ZAUPATI ALI NE ZAUPATI
Digitalni podpisi v kriptografiji, 4. del

Pred petdesetimi leti je imel le malokdo doma telefon, danes pa redkokateri učenec med poukom ne pogleda s svojim mobilcem na Internet (npr. Facebook). Tako se nam vsaj navidezno zdi, da smo obkroženi s številnimi prijatelji. Pa vendar so ljudje že davno prišli do zaključka, da so človeški možgani sposobni res dobro razumeti največ 150 posameznikov in odnosov med njimi (npr. Robin Dunbar iz univerze v Liverpoolu). Tudi v podjetjih in vojski se število 150 izkaže za kritično, kadar je obravnavana najmanjšo neodvisno enoto. Kadar se npr. z neko disciplino ukvarja več kot 200 raziskovalcev, se običajno le-ta razcepi na dve ali več podpodročij. V vaseh, ki štejejo čez 500 prebivalcev, se torej že pojavlja anonimnost, da o večjih mestih niti ne govorimo. V današnjem času interneta in potrošniške družbe bo zato vse pogosteje prihajalo do komuniciranja med ljudmi (celo med napravami), ki se ne poznajo. Kako si torej lahko zaupata dva, ki sta se začela pogovarjati preko mreže?

V tretjem delu [3] smo predstavili koncept *kriptosistemov z javnimi ključi*, ki so ga leta 1976 odkrili W. Diffie, M. Hellman in R. Merkle (zadnji je bil takrat še študent), in tudi idejo *digitalnega podpisa*. V tem sestavku bomo predstavili konkreten kriptografski protokol, ki omenjeno idejo uvaja v prakso. Po razmisleku o lastnostih lastnoročnega in digitalnega podpisa bomo opisali Elgamalovo shemo za digitalni podpis, ki je poleg RSA sheme [5] v praksi najbolj razširjena.

V bistvu se način zapisovanja informacij ni drastično spremenil. Medtem ko smo prej shranjevali in prenašali informacije na papirju, jih sedaj hranimo na diskih in v drugih elektronskih/magnetnih medijih ter jih prenašamo preko omrežij. Bistveno pa se je spremenila možnost kopiranja, prenašanja in spreminjanja informacij. Zlahka naredimo na tisoče kopij neke digitalne informacije in jih v trenutku spravimo na različne konce sveta, pri tem pa se nobena kopija prav nič ne razlikuje od originala. Z informacijo na papirju je bilo vse to precej težje, če že ne nemogoče. Poskrbeti moramo, da bo varnost informacij neodvisna od fizičnega medija, ki jih je zapisal ali prenesel. Temeljiti mora izključno na digitalni vsebini, tj. številkah. Zato zna biti današnja tema zanimiva tudi za nas, Presekovce.

Eno izmed osrednjih orodij za zaščito informacij je *podpis*. Le-ta preprečuje poneverjanje in je dokaz o izvoru, identifikaciji, pričanju. Podpis naj bi bil unikat vsakega posameznika, saj se z njim predstavljamo, nekaj potrjujemo, nekoga pooblaščamo,...

> *Z digitalnim podpisom potrjujemo izvor podatkov ali pa nekoga prepričamo, da je podpis opravil lastnik ustreznega zasebnega ključa.*

Z razvojem digitalne informacije moramo ponovno obdelati bistvo podpisa. S pravo idejo lahko vplivamo na tok zgodovine, saj ni rečeno, da ne bi mogli dodati še kakšne nove lastnosti, na

katero doslej še nihče ni pomislil, le-ta pa bi lahko nam vsem spremenila življenja oziroma vsaj navade.

(STARI) LASTNOROČNI PODPIS

Na podiplomskem študiju mi je moral mentor na začetku vsakega semestra podpisati formular, na katerem so bili vpisani predmeti, ki sem si jih izbral za tisti semester. Ko sem že dobil podpis, sem na seznamu sosednjega oddelka za računalništvo zagledal še dva zanimiva predmeta. Opazil sem, da je v formularju prostor ravno še zanju in ju vpisal. Pa vendar sem pomislil tudi na to, da tak način morda ni ustrezen in sem mentorja obvestil o spremembi. Izkazalo se je, da bi ga moral v resnici še enkrat prositi za odobritev, ne pa samo obvestiti. In zato ni bil nič kaj zadovoljen, da sploh lahko pride do takšnih zapletov. Kakšno leto kasneje sem izvedel, da mentorji dobijo kopije študentskih formularjev neposredno iz pisarne, kamor smo jih oddajali.

Pogled v bližnjo prihodnjost nam razkrije še nekaj pomanjkljivosti lastnoročnega podpisovanja:

J: "Danes sem dobil podpis v šoli," pove Janezek sestri.
S: "Kakšno neumnost si pa zopet naredil?"
J: "Te nič ne briga, raje mi svetuj, kako naj prelisičim mamo."
S: "Nad učiteljev podpis skopiraj obvestilo o športnem dnevu."
J: "Odlična ideja, na ta način se bom zlahka rešil zagate,
pa še smučat grem, namesto da bi šel v šolo."

