Generatori slučajnih brojeva i njihova primjena u kriptografskim sustavima

Mendler, Maja

Master's thesis / Diplomski rad

2015

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **Josip Juraj Strossmayer University of Osijek, Faculty of Electrical Engineering, Computer Science and Information Technology Osijek / Sveučilište Josipa Jurja Strossmayera u Osijeku, Fakultet elektrotehnike, računarstva i informacijskih tehnologija Osijek**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:200:139834

Rights / Prava: In copyright / Zaštićeno autorskim pravom.

Download date / Datum preuzimanja: **2024-03-29**

Repository / Repozitorij:

Faculty of Electrical Engineering, Computer Science and Information Technology Osijek

zir.nsk.hr

Image not found or type unknown

SVEUČILIŠTE JOSIPA JURJA STROSSMAYERA U OSIJEKU

ELEKTROTEHNIČKI FAKULTET

Sveučilišni studij

GENERATORI SLUČAJNIH BROJEVA I NJIHOVA PRIMJENA U KRIPTOGRAFSKIM SUSTAVIMA

Diplomski rad

Maja Mendler

Osijek, 2015.

Sadržaj

1. UVOD 1

2. SLUČAJNI I PSEUDOSLUČAJNI BROJEVI 2

2.1. Pojam entropije 3

2.2. Pravi slučajni brojevi 3

2.2.1. Izvori slučajnih brojeva 4

2.2.2. Problemi s upotrebom pravih slučajnih brojeva 6

2.3. Pseudoslučajni brojevi 6

2.3.1. Modeli napada na generatore pseudoslučajnih brojeva 7

3. ALGORITMI ZA GENERIRANJE PSEUDOSLUČAJNIH BROJEVA 9

3.1. Linearni kongruencijski generator 9

3.1.1. Izbor parametara 12

3.1.2. Vrste linearnog kongruencijskog generatora 13

3.2. RSA generator pseudoslučajnih brojeva 15

3.3. ANSI X9.17 generator pseudoslučajnih bitova 17

3.4. Blum–Blum–Shub generator pseudoslučajnih bitova 17

3.4.1. Sigurnost Blum–Blum–Shub generatora 20

4. KRIPTOGRAFIJA 23

4.1. Osnovni pojmovi kriptografije 23

4.2. Simetrični algoritmi 25

4.2.1. AES 26

4.3. Asimetrični algoritmi 28

4.3.1. RSA 30

4.4. Primjena kriptografije i kriptoanaliza 31

5. STANDARDIZIRANI TESTOVI SLUČAJNOSTI 33

5.1. Hi-kvadrat test 33

5.2. Kolmogorov-Smirnov test 35

5.3. Empirijski test 39

5.4. DIEHARD skup statističkih testova 42

5.5. NIST skup statističkih testova 45

6. PRAKTIČNI RAD 49

6.1. Prikaz rada algoritama 49

6.2. Provedba statističkih testova 57

ZAKLJUČAK 62
LITERATURA 63
SAŽETAK 65
ABSTRACT 66
ŽIVOTOPIS 67
PRILOZI 68

SAŽETAK

U današnjem modernom svijetu gdje je sve udaljeno samo par klikova mišem, naša sigurnost je postala ugrožena. Privatnost se sve više narušava, a osobni podaci se neovlašteno koriste u razne kriminalne svrhe. Da bi se to onemogućilo sve veću upotrebu ima kriptografija, nova grana znanosti koja se neprestano razvija usporedo s tehnologijom.

Kriptografija omogućuje zaštitu podataka upotrebom digitalnih potpisa i certifikata, šifriranje e-poruka i dokumenata koji se šalju nesigurnim komunikacijskim kanalima, za elektroničko plaćanje i još u mnoge druge svrhe. Da bi prijenos podataka bio što sigurniji putem Interneta, razvijeni su različiti algoritmi koji šifriraju podatke. Tim algoritmima su potrebni ključevi za šifriranje koji se sastoje od slučajnih brojeva.

Generator slučajnih brojeva je računalni ili fizički sustav dizajniran za generiranje niza brojeva koji se pojavljuju slučajno. Prave slučajne brojeve je teško dobiti, zato što su računala koja generiraju slučajne brojeve determinističke prirode. Pravi slučajni brojevi u svakodnevnome životu se javljaju samo u prirodnim pojavama i situacijama koje je nemoguće predvidjeti. Upotrebom računala mogu se dobiti pseudoslučajni brojevi čije je glavno svojstvo da budu što više slični pravim slučajnim brojevima. Da bi se dobio zadovoljavajući niz brojeva, koriste se generatori pseudoslučajnih brojeva. Svaki generator ima svoj odgovarajući algoritam, te su ovdje obrađeni najčešće korišteni LCG, RSA, ANSI X9.17 i BBS algoritmi. Da bi provjerili slučajnost dobivenog niza koriste se standardizirani testovi, a neki od najrasprostranjenijih su ovdje opisani, kao što su Hi kvadrat test, Kolmogorov-Smirnov test, skup empirijskih testova, te posebno osmišljeni skupovi testova DIEHARD i NIST. Ovi testovi eliminiraju loše a potvrđuju potencijalno dobre algoritme za generiranje pseudoslučajnih brojeva koji će se kasnije koristiti kao ključevi šifriranja u kriptografiji.

Ključne riječi: generatori slučajnih brojeva (RNG), generatori pseudoslučjanih brojeva (PRNG), Linearni kongruencijski generator (LCG), RSA generator, ANSI X9.17 generator, Blum- Blum – Shub generator (BBS), standardizirani testovi, Hi kvadrat test, Kolmogorov – Smirnov test.

ABSTRACT

In today's modern world everything is at reach of a couple of mouse clicks, but our security has become compromised. Privacy is often violated and personal information is used without authorization in various criminal purposes. In order to prevent that, cryptography is increasingly being used: a new branch of science that is constantly evolving along with technology.

Cryptography enables data protection by using digital signatures and certificates; by encryption of emails and documents that are sent via insecure communication channels; in electronic payment, and in many other ways. Various data encrypting algorithms have been developed to make data transfer through the Internet as safe as possible. These algorithms require encryption keys, which are composed of random numbers.

Random Number Generator is a computer or a physical system designed to generate a series of numbers that appear randomly. True random numbers are difficult to obtain, because the computers that generate random numbers work in a deterministic mode. In everyday life, true random numbers appear only in natural phenomena and in situations that are impossible to predict. Using computers, only pseudorandom numbers can be obtained. Their main feature is being as similar to real random numbers as possible. In order to obtain a satisfactory set of numbers, the pseudorandom number generators are used. Each generator has a matching algorithm. Here are mentioned the most commonly used LCG, RSA, ANSI X9.17 and BBS algorithms. To check the coincidence obtained, a series of standardized tests are used. Some of the most common ones are described here, such as Chi-square test, Kolmogorov – Smirnov test, a set of empirical tests, and specially designed sets of tests DIEHARD and NIST. These tests eliminate the bad and confirm potentially good algorithms for generating pseudorandom numbers that will be later used as encryption keys in cryptography.

Key words: random number generators (RNG), pseudorandom number generators (PRNG), linear congruential generator (LCG), RSA generator, ANSI X9.17 generator, Blum- Blum – Shub generator, standard tests, Chi squer test, Kolmogorov – Smirnov test.