Centar Informacijske Sigurnosti

IBE - Identity Based Encryption

CIS-DOC-2011-04-010

Upozorenje

Podaci, informacije, tvrdnje i stavovi navedeni u ovom dokumentu nastali su dobrom namjerom i dobrom voljom te profesionalnim radom CIS-ovih stručnjaka, a temelje se na njihovom znanju i petnaestak godina iskustva u radu u informacijskoj sigurnosti. Namjera je da budu točni, precizni, aktualni, potpuni i nepristrani.

Ipak, oni su dani samo kao izvor informacija i CIS ne snosi nikakvu izravnu ili posrednu odgovornost za bilo kakve posljedice nastale korištenjem podataka iz ovog dokumenta.

Ukoliko primijetite bilo kakve netočnosti, krive podatke ili pogreške u ovom dokumentu, ili imate potrebu komentirati sadržaj molimo Vas da to javite elektroničkom poštom na adresu info@CIS.hr.

O CIS-u

CIS izrađuje pregledne dokumente (eng. white paper) na teme iz područja informacijske sigurnosti koji će biti korisni zainteresiranoj javnosti, a u svrhu **podizanje njezine svijesti o informacijskoj sigurnosti** i **sposobnosti za čuvanje i zaštitu informacija i informacijskih sustava**. Pored toga, CIS razvija i održava mrežni portal www.CIS.hr kao referalnu točku za informacijsku sigurnost za cjelokupnu javnost; izrađuje obrazovne materijale namijenjene javnosti; organizira događaje za podizanje svijesti o informacijskoj sigurnosti u javnosti i pojedinim skupinama te djeluje u suradnji sa svim medijima.

CIS **okuplja mlade** zainteresirane za informacijsku sigurnost i radi na njihovom pravilnom odgoju i obrazovanju u području informacijske sigurnosti te pripremu za **profesionalno bavljenje informacijskom sigurnošću**.

Centar informacijske sigurnosti [CIS] nastao je 2010. godine na poticaj Laboratorija za sustave i signale[LSS] Zavoda za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu, a kao posljedica 15togodišnjeg rada na istraživanju, razvoju i primjeni informacijske sigurnosti. LSS je među ostalim potaknuo osnivanje CARNetovog CERTa i sudjelovao u izradi Nacionalnog programa informacijske sigurnosti RH.

Smisao CISa je da bude **referentno mjesto za informacijsku sigurnost** za javnost, informatičare i posebno za mlade te da sustavno podiže njihovu svijest i sposobnosti u području informacijske sigurnosti.

Rad CISa podržava Ministarstvo znanosti, obrazovanja i sporta Republike Hrvatske, a omogućuju sponzori.

Prava korištenja

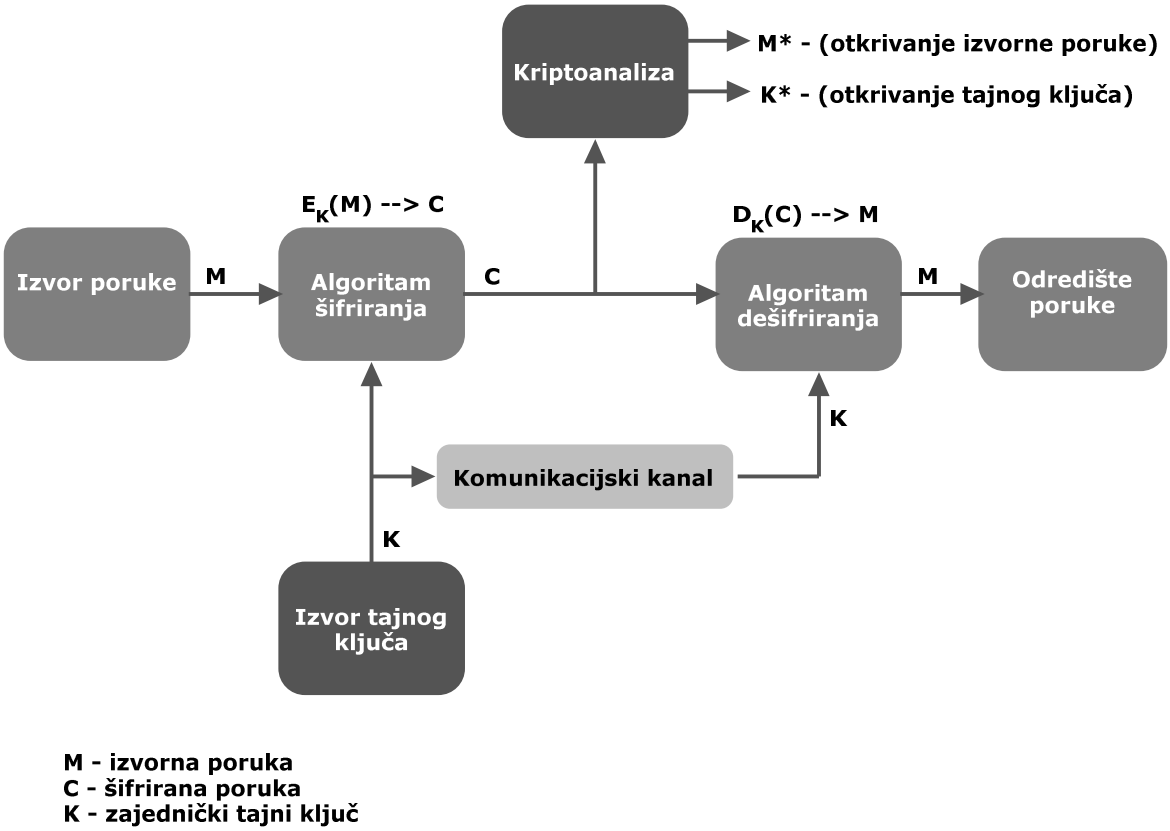
Sadržaj

1. Uvod

Kroz čitavu povijest čovječanstva postojala je potreba za sigurnom razmjenom informacija. Sigurna razmjena informacija podarzumijeva da strane koje sudjeluju u komunikaciji preko javnog komunikacijskog kanala međusobno razmjenjuju poruke čije stvarno značenje ne može odgonetnuti neka treća strana. Osnovni mehanizam kojim se postiže sigurna razmjena informacija je šifriranje. Šifriranje podataka ili poruka u osnovi znači njihovo skrivanje ili pretvorbu u neprepoznatljiv oblik.

