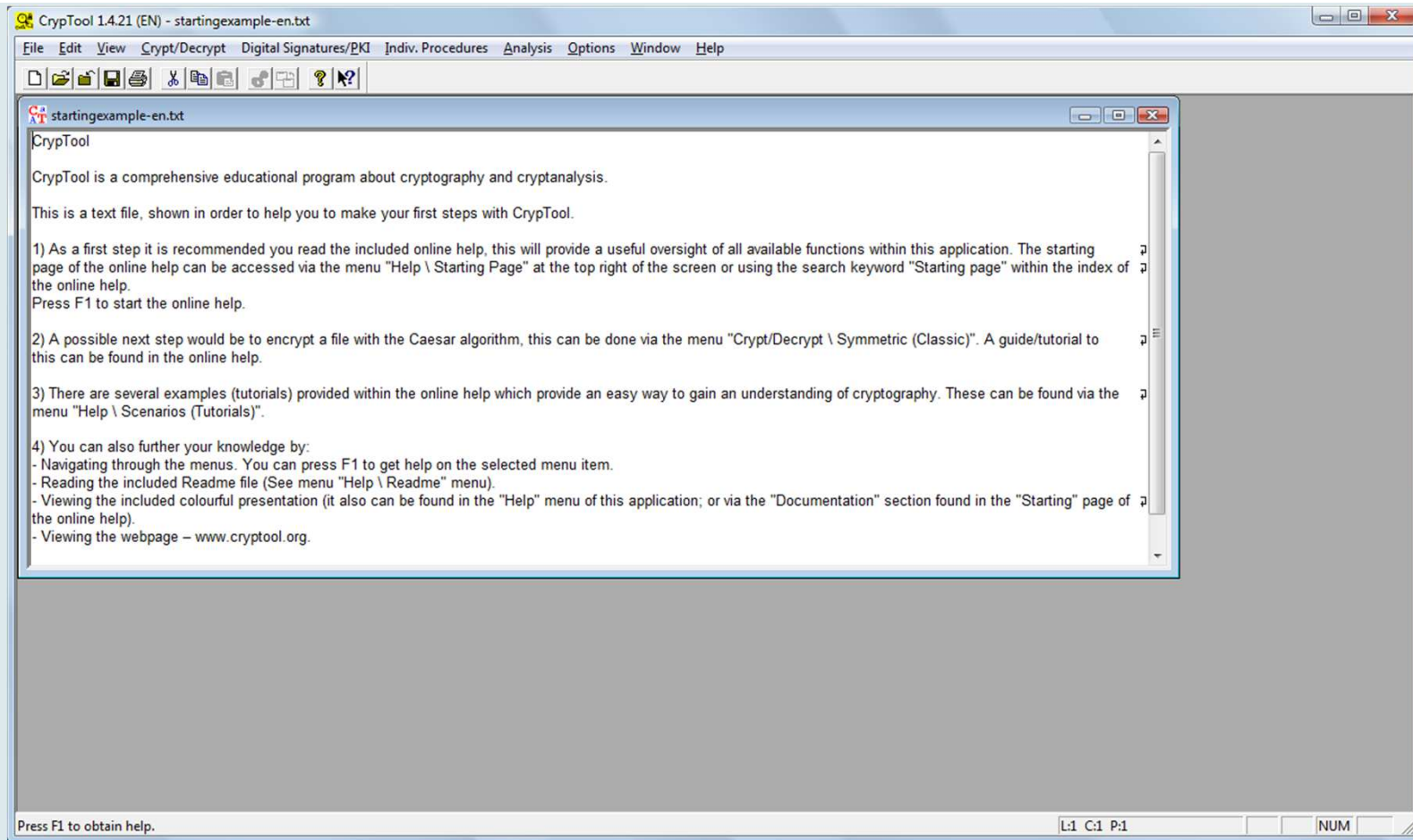
CrypTool Web

9

The screenshot shows the homepage of the CrypTool website. At the top left is the CrypTool logo, a stylized 'Ct' in blue. To its right is the text 'CRYPTOOL' in a bold, blue, sans-serif font. A diagonal banner in the top right corner reads 'Stabilna Beta 1.4.30 preuzmite & testirajte sada'. Below the logo and banner is a dark blue navigation bar with white text for 'O nama', 'Funkcije', 'Slike', 'Dokumentacija', and 'Preuzimanje'. To the right of the navigation bar are flags for Germany, UK, Spain, and Poland. Below the navigation bar is a yellow banner with the text 'Najnovija CT1 verzija: 1.4.21 [Preuzimanje](#)'. The main content area is divided into two columns. The left column has a sidebar with a 'O nama' section containing a list of links: 'Uvod u CrypTool', 'CrypTool u Obrazovanju', 'CrypTool za Svesnost', 'Pokrivenost u Medijima', 'Nagrade', 'Saradnici', 'Srodni Projekti', and 'Kontakt'. Below this is a 'Selected Landmark 2008 in: Germany Land of Ideas' section with a row of colored circles and a quote: '"CrypTool ist einmalig, medial anregend aufgebaut und, soweit ich es uebersehe, ohne Fehler."' followed by 'Prof. Dr. Ruediger Grimm, TU Illmenau'. The right column has a main heading 'Uvod u CrypTool' with a print icon. Below it is a paragraph: 'Aplikacija CrypTool je besplatna aplikacija za e-učenje za Windows. Možete je koristiti za primenu i analizu kriptografskih algoritama. Trenutna verzija CrypTool-a ([Preuzimanje](#)) je korišćena širom sveta. Ona podržava i savremene nastavne metode u školama i univerzitetima, kao i svest za obuku državnih službenika i zaposlenih.' This is followed by a list of features: 'Trenutna verzija, [pored ostalih](#), nudi sledeće funkcije:'. The list includes: 'Brojne klasične i moderne kriptografske algoritme (šifrovanje i dešifrovanje, generisanje ključa, sigurne lozinke, autentikaciju, sigurnosne protokole, ...)', 'Vizualizaciju nekoliko metoda (npr. Caesar, Enigma, RSA, Diffie-Hellman, digitalne potpise, AES)', 'Kriptoanalizu određenih algoritama (npr. Vigenère, RSA, AES)', 