

UPRAVLJANJE KRIPTOLOŠKIM KLJUČEVIMA

Mladen Veinović

Univerzitet Singidunum

e-mail: mveinovic@singidunum.ac.rs

Miroslav Čajić

O.Š. „Sveti Sava“

Preobraženska bb, 73220 Rogatica

e-mail: miroslavcajic@gmail.com

Bogdan Brkić

Ministarstvo finansija Republike Srpske

Trg Republike Srpske I, 78000 Banja Luka

e-mail: bbogdan@teol.net

Sažetak - U ovom radu predstavljen je postupak upravljanja kriptološkim ključevima. Izvršena je analiza generisanja i distribucije ključeva i ukazano je na moguće napade koji se dešavaju u procesu distribucije. U radu su obrađeni Diffie-Hellman i Arithmetica sistemi za razmjenu ključeva i ukazano je na njihove prednosti i nedostatke. Na kraju rada predloženo je rješenje za postizanje većeg nivoa bezbjednosti pri upravljanju kriptološkim ključevima.

Ključne riječi: algoritam, Arithmetica, generator ključeva, Diffie-Hellman, kriptološki sistem.

Abstract -In this paper is presented the process of managing cryptographics keys. The analysis of generation and distribution of keys was performed and is pointed to possible attacks that occur in the process of distribution. In the paper were processed Diffie-Hellman and Arithmetica systems for the exchange of keys and was indicates of their advantages and disadvantages. At the end of the paper was proposed solution for achieve a greater level of security when managing cryptographics keys.

Key words - algorithm, Arithmetica, key generator, Diffie-Hellman, cryptographics system.

1. UVOD

Upravljanje kriptološkim ključevima je jedan od najbitnijih zadataka u savremenoj kriptografiji. Iako ovi algoritmi počivaju na obimnim akademskim istraživanjima sam proces kreiranja sigurnih i kvalitetnih kriptoloških algoritama nije jednostavan. U suštini, generisanje ključeva i održavanje tajnosti ključeva je mnogo teže. Prilikom napada na simetrične i asimetrične sisteme kriptanalitičar će prije napasti sistem za upravljanje ključevima, nego što će pokušati da otkrije zakonitosti kriptografskog algoritma koji je primijenjen. Da bi se sigurno zaštitio jedan šifarski sistem cilj je da se što kvalitetnije izvrše: generisanje, distribucija i upravljanje kriptološkim ključevima. [1]

Apsolutnu slučajnost je teško definisati i njena mjera se predstavlja entropijom. Izvore slučajnosti moguće je postići softverski. Međutim, treba uzeti u obzir da je softver deterministički sistem i da bi se slučajnost povećala u obzir treba uzeti eksterne slučajne

događaje kao što su: kretanje miša, dinamika tastature, mrežna i procesorska aktivnost, termički šum elektronskih komponenti, procesi iz prirode i sl. Uzimanjem u obzir ovih parametara može se dobiti kvalitetan slučajni niz, ali ipak, količina ovakvih nizova ostaje ograničena. Posljedica svega ovog navedenog je da korišćenje pseudo-slučajnih nizova u procesu generisanja tajnih vrijednosti daje rezultat u pseudo-tajnosti. Kao dobri izvori "čiste" slučajnosti mogu se uzeti: detektori radioaktivnog raspada i termičkog šuma, uređaji u kojima je moguće ostvariti i detektovati optički kvantni efekat ili uređaji u kojima nastaju nepredvidive oscilacije frekvencije u fazno kontrolisanoj petlji i sl. [2], [4], [11]

2. UPRAVLJANE KRIPTOLOŠKIM KLJUČEVIMA

Jedan od uslova za uspješnu primjenu bezbjednosnog modela predstavlja i njegova jednostavnost upotrebe. Osnovni zadatak dobro projektovanog rješenja jeste da krajnji korisnici u radu što manje osjećaju prisustvo kriptografskog sistema. To podrazumijeva jednostavnost posla koji obavljaju, statičnost postojećih funkcija i minimum vremenskog perioda potrebnog za obavljanje konkretnog poslovnog zadatka. Model implementacije bezbjednosnog rješenja komunikacionog kanala obezbeđuje odličan metod za zaštitu osjetljivih podataka koji se prenose od predajne do prijemne strane. Usložnjavanjem modela dovodi se do pada nivoa performansi kao i otežavanjem konkretne upotrebe predloženog sigurnosnog rješenja. [5]