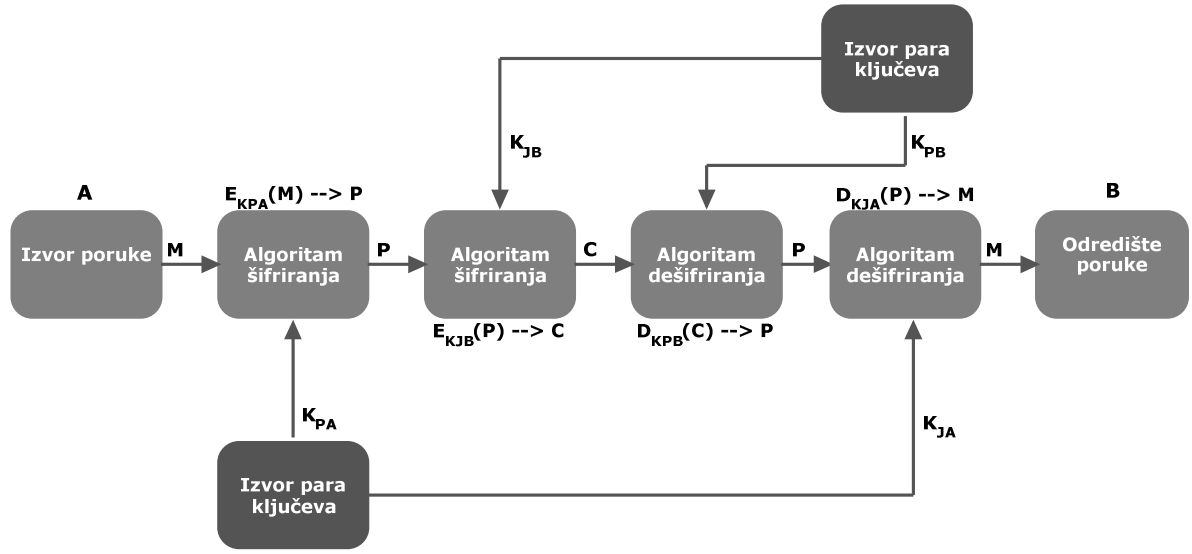
Metode šifriranja su raznovrsne, a njihov razvoj u stopu prati napredak u razvoju suvremenih komunikacijskih tehnologija. Osnovne metode šifriranja danas su metode simetričnog i asimetričnog šifriranja.

Metoda simetričnog šifriranja temelji se na zajedničkom tajnom ključu poznatom stranama koje žele na siguran način razmjenjivati poruke preko javnog komunikacijskog kanala. Poruke se prije slanja šifriraju tajnim ključem. Po njihovu dospijeću primatelj ih dešifrira pomoću istog tog ključa. U teoriji, treća strana nije u mogućnosti otkriti sadržaj šifrirane poruke jer joj tajni ključ nije dostupan. Model rada simetričnog šifriranja nalazi se na sljedećoj slici.



Slika 1. Model rada metode simetričnog šifriranja

Metoda asimetričnog šifriranja ili šifriranja uporabom javnog ključa osmišljena je kako bi ispravila neke od nedostataka koji se javljaju kod metode simetričnog šifriranja. Osnovni je nedostatak svakako problem sigurnosti pohrane i distribucije zajedničkog tajnog ključa. Postupci asimetričnog šifriranja rješavaju taj problem tako što uvode par ključeva šifriranja za svakog od sudionika komunikacije. Par ključeva sastoji se od javnog i privatnog ključa. Privatni ključ dostupan je isključivo korisniku i ne smije se distribuirati. Javni ključ treba biti dostupan svima, što podrazumijeva njegovu distribuciju (objavu) potencijalnim sugovornicima. Ideja je sljedeća: ono što se šifrira javnim ključem, može se dešifrirati samo privatnim, a ono što se šifrira privatnim, može se dešifrirati samo javnim ključem. Model rada asimetričnog šifriranja nalazi se na sljedećoj slici.



M - izvorna poruka
P - potpisana poruka
C - šifrirana poruka

K_{JA} - javni ključ od A
K_{PA} - privatni ključ od A
K_{JB} - javni ključ od B
K_{PB} - privatni ključ od B

Slika 2. Model rada metode asimetričnog šifriranja (autentifikacija i tajnost)

Dakle, ako korisnik A želi koristiti metodu asimetričnog šifriranja za komunikaciju s korisnikom B, onda oboje moraju imati po par ključeva (javni i privatni). Privatne ključeve će na siguran način pohraniti i neće ih objavljivati nikome, a javne ključeve će objaviti jedan drugome. Korisnik A će iskoristiti javni ključ korisnika B i njime šifrirati njemu namijenjenu poruku. Korisnik B će ju moći dešifrirati jedino uporabom svog privatnog ključa. Metoda asimetričnog šifriranja uvodi i mogućnost digitalnog potpisivanja. Korisnik A bi u prethodnom primjeru poslanu poruku mogao potpisati šifriranjem njenog sažetka svojim privatnim ključem. Korisnik B bi mogao dešifrirati takav potpis uporabom javnog ključa korisnika A te provjeriti poklapa li se tako dobiven sažetak sa sažetkom već dešifrirane poruke.

Jedan od nedostataka prisutan kod većine postupaka koji spadaju u metode asimetričnog šifriranja je sljedeći: da bi ih mogao koristiti, primatelj mora imati unaprijed izračunat par ključeva, a pošiljatelj mora biti u mogućnosti vidjeti objavljen javni ključ tog primatelja.

IBE (eng. *Identity Based Encryption*) je oblik asimetričnog šifriranja koji uklanja spomenuti nedostatak. Riječ je o metodi asimetričnog šifriranja koja omogućuje uporabu bilo kakvog oblika informacije o samom korisniku, poput adrese elektroničke pošte, korisničkog imena, domene ili nekog drugog niza znakova, kao njegovog javnog ključa. U ovom slučaju primatelj ne mora imati unaprijed izračunat par ključeva da bi koristio asimetrično šifriranje za zaštitu svojih poruka. Pošiljatelj šifrira poruku uporabom nekog od specifičnih podataka vezanih uz primatelja (primjerice adrese elektroničke pošte). Primatelj potom preko posebnog, povjerljivog entiteta iz podatka koji je korišten za šifriranje poruke izračunava odgovarajući privatni ključ kojim tu poruku i dešifrira. Na ovaj način primatelji mogu izračunavati vlastite privatne ključeve izravno preko povjerljivog poslužitelja u trenutku kada im to zatreba bez briga oko distribucije vlastitih javnih ključeva.

U ovom dokumentu bit će predstavljen upravo IBE oblik asimetričnog šifriranja. U drugom poglavlju bit će predstavljen osnovni koncept oko kojeg se temelji rad IBE-a, a u trećem poglavlju opisati će se razvoj IBE-a uz detaljniji pregled najvažnijih teoretskih izvedbi samog mehanizma. Četvrto poglavlje donosi analizu njegovih prednosti i nedostataka, dok je peto poglavlje vezano uz praktičnu primjenu IBE-a. Konačno, u šestom će poglavlju biti riječi o budućnosti njegova razvoja.