'Kriptoanalitičke metode merenja (npr. entropiju, n-grame, autokorelaciju)', 'Pomoćne metode (npr. testovi na proste brojeve, rastavljanje na proste činioce, base64 kodiranje)', 'Tutorijal o prostim brojevima', 'Sveobuhvatnu online pomoć', and 'Skriptu sa podrškom za dalje informacije o kriptologiji'. Below the list is a paragraph: 'Od svoje prvobitne upotrebe u oblasti sigurnosti informacija za firme, CrypTool se razvio u izvanredan projekat otvorenog koda za teme vezane uz kriptologiju.' This is followed by another paragraph: 'Počev od proleća 2008, CrypTool projekat radi sa [Crypto Portalom za Nastavnike](#). Do danas, portal je dostupan samo na Nemačkom i zamišljen je kao platforma za nastavnike da podele svoje materijale za nastavu o kriptologiji i srodnim temama.' The final paragraph reads: 'Od proleća 2009, CrypTool projekat takođe poseduje i [CrypTool-Online](#). Ovaj portal daje ljudima zainteresovanim za kriptologiju mogućnost da probaju razne šifre i metode šifrovanja u svom pretraživaču bez preuzimanja ili instaliranja bilo kakvog dodatnog software-a. Na ovom web site-u za korisnike koji dolaze prvi put, kao i mlade ljude, mi pružamo kriptologiju na privlačan i lak način. Za napredne zadatke i probleme i dalje postoji lokalna verzija CrypTool-a koji se može preuzeti i instalirati.'

CrypTool basic screen

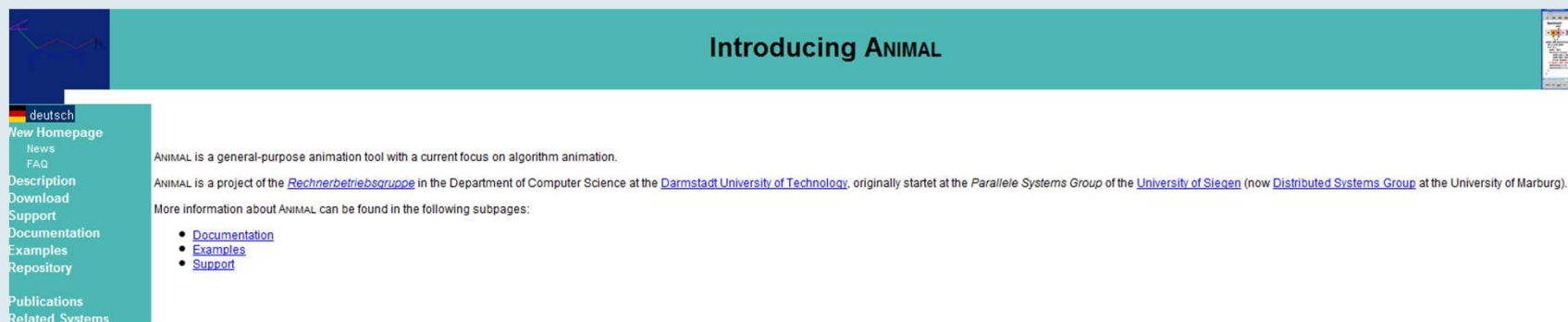
10



Animal

11

- www.animal.ahrgr.de/index.php3?lang=en
- From Web site:
 - ANIMAL is a general-purpose animation tool with a current focus on algorithm animation.
 - ANIMAL is a project of the [Rechnerbetriebsgruppe](#) in the Department of Computer Science at the [Darmstadt University of Technology](#), originally started at the *Parallele Systems Group* of the [University of Siegen](#) (now [Distributed Systems Group](#) at the University of Marburg).



Introducing ANIMAL

deutsch

New Homepage

News

FAQ

Description

Download

Support

Documentation

Examples

Repository

Publications

Related Systems

ANIMAL is a general-purpose animation tool with a current focus on algorithm animation.

