Digitalni potpis

Bernadin Ibrahimpašić* Edin Liđan†

Sažetak. *Razmjena ključeva među osobama koje sudjeluju u komunikaciji nije uvijek izvediva na siguran način u komunikacijskom sustavu preko kojeg se vrši razmjena ključeva. Jedan od mogućih načina rješavanja ovog problema je u korištenju kriptosustava javnog ključa prilikom slanja poruke. Cilj nam je očuvati njenu vjerodostojnost, netaknutost i nepobitnost. Tu mogućnost nudi nam digitalni potpis, a kako je RSA jedan od najsigurnijih kriptosustava s javnim ključem koji ujedno omogućuje direktno potpisivanje poruke, u radu je opisano RSA digitalno potpisivanje.*

Ključne riječi: *RSA kriptosustav, digitalni potpis, RSA digitalni potpis*

Digital Signature

Abstract. *A digital signature is a mathematical scheme for demonstrating the authenticity of a message stored in electronic form. A valid digital signature gives a recipient reason to believe that the message was created by a known sender. Digital signatures are commonly used in everyday situations such as writing a letter, software distribution and financial transactions, etc. The first practical public–key cryptosystem is the RSA. One of the primary applications of RSA is in the use of digital signature. In this paper we describe the RSA digital signature sheme.*

Key words: *RSA cryptosystem, Digital Signature, RSA Digital Signatures*

1. Uvod

Relativno vrlo rano, u povijesti čovječanstva javila se potreba za komunikacijom. Čovjek po svojim društvenim osobinama svakodnevno pokazuje potrebu za komunikacijom. Međutim, često smo u situaciji da ne želimo sve informacije podijeliti sa svima tj. želimo ih uputiti samo jednoj osobi. Tada na scenu stupa znanost koja se

*Pedagoški fakultet, Univerzitet u Bihaću, Džanića mahala 36, 77000 Bihać, Bosna i Hercegovina, e-mail: bernadin@bih.net.ba

†Pedagoški fakultet, Univerzitet u Bihaću, Džanića mahala 36, 77000 Bihać, Bosna i Hercegovina, e-mail: lidjan_edin@hotmail.com

zove *kriptografija*. Riječ kriptografija potječe od grčkih riječi *kripto* što znači *tajno* i *grafein* što znači *pisati*, pa bismo u doslovnom prijevodu mogli reći da kriptografija znači *tajnopis*. Kriptografiju kao znanstvenu disciplinu definiramo kao znanost koja se bavi proučavanjem metoda za slanje poruka u takvom obliku da ih samo onaj kome su namijenjene može razumjeti. Na osnovu toga možemo reći da je osnovni cilj kriptografije omogućiti dvjema osobama komunikaciju preko nesigurnog komunikacijskog kanala, tako da ih treća osoba ne rezumije. Osoba koja šalje poruku naziva se *pošiljatelj* (čest naziv u literaturi je Alice), a osoba koja prima poruku naziva se *primatelj* (čest naziv u literaturi je Bob), dok treću osobu koja želi presresti poruku nazivamo *napadač* (neprijatelj ili protivnik) (čest naziv u literaturi je Eva). Pošiljatelj najprije, pomoću već unaprijed dogovorenog ključa, mora transformirati poruku koju šalje. Poruku koju pošiljatelj transformira nazivamo *otvoreni tekst* (engl. plaintext), postupak transformacije nazivamo *šifriranje* (kriptiranje), a dobiveni rezultat nazivamo *šifrat* (kriptat ili šifrirana poruka) (engl. chipertext). Nakon toga pošiljatelj šalje poruku preko nesigurnog komunikacijskog kanala. Ako napadač presretne poruku i sazna sadržaj šifrata, on zbog nepoznavanja ključa, za razliku od primatelja ne može dešifrirati poruku i razumjeti je. Šifra predstavlja matematičku funkciju koju koristimo za šifriranje i dešifriranje. Sve moguće poruke, šifrati i ključevi zajedno s funkcijom za šifriranje i dešifriranje čine kriptosustav. Na osnovu ovih elemenata možemo izreći formalnu definiciju kriptosustava.