2. Osnovni koncept

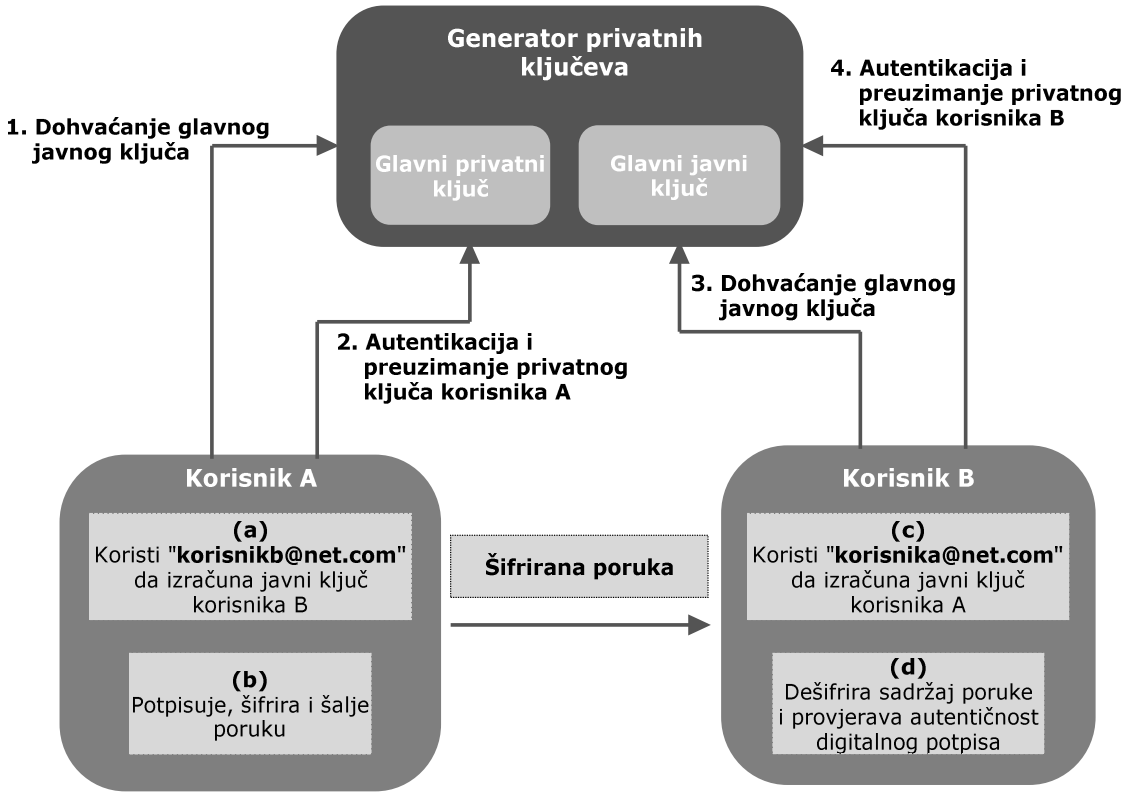
Cilj ovog poglavlja detaljnija je definicija IBE mehanizma asimetričnog šifriranja i prikaz osnovnog koncepta na kojem se temelji njegov rad.

2.1. Definicija

Šifriranje temeljeno na identitetu ili IBE (eng. *Identity Based Encryption*) poseban je oblik asimetričnog šifriranja u kojem javni ključ korisnika može biti bilo koji niz znakova koji predstavlja neku konkretnu informaciju o tom korisniku. Najbolji primjeri takvih podataka su razna korisnička imena i adrese elektroničke pošte.

2.2. Osnovni koncept

Slika 3. daje prikaz mehanizma na kojem se temelji rad IBE-a.



Slika 3. Shema mehanizma na kojem se temelji rad IBE-a

Za IBE metodu šifriranja poruka između strana koje komuniciraju potrebna je prisutnost povjerljive treće strane koja se naziva **generator privatnih ključeva** (eng. *Private Key Generator*). Njegova uloga je stvaranje odgovarajućih privatnih ključeva na temelju podataka koji se koriste kao javni ključevi. Generator privatnih ključeva za obavljanje svojih funkcija treba imati izračunata dva osnovna ključa:

- glavni javni i
- glavni privatni ključ.

Glavni javni ključ se objavljuje kako bi bio dostupan svim zainteresiranim stranama i koristi se u izračunu korisničkih javnih ključeva. Glavni privatni ključ se ne distribuira i koristi se kod izračuna korisničkih privatnih ključeva.

Mehanizam na kojem se temelji rad IBE-a bit će objašnjen na primjeru komunikacije između korisnika A i korisnika B (Slika 3).

Korisnik A želi poslati poruku korisniku B šifriranu njegovim javnim ključem i potpisanu svojim privatnim ključem. Pretpostavimo da su podaci koje će oba korisnika koristiti za izračun svojih javnih ključeva biti njihove adrese elektroničke pošte (*korisnika@net.com* i *korisnikb@net.com*). Korisnik A dohvaća glavni javni ključ generatora privatnih ključeva te ga, zajedno s adresom elektroničke pošte korisnika B, koristi za izračun javnog ključa korisnika B. Javnim ključem korisnika B šifrira njemu namijenjenu poruku. Uz to, autenticira se kod generatora privatnih ključeva te dohvaća privatni ključ povezan s podatkom koji koristi za izračun vlastitog javnog ključa (vlastita adresa elektroničke pošte). Tako dobivenim, vlastitim privatnim ključem potpisuje šifriranu poruku i šalje ju korisniku B.

Korisnik B po primitku poruke prvo dohvaća glavni javni ključ generatora privatnih ključeva. Pomoću njega i adrese elektroničke pošte korisnika A izračunava njegov javni ključ. Potom se autenticira kod generatora privatnih ključeva te dohvaća vlastiti privatni ključ. Pomoću tog ključa dešifrira dobivenu poruku. Pomoću javnog ključa korisnika A provjerava autentičnost njegovog digitalnog potpisa.

Opisani postupak omogućuje slanje šifriranih poruka bez obzira na to posjeduje li primatelj unaprijed izračunat par ključeva ili ne. Ako primatelj nema unaprijed izračunat par ključeva, pošiljatelju jedino preostaje obavijestiti ga o konkretnom podatku korištenom za šifriranje te o generatoru privatnih ključeva čije su se usluge koristile. Privatni ključ za određen podatak dovoljno je dohvatiti samo jednom i on ostaje važeći za svako sljedeće šifriranje uporabom tog podatka. Valja naglasiti kako se IBE ne bavi mehanizmima autentikacije između korisnika i generatora privatnih ključeva prilikom dohvaćanja privatnih ključeva. Njegova je uloga isključivo vezana uz izračun javnih korisničkih te odgovarajućih privatnih ključeva.

Jedan od osnovnih nedostataka opisanog mehanizma vezan je uz činjenicu da su generatoru privatnih ključeva dostupni svi potrebni podaci za šifriranje, dešifriranje i potpisivanje poruka koji se onda mogu koristiti bez znanja korisnika. Izuzetno važnu ulogu ovdje igra povjerenje prema entitetu koji obavlja ulogu generatora privatnih ključeva. Neke od inačica IBE metode šifriranja, kao što su šifriranje temeljeno na certifikatima (eng. *certificate-based encryption*), šifriranje temeljeno na sigurnoj dodjeli ključeva (eng. *secure key issuing cryptography*) te šifriranje bez certifikata (eng. *certificateless cryptography*) ispravljaju i taj, vrlo važan nedostatak. Više informacija o navedenim metodama može se pronaći u nastavku dokumenta.