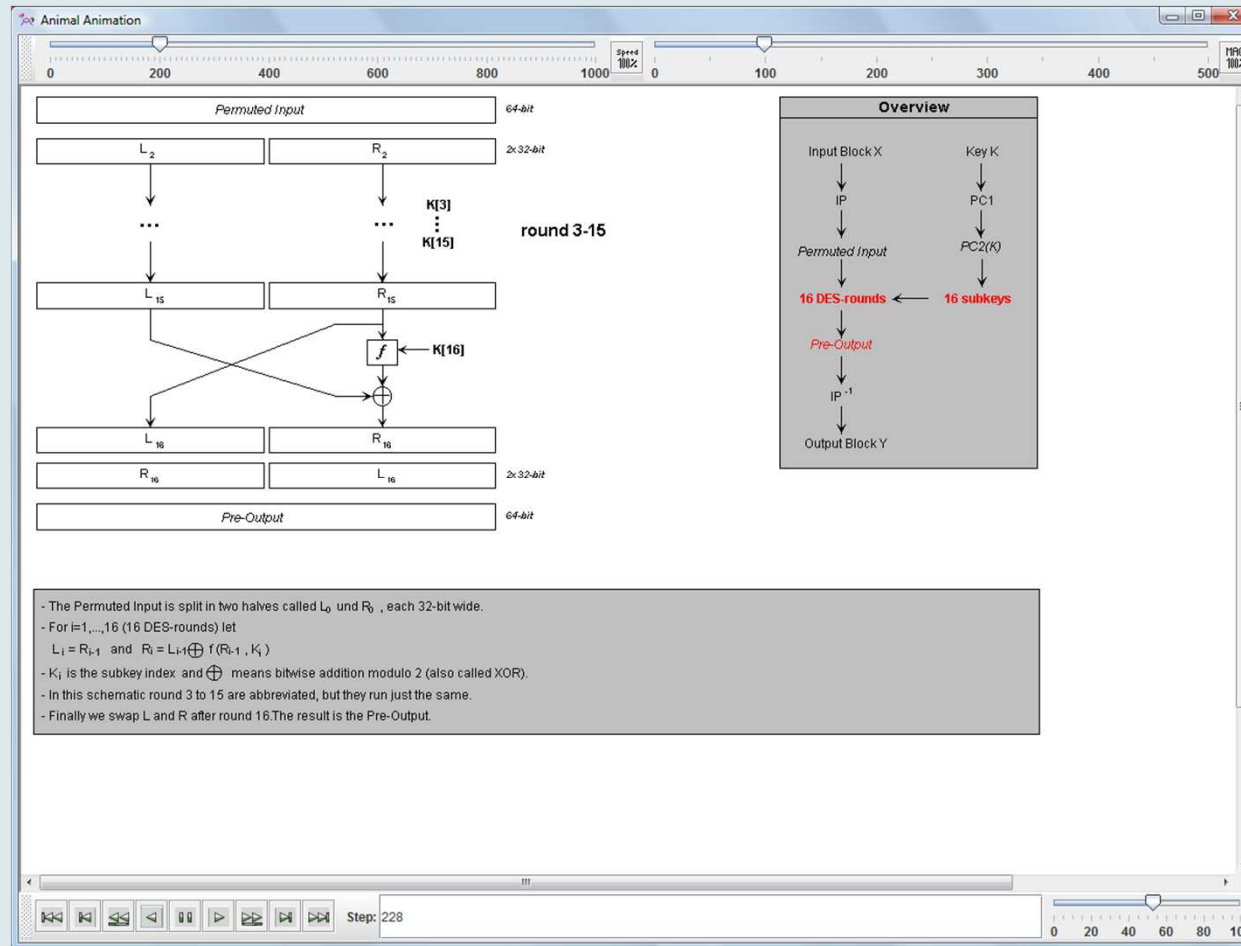
ANIMAL is a project of the [Rechnerbetriebsgruppe](#) in the Department of Computer Science at the [Darmstadt University of Technology](#), originally started at the *Parallele Systems Group* of the [University of Siegen](#) (now [Distributed Systems Group](#) at the University of Marburg).

More information about ANIMAL can be found in the following subpages:

- [Documentation](#)
- [Examples](#)
- [Support](#)

Animal Animation - DES

12



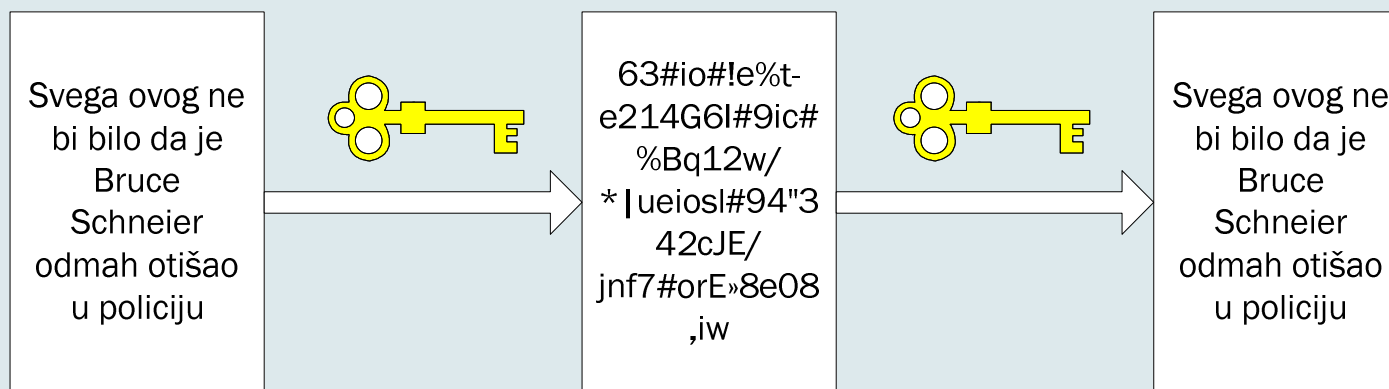
Osnovni pojmovi

13

- **Šifrovanje** (engl. *encryption*) obuhvata matematičke postupke modifikacije podataka takve da šifrovane podatke mogu pročitati samo korisnici sa odgovarajućim ključem
- **Dešifrovanje** (engl. *decryption*) je obrnut proces: šifrovani podaci se pomoću ključa transformišu u originalnu poruku ili datoteku.