Upravljanje ključevima se bavi sigurnim generisanjem, distribucijom i čuvanjem ključeva. Sigurnost metoda upravljanja ključevima je od ekstremnog značaja. Kada je ključ jednom generisan on mora ostati tajan da bi se izbjegle situacije kao što je impersonalizacija. Kada je riječ o infrastrukturi sa javnim ključevima, u praksi se najviše napada dešava na nivou upravljanja ključevima, a vrlo rijetko napadi na same algoritme. Učesnici u PKI sistemima moraju biti sposobni da od treće strane od povjerenja dobiju sertifikate koji im služe za generisanje ključeva. Takođe, moraju imati mogućnost da publikuju svoj javni ključ i da im budu dostupni javni ključevi ostalih korisnika u sistemu, za šta koriste sertifikate. Ukoliko dođe do kompromitacije ili gubitka nečijeg privatnog ključa ostali učesnici moraju biti upozoreni. Korisnicima mora biti omogućeno da na siguran način čuvaju svoje ključeve i učine ih nedostupnim osim za legitimnu upotrebu. Napomenimo da ključeve možemo podijeliti na: simetrične, javne i privatne ključeve. Simetrični i privatni ključevi su po svojoj prirodi tajni ključevi. [6]

3. GENERISANJE KRIPTOLOŠKIH KLJUČEVA

U kriptologiji, velika pažnja se poklanja izboru samog generatora, odnosno, njegovim osobinama i potencijalnim slabostima koje se mogu upotrijebiti pri kriptanalizi. Uz pomoć statističkih testova za određivanje osobine generisanog niza može se zaključiti da nijedan generator ne posjeduje sigurno zadovoljavajuće parametre. 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. [6]

Upotrebom pseudoslučajnih brojeva ne postiže se dovoljan nivo sigurnosti. Period generatora mora biti veoma velik. Ulaz u generator mora biti tako odabran da ga je praktično nemoguće otkriti nekom metodom pogađanja. Ovim se omogućava generisanje vrlo velikog broja niza slučajnih brojeva koje je nemoguće analizirati u realnom vremenu. Ovako dobijeni nizovi se mogu upotrijebiti kao kriptološki ključevi. Ovakvi generatori slučajnih brojeva kod kojih je uz poznavanje algoritma i nepoznavanje početnih uslova nemoguće predvidjeti niz generisanih brojeva zovu se generatori kriptografskih sigurnih pseudoslučajnih brojeva

CSPRNG. Kako su algoritmi javno dostupni, način izbora početnih uslova mora ostati tajna. Algoritmi ovakvih generatora su veoma složeni ali i veoma spori. Ovo ne predstavlja problem za primjenu u kriptografiji jer se ovakvi generatori ne koriste za generisanje velike količine slučajnih brojeva. [7], [8], [9]

3.1. Pseudoslučajno generisanje bita PRBG

Pseudoslučajni biti se mogu generisati tako što se prvo generiše slučajna početna vrijednost s , a zatim jednosmjernu funkciju (npr. SHA-1 ili DSA) primijenjena na sekvence s , $s+1$, $s+2$, ... čime se dobije izlazna sekvenca $f(s)$, $f(s+1)$, $f(s+2)$, Da bi se izbjegle moguće korelacije zbog uzastopnih vrijednosti, uzimamo samo neke bite iz sekvenci $f(s+i)$. Ovakav metod nije kriptografski siguran ali zadovoljava većinu primjena. Zbog ograničenog broja stranica, u ovom radu će biti nabrojani samo neki, a to su:

1. *ANSI X9.17 generator* - koristi se za pseudoslučajno generisanje ključeva k i inicijalnih vektora IV koji se koriste u DES algoritmu. X9.17 koristi trostruko šifrovanje sa dva ključa na sledeći način gdje je: $E(x) = E_{K1}(D_{K2}(E_{K1}(x)))$.
2. *FIPS 186 generator* - je generator pseudoslučajnih brojeva koji se koriste kao privatni ključevi u DSA algoritmu. Algoritam koristi slučajno generisanu početnu vrijednost s i jednosmjernu funkciju zasnovanu na SHA-1 ili DES algoritmu

3.2. Pseudoslučajno generisanje bita CSPRBG

Zbog svog već pomenutog ograničenja generisanje pseudoslučajnih bita može biti od koristi ako se izvodi na uređaju koji već ima mogućnosti modularnog množenja, a neki od njih su:

1. *RSA*,
2. *Micali-Schnorr* ili
3. *Blum Blum Shub generator*.