3. Razvoj i teoretske izvedbe

Šifriranje temeljeno na identitetu prvi puta je predložio Adi Shamir 1984. godine. Izvorna zamisao bila je vezana uz mogućnost provjere digitalnih potpisa korisnika uporabom isključivo javnih korisničkih podataka kao što su korisnički identifikatori. Prva implementacija takve ideje temeljila se na adresama elektroničke pošte kao javnim podacima koji su se koristili za provjeru digitalnih potpisa. Premda je osmislio sustav provjere digitalnih potpisa temeljen na identitetu korisnika, Shamir ipak nije uspio predložiti konkretnu shemu kojom bi ostvario mehanizam šifriranja temeljenog na identitetu. Taj je problem ostao neriješen sve do 2001. godine kada su se pojavila tri različita rješenja u obliku Boneh-Franklinove, Cocksove i Sakai-Ohgishi-Kasaharine sheme šifriranja. U nastavku poglavlja opisana je matematička podloga na kojoj se temelje Boneh-Franklinova i Cocksova shema. Zbog svoje nepraktičnosti, Sakai-Ohgishi-Kasaharina shema neće biti razmatrana. Valja naglasiti kako je ovo poglavlje puno matematičkih zapisa koji se neće dodatno objašnjavati već se pretpostavlja određena razina znanja čitatelja kojeg će zanimati teoretske definicije navedenih shema.

3.1. Boneh-Franklinova shema šifriranja

Boneh-Franklinova shema predstavlja mehanizam šifriranja temeljen na identitetu kojeg su 2001. godine osmislili Dan Boneh i Matthew K. Franklin. Shema se temelji na primjeni Weilovog sparivanja [7] preko eliptičkih krivulja [8] i konačnih polja [9]. Iz sheme je nastao poseban protokol nazvan *BasicIdent*. Sigurnost sheme i deriviranog protokola temelji se na složenosti bilinearnog Diffie-Hellmanova problema [12] za korištene grupe.

3.1.1. Osnovni parametri

S obzirom na činjenicu da se shema temelji na sparivanju, svi izračuni izvode se unutar dvije grupe, G_1 i G_2. Za grupu G_1 neka p bude prost broj takav da vrijedi $p \equiv 2 \bmod 3$ i neka je definirana formula eliptičke krivulje $E: y^2 = x^3 + 1$ na skupu $\mathbb{Z}/p\mathbb{Z}$. Tako definirana krivulja nije singularna poput formule $4a^3 + 27b^2 = 27 = 3^3$, već je jednaka nuli samo u slučaju kada je $p = 3$, što je isključeno iz daljnjih ograničenja.

Neka je $q > 3$ prost faktor broja $p + 1$ (koji je reda E), a $P \in E$ neka točka reda q. Grupa G_1 skup je točaka koje generira $P: \{nP || n \in \{0, \dots, q-1\}\}$. Grupa G_2 je podgrupa skupa $GF(p^2)^*$ koja je reda q. Ta grupa ne mora biti izgrađena eksplicitno već je to obavljeno samim postupkom sparivanja.

3.1.2. Opis protokola

Protokol na kojem se temelji rad Boneh-Franklinove sheme složen je algoritam koji se sastoji od četiri koraka:

- **Priprema (eng. *Setup*):** generator privatnih ključeva odabire:
  1. javne grupe G_1 (s generatorom P) i G_2, definirane u poglavlju iznad, a veličine q ovisno o sigurnosnom parametru k,
  2. odgovarajuće sparivanje e,
  3. nasumičan privatni glavni ključ $K_m = s \in \mathbb{Z}_q^*$,
  4. glavni javni ključ $K_{pub} = sP$,
  5. javnu *hash* [10] funkciju $H_1: \{0,1\}^* \rightarrow G_1^*$,
  6. javnu hash funkciju $H_2: G_2 \rightarrow \{0,1\}^n$ za neki određeni n te
  7. prostor poruka i prostor šifri $M = \{0,1\}^n$, $C = G_1^* \times \{0,1\}^n$.

- **Izvlačenje (eng. *Extract*):** da bi se stvorio javni ključ za neki identifikator $\boldsymbol{ID} \in \{\mathbf{0},\mathbf{1}\}^*$, generator privatnih ključeva izračunava:
  1. $\boldsymbol{Q_{ID}} = \boldsymbol{H_1}(\boldsymbol{ID})$ i
  2. privatni ključ $\boldsymbol{d_{ID}} = \boldsymbol{sQ_{ID}}$ koji se daje korisniku.
- **Šifriranje (eng. *Encrypt*):** za dobivenu poruku $\boldsymbol{m} \in \boldsymbol{M}$ šifrat (šifrirani tekst) $\boldsymbol{c}$ se dobiva na sljedeći način:
  1. $\boldsymbol{Q_{ID}} = \boldsymbol{H_1}(\boldsymbol{ID}) \in \boldsymbol{G_1^*}$,
  2. odabire se nasumičan broj $\boldsymbol{r} \in \mathbb{Z}_q^*$,
  3. izračunava se $\boldsymbol{g_{ID}} = \boldsymbol{e}(\boldsymbol{Q_{ID}}, \boldsymbol{K_{pub}}) \in \boldsymbol{G_2}$ i
  4. određuje se šifrat c kao $\boldsymbol{c} = (\boldsymbol{rP}, \boldsymbol{m} \oplus \boldsymbol{H_2}(\boldsymbol{g_{ID}^r}))$.

  Valja primijetiti da je glavni javni ključ generatora privatnih ključeva $\boldsymbol{K_{pub}}$ neovisan o primateljevom identifikatoru ($\boldsymbol{ID}$).
- **Dešifriranje (eng. *Decrypt*):** za dobiven šifrat $\boldsymbol{c} = (\boldsymbol{u}, \boldsymbol{v}) \in \boldsymbol{C}$ izvorna poruka se izračunava korištenjem privatnog ključa korisnika preko sljedeće formule: $\boldsymbol{m} = \boldsymbol{v} \oplus \boldsymbol{H_2}(\boldsymbol{e}(\boldsymbol{d_{ID}}, \boldsymbol{u}))$.

3.1.3. Ispravnost algoritma

Osnovni korak postupaka šifriranja i dešifriranja je uporaba sparivanja i funkcije $\boldsymbol{H_2}$ te stvaranje svojevrsne maske (poput simetričnog ključa) koja se funkcijom ekskluzivnog ILI (XOR) spaja s tekstom izvorne poruke. Da bi se odredila ispravnost cjelokupnog protokola potrebno je izvršiti provjeru mehanizma i vrijednosti šifrirane poruke koje na kraju dobiju pošiljatelj i primatelj. Za šifriranje se koristi funkcija $\boldsymbol{H_2}(\boldsymbol{g_{ID}^r})$, a za dešifriranje $\boldsymbol{H_2}(\boldsymbol{e}(\boldsymbol{d_{ID}}, \boldsymbol{u}))$. Zbog svojstava sparivanja vrijedi sljedeće:

$$\begin{aligned} H_2(e(d_{ID}, u)) &= H_2(e(sQ_{ID}, rP)) \\ &= H_2(e(Q_{ID}, P)^{rs}) \\ &= H_2(e(Q_{ID}, sP)^{r}) \\ &= H_2(e(Q_{ID}, K_{pub})^{r}) \\ &= H_2(g_{ID}^{r}) \end{aligned}$$

3.2. Cocksova shema šifriranja

Cocksovu shemu IBE šifriranja osmislio je Clifford Cocks 2001. godine. Sigurnost ove sheme temelji se na težini problema kvadratnih ostataka [11].