Proces šifrovanja i dešifrovanja

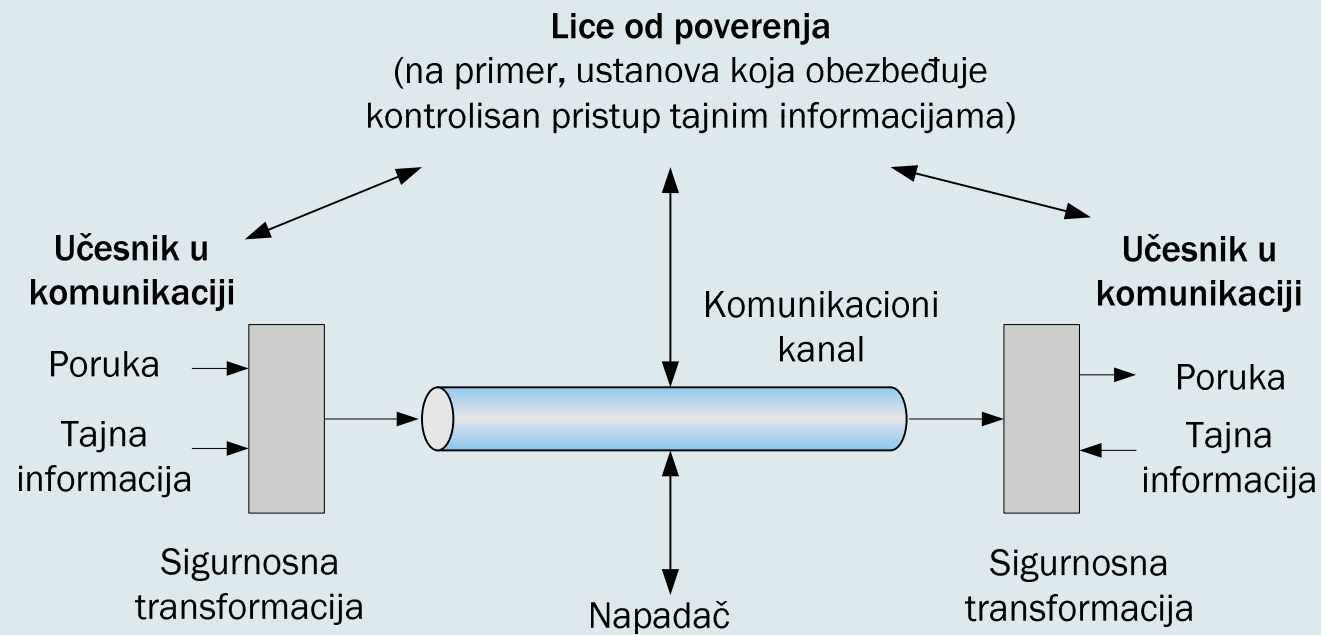
14



Sigurnosni model kriptografije

15

- Model sa nesigurnim komunikacionim kanalom



Definicije

16

- **Kriptografija** – nauka o tajnom pisanju (zapisivanju), nauka koja se bavi metodama očuvanja tajnosti informacija
 - ▣ Grčke reči kryptos (tajno, sakriti, skriveno) i grafos (pisati, pisanje)
 - Cryptography or cryptology; from Greek κρυπτός, kryptos, "hidden, secret"; and γράφω, gráphō, "I write", or -λογία, -logia

- **Kriptografski algoritam** - transformiše čitljiv tekst P (**plain text**) u nečitljiv tekst C (**crypted, chiphered text**)

- **Kriptoanaliza** – nauka o dobijanju čitljivog teksta P (ili ključeva...) na bazi šifrovanog teksta

- **Napad** – pokušaj kryptoanalize

- **Kompromitovanje** – dobijanje tajne bez kryptoanalitičkih metoda (krađa, tortura...)

Ciljevi kriptografije

17

- **Poverljivost (tajnost)** – prevencija od neautorizovanog pristupa informacijama (obezbeđuje privatnost za poruke)
- **Integritet (celovitost)** – prevencija od neautorizovanog menjanja informacija (obezbeđuje potvrdu da poruka ostaje nepromenjena)
- **Raspoloživost** – prevencija od neautorizovanog onemogućavanja pristupa informacijama ili resursima
- **Autentifikacija** – prevencija od lažnog predstavljanja (identifikacija izvora poruke i verifikacija identiteta osobe)
- **Neporicanje** – prevencija od lažnog poricanja slanja date poruke/dokumenta (može se dokazati da poruka/dokument dolazi od datog entiteta iako taj entitet to poriče)

Gde se koristi šifrovanje?