4. DISTRIBUCIJA KLJUČEVA U SIMETRIČNOJ KRIPTOGRAFIJI

Da bi simetrično šifrovanje i dešifrovanje sa druge strane funkcionisalo, obje strane moraju da posjeduju isti ključ. Ovdje se javlja problem distribucije ključeva. Da bi tajnost komunikacije između svaka dva korisnika u grupi od N korisnika bila zagarantovana, svaki učesnik mora da posjeduje $N-1$ ključ za komunikaciju sa ostalim korisnicima. To nas dovodi do ukupno $N(N-1)/2$ ključeva. Za grupu od npr. 1000 korisnika potrebno je približno 500000 ključeva, a svaki korisnik bi morao da posjeduje 999 ključeva. Ovakav sistem bi bio vrlo nepraktičan i težak za održavanje. Jedan od primjera je distributivni centar koji podrazumijeva da svaka strana u komunikaciji dijeli jedinstveni ključ sa distributivnim centrom. [5]

5. DISTRIBUCIJA JAVNIH KLJUČEVA U ASIMETRIČNOJ KRIPTOGRAFIJI

Postoji nekoliko tehnika za distribuciju javnih ključeva u asimetričnoj kriptografiji:

- **javno objavljivanje**– ključevi su javno objavljeni, odnosno, svaki učesnik šalje javni ključ strani sa kojom želi da komunicira. Nedostaci su što bilo ko može da se predstavi kao osoba A i pošalje svoj javni ključ, navodeći drugu stranu na pomisao da će šifrovane poruke razmjenjivati sa osobom A. Ovakav način razmjene ključeva ne obezbjeđuje povezanost javnog ključa sa njegovim vlasnikom.
- **javno dostupan direktorijum** - postiže se korištenjem javno dostupnog direktorijuma. Održavanje i distribucija javnog direktorijuma je u nadležnosti nekog entiteta od povjerenja ili neke organizacije. Nedostaci su što ako napadač uspije u namjeri da pribavi ili rekonstruiše privatni ključ entiteta koji je u posjedu direktorijuma, može doći do kompromitacije bilo kog učesnika u sistemu. Drugi problem koji se javlja je mogućnost krivotvorenja javnih ključeva u direktorijumu od strane napadača.
- **autoritet za javne ključeve** (Public-Key Authority) - svaki učesnik poznaje javni ključ autoriteta, a privatni ključ autoriteta je dostupan isključivo njemu samom.
- **sertifikati** – omogućava dostavljanje vlastog javnog ključa na način kao da je to učinio autoritet. Sertifikat se sastoji od javnog ključa i identifikacije vlasnika tog ključa. Ovi podaci su potpisani od strane "treće strane", odnosno, sertifikacionog tijela u koji svi učesnici u sistemu imaju povjerenje. Sertifikat je moguće dešifrovati samo javnim ključem autoriteta, što garantuje da je baš taj autoritet izdao sertifikat. Ova šema je postala opšteprihvaćena i formalizovana je kroz standard X.509. [9], [10]

6. SISTEMI ZA RAZMJENU KRIPTOLOŠKIH KLJUČEVA

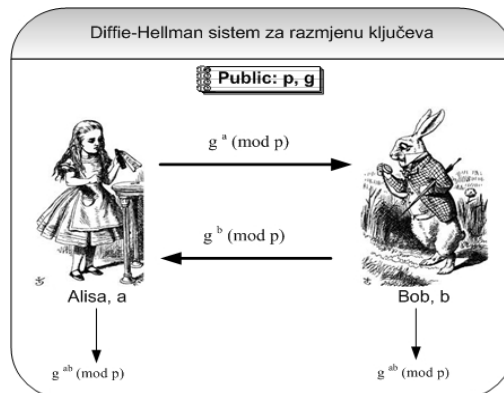
U ovom radu analizirana su dva sistema za razmjenu kriptoloških ključeva, a to su Diffie-Hellman i Arithmetika.

6.1. Diffie-Hellman algoritam za razmjenu ključeva

U simetričnoj kriptografiji, obadvije strane koriste isti ključ za šifrovanje i dešifrovanje. Diffie-Hellman algoritam za razmjenu ključeva omogućava bezbjedno razmjenjivanje ključeva između strana u komunikaciji preko javno dostupnog kanala [2], [3].

Diffie-Hellman algoritam se zasniva na činjenici da je teško izračunati broj α^{ab} ukoliko su poznati brojevi α^a i α^b [9]. Postupak razmjene ključeva se odvija na sledeći način:

- dva korisnika izaberu slučajan broj α ,
- korisnik A izabere slučajan broj a i izračuna α^a i pošalje ga korisniku B,
- korisnik B izabere slučajan broj b i izračuna α^b i pošalje ga korisniku A,
- zajednički tajni element je α^{ab} koji korisnik A dobije kao $(\alpha^b)^a$, a korisnik B izračunavanjem $(\alpha^a)^b$.