Definicija 1. Kriptosustav *je uređena petorka* $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ *za koju vrijedi:*

1. $\mathcal{P}$ *je konačan skup svih mogućih otvorenih tekstova;*
2. $\mathcal{C}$ *je konačan skup svih mogućih šifrata;*
3. $\mathcal{K}$ *je prostor ključeva, tj. skup svih mogućih ključeva;*
4. *za svaki ključ* $K \in \mathcal{K}$ *postoji algoritam šifriranja* $e_K \in \mathcal{E}$ *i odgovarajući algoritam dešifriranja* $d_K \in \mathcal{D}$*, gdje su* $e_K : \mathcal{P} \longrightarrow \mathcal{C}$ *i* $d_K : \mathcal{C} \longrightarrow \mathcal{P}$ *funkcije sa svojstvom da je*
$$d_K(e_K(x)) = x,$$
za svaki otvoreni tekst $x \in \mathcal{P}$*.*

Kriptosustave na osnovu tajnosti i javnosti ključa možemo klasificirati na sljedeći način:

- *Simetrični kriptosustavi* kod kojih se ključ za dešifriranje može izračunati poznajući ključ za šifriranje i obratno. Sigurnost im leži u tajnosti ključa, pa ih zbog toga nazivamo i *kriptosustavi s tajnim ključem.*
- *Asimetrični kriptosustavi* kod kojih se ključ za dešifriranje ne može, u nekom razumnom vremenu, odrediti iz ključa za šifriranje. Kod ovog kriptosustava ključ za šifriranje je javni ključ, tj. bilo tko može šifrirati poruku, ali samo osoba koja poznaje ključ za dešifriranje može dešifrirati tu poruku. Ovakve kriptosustave nazivamo *kriptosustavi javnog ključa.*

Ideju kriptosustava javnog ključa iznijeli su Whitfield Diffie i Martin Hellman 1976. godine i nazvali su ga kriptosustav javnog ključa.

2. RSA kriptosustav

Ideju koju su iznijeli Diffie i Hellman, iskoristili su Ronald **R**ivest, Adi **S**hamir i Leonard **A**dleman i 1977. godine izumili prvi kriptosustav s javnim ključem koji su nazvali *RSA kriptosustav*. Sigurnost RSA kriptosustava leži u činjenici da je faktorizacija velikih prirodnih brojeva na produkt dva prosta broja izuzetno teška, a možemo ga i formalno definirati.

Neka je $n = pq$, gdje su p i q prosti brojevi. Neka je $\mathcal{P} = \mathcal{C} = \mathbb{Z}_n$, te

$$\mathcal{K} = \{(n, p, q, d, e) \,:\, n = pq,\ de \equiv 1 \pmod{\varphi(n)}\},$$

gdje je $\varphi(n)$ Eulerova funkcija koja prirodnom broju n pridružuje broj prirodnih brojeva manjih od n koji su relativno prosti s n. Kako je φ multiplikativna funkcija, a p i q prosti, to je kod RSA kriptosustava $\varphi(n) = (p-1)(q-1)$.

Za $K = (n, p, q, d, e) \in \mathcal{K}$ definiramo

$$e_K(x) = x^e \bmod n \qquad \text{i} \qquad d_K(y) = y^d \bmod n,$$

gdje su $x, y \in \mathbb{Z}_n$.

Vrijednosti n i e su javne, dok su vrijednosti p, q i d tajne.

Opišimo sada kako se implementira RSA kriptosustav.

1. Bob tajno odabere dva različita prosta broja p i q, od kojih svaki ima oko 100 znamenki. Obično se odaberu tako da jedan od njih ima nekoliko znamenki više od drugog. Odabir se izvrši tako da se, pomoću nekog generatora slučajnih brojeva, generira dovoljno velik prirodan broj w, a zatim se korištenjem nekog testa za testiranje prostosti, traži prvi prosti broj koji je veći ili jednak w. Kako prostih brojeva manjih od w ima približno $k/\ln w$, to je za očekivati da ćemo trebati testirati $O\left(\ln w\right)$[1] brojeva dok ne nađemo prvi prosti broj veći ili jednak w.