18

- Za realizaciju sigurnosnih protokola
- U komunikaciji
- Za autentifikaciju
- Za digitalne potpise
- Za digitalne sertifikate

Kriptosistem

19

- Kriptosistem se definiše kao uređena petorka (P, C, K, E, D) , gde je:
 - P – skup poruka
 - C – skup šifrata
 - K – skup ključeva
 - $E(P, K) \rightarrow C$ – funkcija šifrovanja
 - $D(C, K) \rightarrow P$ – funkcija dešifrovanja

Kriptografski algoritmi

20

- **Simetrični** – sistemi kod kojih su ključ za šifrovanje i dešifrovanje **isti**

- **Asimetrični** – sistemi kod kojih su ključ za šifrovanje i dešifrovanje **različiti**

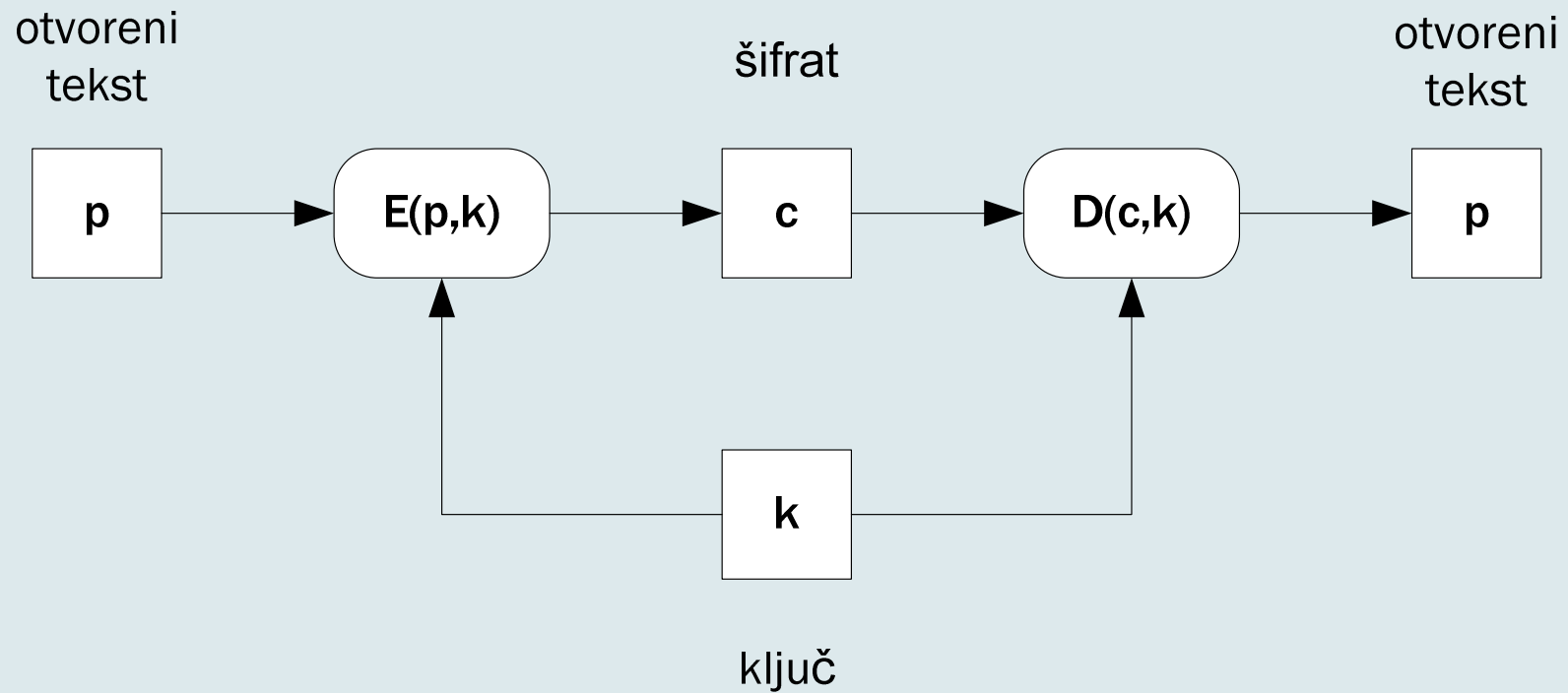
Klasični algoritmi

21

- Cezarova šifra
- Vižnerova šifra (Vigenère)
- Playfair
- ...

