Analiza sistema za distribuciju kriptografskih ključeva

Miroslav Ćajić, Mladen Veinović, Bogdan Brkić

***Sadržaj* — U ovom radu predstavljen je problem distribucije kriptografskih ključeva. Ukazano je na nedostatke koji se susreću u procesu distribucije, i na njihova moguća rješenja. Kao osnova sistema za razmjenu kriptografskih ključeva detaljno su analizirani Diffie-Hellman i Arithmetica algoritamski modeli. Predstavljene su prednosti i nedostaci jednog i drugog sistema, izvršeno je njihovo poređenje i dat je krajnji zaključak u vidu rezultata.**

***Ključne riječi* — Algoritam, Arithmetica, Diffie-Hellman, kriptografski ključ.**

I. UVOD

PROCES upravljanja kriptografskim ključevima spada u jedan od najtežih zadataka koji se nameće u savremenoj kriptografiji. Iako kriptografski algoritmi počivaju na obimnim akademskim istraživanjima sam proces njihovog kreiranja nije tako jednostavan. U suštini, održavanje tajnosti ključeva je mnogo teže. Prilikom napada na simetrične i asimetrične sisteme kriptoanalitičar će prije napasti sistem za upravljanje ključevima, nego što će pokušati da otkrije zakonitosti kriptografskog algoritma koji je primijenjen. Matematička osnova kriptografskih algoritama kao i razne analize u pogledu njihove ranjivosti su za pojedine algoritme javno dostupne. Važno je napomenuti da je kriptografija, osim u nekim specifičnim slučajevima kao što su vojska, policija, i neke bezbjednosne organizacije, uglavnom bazirana na poznatim kriptografskim rješenjima [1].

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. Usložnjavanjem sigurnosnog modela dovodi se do pada nivoa performansi kao i otežavanje funkcija predloženog sigurnosnog rješenja.

Sigurnosni model za razmjenu kriptografskih ključeva je od ekstremnog značaja za cjelokupan bezbjedonosni sistem. U kriptološkoj infrastrukturi, veliki broj napada se dešava na nivou upravljanja kriptografskim ključevima, dok se napadi na same algoritme dešavaju vrlo rijetko. Jednom generisan kriptografski ključ mora ostati tajan, odnosno, mora se izbjeći situacija kao što je impersonalizacija. Učesnici u kriptološkom sistemima moraju biti sposobni da generišu ključeve, odnosno, ti ključevi moraju biti dostupni korisnicima u komunikaciji. U slučaju da dođe do kompromitacije ili gubitka ključa on strane X, ostali učesnici u komunikaciji moraju biti blagovremeno upozoreni. U suprotnom, napadač će ukradenim ključem moći dešifrovati sve poruke koje su šifrovane tim istim ključem. Takođe, korisnicima mora biti omogućeno da na siguran način čuvaju svoje ključeve i učine ih nedostupnim osim za legitimnu upotrebu.

Pošto ključevi imaju ograničen životni vijek, najvažniji razlog za nihovo periodično mijenjanje je zaštita od kriptoanalize. Svaki put kada se ključ upotrijebi generiše se šifrat određene dužine i veličine. Skupljanjem ovakvih šifrata napadač prikuplja podatke neophodne za kriptoanalizu. Iz tog razloga, ključevi trebaju da imaju ograničen životni vijek

Da bi se efikasno zaštitio kriptološki sistem cilj je da se izvrši što kvalitetnija razmjena kriptografskih ključeva. Najvažniji razlog za ovo je zaštita od kriptoanalize [2].

II. PROCES PRIMJENE

Jedan od uslova za uspješno implementiran process primjene sigurnosnog modela predstavlja potpuna ili apsolutna slučajnost [3].

Ovu slučajnost je teško definisati i njena mjera se predstavlja entropijom. Izvore slučajnosti moguće je postići softverski, ali 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 i sl. Uzimanjem u obzir ovih parametara može se dobiti kvalitetan slučajan 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 navode se: detektori radioaktivnog raspada, detektori termičkog šuma, uređaji u kojima je moguće ostvariti i detektovati optički kvantni efekat ili uređaji u kojima nastaju nepredvidive oscilacije frekvecije u fazno kontrolisanoj petlji.