2. Bob računa $n = pq$ i $\varphi\left(n\right) = \left(p-1\right)\left(q-1\right)$.

3. Bob odabere na slučajan način broj e takav da je $10^5 < e < \varphi\left(n\right)$ i takav da je $\operatorname{nzd}\left(e, \varphi\left(n\right)\right) = 1$.

4. Bob računa d takvo da je $d \equiv e^{-1} \pmod{\varphi\left(n\right)}$.
   Izračunavanje d vrši se pomoću proširenog Euklidovog algoritma koji za dane a i b računa $b^{-1} \bmod a$.

   Napomenimo da i prošireni Euklidov algoritam, kao i Euklidov algoritam za računanje najvećeg zajedničkog djelitelja, trebaju $O\left(\ln^2 n\right)$ operacija. Euklidov algoritam je vrlo efikasan za računanje najvećeg zajedničkog djelitelja dva

[1] Za točnije opisivanje vremena izvođenja algoritma koristimo se tzv. $\mathcal{O}$-notacijom, čime se određuje gornja granica vremenskog izvođenja algoritma. Neka su $f, g\colon \mathbb{N} \to \mathbb{R}$ dvije funkcije. Tada pišemo: $f\left(n\right) = \mathcal{O}\left(g\left(n\right)\right)$, ako postoji pozitivna konstanta C i prirodan broj n_0, tako da je $0 \leq f\left(n\right) \leq C \cdot g\left(n\right)$, za sve $n \geq n_0$. Za dovoljno veliki n vrijedi $\mathcal{O}(1) < \mathcal{O}(\log n) < \mathcal{O}(n) < \mathcal{O}(n \log n) < \mathcal{O}(n^2) < \mathcal{O}(n^3) < \cdots < \mathcal{O}(2^n) < \mathcal{O}(n!)$. $\mathcal{O}(1)$ znači da je vrijeme izvođenja ograničeno konstantom, dok ostale vrijednosti do predzadnje predstavljaju polinomna vremena izvođenja algoritma. Predzadnje vrijeme predstavlja eksponencijalno vrijeme izvođenja algoritma. Algoritmi koji zahtijevaju eksponencijalno vrijeme mogu biti nerješivi u razumnom vremenu bez obzira na brzinu korištenog računala.

broja koji ne zahtijeva njihovu prethodnu faktorizaciju. Nalazi se u knjizi VII Euklidovih elemenata, iako se vjeruje da algoritam nije njegovo vlastito djelo, nego da je bio poznat više od 200 godina ranije.

5. Bob zadržava p, q, d kao tajnu, a n i e postavlja u javni direktorij.

6. Alice svoju poruku x šifrira i dobija šifrat $y = x^e \bmod n$ koji šalje Bobu. U slučaju da je $x > n$, x se razbija u blokove.

7. Bob dešifrira y računajući $x = y^d \bmod n$.

Postupak šifriranja poruke, tj. računanja šifrata $y = x^e \bmod n$, naziva se *modularno potenciranje*. Za efikasnost RSA kriptosustava bitno je vrlo efikasno provesti računanje $x^e \bmod n$ pomoću algoritma "*kvadriraj i množi*":

$y = 1$
za $i = l-1, \ldots, 1, 0$ radi
    $y = y^2 \bmod n$
    ako je $e_i = 1$ tada je $y = y \cdot x \bmod n$

gdje je $e = \sum_{i=0}^{l-1} e_i 2^i$ binarni zapis broja e.

Primjer 1. *Pokažimo kako Alice, šalje poruku*

$$MORE$$

Bobu i kako je on dešifrira.