Simetrični algoritmi

22



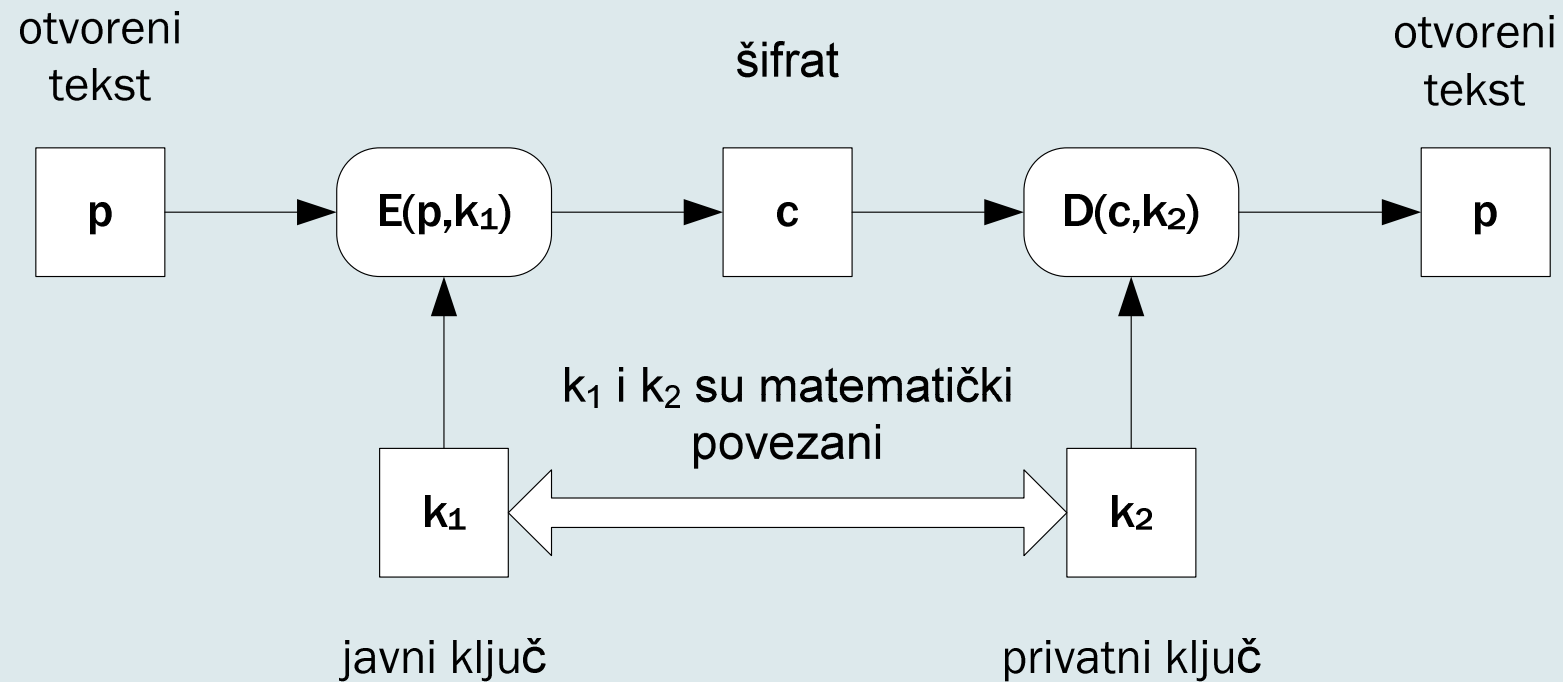
Poznati simetrični algoritmi

23

- **DES** (Data Encryption Standard) – ključ je dužine 56 bita
- **Triple DES (ECB, CBC)**, DESX, GDES, RDES – ključ je dužine 168 bita
- (Rivest) **RC2, RC4, RC5, RC6** – promenljiva dužina ključa do 2048 bita
- **IDEA** – osnovni algoritam za PGP – ključ je dužine 128 bita
- **Blowfish** – promenljiva dužina ključa do 448 bita
- **Twofish** – šifruje 128-bitne blokove otvorenog teksta ključem dužine do 256 bitova
- **AES (Advanced Encryption Standard)** - radi sa blokovima od po 128 bita i koristi ključeve dužine 128, 192 i 256 bita

Algoritmi sa javnim ključem

24



Poznati asimetrični algoritmi

25

- **RSA** (Rivest, Shamir, Adleman)
- **ElGamal**

Cezarova šifra

26

- Demonstracija - CrypTool

Vižnerova šifra (Vigenère)

27

- Demonstracija - CrypTool

DES

28

- Demonstracija - CrypTool

AES

29

- Demonstracija - CrypTool

RSA

30

- Demonstracija - CrypTool

Pseudoslučajne sekvence i protočno šifrovanje

31

- Generatori pseudoslučajnih sekvenci
 - Linearni kongruentni generator
 - Korišćenje jednosmernih funkcija
 - ANSI X9.17
 - FIPS 186
 - RSA
 - $x^2 \bmod n$

Ispitivanje slučajnosti

32

- Monotona sekvenca
- Autokorelaciona funkcija

- Tri Golombova postulata slučajnosti

- Monobitni test
- Poker test
- Test sekvenci različitih dužina
- Test dugačkih sekvenci

Protočno šifrovanje

33

- Protočno šifrovanje (engl. *stream cipher*)
- Sinhrono i asinhrono protočno šifrovanje
- Linearni pomerački registar sa povratnom spregom
- RC4 je simetrični protočni algoritam sa ključem promenljive veličine

Heš funkcije

34

- Jednosmerna funkcija (engl. *one-way function*) jeste funkcija oblika $y=f(x)$ takva da važi:
 - ▣ za dato x , $f(x)$ se određuje relativno lako i efikasno, i
 - ▣ za dato $y=f(x)$, $x=f^{-1}(y)$ se određuje relativno teško.

Značajnije heš funkcije

35

- MD family (*Message Digest*)
 - MD2
 - MD4
 - **MD5**
 - **MD5 (Message-Digest algorithm 5) is a widely used cryptographic hash function with a 128-bit hash value.**
 - MD6
 - The MD6 hash algorithm is a cryptographic hash algorithm developed at MIT by a team led by Professor Ronald L. Rivest in response to the call for proposals for a SHA-3 cryptographic hash algorithm by the National Institute of Standards and Technology.

- SHA (*Secure Hash Algorithm*)
 - SHA-0, SHA-1
 - SHA-2 family (SHA-224, SHA-256, SHA-384, SHA-512)
 - SHA-3 (in development)

MD5

36

- Demonstracija - CrypTool

Primena heš funkcija

37

- Heš funkcije i čuvanje lozinki na disku sistema
- Heš funkcije i CHAP provera identiteta
 - ▣ CHAP (*Challenge Handshake Authentication Protocol*)
- Heš funkcije i digitalno potpisivanje

Problemi sa heš funkcijama

38

- „Efekat lavine“ (engl. *avalanche*) – da li postoji?
 - ▣ Mala promena u originalnoj poruci izaziva veliku promenu na izlazu tj. u rezultatu heš funkcije.
- Kolizije (engl. *collision*)
 - ▣ Ukoliko dve ili više različitih poruka (ili datoteka) imaju isti rezultat heš funkcije, onda kažemo da se radi o koliziji.