3.2.1. Opis protokola

Protokol na kojem se temelji rad Cocksove sheme složen je algoritam koji se sastoji od četiri koraka identična koracima kod Boneh-Franklinove sheme:

- **Priprema (eng. *Setup*):** generator privatnih ključeva odabire:
  1. javni RSA (eng. *Rivest, Shamir and Adleman*) modul $\boldsymbol{n} = \boldsymbol{pq}$, gdje su $\boldsymbol{p}, \boldsymbol{q}$, $\boldsymbol{p} \equiv \boldsymbol{q} \equiv \mathbf{3}\ \boldsymbol{mod}\ \mathbf{4}$ prosti i tajni brojevi,
  2. prostor poruka i prostor šifri $\boldsymbol{M} = \{-\mathbf{1}, \mathbf{1}\}$, $\boldsymbol{C} = \mathbb{Z}_{\boldsymbol{n}}$ te
  3. sigurnu javnu *hash* funkciju $\boldsymbol{f} : \{\mathbf{0},\mathbf{1}\}^* \rightarrow \mathbb{Z}_{\boldsymbol{n}}$.

- **Izvlačenje (eng. *Extract*):** kad korisnik nekog identifikatora ($\boldsymbol{ID}$) želi dohvatiti vlastiti privatni ključ, on kontaktira generator privatnih ključeva preko sigurnog komunikacijskog kanala. Generator privatnih ključeva tada:
  1. determinističkim postupkom izračunava $\boldsymbol{a}$ s $\left(\frac{\boldsymbol{a}}{\boldsymbol{n}}\right) = \boldsymbol{1}$ iz $\boldsymbol{ID}$ (višestrukom uporabom funkcije $\boldsymbol{f}$),
  2. izračunava $\boldsymbol{r} = \boldsymbol{a}^{\frac{n+5-p-q}{8}} \boldsymbol{mod}\, \boldsymbol{n}$ (koji zadovoljava jednadžbu $\boldsymbol{r^2} = \boldsymbol{a}\, \boldsymbol{mod}\, \boldsymbol{n}$ ili $\boldsymbol{r^2} = -\boldsymbol{a}\, \boldsymbol{mod}\, \boldsymbol{n}$) te
  3. šalje $\boldsymbol{r}$ korisniku.
- **Šifriranje (eng. *Encrypt*):** da bi šifrirao jedan bit (kodiran s $\boldsymbol{1}$ ili $-\boldsymbol{1}$) $m \in \boldsymbol{M}$ za $\boldsymbol{ID}$ korisnik:
  1. odabire nasumičan $\boldsymbol{t}$ tako da vrijedi $\boldsymbol{m} = (\frac{\boldsymbol{t}}{\boldsymbol{n}})$,
  2. izračunava $\boldsymbol{c_1} = \boldsymbol{t} + \boldsymbol{at^{-1}}\, \boldsymbol{mod}\, \boldsymbol{n}$ i $\boldsymbol{c_2} = \boldsymbol{t} - \boldsymbol{at^{-1}}\, \boldsymbol{mod}\, \boldsymbol{n}$ te
  3. šalje $\boldsymbol{s} = (\boldsymbol{c_1}, \boldsymbol{c_2})$ sugovorniku.
- **Dešifriranje (eng. *Decrypt*):** da bi se dešifrirao šifrat $\boldsymbol{s} = (\boldsymbol{c_1}, \boldsymbol{c_2})$ za zadan $\boldsymbol{ID}$ korisnik:
  1. izračunava $\boldsymbol{a} = \boldsymbol{c_1} + \boldsymbol{2r}$ ako vrijedi $\boldsymbol{r^2} = \boldsymbol{a}$ ili $\boldsymbol{a} = \boldsymbol{c_2} + \boldsymbol{2r}$ inače te
  2. izračunava $\boldsymbol{m} = (\frac{\boldsymbol{a}}{\boldsymbol{n}})$.

Ovdje se pretpostavlja da entitet koji obavlja šifriranje ne zna ima li $\boldsymbol{ID}$ kvadratni korijen $\boldsymbol{r}$ od $\boldsymbol{a}$ ili $-\boldsymbol{a}$. U tom slučaju šifrat se šalje tako da se u obzir uzmu obje mogućnosti. Čim entitet koji obavlja šifriranje sazna taj podatak, potrebno je poslati samo podatke za odgovarajuć slučaj.

3.2.2. Ispravnost algoritma

Prvo valja primijetiti da s obzirom na činjenicu da vrijedi $\boldsymbol{p} \equiv \boldsymbol{q} \equiv \boldsymbol{3}\, \boldsymbol{mod}\, \boldsymbol{n}$ i $\left(\frac{\boldsymbol{a}}{\boldsymbol{n}}\right) \Rightarrow \left(\frac{\boldsymbol{a}}{\boldsymbol{p}}\right) = (\frac{\boldsymbol{a}}{\boldsymbol{q}})$ ili $\boldsymbol{a}$ ili $-\boldsymbol{a}$ je kvadratni ostatak modula $\boldsymbol{n}$. Stoga je $\boldsymbol{r}$ kvadratni korijen od $\boldsymbol{a}$ ili $-\boldsymbol{a}$:

$$
\begin{aligned}
r^2 &= \left(a^{\frac{n+5-p-q}{8}}\right)^2 \\
&= \left(a^{\frac{n+5-p-q-\Phi(n)}{8}}\right)^2 \\
&= \left(a^{\frac{n+5-p-q-(p-1)(q-1)}{8}}\right)^2 \\
&= \left(a^{\frac{n+5-p-q-n+p+q-1}{8}}\right)^2 \\
&= \left(a^{\frac{4}{8}}\right)^2 \\
&= \pm a
\end{aligned}
$$

Nadalje, za slučaj kada je $\boldsymbol{a}$ kvadratni ostatak, isto vrijedi i za $-\boldsymbol{a}$:

$$\left(\frac{s+2r}{n}\right) = \left(\frac{t+at^{-1}+2r}{n}\right) = \left(\frac{t\left(1+at^{-2}+2rt^{-1}\right)}{n}\right)$$
$$= \left(\frac{t\left(1+r^2t^{-2}+2rt^{-1}\right)}{n}\right) = \left(\frac{t\left(1+rt^{-1}\right)^2}{n}\right)$$
$$= \left(\frac{t}{n}\right)\left(\frac{1+rt^{-1}}{n}\right)^2 = \left(\frac{t}{n}(\pm 1)\right)^2 = \left(\frac{t}{n}\right)$$

Glavni nedostatak ove sheme činjenica je da se šifriranje provodi bit po bit. Zbog toga je prikladna samo kod šifriranja malih podatkovnih paketa poput ključeva sjednice.

