

GENERATORI PSEUDOSLUČAJNIH BROJEVA

Milan Milosavljević

Univerzitet Singidunum
Danijelova 32, Beograd
Telefon: +381113093283

E-mail: mmilosavljevic@singidunum.ac.rs

Miloš Milenković

Univerzitet Singidunum
Danijelova 32, Beograd
Telefon: +381113093295

E-mail: mmilenkovic@singidunum.ac.rs

Saša Adamović

Univerzitet Singidunum
Danijelova 32, Beograd
Telefon: +381113093295

E-mail: sadamovic@singidunum.ac.rs

Sažetak – U ovom radu se analiziraju generatori pseudoslučajnih brojeva (eng. *pseudorandom number generator*, PRNG) – ANSI X9.17 i FIPS 186. ANSI X9.17 se koristi za generisanje ključeva kod DES algoritma, dok se FIPS 186 koristi za generisanje privatnih ključeva kod DSA algoritma. Rad opisuje primenu pseudoslučajnih brojeva u kriptografiji danas i daje pregled statističkih testova pomoću kojih se može ustanoviti stepen slučajnosti nizova generisanih pomoću PRNG. Na kraju rada se komentarišu neki tipični kriptanalitički napadi zasnovani na statističkim slabostima pseudoslučajnih nizova.

Ključne reči: generator pseudoslučajnih brojeva, ANSI X9.17, FIPS 186, tajni ključ

Abstract – In this paper we analyze the pseudorandom number generators, PRNG – ANSI X9.17 and FIPS 186. ANSI X9.17 is used to generate keys for the DES algorithm, while the FIPS 186 is used to generate the private key for DSA algorithm. Paper describes the application of pseudorandom numbers in cryptography today and provides an overview of statistical tests which can determine the degree of coincidence sequences generated using the PRNG. At the end of the paper there is a typical comment of cryptoanalysis attacks based on statistical weaknesses of pseudorandom sequences.

Keywords: pseudorandom number generator, ANSI X9.17, FIPS 186, secret key

1. UVOD

U ovom radu biće dat pregled generatora pseudoslučajnih brojeva koji se koriste u kriptografiji. Razni kriptografski algoritmi i protokoli zahtevaju u određenim fazama njihove primene nizove slučajnih brojeva. Te faze mogu biti generisanje slučajnih bitova u postupcima autentifikacije, zatim ključevi u digitalnom potpisu, kao i generisanje javnih ključeva. Jasno je da se u praksi ne može svaki niz brojeva smatrati slučajnim. U radu će biti opisana svojstva koja se očekuju od generisanog niza kao i metode testiranja generatora.

Važno je napomenuti da se slučajni brojevi u stvarnosti javljaju samo u prirodnim pojavama i situacijama koje je nemoguće predvideti kao što je na primer bacanje simetričnog novčića. U praksi, brojevi koji izgledaju kao slučajni se na računaru generišu determinističkim algoritmom i zato nikako ne mogu biti slučajni brojevi. Pravu slučajnost je nemoguće dobiti na determinističkom računaru, pa se iz tog razloga koriste generatori pseudoslučajnih brojeva takvi da dobijeni niz brojeva prolazi većinu statističkih testova slučajnosti. Pseudoslučajne sekvence se mogu generisati i pomoću jednosmernih funkcija ukoliko na raspolaganju imamo neku od jednosmernih hash funkcija, kao što su MD5 ili SHA1.

2. GENERATORI PSEUDOSLUČAJNIH BROJEVA

Generatori pseudoslučajnih brojeva (*PRNG – Pseudorandom number generators*) su algoritmi koji na osnovu početnih uslova daju izlazni niz pseudoslučajnih brojeva. Početni uslov je zadovoljen ukoliko je ulaz u generator „istinski“ slučajan. Početni „istinski“ slučajan niz se dobija primenom generatora „istinski“ slučajnih brojeva (*RNG – Random number generators*) , i predstavlja ključ k odnosno seed. Generisana pseudoslučajna sekvenca je znatno duža od ključa i smatra se pouzdanom ukoliko zadovoljava određene statističke testove. Determinističke karakteristike generatora se ogledaju u mogućnosti predviđanja brojeva u nizu, odakle i sami generatori nose naziv pseudoslučajni. Reprodukovanje izlaznih nizova je moguće samo uz poznavanje početnih vrednosti, odnosno početnih uslova. Zanimljivo je da se pseudoslučajni brojevi ponekad pokazuju uspešnijim od slučajnih brojeva dobijenih iz fizičkih izvora. Dobre karakteristike PRNG pokazuje uz veoma oprezan odabir početnih stanja, što dovodi do prikrivanja determinističkih metoda koje se upotrebljavaju i karakteristika slučajnosti u izlaznom nizu.