NIST: Cryptographic Hash Algorithm Competition

39

- NIST Cryptographic Hash Algorithm Competition
 - ▣ Official homepage:
<http://csrc.nist.gov/groups/ST/hash/sha-3/index.html>
- 1st round candidates:
 - ▣ http://csrc.nist.gov/groups/ST/hash/sha-3/Round1/submissions_rnd1.html
- 2nd round candidates:
 - ▣ http://csrc.nist.gov/groups/ST/hash/sha-3/Round2/submissions_rnd2.html

NIST: Cryptographic Hash Algorithm SHA-3 Competition Third (Final) Round Candidates

40

NIST has selected the third (final) round candidates of the SHA-3 competition. Following 5 third (final) round candidates continue the competition:

- **BLAKE**
- **Grøstl**
- **JH**
- **Keccak**
- **Skein**

Kriptografija s javnim ključevima

41

- RSA
- Diffie-Hellmanov protokol za razmenu ključeva
- Kriptosistemi s javnim ključem

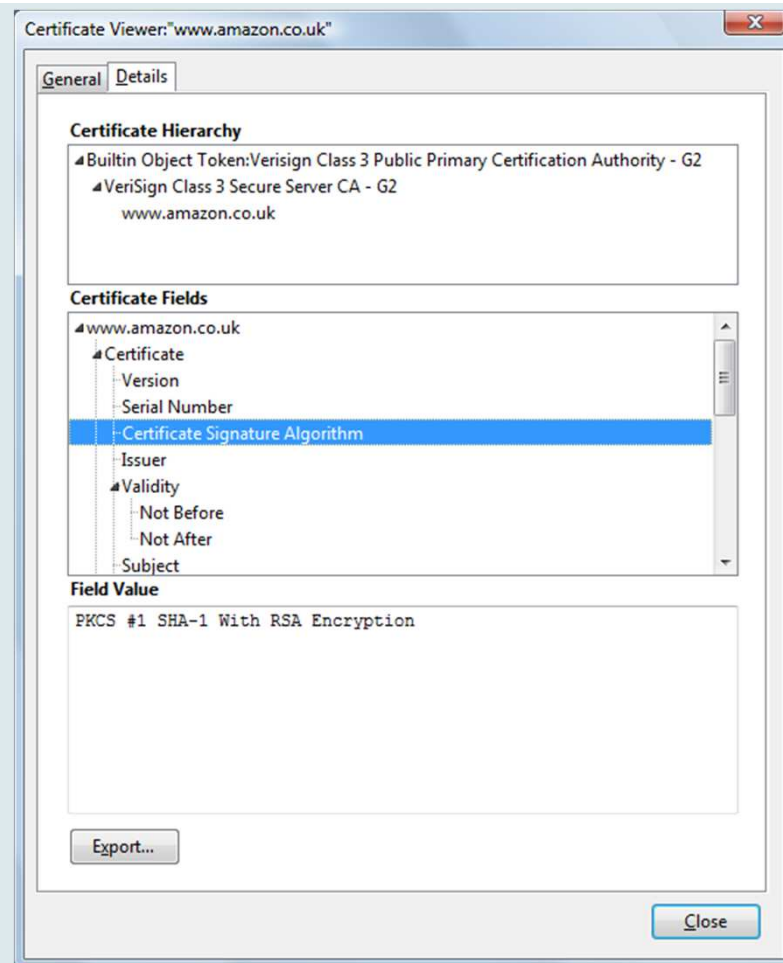
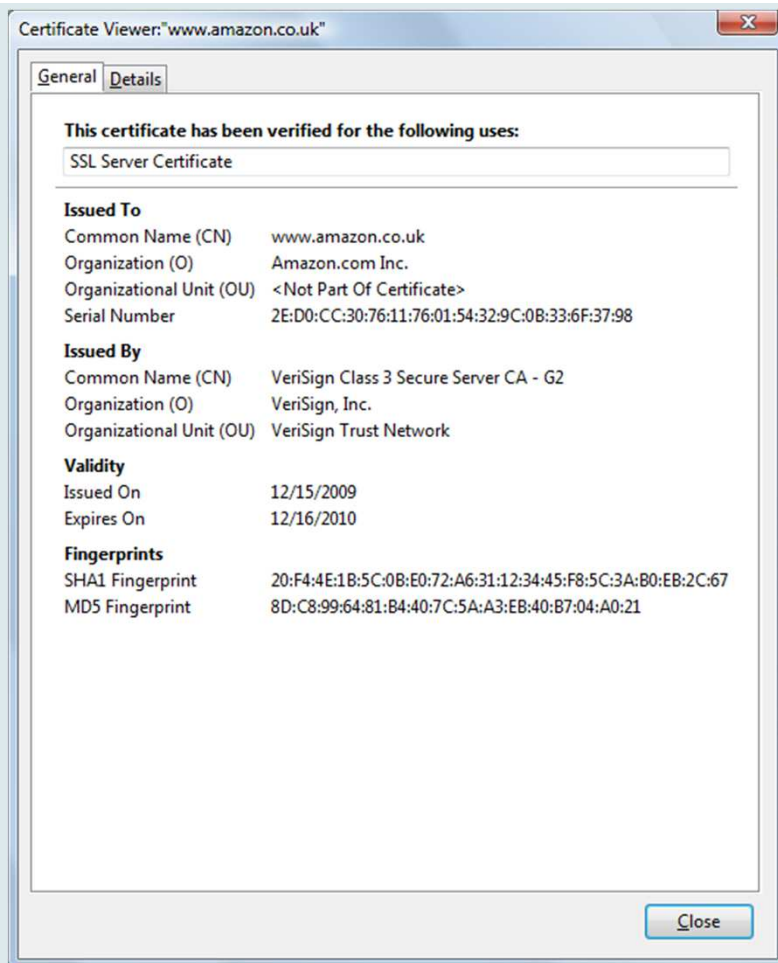
Sertifikati i infrastruktura javnih ključeva