Slika 1. Diffie-Hellman sistem za razmjenu kriptoloških ključeva.

6.2. Arithmetika algoritam za razmjenu ključeva

Arithmetica je relativno nov sistem za razmjenu kriptografskih ključeva. Njegov princip rada je drugačiji u odnosu na Diffie-Hellman algoritam za razmjenu ključeva. Arithmetica koristi složene matematičke formule. U Arithmetica sistemu za razmjenu ključeva određena vrijednost G sadrži sve varijacije ove vrijednosti, kao što je prikazano:

$$\{1_G, a, b, a^{-1}, b^{-1}\}$$

Tipični element G sadrži:

$$abaab^{-1}b^{-1}, bba^{-1}a1_Gba, bbb, aba^{-1}b^{-1}, a, b^{-1}, 1_G$$

Jedan od primjera bi bila pretpostavka da Alisa i Bob žele koristiti simetrične ključeve. Prvi korak je da naprave podgrupu svojih javnih ključeva iz grupe javnih ključeva G , tako da vrijedi:

$$S_A = (s_0, s_1, \dots, s_{n-1}) \text{ i } S_B = (t_0, t_1, \dots, t_{m-1})$$

·
·

Alisa izračunava:

$$a^{-1}(b^{-1}ab) = (y^{-1})^{-1}(x^2y) = yx^2y = x^2.$$

Slično tome Bob izračunava:

$$\begin{aligned} a^{-1}ba &= (yxy)^3 = yxy * yxy * yxy \\ &= yxy^2xy^2xy = yx * 1_G * x * 1_G * xy \\ &= yx^3y = x. \end{aligned}$$

U posljednjem koraku, Bob izračunava vrijednost od $a^{-1}b^{-1}a = (a^{-1}ba)^{-1} = x^{-1}$, koje koristi za dobijanje zajedničke tajne $(a^{-1}b^{-1}a)b = x^{-1} * x^3 = x^2$. Ostalo je još da Alisa i Bob izračunavaju zajednički simetrični ključ koji je baziran na zajedničkoj tajni [1], [2].

7. ZAKLJUČAK

Bezbjednosno upravljanje kriptološkim ključevima je jedan od ključnih postupaka u kriptologiji. Nakon što se ključevi generišu, počinje njihov životni vijek. Posebno mjesto u upravljanju ključevima ima distribucija ključeva. Za distribuciju tajnih, privatnih i javnih ključeva treba primjenjivati novije metode, a posebno one kod kojih su uočeni nedostaci

otklonjeni. Samo u tom slučaju korisnicima sistema kriptološke zaštite mogu se garantovati: autentičnost pošiljaoca poruke, zaštita integriteta podataka u poruci, neporecivost slanja poruke i tajnost. Ako su osnovni kriteriji za generisanje kriptografskih ključeva brzina, komercijala i sl. što nameće manji nivo sigurnosti, treba koristiti pseudoslučajne generatore.

LITERATURA

- [1] William Stallings, "Cryptography and Network Security", Prentice Hall, 2005.
- [2] Mark Stamp, "Applied Cryptanalysis", John Wiley & Sons, 2007.
- [3] Mark Stamp. *Information security: principles and practice*. John Wiley & Sons, Inc, 2006.
- [4] ANSI X 9.17 (Revised), —American National Standard for Financial Institution Key Management (Wholesale),|| American Bankers Association, 1985.
- [5] Bruce Schneier, "Applied Cryptography", John Wiley & Sons, 1996.
- [6] A.Menzes, P.van Oorschot, S. Vanstone, "Handbook of Applied Cryptography", CRC Press, 1996.
- [7] National Institute for Standards and Technology, —*Key Management Using X9.17*,|| NIST FIPS PUB 171, U.S Department of Commerce, 1992.
- [8] National Institute for Standards and Technology, —*Secure Hash Standard*,|| NIST FIPS PUB 180, U.S Department of Commerce, 1993.
- [9] National Institute for Standards and Technology, —*Digital Signature Standard*,|| NIST FIPS PUB 186 U.S Department of Commerce, 1994.
- [10] Andrew Nash, William Duane, Celia Joseph, Derek Brink, "PKI Implementing and Managing E-Security", RSA Press, 2001.
- [11] Milan Milosavljević i Gojko Grubor, "Osnovi bezbednosti i zaštite informacionih sistema", Univerzitet Singidunum, 2006.