3.3. Daljnji razvoj

Pregledom navedenih shema mogu se uočiti zajednički koraci karakteristični za sve danas razvijene mehanizme implementacije IBE sustava šifriranja. Općenito, radi se o četiri posebna algoritma. Oni su:

1. **Pripremne radnje (eng. *Set-up*):** podrazumijevaju stvaranje skupa javnih parametara zajedno s glavnim ključevima (javnim i privatnim) generatora privatnih ključeva.
2. **Izračun ključa (eng. *Key-Gen*):** koji se sastoji od izračuna privatnog ključa korisnika ovisno o specifičnom podatku koji ga opisuje.
3. **Šifriranje (eng. *Encrypt*):** predstavlja mehanizam šifriranja poruke preko specifičnog podatka korisnika.
4. **Dešifriranje (eng. *Decrypt*):** koje se sastoji od dešifriranja poruke preko privatnog ključa korisnika.

S vremenom je došlo i do razvoja naprednijih inačica IBE-a. Jedna od njih je i hijerarhijski IBE (eng. *Hierarchical Identity Based Encryption, HIBE*). Riječ je o proširenju osnovnog sustava uvođenjem hijerarhije generatora privatnih ključeva radi rasterećenja prilikom obrade brojnih zahtjeva za stvaranjem privatnih korisničkih ključeva. Do danas je razvijen popriličan broj unaprijeđenih inačica osnovnog teoretskog koncepta. Najpraktičnija i najučinkovitija rješenja čeka konkretna implementacija. Neki od primjera njihove praktične primjene predstavit će se u nastavku dokumenta.

4. Analiza sustava

U ovom poglavlju dan je pregled prednosti i nedostataka IBE sustava šifriranja.

4.1. Prednosti šifriranja temeljenog na identitetu

Prva i osnovna prednost IBE sustava šifriranja svakako je već spomenuta činjenica da primatelj tako šifriranih poruka ne mora imati unaprijed izračunat par ključeva šifriranja. Nadalje, s obzirom na mehanizam koji javne ključeve korisnika povezuje s konkretnim podacima koji su s njima povezani, eliminira se potreba za izgradnjom, često složene, infrastrukture koja omogućuje distribuciju javnih ključeva. Autentičnost javnih ključeva implicitno je jamčena sve dok su mehanizmi distribucije privatnih korisničkih ključeva sigurni (s obzirom na autentičnost korisnika te integritet i povjerljivost komunikacije).

Još jedna važna prednost IBE koncepta vezana je uz činjenicu da se, u slučaju konačnog broja korisnika, nakon što svi korisnici dobiju svoje privatne ključeve tajni podaci pohranjeni u generatoru privatnih ključeva mogu uništiti. To je moguće jer jednom kada se izračunaju, privatni ključevi ostaju ispravni zauvijek (s obzirom na nedostatak mehanizma ukidanja njihove ispravnosti). Većina unaprijeđenih inačica osnovnog IBE koncepta koje sadrže mehanizam ukidanja ispravnosti ključeva gubi ovu prednost.

Dodatno, IBE nudi zanimljive funkcionalnosti koje proizlaze iz mogućnosti ugradnje dodatnih informacija u korisničke podatke korištene za izračun javnih ključeva. Primjerice, pošiljatelj bi tako mogao odrediti rok uporabe neke poruke dodavanjem vremenske oznake na korisnički podatak sugovornika (korišten za izračun javnog ključa). Za to se može poslužiti nekim binarnim formatom kao što je X.509. Po primitku poruke, spomenuti sugovornik kontaktira generator privatnih ključeva koji provjerava vremensku oznaku i, ovisno o tome je li oznaka istekla, izračunava ili odbija izračunati odgovarajući privatni ključ. Općenito, ugradnja dodatnih informacija u korisničke podatke korištene za izračun javnih ključeva odgovara otvaranju dodatnog komunikacijskog kanala između pošiljatelja i generatora privatnih ključeva s autentičnošću zajamčenom preko ovisnosti privatnog ključa i identifikacijskog podatka koji se za izračun odgovarajućeg javnog ključa koristi.

4.2. Nedostaci šifriranja temeljenog na identitetu

Nedostaci primjene IBE sustava šifriranja su sljedeći:

- U slučaju kompromitacije generatora privatnih ključeva sve šifrirane poruke stvorene parovima javnih i privatnih ključeva koji su do tada bili u uporabi također su kompromitirane. Zbog toga su generatori privatnih ključeva velika meta zlonamjernim korisnicima i napadačima. Da bi se smanjila izloženost kompromitiranog poslužitelja, par glavnih ključeva mogao bi se periodično zamijeniti potpuno novim parom ključeva. To sa sobom povlači problem upravljanja ključevima jer bi svi korisnici trebali koristiti najnoviji javni ključ generatora privatnih ključeva.
- Zbog činjenice da generator privatnih ključeva sadrži sve podatke potrebne za šifriranje, dešifriranje i potpisivanje korisničkih poruka, sam IBE sustav ne može se koristiti kako bi očuvao načelo neporecivosti. Neporecivost (eng. *non-repudiation*) znači da pošiljatelj ne može poreći sudjelovanje u transakciji jer jedino on ima pristup do svog tajnog ključa kojim potpisuje i dešifrira poruke. To možda ne predstavlja problem organizacijama koje imaju vlastite generatore privatnih ključeva, ali običnim korisnicima svakako ostaje nužna prisutnost povjerenja prema entitetu koji obnaša aktivnosti generatora privatnih ključeva.
- Za isporuku privatnih ključeva potreban je siguran komunikacijski kanal između korisnika i generatora privatnih ključeva. Za velike sustave često rješenje je primjena mehanizama kao što je SSL (eng. *Secure Socket Layer*). Važno je primijetiti da korisnici koji imaju korisničke račune kod generatora privatnih ključeva moraju proći mehanizme autentikacije prije dohvata privatnih ključeva.

- Rad IBE-a se oslanja na kriptografske tehnike koje nisu u potpunosti sigurne kada su u pitanju napadi posebnim metodama koje koriste kvantna računala [13] (primjer je Shorov algoritam [14]).

5. Praktična primjena

Izvorna motivacija prilikom objave IBE sustava šifriranja bila je vezana uz pojednostavljenje postojeće infrastrukture javnog ključa. Šifriranje temeljeno na identitetu može pojednostavniti upravljanje velikim brojem javnih ključeva.

Jedna od mogućih primjena vezana je uz metode povlačenja valjanosti javnih ključeva. Dok je to u postojećoj infrastrukturi javnog ključa ostvareno rokom trajanja pojedinih javnih ključeva, IBE nudi mogućnost fleksibilnijeg određivanja valjanosti javnog ključa za šifriranju poruka. Pošiljatelj poruke prilikom njenog slanja može sam odrediti rok trajanja u kojem je moguće njeno dešifriranje. Druga moguća primjena IBE-a vezana je uz sigurnije mehanizme dodjele ključeva šifriranja.

Danas postoji nekoliko popularnih izvedbi IBE sustava šifriranja. Premda se one međusobno razlikuju po svrsi i funkcionalnosti, važno je da se u pozadini nalazi osnovni mehanizam šifriranja temeljenog na identitetu.Uz to, prisutne su i brojne praktične primjene naprednijih inačica osnovnog koncepta u kojima se pokušavaju otkloniti neki od značajnijih nedostataka sustava. U ovom poglavlju slijedi pregled najznačajnijih praktičnih izvedbi IBE-a te opis nekih njegovih naprednijih inačica.