Rješenje: Bob bira $p = 97$ i $q = 101$ i računa

$$n = pq = 9797,$$
$$\varphi(n) = (p-1)(q-1) = 9600,$$

te izabere $e = 19$, vodeći računa da je zadovoljeno $e < \varphi(n)$ i $\text{nzd}(e, \varphi(n)) = 1$. Zatim, pomoću proširenog Euklidovog algoritma računa d, takav da je

$$de \equiv 1 \pmod{\varphi(n)}$$

i dobija da je $d = 7579$. Vrijednosti od p, q, d zadržava za sebe, a n i e šalje Alice ili ih jednostavno upisuje u javni direktorij. Alice želi poslati poruku MORE, čiji je numerički ekvivalent

$$x = 13151805,$$

jer je 00 = razmak, 01 = A, 02 = B,..., 24 = X, 25 = Y, 26 = Z. Kako je $x > n$, x razdvaja u četveroznamenkaste blokove. Sada imamo

$$\begin{aligned} x &= (x_1, x_2) \\ &= (1315, 1805). \end{aligned}$$

Poznavajući Bobove javne $n = 9797$ i $e = 19$, Alice računa

$$y_i = x_i^e \bmod n, \qquad i = 1, 2,$$

i dobija šifrat

$$\begin{aligned} y &= (y_1, y_2) \\ &= (1916, 7288) \\ &= 19167288, \end{aligned}$$

koji šalje Bobu. Bob pomoću samo njemu poznatoga $d = 7579$, na isti način računa x, dijeleći y na blokove

$$x_i = y_i^{7579} \bmod 9797, \qquad i = 1, 2,$$

i dobija originalnu poruku MORE. □

Iz primjera uočavamo kako je implementacija RSA kriptosustava vrlo jednostavna. Analogno tome i napad na RSA kriptosustav može se vrlo efikasno provesti ako je poznat eksponent d. Očigledno je faktorizacija broja n jedan od mogućih napada na RSA kriptosustav, jer se iz poznavanja faktorizacije $n = pq$ može odrediti $\varphi(n) = (p-1)(q-1)$. Međutim, sigurnost RSA kriptosustava leži u činjenici da ne postoji polinomijalan algoritam za faktorizaciju velikih prirodnih brojeva.

3. Digitalni potpis

Internet je najrasprostranjenija računarska mreža koja omogućuje pojedincima iz svih dijelova svijeta međusobnu komunikaciju, razmjenu informacija i dokumenata. Tipična situacija je kada osoba A putem interneta želi kupiti nešto od osobe B. Međutim u takvom vidu komunikacije, uz klasične, pojavljuju se i neki sasvim novi problemi. Tako treba biti siguran da poruku koju je osoba A poslala osobi B ne može pročitati niko drugi, te da ta poruka nije promijenjena. Također, problem je da osoba B može biti u potpunosti sigurna da joj je upravo osoba A poslala primljenu poruku i da osoba A ne može poreći da je upravo osoba B poslala tu poruku. U rješavanju ovih potonjih problema pomaže nam *digitalni potpis* (engl. Digital signature).

Digitalni potpis predstavlja metodu za potpisivanje poruka u elektronskoj formi. Tako potpisana poruka može se prenositi računarskim mrežama. Ipak, treba biti oprezan jer kopija digitalno potpisane poruke identična je originalu, za razliku od poruke koja je na papiru potpisana na konvencionalan način. Digitalni potpis predstavlja kriptografsko obilježje poruke potpisnikovim tajnim parametrom. Digitalni potpis je kriptosustav s javnim ključem koji omogućuje prenošenje korisnih svojstava konvencionalnog papirnog potpisa u digitalni svijet. Međutim, ono što je vrlo bitno, digitalni potpis omogućuje

1. *autentifikaciju* – osoba B može provjeriti je li poruka koju je primila zaista poslala osoba A;

2. *nepobitnost* – osoba A ne može poreći da je ona poslala poruku ako osoba B posjeduje poruku s njenim potpisom.

Na ovaj način, u slučaju spora, obje strane u potpunosti su zaštićene digitalnim potpisom.