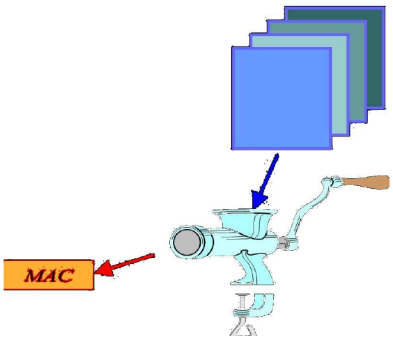
Janezek to naredi in mama pod digitalno obvestilo o smučarskem dnevu pripne svoj "digitalni" podpis. Preden pa ga Janezek na ključku odnese v šolo, zopet zamenja obvestilo o športnem dnevu s prejšnjim tekstom. V resnici je škoda za starše še večja, saj ima sedaj Janezek mamin "digitalni" podpis in ga bo odslej lahko izrabljal po mili volji. V času elektronskih medijev je zato izredno nevarno podpis skenirati (posneti) oziroma sprejemati skenirane podpise, ki so v resnici le posnetki. Postopek digitalnega podpisa mora biti dobro premišljen, saj moramo preprečiti spreminjanje vsebine podpisanega sporočila in ponarejanje oziroma kopiranje podpisa. Zgoraj opisani digitalni podpis ni več unikat, ki enolično določa podpisnika. Z lahkoto ga kopiramo oziroma dodamo na poljuben dokument. Potrebujemo protokole, ki imajo podobne lastnosti kot trenutni "papirni protokoli". Današnja družba ima enkratno priložnost, da vpelje nove in še učinkovitejše načine, ki nam bodo zagotovili boljšo varnost informacij.

Digitalni podpis naj bi bil nadomestek za lastnoročni podpis
pri elektronski izmenjavi in digitalnemu hranjenju podatkov.
Nastopa kot število oziroma še bolj splošno kot zaporedje bitov.

Digitalni podpis mora imeti vse dobre lastnosti, ki veljajo za lastnoročni podpis, poleg tega pa mora veljati, da vsebine digitalno podpisanega dokumenta ni mogoče spreminjati in podpisa ni mogoče kopirati in ponarejati. Obe obliki podpisovanja pa imata še nekaj pomembnih lastnosti:

- Lastnoročni podpis je fizično del podpisanega dokumenta.
- Lastnoročni podpis preverjamo s primerjanjem, digitalnega pa z algoritmom, ki ga izvaja računalnik. Rezultat tega preverjanja je odvisen od ključa ter dokumenta, ki smo ga podpisali.
- Digitalnega podpisa ne moremo razlikovati od njegove kopije, zato si želimo podpis, ki bo vedno drugačen (četudi podpišemo isto stvar).

Povedali smo že, da je digitalni podpis odvisen od dokumenta, ki ga podpisujemo. Ker pa so dokumenti poljubno veliki, običajno iz dokumenta skonstruiramo izvleček fiksne dolžine (lahko bi mu rekli tudi prstni odtis) in nato podpišemo le-tega. Tokrat se ne bomo spuščali v podrobnosti teh postopkov, ki jim rečemo *zgoščevalne funkcije*, pač pa omenimo le, da je mogoče priti do izvlečka z bločnimi simetričnimi šiframi, ki smo jih spoznali v prvem delu [1], glej tudi 2. in 3. nalogo.



(NOVI) DIGITALNI PODPIS

Shema za digitalni podpis je sestavljena iz treh delov:

- iz algoritma za generiranje ključa,
- algoritma za generiranje digitalnega podpisa in
- algoritma za preverjanje digitalnega podpisa.

Za lažje razumevanje definirajmo nekaj osnovnih pojmov.

- Pravilo $\texttt{sgn}_{Z(A)}$, ki sporočilo podpiše (angl. sign), imenujemo *funkcija za podpis* osebe A. Zasebni ključ $Z(A)$ varuje oseba A in ga uporablja le za podpisovanje dokumentov.
- Pravilu $\texttt{ver}_{J(A)}$, ki za dokument in njegov podpis preveri oz. verificira (angl. verify), tj. priredi vrednost "veljaven" oziroma "neveljaven", rečemo *funkcija za preverjanje podpisov* osebe A. Javni ključ $J(A)$ pripada osebi A, a je vseeno javno znan. "Tretja" oseba uporablja $\texttt{ver}_{J(A)}$ za preverjanje podpisov, ki jih je opravila oseba A.