5.1. Praktična primjena osnovnog mehanizma

Jedna od primjena osnovnog mehanizma IBE-a vezana je uz operacijski sustav Debian GNU/Linux. Njen je naziv *Stanford IBE System*, a među ljudima koji su razvili takav sustav nalaze se i spomenuti Boneh i Franklin [6].

Tvrtka Shamus Software razvila je kriptografsku biblioteku naziva “MIRACL“ čiji se rad također temelji na Boneh-Franklinovoj shemi IBE šifriranja [6].

Obje spomenute implementacije razvijene su uporabom programskih jezika C i C++. Koliko je poznato, za sada ne postoji javna implementacija IBE mehanizma u programskom jeziku Java.

Dvije najznačajnijie praktične primjene IBE sustava šifriranja svakako su *IBE Secure E-mail* i *IBE Toolkit*.

5.1.1. IBE Secure E-mail

IBE Secure E-mail je sustav namijenjen šifriranju poruka elektroničke pošte temeljenog na IBE sustavu šifriranja. Tim ljudi koji je razvio ovaj sustav čine Dan Boneh, Matt Franklin, Ben Lynn, Matt Pauker, Rishi Kacker te Gene Tsudik.

IBE Secure E-mail svoj rad temelji na osnovnom IBE mehanizmu predstavljenom u drugom poglavlju te Boneh-Franklinovoj IBE shemi opisanoj u trećem poglavlju.

Ovaj sustav šifriranja poruka elektroničke pošte nudi sljedeće mogućnosti:

- pošiljatelji mogu slati šifrirane poruke elektroničke pošte primateljima koji nemaju unaprijed određen javni ključ,
- prilikom slanja poruka elektroničke pošte nije potrebno traženje primateljevog javnog ključa po *webu*, već se za to koristi neki specifičan podatak o primatelju (najčešće sama adresa elektroničke pošte),
- pošiljatelji mogu slati poruke elektroničke pošte koje smiju biti pročitane tek u neko određeno vrijeme u budućnosti te
- sustav šifriranja proaktivno periodički osvježava korisnički privatni ključ.

5.1.2. IBE Toolkit

Tvrtka Voltage razvila je *IBE Toolkit*, skup alata koji programerima i ostalim razvijateljima programske podrške omogućuju primjenu i jednostavnu ugradnju IBE mehanizama u vlastite aplikacije. Uporabom *IBE Toolkita* mogu se osigurati poruke elektroničke pošte ili ostali proizvoljni podaci u manje od petnaest linija programskog koda te bez potrebe za certifikatima. Uz implementaciju IBE sustava šifriranja, *IBE Toolkit* nudi i brojne druge pogodnosti za razvoj sigurnih aplikacija.

5.2. Pregled nekih naprednijih mehanizama i njihova primjene

U dokumentu su već spomenuti mehanizmi koji su na razne načine pokušali ispraviti velik nedostatak prisutan u osnovnom IBE konceptu – činjenicu da generator privatnih ključeva sadrži sve potrebne podatke za šifriranje, dešifriranje i potpisivanje poruka njegovih korisnika. Ti mehanizmi su:

- šifriranje temeljeno na certifikatima,
- šifriranje temeljeno na sigurnoj dodjeli ključeva te
- šifriranje bez certifikata.

5.2.1. Šifriranje temeljeno na certifikatima

Šifriranje temeljeno na certifikatima je sustav šifriranja u kojem entitet koji objavljuje certifikate (eng. Certificate Authority, CA) koristi IBE za stvaranje certifikata. Ovaj sustav omogućuje implicitno i eksplicitno certificiranje – certifikati se mogu koristiti na uobičajen način (primjerice, digitalni potpisi), te implicitno, za potrebe šifriranja.

Konkretno, korisnici ovdje mogu dvostruko šifrirati poruke uporabom primateljevog javnog ključa i podatka vezanog uz njegov identitet. Primatelj tako ne može dešifrirati poruku bez aktivnog certifikata, a entitet koji objavljuje certifikate nije u mogućnosti dešifrirati poruku jer nema pristupa primateljevom privatnom ključu.

Najbolji primjer praktične uporabe šifriranja temeljenog na certifikatima pruža CSS (eng. *Content Scrambling System*) koji se koristi za šifriranje filmova u DVD (eng. *Digital Video Disc*) formatu. CSS šifrira filmove na takav način da ih je moguće reproducirati samo u onom dijelu svijeta gdje se prodaju [15].

5.2.2. Šifriranje temeljeno na sigurnoj dodjeli ključeva

Šifriranje temeljeno na sigurnoj dodjeli ključeva inačica je IBE šifriranja koja smanjuje razinu potrebnog povjerenja prema trećoj strani zaduženoj za stvaranje privatnih ključeva. To ostvaruej tako da se umjesto jednog entiteta koristi više njih. Dodatno, korisnik šalje i tzv. maskirajuće podatke (eng. "*blinding*" *information*) kojima prikriva osjetljive informacije. Svaki od višestrukih entiteta zaduženih za generiranje privatnog ključa stvara tek jedan dio privatnog ključa, dok se svi dijelovi povezuju kod samog korisnika. Ti dijelovi privatnog ključa također su djelomično maskirani.

Ovaj pristup nudi velike prednosti u postupku upravljanja ključevima, ali konkretne implementacije trenutno još nisu zaživjele [16].

5.2.3. Šifriranje bez certifikata

Šifriranje bez certifikata inačica je IBE šifriranja ostvarena kako bi uklonila nedostatak vezan uz prisutnost korisničkih tajnih ključeva kod generatora privatnih ključeva. Postupak stvaranja privatnih ključeva ovdje je podijeljen između korisnika i entiteta zaduženog za stvaranje i dodjelu privatnih ključeva. Entitet zadužen za stvaranje i dodjelu privatnih ključeva prvo stvara par ključeva u kojem je privatni ključ tek djelomično izračunat. Ostatak

privatnog ključa računa se kod korisnika i ne otkriva se nikome. Sve kriptografske operacije obavljaju se uporabom kompletnog privatnog ključa koji uključuje dio dobiven od povjerljivog entiteta te dio izračunat kod samog korisnika.

Problem kod ovog sustava je činjenica da neki konkretan podatak o samom korisniku više nije dovoljan za stvaranje cjelokupnog javnog ključa. [17]

6. Budućnost

Daljnji rad na sustavu šifriranja temeljenom na identitetu sastojat će se od rada na unaprjeđenju njegovih teoretskih pretpostavki i koncepata te rada na unaprjeđenju i izvedbi učinkovitih praktičnih implementacija sustava.

Premda su objavljene teoretske osnove za razvoj IBE sustava šifriranja relativno sigurne, niti jedna od objavljenih shema ne može garantirati sto postotnu sigurnost osmišljenog algoritma. Novije i naprednije inačice osnovnih shema objavljuju se relativno često te se pretpostavlja kako će takav trend biti i nastavljen.

S druge strane, razvoj praktičnih implementacija IBE-a kreće se u smjeru otklanjanja ili zaobilaženja nekih od značajnijih nedostataka obrađenih u ovom dokumentu. S obzirom na velike mogućnosti koje sama ideja šifriranja temeljenog na identitetu sa sobom donosi, pitanje je samo trenutka kada će na tržištu biti objavljen učinkovit i, na kraju krajeva, popularan sustav koji će iskoristiti većinu njenih prednosti, a otkloniti osnovne nedostatke.