Definicija 2. Kriptosustav digitalnog potpisa *je uređena petorka* $(\mathcal{P}, \mathcal{A}, \mathcal{K}, \mathcal{S}, \mathcal{V})$, *gdje je:*

1. $\mathcal{P}$ *konačan skup svih mogućih poruka;*
2. $\mathcal{A}$ *konačan skup svih mogućih potpisa;*
3. $\mathcal{K}$ *je* prostor ključeva*, tj. konačan skup svih mogućih ključeva;*
4. *Za svaki* $K \in \mathcal{K}$ *postoji* algoritam za potpisivanje $\text{sig}_K \in \mathcal{S}$ *i odgovarajući* algoritam za verifikaciju $\text{ver}_K \in \mathcal{V}$*, takvi da su za sve algoritme*

$$\text{sig}_K : \mathcal{P} \longrightarrow \mathcal{A} \qquad i \qquad \text{ver}_K : P \times A \longrightarrow \{0, 1\},$$

gdje 0 *predstavlja netočno, a* 1 *točno, zadovoljene jednakosti*

$$ver_K(x, y) = \begin{cases} 1, & \text{ako je} \quad y = \text{sig}_K(x) \\ 0, & \text{ako je} \quad y \neq \text{sig}_K(x), \end{cases}$$

su za svaku poruku $x \in \mathcal{P}$ *i svaki potpis* $y \in \mathcal{A}$*.*

Par (x, y)*, gdje je* $x \in \mathcal{P}$ *i* $y \in \mathcal{A}$*, se naziva* potpisana poruka*.*

Za svaki $K \in \mathcal{K}$, funkcije sig_K i ver_K trebaju biti izračunljive u polinomijalnom vremenu. Funkcija ver_K je javna, dok je sig_K tajna (privatna). Za danu poruku x trebalo bi biti računarski nemoguće da bilo tko drugi osim Alice izračuna potpis y takav da je $\text{ver}_K(x, y) = 1$.

Ako napadač može izračunati par (x, y) takav da je $\text{ver}_K(x, y) = 1$, a da osoba A nije prije toga potpisala poruku x, tada se potpis y naziva *krivotvorina*. Neformalno, krivotvoren potpis je valjan potpis koji je izračunao netko drugi osim osobe A.

Kriptosustavi s javnim ključem na vrlo jednostavan način omogućuju digitalno potpisivanje. Alice može poruku x potpisati tako da uz x dopiše šifrat $d_A(x)$, koji je šifriran njenim tajnim ključem d_A. Kako Bob poznaje njen javni ključ e_A, može dešifrirati taj dio i provjeriti je li zaista Alice potpisala poruku x. Iako na ovaj način ostvarujemo digitalni potpis, ovakvo potpisivanje je vrlo sporo jer se radi o šifriranju javnim ključem koje je izuzetno sporo. Također, na ovaj se način udvostručuje duljina poruke. Stoga se umjesto originalne poruke često koristi *sažetak poruke* (engl. message digest) koji se dobije primjenom neke hash funkcije.

Najpoznatiji algoritmi za generiranje digitalnih potpisa su *Digital Signature Algorithm* (DSA/DSS) i *Eliptic Curve Digital Signature Algorithm* (ECDSA). DSA je zasnovan na problemu diskretnog logaritma u multiplikativnoj grupi konačnog polja i razvijen je prema uzoru na ElGamalov kriptosustav digitalnog potpisa. DSA je dio NIST-ovog (USA National Institute of Standards and Technology) Digital Signature Standarda. ECDSA je analogon DSA algoritmu koji umjesto multiplikativne grupe konačnog polja koristi eliptičke krivulje. ECDSA je prihvaćen kao ANSI (American National Standard Institute) standard.

4. RSA digitalni potpis

Neki kriptosustavi s javnim ključem mogu direktno biti iskorišteni za digitalno potpisivanje poruke. Među takvim kriptosustavima ističe se RSA kriptosustav. U skladu s tim, imamo i formalnu definiciju RSA digitalnog potpisa.

Neka je $n = pq$, gdje su p i q prosti brojevi. Neka je $\mathcal{P} = \mathcal{A} = \mathbb{Z}_n$, te

$$\mathcal{K} = \{(n, p, q, d, e) \,:\, n = pq,\ de \equiv 1 \pmod{\varphi(n)}\}.$$

Vrijednosti n i e su javne, dok su vrijednosti p, q i d tajne.

Za $K = (n, p, q, d, e) \in \mathcal{K}$ definiramo

$$\text{sig}_K(x) = x^e \bmod n \qquad \text{i} \qquad \text{ver}_K(x, y) = 1 \quad \Leftrightarrow \quad x = y^d \bmod n,$$

gdje su $x, y \in \mathbb{Z}_n$.