Generatori pseudoslučajnih brojeva su brzi i lako ostvarivi. Kada je reč o kriptografiji, velika pažnja se poklanja odabiru samog generatora, njegovim osobinama i potencijalnim statističkim slabostima koje se mogu upotrebiti prilikom kriptanalitičkih napada. Kada je reč o statističkim testovima pomoću kojih se utvrđuju osobine generisanog niza, nijedan generator ne poseduje stoprocentno zadovoljavajuće parametre. Loši generatori padaju na prostim testovima, kao što dobri generatori padaju na komplikovanim testovima. Pošto ne postoji univerzalna kolekcija testova čiji prolaz garantuje da je dati generator potpuno pouzdan, generatori pseudoslučajnih brojeva se konstruišu na osnovu ozbiljne matematičke analize njihovih strukturalnih osobina. U nastavku rada daje se opis poželjnih svojstava koja se očekuju od generisanog niza:

- Mogućnost pojave jednog broja treba biti ista za sve brojeve u prostoru u kome se generišu nizovi. Ova osobina se odnosi na ceo generisani niz, ali i za njegov podniz.
- Korelacija između generisanih brojeva podniza ne sme da postoji, odnosno nijedan podniz ne sme biti zavisn od nekog drugog podniza.
- Generator je dobro konstruisan ukoliko je broj stanja kroz koja on prolazi prilično velik. Ukoliko se generator u jednom trenutku nađe u stanju u kojem je već bio, dolazi do ponavljanja nekog već generisanog podniza. Period dobrog generatora mora biti što je moguće veći.[8]

U nastavku rada biće opisani neki od generatora pseudoslučajnih brojeva i metode testiranja koje se najčešće upotrebljavaju.

2.1. KRIPTOGRAFSKI GENERATORI PSEUDOSLUČAJNIH BROJEVA

Veliki broj generatora pseudoslučajnih brojeva se koristi u svrhe računarskih simulacija. Najpoznatiji generatori te vrse su linearni kongruentni generator (*LCG - Linear Congruential Generator*) i *LFG (Lagged Fibonacci Generator)*. U kriptografskim primenama potrebna je dodatna sigurnost. Generisani slučajni bitovi mogu da posluže kao ključevi za šifrovanje, pa je iz tog razloga neophodno osigurati nepredvidivost brojeva u generisanom nizu. Ulaz u generator mora biti tako odabran da ga je praktično nemoguće otkriti bilo kom metodom pogađanja ili pretraživanjem svih mogućih kombinacija. Period generatora mora biti izuzetno velik, čime se dobija veliki broj različitih nizova koje je nemoguće pretražiti u konačnom prostoru. Dobro konstruisan generator ne sadrži elemente pravilnosti, tako da su metode predviđanja svedene na minimum.

Algoritmi generatora pseudoslučajnih brojeva su javno dostupni, a osobine nekih od njih razmotriće se u nastavku rada. Za određeni kriptografski sistem kada je reč o kriptografskim generatorim pseudoslučajnih brojeva tajnost odnosno privatnost mora da počiva u načinu izbora početnih uslova. To podrazumeva da bez znanja početnih stanja odnosno početnih ključeva mogućnost kriptanalitičkih napada postaje svedena na minimum, uprkos poznavanju algoritma odnosno načina na koji funkcioniše generator.

Generatori koji imaju primenu u kriptografiji su daleko kvalitetniji od standardnih generatora koji se koriste za računarske simulacije. Zbog složenosti algoritma oni su daleko sporiji od standardnih, ali imaju veliku primenu u kriptografiji gde je potrebno generisati mali broj podataka, pa brzina izvođenja ne predstavlja presudan faktor pri izboru samog generatora. U nastavku rada razmatraće se neki od najpoznatijih generatora pseudoslučajnih brojeva koji se koriste u kriptografiji.