42

- Digitalni sertifikat
- Infrastruktura javnih ključeva (PKI – Public Key Infrastructure)
- X.509 sertifikati

Primer sertifikata

43



Kriptografski softver

44

- Šifrovanje komunikacionih kanala
- Šifrovanje podataka na diskovima
- Pretty Good Privacy
- GNU Privacy Guard
- TrueCrypt
- EFS (Encryption File System)
- *loopback* šifrovanje na operativnom sistemu Linux
- Cryptographic File System (CFS)

Značaj ključa

45

- Zaštita zavisi od zaštite ključa, a ne od zaštite algoritma
- Podrazumeva se da je algoritam javno poznat
- Ova otvorenost omogućava proveru algoritma od strane velikog broja stručnjaka i potvrdu njegove snage
- Simetrični algoritmi – problem upravljanja i distribucije ključeva
- Asimetrični algoritmi - koncept javnog i tajnog ključa

Napadi

46

- Uobičajene pretpostavke
 - ▣ Napadač ima potpun pristup komunikacionom kanalu između pošiljaoca i primaoca
 - ▣ Napadač poseduje potrebno znanje o algoritmu šifrovanja

Opšti tipovi napada

47

- **Ciphertext – only.** Poznat je šifrovani tekst nekoliko poruka, pronalaženje čitljivog teksta i ključeva
- **Known – plaintext.** Poznat je šifrovani tekst i dešifrovani tekst za nekoliko poruka, nalaženje ključeva
- **Chosen – plaintext.** Nisu samo šifrovani i dešifrovani tekst poznati za nekoliko poruka, već napadač bira originalnu poruku
- **Adaptive chosen – plaintext.** Kao i prethodno, ali napadač može da menja originalnu poruku na osnovu prethodnih rezultata

Sigurnost kriptografskog algoritma

48

- **Cena “razbijanja”** algoritma mora da bude veća od cene šifrovanih podataka
- **Vreme potrebno za “razbijanje”** algoritma mora da bude duže od vremena u kome podaci moraju da ostanu tajni
- **Broj podataka šifrovanih jednim ključem** mora da bude manji od broja potrebnih podataka da se dati algoritam “razbije”

Formalne metode

49

- Obezbeđuju mogućnost modeliranja, analize i verifikacije (i projektovanja) kriptografskih algoritama i protokola koji ih koriste

Literatura

50



- D. Pleskonjić, N. Maček, B. Đorđević, M. Carić: **“Sigurnost računarskih sistema i mreža”**, Mikro knjiga, Beograd, 2007., ISBN: 978-86-7555-305-2, knjiga – udžbenik
- www.conwex.info/draganp/books_SRSiM.html
- www.mikroknjiga.rs/store/prikaz.php?ref=978-86-7555-305-2

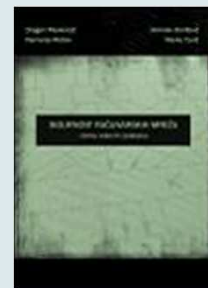
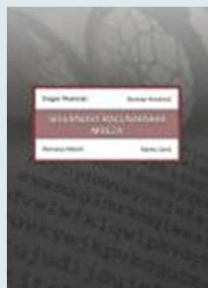
- Za predavanje 3:
 - ▣ Poglavlje 3: Kriptografija
 - ▣ Dodatak C: Kriptografske tablice
 - ▣ Dodatak D: Izvorni kod

Literatura - nastavak

51

- D. Pleskonjić, B. Đorđević, N. Maček, Marko Carić: **“Sigurnost računarskih mreža”**, Viša elektrotehnička škola, Beograd, 2006., ISBN 86-85081-16-5, knjiga - udžbenik
- D. Pleskonjić, B. Đorđević, N. Maček, Marko Carić: **“Sigurnost računarskih mreža - priručnik za laboratorijske vežbe”**, Viša elektrotehnička škola, Beograd, 2006., ISBN 86-85081-49-1
- D. Pleskonjić, B. Đorđević, N. Maček, Marko Carić: **“Sigurnost računarskih mreža - zbirka rešenih zadataka”**, Viša elektrotehnička škola, Beograd, 2006., ISBN 86-85081-55-6

www.conwex.info/draganp/books.html



Dodatna literatura

52

- **Handbook of Applied Cryptography**
Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone
CRC Press, www.cacr.math.uwaterloo.ca/hac/, Google Books

- **Applied Cryptography**
Bruce Schneier
John Wiley & Sons, 1995
 - **Primenjena kriptografija**
Prevod drugog izdanja, Mikro knjiga, Beograd, 2007.
www.mk.co.yu/store/prikaz.php?ref=978-86-7555-317-5

- **Cryptography and Network Security**
William Stallings
Prentice Hall, 1998

- Druge knjige i razni *online* resursi

- **Napomena:** tokom predavanja će biti naglašena dodatna literatura, po potrebi.

Pitanja

53

?