Treba istaknuti da kriptosustavi digitalnog potpisa uključuju tri algoritma:

1. Generiranje ključa (javnog i tajnog) za potpisivanje;
2. Potpisivanje poruke – generiranje poruke koju nazivamo potpis;
3. Provjera potpisa.

Pogledajmo kako to izgleda kod RSA digitalnog potpisa, ako Alice želi potpisati poruku koju šalje Bobu. Neka je x otvoreni tekst koji Alice želi poslati Bobu koristeći njegov javni ključ (n_B, e_B).

Algoritam za generiranje ključa

Da bi Alice generirala ključ, postupa na sljedeći način:

- Kao kod RSA kriptosustava, Alice odabere dva velika prosta broja p i q.
- Računa $n_A = p \cdot q$ i $\varphi(n_A) = (p-1)(q-1)$.
- Bira eksponent e_A takav da je $1 < e_A < \varphi(n_A)$ i $\text{nzd}(e_A, \varphi(n_A)) = 1$, te računa svoj tajni eksponent d_A za koji vrijedi da je $1 < d_A < \varphi(n_A)$ i $e_A \cdot d_A \equiv 1 \pmod{\varphi(n_A)}$.
- Alicein javni ključ je (n_A, e_A), a tajni ključ je d_A.

Algoritam za generiranje potpisa

Da bi se Alice potpisala, radi sljedeće:

- Računa svoj potpis $y = \text{sig}_A(x) = x^{d_A} \bmod n_A$.
- Šifrira i poruku i potpis koristeći Bobov javni ključ e_B računajući: $z_1 = x^{e_B} \bmod n_B$ i $z_2 = y^{e_B} \bmod n_B$.
- Šalje Bobu par (z_1, z_2).

Algoritam za provjeru potpisa

Kada Bob želi provjeriti potpis od Alice, koristeći svoj tajni ključ d_B radi sljedeće:

- Računa $z_1^{d_B} \bmod n_B = (x^{e_B})^{d_B} \bmod n_B = x$ i dobija otvoreni tekst.
- Računa $z_2^{d_B} \bmod n_B = (y^{e_B})^{d_B} \bmod n_B = y$ i dobija potpis od Alice.
- Koristeći javni ključ (n_A, e_A) od Alice, provjerava njen potpis računajući $y^{e_A} \bmod n_A = \left(x^{d_A}\right)^{e_A} \bmod n_A = x$.
- Ako provjerom potpisa dobije isti otvoreni tekst x, onda je Alicein potpis provjeren.

Pokažimo na primjeru kako se implementira RSA digitalno potpisivanje.

Primjer 2. *Pokažimo kako Alice potpisuje poruku i šalje potpisanu poruku MORE iz Primjera 1, te kako Bob verificira njen potpis.*

Rješenje Alice najprije generira ključ. Bira dva prosta broja $p = 89$ i $q = 113$ i računa

$$\begin{aligned} n_A &= pq = 10057, \\ \varphi(n_A) &= (p-1)(q-1) = 9856, \end{aligned}$$

te odabere slučajan broj $e_A = 17$, gdje je $1 < e_A < \varphi(n_A)$ i $\text{nzd}(e_A, \varphi(n_A)) = 1$, a zatim pomoću proširenog Euklidovog algoritma, iz kongruencije

$$e_A d_A \equiv 17 d_A \equiv 1 \pmod{9856},$$

izračuna tajni ključ $d_A = 7537$. Nakon što je generirala ključ, slijedi generiranje potpisa, odnosno potpisivanje poruke. Da bi generirala potpis, računa

$$y = sig_A(x) = sig_A(13151805) = 13151805^{7537} \pmod{10057} = 23869521.$$

Nakon toga šifrira poruku i potpis koristeći Bobov javni ključ $e_B = 19$ računajući

$$\begin{aligned} z_1 &= x^{e_B} \bmod n_B = 13151805^{19} \bmod 9797 = 19167288, \\ z_2 &= y^{e_B} \bmod n_B = 23869521^{19} \bmod 9797 = 39544580, \end{aligned}$$

a zatim Bobu šalje par $(z_1, z_2) = (19167288, 39544580)$.