2.2. ANSI X9.17

ANSI X9.17 je jedan od najčešće korišćenih generatora pri konstruisanju kriptografskih aplikacija. Koristi se za generisanje tajnih ključeva kod DES algoritma, kao i prilikom dobijanja početnih vrednosti inicijalizacionog vektora. Osnovu ovog generatora pseudoslučajnih brojeva čini nasumična odnosno nepredvidiva vrednost početnog stanja odnosno seed-a, i vremenski parametar. Vrednost generatora je niz koji zadovoljava ANSI X9 standard po preporuci NIST-a (*National Institute of Standards and Technology*).

ANSI X9.17 generator šifrovanje obavlja pomoću trostrukog DES algoritma sa dva ključa. Ulazni podaci generatora su 64-bitna vrednost s (seed) koja se generiše na osnovu trenutnog vremena i datuma, zatim celi broj m i ključevi za šifrovanje K_1 i K_2 . Generator obavlja šifrovanje pomoću sledeće funkcije:

$$I = E_k^3(s)$$

Algoritam se dalje odvija prema sledećim koracima:

- Računa se vrednost $I = E(D)$, gde je D 64-bitni zapis trenutnog vremena
- $x_i = E_k(I \oplus s)$ i $s = E_k(x_i \oplus I)$

- Izlaz iz generatora je 64-bitni niz slučajnih brojeva $X_1, X_2 \dots X_m$

Ovaj generator se pokazao dovoljno sigurnim odnosno upotrebljivim u većini primena, ali je potrebno napomenuti da nije formalno dokazano da je ovaj algoritma kriptografski siguran. Prednosti primene ANSI X9.17 generatora su jednostavnije izvođenje i znatno veća brzina u odnosu na ostale kriptografske generatore pseudoslučajnih brojeva.[7]

2.3. FIPS 186

FIPS 186 se koristi za generisanje privatnih ključeva za DSA algoritam (*Digital Signature Algorithm*). DSA je algoritam koji se koristi pri digitalnom potpisivanju propisan od strane NIST-a. Ovaj algoritma se koristi isključivo za digitalno potpisivanje i ne predstavlja algoritam za šifrovanje. DSA algoritma primenu ima kada je reč o infrastrukturi javnih ključeva. Tajni ključ se primenjuje na heš vrednost generisanu primenom SHA-1 algoritma. Da bi se potpis verifikovao primalac dešifruje potpis javnim ključem pošiljaoca i zatim poredi vrednosti.

Osnovu ovog algoritma čini jednosmerna funkcija $G(t, c)$. Kao ulazni podatak FIPS 186 generatora koristi se prost 160-bitni broj. Za interne potrebe generatora definiše se parametar t , koji ima heksadecimalnu vrednost. U početnoj fazi rada generatora generiše se slučajna početna vrednost s pomoću nekog izvora slučajnosti. Nakon početne faze u petlji $i = 1 \dots n$ (n je određeno dužinom sekvence) se obavljaju sledeće operacije:

- $z_i = (s + y_i) \bmod 2^b$ - parametar y_i se koristi za prikupljanje slučajnosti, dok parametar b predstavlja dužinu bitova.
- $a_i = G(t, z_i) \bmod q$ - primena FIPS 186 jednosmerne funkcije
- $s = (1 + s + a_i) \bmod 2^b$

Izlazna sekvenca FIPS 186 generatora pseudoslučajnih brojeva je niz od n brojeva $a_1, \dots, a_m$ u intervalu $0 \leq a_i \leq q$. [7]

ANSI X9.17 i FIPS 186 spadaju u sigurne kriptografske generatore pseudoslučajnih brojeva. Da bi se za određeni generator tvrdilo da je siguran, on mora proći određene statističke testove. Ne postoji univerzalan broj testova koji se koriste pri utvrđivanju osobina niza generatora, ali primenom određenih metoda može se doneti sud o kvalitetu samog generisanog niza. U nastavku rada daje se pregled metoda i statističkih testova koji se primenjuju za utvrđivanje kvaliteta generatora pseudoslučajnih brojeva.[8]

2.4. ISPITIVANJE GENERATORA PSEUDOSLUČAJNIH BROJEVA

Za ispitivanje kvaliteta generisanog niza koristi se mnoštvo testova. Međutim ne postoji jedan univerzalni test na osnovu koga se može tvrditi da je određeni niz generisanih brojeva potpuno slučajan. Na osnovu testova je moguće zaključiti pokazuje li niz neka od ponašanja koja bi pokazivao niz generisan od strane idealnog generatora (prirodne pojave). Nasuprot tome, na osnovu rezultata se može sigurno zaključiti da neki niz nije slučajan, odnosno da generator radi neispravno.