7. Zaključak

U ovom dokumentu predstavljen je IBE sustav šifriranja. Radi se o prilično zanimljivoj metodi asimetričnog šifriranja koja omogućuje uporabu bilo kojeg korisničkog podatka kao javnog ključa. Spomenut mehanizam nudi veliku fleksibilnost i jednostavnost u procesu upravljanja javnim i privatnim ključevima.

S obzirom na jednostavnost osnovnog koncepta zanimljivo je vidjeti kako se cjelokupni mehanizam temelji na složenim matematičkih shemama koje su dugo bile neotkrivene. Ipak, uz brojne prednosti ove metode šifriranja prisutni su i neki značajni nedostaci. Daljnji rad na razvoju cjelokupne tehnologije temeljit će se upravo na otklanjanju spomenutih nedostataka i stvaranju učinkovitog sustava koji će se koristiti samostalno ili kao potpora klasičnoj te vrlo popularnoj infrastrukturi javnog ključa.

8. Leksikon pojmova

Simetrično šifriranje

Metoda šifriranja koja se temelji na zajedničkom tajnom ključu poznatom stranama koje žele na siguran način razmjenjivati poruke preko javnog komunikacijskog kanala. Poruke se prije slanja šifriraju tajnim ključem. Po njihovu dospijeću primatelj ih dešifrira pomoću istog tog ključa. U teoriji, treća strana nije u mogućnosti otkriti sadržaj šifrirane poruke jer joj tajni ključ potreban za dešifriranje nije dostupan.

http://en.wikipedia.org/wiki/Symmetric-key_algorithm

Asimetrično šifriranje (šifriranje uporabom javnog ključa ili infrastrukture javnog ključa)

Metoda šifriranja osmišljena kako bi ispravila neke od nedostataka koji se javljaju kod metode simetričnog šifriranja. Osnovni je nedostatak svakako problem sigurnosti pohrane i distribucije zajedničkog tajnog ključa. Postupci asimetričnog šifriranja rješavaju taj problem tako što uvode par ključeva šifriranja za svakog od sudionika komunikacije. Par ključeva sastoji se od javnog i privatnog ključa. Privatni ključ dostupan je isključivo korisniku i ne smije se distribuirati. Javni ključ treba biti dostupan svima što podrazumijeva njegovu distribuciju (objavu) potencijalnim sugovornicima. Ideja je sljedeća: ono što se šifrira javnim ključem, može se dešifrirati samo privatnim, a ono što se šifrira privatnim, može se dešifrirati samo javnim ključem.

http://en.wikipedia.org/wiki/Public-key_cryptography

Šifriranje temeljeno na identitetu (eng. *Identity Based Encryption, IBE*)

Metoda asimetričnog šifriranja koja omogućuje uporabu bilo kakvog oblika informacije o samom korisniku, poput adrese elektroničke pošte, korisničkog imena, domene ili nekog drugog niza znakova, kao njegovog javnog ključa.

http://en.wikipedia.org/wiki/ID-based_encryption

Šifriranje temeljeno na certifikatima (eng. *certificate-based encryption*)

Sustav šifriranja u kojem entitet koji objavljuje certifikate (eng. Certificate Authority, CA) koristi IBE za stvaranje certifikata.

http://en.wikipedia.org/wiki/Certificate-based_encryption

Šifriranje temeljeno na sigurnoj dodjeli ključeva (eng. *secure key issuing cryptography*)

Inačica IBE šifriranja koja smanjuje razinu potrebnog povjerenja prema trećoj strani zaduženoj za stvaranje privatnih ključeva. Način na koji to ostvaruje je sljedeći: umjesto jednog entiteta koristi se više njih. Dodatno, korisnik šalje i tzv. maskirajuće podatke (eng. "*blinding" information*) kojima prikriva osjetljive informacije. Svaki od višestrukih entiteta zaduženih za generiranje privatnog ključa stvara tek jedan dio privatnog ključa, dok se svi dijelovi povezuju kod samog korisnika.

http://en.wikipedia.org/wiki/Secure_key_issuing_cryptography

Šifriranje bez certifikata (eng. *certificateless cryptography*)

Inačica IBE šifriranja ostvarena kako bi uklonila nedostatak vezan uz prisutnost korisničkih tajnih ključeva kod generatora privatnih ključeva. Postupak stvaranja privatnih ključeva ovdje je podijeljen između korisnika i entiteta zaduženog za stvaranje i dodjelu privatnih ključeva.

http://en.wikipedia.org/wiki/Certificateless_cryptography

9. Reference

[1] Chatterjee, S., Sarkar, P.: Identity-Based Encryption, 1st Edition, Springer, 2011. New York (NY), USA

[2] Boneh, D., Franklin, M.: Identity-Based Encryption from the Weil Pairing, SIAM J. Of Computing, Vol. 32, No. 3, 2001.

[3] Baek, J., Newmarch, J., Safavi-Naini, R., Susilo, W.: A Survey of Identity-Based Cryptography, School of Information Technology and Computer Science, University of Wollongang, School of Network Computing, Monash University, 2004.

[4] Wikipedia: ID-based encryption, http://en.wikipedia.org/wiki/ID-based_encryption, travanj 2011.

[5] Voltage Security: Building Applications Using Voltage Identity-Based Encryption, http://www.voltage.com/technology/securing-applications-using-IBE.htm, travanj 2011.

[6] Stanford IBE Security: IBE Secure E-mail, http://crypto.stanford.edu/ibe/, travanj 2011.

[7] Wikipedia: Weil pairing, http://en.wikipedia.org/wiki/Weil_pairing, travanj 2011.

[8] Wikipedia: Eliptic curve, http://en.wikipedia.org/wiki/Elliptic_curve, travanj 2011.

[9] Wikipedia: Finite fields, http://en.wikipedia.org/wiki/Finite_fields, travanj 2011.

[10] Wikipedia: Hash function, http://en.wikipedia.org/wiki/Hash_function, travanj 2011.

[11] Wikipedia: Quadratic residuosity problem, http://en.wikipedia.org/wiki/Quadratic_residuosity_problem, travanj 2011.

[12] Bethencourt, J.:Intro to Bilinear Maps, prezentacija, Carnegie Mellon University, Computer Sciences Department, 2011.

[13] Wikipedia: Quantum computer, http://en.wikipedia.org/wiki/Quantum_computer, travanj 2011.

[14] Wikipedia: Shor's algorithm, http://en.wikipedia.org/wiki/Shor%27s_algorithm, travanj 2011.

[15] Wikipedia: Certificate-based encryption, http://en.wikipedia.org/wiki/Certificate-based_encryption, travanj 2011.

[16] Wikipedia: Secure key issuing cryptography, http://en.wikipedia.org/wiki/Secure_key_issuing_cryptography, travanj 2011.

[17] Wikipedia: Certificateless cryptography, http://en.wikipedia.org/wiki/Certificateless_cryptography, travanj 2011.