Da bi Bob provjerio Alicein potpis, koristeći svoj tajni ključ e_B računa:

$$\begin{aligned} z_1^{d_B} \bmod n_B &= 19167288^{7579} \bmod 9797 = 13151805, \\ z_2^{d_B} \bmod n_B &= 39544580^{7579} \bmod 9797 = 23869521. \end{aligned}$$

Koristeći Alicein javni ključ $e_A = 17$, provjerava njen potpis računajući

$$y^{e_A} \bmod n_A = 23869521^{17} \bmod 10057 = 13151805.$$

Kako je provjerom potpisa dobio otvoreni tekst, Bob zaključuje da mu je poruku zaista poslala Alice.

Analogno razbijanju poruke x u četveroznamenkaste blokove, napomenimo da je isti princip korišten pri provjeri potpisa i pri izračunavanju y, z_1 i z_2. □

5. Zaključak

Kako je danas rad bez računala i interneta u obavljanju bilo kakvog posla skoro nezamisliv, potreba za očuvanjem autentičnosti i sigurnosti dokumenata postaje sve veća. Iz navedenog razloga digitalni potpis poprima sve širu upotrebu i samo je pitanje vremena kada će u potpunosti zamijeniti klasično potpisivanje, pa je neophodno osigurati njegovu sigurnu upotrebu. Nakon dugog niza godina intenzivnog proučavanja i pokušaja "razbijanja" RSA kriptosustava, još nije pronađena metoda kojom bi se RSA kriptosustav u potpunosti razbio. Poznati napadi na RSA kriptosustav pokazuju kakve parametre treba izbjegavati a kakve birati. Zbog toga RSA kriptosustav smatramo sigurnim kriptosustavom te ga možemo iskoristiti za efikasno digitalno potpisivanje dokumenata.

Ipak, napomenimo da kriptosustavi s javnim ključem imaju jedan nedostatak. Taj nedostatak ogleda se u problemu sigurnog povezivanja ključa i osobe, tj. ostaje otvoreno pitanje identiteta ključa, što je u praksi problematično. Opasnost koja se javlja je da se Eva lažno predstavi kao Bob. Tada Alice može misliti da je šifrirala poruku za Boba, ali tu poruku može pročitati samo Eva. Tu poruku Bob čak ne može ni dešifrirati jer ju je Alice šifrirala koristeći javni ključ od Eve. Također, efikasna provjera potpisa ne znači da je poruku potpisala Alice, nego smo samo sigurni da je potpisana tajnim ključem koji odgovara javnom ključu za koji mi vjerujemo da pripada Alice. Stoga zaključujemo da i pored velike sigurnosti kriptosustava s javnim ključem i njihove pogodnosti za digitalno potpisivanje, od njih imamo koristi samo ako smo sigurni da smo uspješno razmijenili ključeve i imamo povjerenja u identitet osobe koja posjeduje dani ključ.

Jedno rješenje ovog problema daje sustav protokola koji nazivamo *infrastruktura javnog ključa* (engl. Public Key Infrastructure – PKI). U PKI sustavu protokola treća strana jamči za identitete osoba i ključeva. Ovakav autoritet koji jamči za identitete naziva se *središnji autoritet* (engl. certificate authority – CA). Ukoliko usporedimo papirne i digitalne potpise, onda CA predstavlja ulogu javnog bilježnika u digitalnom svijetu.

Literatura

[1] J. A. BUCHMAN, *Introduction to Cryptography*, Springer – Verlag, New York, 2001.

[2] A. DUJELLA, M. MARETIĆ, *Kriptografija*, Element, Zagreb, 2007.

[3] B. IBRAHIMPAŠIĆ, *RSA kriptosustav*, Osječki matematički list, **5**(2005), 101–112.

[4] D. R. STINSON, *Cryptography. Theory and Practice*, CRC Press, Boca Raton, 1996.

[5] S. Y. YAN, *Number Theory for Computing*, Springer – Verlag, Berlin, 2002.