Prilikom ispitivanja slučajnih nizova potrebno je odrediti statističku vrednost pomoću koje se određeni rezultat prihvata ili odbacuje. Takođe je potrebno odrediti kritičku vrednost za koju se ne očekuje da će biti premašena. Kritička vrednost bi predstavljala veoma malu verovatnoću realizacije određenog događaja. Na osnovu pomenutih vrednosti se određuju granice preko kojih se ne sme ići ili ispod kojih se dobijena statistička vrednost ne sme spuštati. U skladu sa tim generisani nizovi se smatraju slučajnim ili suprotno generatori se smatraju neispravnim. Mera sigurnosti sa kojom se generator prihvata ili ne, naziva se nivo značaja. Prevelika odnosno premala vrednost ovog parametra može dovesti do odbacivanja niza. Svaki ispit za određivanje kvaliteta generatora meri neku od poželjnih karakteristika slučajnih brojeva. Nakon serije ispitivanja moguće je zaključiti da ispitivani generator poseduje željena svojstva i da bi kao takav mogao biti dobar generator. Sa druge strane moguće je zaključiti da ispitivani generator nije odgovarajući. Ovakve tvrdnje moguće je donositi sa 99% sigurnošću. Obično se u ispitima upotrebljavaju dve osnovne raspodele:

- Očekivana raspodela posmatranih vrednosti u nekom prostoru
- Očekivana raspodela učestalosti pojave nekih događaja

U nastavku rada će biti prikazan određeni broj ispita za generatore pseudoslučajnih brojeva koje preporučuje NIST (*National Institute of Standards and Technology*):

- Maurerov univerzalni statistički test – ispitivanje mogućnosti kompresije niza bez gubitka informacije. Za niz koji se može značajno kompresovati smatra se da nije niz slučajnih bitova zbog činjenice da je kompresija niza efikasnija ukoliko niz pokazuje periodična svojstva.
- Ispitivanje preklapajućih uzoraka – posmatrana karakteristika u ovom testu je učestalost pojave svih mogućih n-bitnih uzoraka uz preklapanje u celom ispitivanom nizu. Test bi trebalo da otkrije da li je broj pojava preklapajućih uzoraka približno jednak broju koji se očekuje za niz slučajnih brojeva.
- Ispitivanje približne entropije – u ovom testu posmatra se takođe učestalost pojave svih mogućih preklapajućih n-bitnih uzoraka u nizu. Cilj je poređenje učestalosti preklapajućih blokova sa očekivanim rezultatima.
- Ispitivanje učestalosti u nizu – u ovom testu ispituje se odnos jedinica i nula u nizu bitova. Cilj je uočavanje jednakosti pojavljivanja ove dve vrednosti.
- Ispitivanje učestalosti u bloku – posmatra se odnos jedinica i nula u n-bitnim blokovima. Cilj predstavlja uočavanje jednakosti broja jedinica i nula u svakom n-bitnom bloku.
- Ispitivanje uzastopnih ponavljanja istih bitova u nizu – posmatrana karakteristika u ovom testu je ukupan broj uzastopnih ponavljanja jednog broja u nizu.
- Ispitivanje najdužeg uzastopnog ponavljanja jedinica u bloku – u ovom testu posmatra se najduže uzastopno ponavljanje jedinica u n-bitnim blokovima. Svrha je određivanje da li se dužina najdužeg uzastopnog ponavljanja poklapa sa dužinom koja bi se očekivala u nizu slučajnih brojeva.[8]

2.5. KRIPTOANALITIČKI NAPADI NA GENERATORE PSEUDOALUČAJNIH BROJEVA

U ovom delu rada razmotriće se nekoliko vrsta napada na generatore pseudoslučajnih brojeva. Generatori pseudoslučajnih brojeva se smatraju jednom od ključnih tačaka kriptosistema, i kao takvi predstavljaju potencijalnu opasnost ukoliko se odigra uspešan kriptanalitički napad na njih. U jednom kompleksnom kriptosistemu, napad na PRNG dovodi do irelevantnosti veoma ozbiljan i sistematičan pristup u odabiru algoritma i sigurnosnih protokola. Mnogi sistemi koriste loše dizajniran PRNG, ili se generatori koriste na način koji razne napade čine lakšim nego što bi to trebalo biti. U nastavku rada navode se neki od poznatih kriptanalitičkih napada:

- Direktni kriptanalitički napadi – napadač je u stanju da primeti razliku između PRNG izlaza i slučajnosti u nizu. Drugim rečima niz koji predstavlja izlaz iz generatora nije slučajan i ne zadovoljava statističke parametre. Ova vrsta napada se odnosi na većinu, ali ne i na sve generatore pseudoalučajnih brojeva. PRNG koji generiše ključeve za trostruki DES algoritam nije podložan ovim napadima jer izlaz iz generatora nije vidljiv.
- Napadi zasnovani na ulaznim vrednostima generatora – ovakvi napadi događaju se kada je kriptanalitičar u stanju da koristi znanje ili kontrolu nad ulaznim parametrima generatora pseudoslučajnih brojeva. Ukoliko u bilo kojoj situaciji predviđanje ulaznih parametara u generator bude olakšano, ovakvi napadi su realno mogući. U praksi napadi na smart kartice su jedan od primera.
- Produženi napadi – ovi napadi mogu biti uspešni kada PRNG počinje generisanje nizova iz takozvanog nesigurnog stanja, odnosno na osnovu seed-ova koje je moguće predvideti. Oni se pojavljuju kao deo strategije kriptanalitičara kada se primenjuju poznati napadi na ceo sigurnosni sistem.[2]

3. ZAKLJUČAK

Pseudoslučajni brojevi imaju primenu pri generisanju sesijskih ključeva, inicijalizacionih vektora, jedinstvenih parametara digitalnog potpisa kao i veliku primenu u sigurnosnim protokolima. Kriptografske aplikacije je teško zamisliti bez upotrebe generatora pseudoslučajnih brojeva. Ovaj rad daje pregled algoritama koji predstavljaju standard kada je reč o korišćenju generatora u kriptografiji. Zbog velike važnosti koju slučajni brojevi imaju prilikom dizajniranja sistema ispitivanju slučajnih nizova se posvećuje velika pažnja. Nedovoljno dobar izbor ili konstrukcija generatora dovodi do loših rezultata i ugrožavanja sigurnosnog sistema. Validnost i kvalitet generatora se ocenjuju na osnovu testova, a u ovom radu predstavljeni su neki od njih po preporuci NIST-a. Moglo bi se reći da potreba za slučajnim brojevima raste koliko i količina računara u upotrebi. Razvojem kvantne kriptografije otvaraju se nove mogućnosti pri generisanju nizova. Kvalitet generatora pseudoslučajnih brojeva zavisi od seed-a i realne odnosno istinitosne slučajnosti tih vrednosti. Ostaje nam da pomno pratimo nove pravce razvoja kriptografije, a samimi tim i mogućnosti

za dobijanje realnih slučajnih brojeva na sistemima koji će se u budućnosti koristiti, a sve u cilju ostvarivanja apsolutno tajnog kript sistema odnosno perfektne tajnosti.

LITERATURA

- [1] M. Stamp. *Information security: principles and practice*. John Wiley & Sons, Inc, 2006.
- [2] B. Schneier. *Applied Cryptography*. John Wiley & Sons, Inc, 1996.
- [3] ANSI X 9.17 (Revised), “American National Standard for Financial Institution Key Management (Wholesale),” American Bankers Association, 1985.
- [4] National Institute for Standards and Technology, “*Key Management Using X9.17*,” NIST FIPS PUB 171, U.S Department of Commerce, 1992.
- [5] National Institute for Standards and Technology, “*Secure Hash Standard*,” NIST FIPS PUB 180, U.S Department of Commerce, 1993.
- [6] National Institute for Standards and Technology, “*Digital Signature Standard*,” NIST FIPS PUB 186 U.S Department of Commerce, 1994.
- [7] D. Pleskonjić, N. Maček, B. Đorđević, M. Carić. *Sigurnost računarskih sistema i mreža*, Mikro knjiga 2007.
- [8] <http://os2.zemris.fer.hr>