Prilikom generisanja: simetričnih ključeva, RSA prostih brojeva, Diffie-Hellman-ove tajne vrijednosti i dr. neophodno je koristiti slučajne brojeve, odnosno, prirodne vrijednosti, koje moraju biti statistički slučajni ili nepredvidivi brojevi. Za razliku od kriptografskih nizova koji nisu, pseudoslučajni brojevi su prediktibilni, i samo je pitanje koliko od izlaznog niza moramo poznavati da bi smo otkrili cjelokupni mehanizam generisanja. U ovom

Miroslav Ćajić, OŠ „Sveti Sava“, Preobraženjska bb, 73220 Rogatica, tel.: +387 65/631-675, fax: 387 58/417-517, e-mail: miroslavcajic@gmail.com

Mladen Veinović, Univerzitet “Singidunum”, Bulavar Zorana Đinđića 44, Novi Beograd, tel.: +381 11 31 21 349, e-mail: mveinovic@singidunum.ac.rs

Bogdan Brkić, Ministarstvo finansija Republike Srpske, Kralja Petra I Karađorđevića, 78000 Banja Luka, tel.: +387 65/567-941, e-mail: bbogdan@teol.net

slučaju, jedino ostaje otvoreno pitanje generisanja "seed"-a tj. unutrašnjih ključeva, odnosno, početnih slučajnih vrijednosti [4].

Istraživanja u kriptoanalizi dovode do otkrivanja potencijalnih slabosti i napada, pa se svakih nekoliko godina povećava preporučena minimalna dužina ključeva za pojedine algoritme. Npr. za RSA algoritam trenutno se preporučuje minimalna dužina ključa od 512 bita. Ovo se odnosi na privremene ključeve čiji je vremenski indeks upotrebe jedan ili nekoliko dana. Preporučena dužina ključeva za dužu upotrebu je minimalno 1024 bita [6]. Napominjemo da ključeve možemo podijeliti na: simetrične, javne i privatne ključeve, a samo su simetrični i privatni ključevi su po svojoj prirodi tajni ključevi [6], [11].

III. DISTRIBUCIJA KLJUČEVA

Upravljanje ključevima se bavi sigurnim generisanjem, distribucijom i čuvanjem ključeva. Izbor sigurne metode za upravljanje 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 [5].

Problem distribucije ključeva je prisutan kroz cijelu istoriju kriptografije. Bez obzira koliko je u teoriji kriptografski algoritam siguran, povjerljivost njegovog mehanizma može ugroziti problem distribucije ključeva. Pitanje distribucije ključeva može se činiti trivijalnim, ali on je za pouzdan kriptološki sistem najslabija karika. Za dešifrovanje poruke strana B mora posjedovati validnu kopiju alata koji je strana A koristila za šifrovanje, ali i ključ kojim je poruka šifrovana U procesu razmjene podataka u bezbjednosnom okruženju dvije osobe se moraju pouzdati u treću, osobu C, koja će im dostaviti ključ, koji u ovom slučaju postaje slaba karika u lancu bezbjednosti [4] .

Učesnici u PKI sistemima moraju biti sposobni da generišu ključeve. Takođe moraju imati mogućnost da objave svoj javni ključ i da im budu dostupni javni ključevi ostalih korisnika u sistemu, za šta se koriste sertifikati. Ukoliko dođe do kompromitacije ili gubitka nečijeg privatnog ključa ostali učesnici moraju biti upozoreni. U suprotnom, napadač će ukradenim privatnim ključem moći dešifrovati sve poruke koje su šifrovane odgovarajućim javnim ključem ili će moći vršiti neovlašteno digitalno potpisivanje. Korisnicima mora biti omogućeno da na siguran način čuvaju svoje ključeve i učine ih nedostupnim osim za legitimnu upotrebu [7], [12].

Prema tome faze u životnom ciklusu ključeva su:

- generisanje ključeva,
- distribucija ključeva,
- aktivacija / deaktivacija ključeva,
- zamjena (replace) ili osvježavanje (update) ključeva,
- opoziv ključeva,
- kraj validnosti ključeva, uništavanje ključeva i eventualno arhiviranje.

IV. DIFFIE-HELLMANOV 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 [8].

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

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

Primjer bi bio sledeći:
Neka je *p* neki veliki broj, a *g* broj tipa intidžer, gdje je $2 \leq g \leq p - 2$. Obadva elementa p i g su javno poznati. Alisa bira slučajni broj a, gdje važi da je $1 \leq a \leq p - 2$, i izračunava $\alpha = g^{a} \pmod p$. Zatim, Alisa šalje svoju vrijednost α Bobu, dok vrijednost a ostaje poznata samo za Alisu. Bob takođe bira slučajan broj b, gdje važi $1 \leq b \leq p - 2$ i izračunava $\beta = g^{b} \pmod p$ i šalje Alisi vrijednost svoje β, dok vrijednost njegovog b ostaje kod njega.

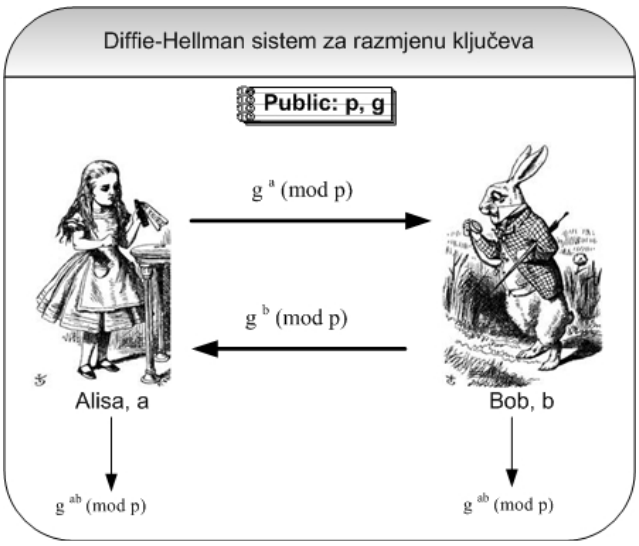
Alisa zatim izračunava:

$$\beta^{a} \pmod p = (g^{b})^{a} \pmod p = g^{ab} \pmod p$$

Bob zatim izračunava sledeće:

$$\alpha^{b} \pmod p = (g^{a})^{b} \pmod p = g^{ab} \pmod p$$

Alisa i Bob sada dijele zajedničko $g^{ab} \pmod p$, koji mogu koristiti kao simetrični ključ.



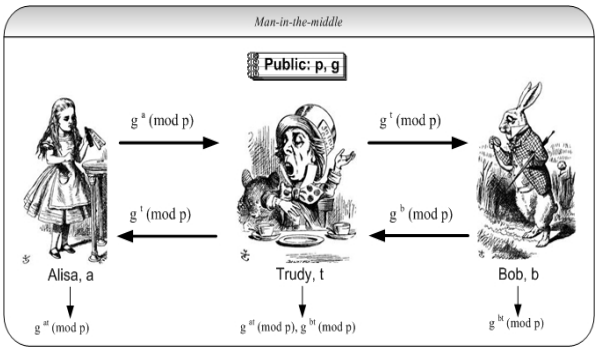
Sl. 1. Diffie-Hellman sistem za razmjenu ključeva

V. MAN IN THE MIDDLE NAPADI

Razmjena ključeva u Diffie-Hellmanovom algoritmu je predmet napada, *man-in-the-middle*, ako već ne postoji procedura, odnosno, protokol za autorizaciju strana u komunikaciji tokom razmjene ključeva.

Pretpostavimo da Trudy želi čitati poruke koje su poslate između Alise i Boba, pri čemu Alisa i Bob koriste Diffie-Hellman sistem za razmjenu ključeva. Kao prvo, Trudy bira jedan exponent t. Ona onda izračunava g^a (mod p) i g^b (mod p) i šalje g^t (mod p) Alisi i Bobu. U suštini, Alisa vjeruje da je g^b (mod p) poslato od Boba, i Bob vjeruje da je g^t (mod p) došlo od Alise. Sada Trudy izračunava $K_A=(g^a)^t$ (mod p) i $K_B=(g^b)^t$ (mod p). Alisa ne primjećuje da je Trudy u sredini komunikacije, i prati Diffie-Hellmanovom protokol i izračunava K_A. Slično tome, Bob izračunava K_B., a Alisa šalje poruku Bobu koja je kriptovana sa K_A. Trudy prihvata tu poruku, dešifruje je, ponovo šifruje istu ili neku drugu poruku sa K_B i šalje je Bobu. U ovom slučaju Trudy može prihvatati, čitati i mijenjati svaku poruku poslatu između Alise i Boba, a da njih dvoje ne uoče nikakav problem [1].

Sledeća slika ilistruje *man-in-the-middle* napad.



Sl. 2. Man in the middle napad u Diffie-Hellmanovom sistemu za razmjenu kriptografskih ključeva.

Ipak, postoji više načina za prevenciju ovog napada. Na primjer *Station-to-Station* protokol, može biti upotrebljen za ovu vrstu autentifikacije.

Ipak, rješenja za ovaj problem mogu biti i sledeća:

- šifrovanje pomoću Diffie-Hellmana u razmjeni simetričnog ključa,
- šifrovanje pomoću Diffie-Hellmana u razmjeni javnog ključa,
- digitalno potpisivanje Diffie-Hellman vrijednosti privatnim ključem i
- implementiranje sigurnosnog protokola.

VI. ARITHMETICA 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 bio bi sledeći:

Pretpostavimo 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:

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

Za podgrupu S_A i S_B možemo pretpostaviti da su to skupovi tipičnih riječi engleskog alfabeta, koji se sastoje od s_i i t_j, a čine je određeni binarni operatori. Zatim, Alisa i Bob biraju svoje privatne ključeve:

$$a= s$$

Poslije toga, Alisa izračunava skup elemenata:
$\{a^{-1}\ t_{0a}, \ldots, a^{-1}t_{m-1a}\}$, i rezultat šalje Bobu. Bob izračunava $\{b^{-1}\ s_{1b}, \ldots, b^{-1}s_{n-1b}\}$ i vraća Alisi. Prije razmjene, svaki ovaj skup je ponovo zapisan upotrebom specijalnih relacija da bi se osigurali privatni ključevi a i b. Sa primljenim podacima od Boba, Alisa može izračunati $b^{-1}ab$ kao:

$$b^{-1}ab$$

Slično tome, Bob može izračunati $a^{-1}ba$. Upotrebom njihovih privatnih ključeva, Alisa i Bob izračunavaju svaku vrijednost za $a^{-1}b^{-1}ab$, koja može služiti kao zajednički simetrični ključ.

Iako ovaj scenario izgleda kao veoma komplikovan, u suštini i nije. Uzmimo da Alisa i Bob žele razmjeniti ključeve. Kao prvo moraju odrediti grupu javnih ključeva, npr:

$$G=(x, y \mid x^4, y^2, yxyx)$$

Alisa i Boba zatim biraju svoje javne ključeve:

- $S_A= (s_0, s_1)= (x^2, y)=\{1_G,x^2, y,x^2y\}$ i
- $S_B= (t_0)= (x)=\{1_G,x, x^2,x^3\}$, i svoje privatne ključeve
- $a=(x^2)^2*(y)^{-1}=x^4y^{-1}=1_G*y^{-1}=y^{-1}$, i
- $b=(x)^3=x^3$

U narednom koraku Alisa izračunava $a^{-1}t_0a=y^{-1}xy$ i prepisuje ga kao svoj yxy, koji šalje Bobu. Na sličan način Bob izračunava i prepisuje:

$$b^{-1}s_0b=x^{-3}x^2x^3=x^2=x^{-2}, \text{ i}$$
$$b^{-1}s_1b=x^{-3}yx^3=xyx^3=x*x^{-3}=x^{-2}y=x^2y$$

Bob u sledećem koraku Alisi šalje $\{x^{-2},x^2y\}$. Da bi dobila zajednički ključ Alisa treba da izračuna:

$$b^{-1}ab=(x^{-2})^2(x^2y)^{-1}=(x^2)^2(y^{-1}x^{-2})$$
$$=x^4y^{-1}x^{-2}=1_G*y^{-1}x^{-2}=yx^2=x^2y$$

Konačno, Alisa izračunava:

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

Slično tome Bob izračunava:

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

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

VII. ZAKLJUČAK

Distribucija kriptografskih ključeva je jedan od ključnih postupaka u kritptografiji. 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 [10]. Ako su osnovni kriteriji za generisanje kriptografskih ključeva brzina i manji nivo sigurnosti treba koristiti pseudoslučajne generatore.

Iako postoje tvrdnje da je problem distribucije kriptografskih ključeva nerješiv problem, sredinom sedamdesetih godina prošlog vijeka otkriveno je pouzdano rješenje. Najveću revoluciju u kriptologiji dvadesetog vijeka izazvao razvoj tehnika za svladavanje problema distribucije kriptografskih ključeva. To se otkriće smatra najvećim kriptološkim ostvarenjem još od izuma monoalfabetske metode kriptovanja (jedne od najranijih metoda kriptovanja poruka) prije dvije hiljade godina.

Diffie-Hellman obezbjeđuje jedno lagano rješenje od jednog veoma izazovnog problema u cijeloj kriptologiji koji se zove problem distribucije ključeva (key distribution problem or key establishment problem), koji je baziran kako je utvrđeno na zajedničkom simetričnom ključu [7].

Man-in-the-middle napad u Diffie-Hellman razmjeni ključeva može biti otklonjen pouzdanim sistemom autentifikacije. Na primjer, autentifikacioni protokol koji koristi digitalni potpis može osigurati Alisu i Boba da primljena poruka bude od prave osobe. Slično tome, Trudy ne može lažirati Alisin i Bobov potpis svojim *man-in-the-middle* napadom koji bi u ovom slučaju bio neuspješan. Naravno, upotreba digitalnog popisa bi spriječila ponavljanje ove vrste napada.

U slučaju Diffie-Hellman, *man-in-the-middle* napad je veoma ozbiljan problem, koji može biti riješen u većini aplikacija. Diffie-Hellman sistem za razmjenu ključeva je jedan veoma koristan sistem za javnu razmjenu kriptografskih ključeva. Upotrebljava se na primjer u IPSec protokolu za osiguravanje perfect forward secrecy (PFS). Diffie-Hellman može biti implementiran u određenom PIN-baziranom ili password-baziranom protokolu određene aplikacije i sl.

U poređenju sa Diffie-Hellman ili nekim drugim kriptografskim algoritmom, Arithmetica koristi veoma komplikovane matematičke proračune, pa zbog toga nije praktično popularna u realnom svijetu kriptografije.

U realnom svijetu implementacija Arhitmetica algoritma je bazirana na izračunavanju kompleksnog problema konjukcije, jer za jednu grupu G nije poznat efikasan algoritam za rješavanje problema gdje za date dvije riječi x i y u određenom skupu G ne postoji riječ za koju važi da je g pripada skupu G, odnosno, da je $y=g^{-1}xg$.

LITERATURA

[1] Mark Stamp, "Applied Cryptoanalysis", *John Wiley & Sons, 2007.*

[2] William Stallings,"Cryptography and Network Security", *Prentice Hall*, 2005.

[3] Bruce Schneier, "Applied Cryptography", *John Wiley & Sons*, 1996.

[4] A.Menzes, P.van Oorschot, S. Vanstone, "Handbook of Applied Cryptography", CRC Press, 1996.

[5] Carlisle Adams, Steve Lloyd, "Understanding PKI: Concepts, Standards and Deployment Considerations", Addison Wesley, 2002.

[6] Steve Burnett, Stephen Paine, "RSA Security's Official Guide to Cryptography", RSA Press, 2001.

[7] Andrew Nash, William Duane, Celia Joseph, Derek Brink, "PKI Implementing and Managing E-Security", RSA Press, 2001.

[8] Milan Milosavljević i Gojko Grubor, "Osnovi bezbednosti i zaštite informacionih sistema", *Univerzitet Singidunum*, 2006.

[9] Miroslav Ćajić i Bogdan Brkić, "Modeli sigurnosnog rješenja za mobilne uređaje zasnovanih na Android operativnom sistemu", *Telfor 2009.*

[10] Bogdan Brkić i Miroslav Ćajić, "Metodi i napadi na distribuciju simetričnih i asimetričnih kriptoloških ključeva", *Telfor 2009.*

[11] http://www.rsa.com/

[12] http://www.pki-page.org/

ABSTRACT

In this paper we present the problem of distributing cryptographic keys. It was pointed out the shortcomings encountered in the process of distribution, and their possible solutions. As a basic system for the exchange of cryptographic keys, Diffie-Hellman algorithm and Arithmetic algorithm models are analyzed. The advantages and disadvantages of both systems were performed and their comparison was made and was given the final conclusion in terms of results.

ANALYSIS SYSTEM FOR THE DISTRIBUTION OF CRYPTOGRAPHIC KEYS

Miroslav Ćajić, Mladen Veinović, Bogdan Brkić