Postopek pošiljanja digitalno podpisanega sporočila med Anito in Bojanom je naslednji:

1. Najprej si Bojan izbere svoj zasebni ključ $Z(B)$ ter sporoči Aniti ustrezni javni ključ $J(B)$.
2. Za podpis sporočila x, Bojan uporabi algoritem za generiranje digitalnega podpisa s svojim zasebnim ključem $Z(B)$ in izračuna podpis $\texttt{sgn}_{Z(B)}(x)$. Nato ga skupaj s sporočilom pošlje Aniti.
3. Če Anita pozna Bojanov javni ključ $J(B)$, lahko uporabi algoritem za preverjanje digitalnega podpisa $\texttt{ver}_{J(B)}$ ter tako preveri pristnost podpisa.

Vrstni red šifriranja in digitalnega podpisovanja je pomemben.

(a) Če hoče Anita poslati Bojanu podpisano, zašifrirano sporočilo, potem danemu čistopisu x najprej izračuna svoj podpis $y = \texttt{sgn}_{Z(A)}(x)$, nato zašifrira x in y z Bojanovo javno šifrirno funkcijo $e_{J(B)}$ in dobi $z = e_{J(B)}(x, y)$. Tajnopis z pošlje Bojanu. Ta ga odšifrira s svojo zasebno odšifrirno funkcijo $d_{Z(B)}$ in dobi par (x, y). Potem uporabi Anitino javno funkcijo $\texttt{ver}_{J(A)}$, da preveri, ali je $\texttt{ver}_{J(A)}(x, y) =$ veljaven.

(b) Če pa bi Anita najprej zašifrirala sporočilo x in potem podpisala rezultat, bi izračunala $z = e_{J(B)}(x)$ in $y = \texttt{sgn}_{Z(A)}(z)$ ter par (z, y) poslala Bojanu. Bojan bi z odšifriranjem tajnopisa z dobil $x = d_{Z(B)}(y)$, nato bi preveril podpis y na x z uporabo funkcije $\texttt{ver}_{J(A)}$. Če prestreže takšen par (z, y) Oskar, nastane problem, saj lahko zamenja Anitin podpis s svojim $y' = \texttt{sgn}_{Z(O)}(z)$, čeprav ne pozna čistopisa x. Ko pošlje par (z, y') Bojanu, bi ta lahko mislil, da mu je sporočilo x poslal Oskar.

Zato priporočamo najprej podpisovanje in nato šifriranje sporočil, glej 4. nalogo.

Če veljata naslednji dve lastnosti:

- Anita je edina, ki lahko podpiše sporočilo, torej edina, ki zna pri danem x izračunati y, tako da je $\texttt{ver}_{Z(A)}(x, y) =$ veljaven,
- Bojan se je sposoben prepričati, ali gre za Anitin podpis ali pa gre za ponaredek,

potem rečemo, da je algoritem digitalnega podpisa *varen*. V naslednjem razdelku bomo predstavili konkretne opise funkcij `sgn` in `ver`, ki ju smatramo za varne.

ELGAMALOV DIGITALNI PODPIS

Opišimo Elgamalovo shemo za digitalni podpis (1985), ki temelji na težavnosti *problema diskretnega logaritma* (oznaka DLP) v grupi $\mathbb{Z}_p^*$ in Diffie-Hellmanovega dogovora o ključu, ki smo ju opisali v drugem delu [2]. Spomnimo se, da smo za praštevilo p z $\mathbb{Z}_p$ označili obseg z elementi $\{0, 1, \ldots, p-1\}$ in operacijama $+_p, *_p$, kjer oznaka p pri $+$ in $*$ pomeni, da običajno vsoto oziroma produkt nadomestimo z ustreznim ostankom pri deljenju s p. V $\mathbb{Z}_p$ vedno obstaja tak element α, ki generira multiplikativno grupo $\mathbb{Z}_p^* = (\{1, \ldots, p-1\}, *_p)$, tj. množica $\{\alpha^0, \alpha^1, \ldots, \alpha^{p-2}\}$ pokrije vse elemente v $\mathbb{Z}_p^*$. DLP v $\mathbb{Z}_p^*$ je, da za dani generator α in $\beta = \alpha^a$, kjer je a neko naravno število, iščemo učinkovit način (algoritem) za izračun števila a.

ELGAMALOV ALGORITEM.

Priprava: *naj bo p tako praštevilo, da je v obsegu $\mathbb{Z}_p$ težko rešiti DLP in α generator grupe $\mathbb{Z}_p^*$.*

Generiranje ključev: *za (skriti) zasebni ključ $a \in \{0, \ldots, p-1\}$ izračunaj javni ključ $\beta = \alpha^a \bmod p$.*

Podpisovanje: *za sporočilo $x \in \{0, \ldots, p-2\}$ izberi naključno skrito naravno število $k \leq p-2$, tako da je $D(k, p-1) = 1$, nato pa z zasebnim ključem a izračunaj $\mathtt{sgn}_a(x, k) = (\gamma, \delta)$, kjer je*

$$\gamma = \alpha^k \bmod p \qquad \text{in} \qquad \delta = (x - a\gamma)k^{-1} \bmod (p-1).$$

Preverjanje podpisa (γ, δ) *sporočila x z javno trojico (p, α, β):*

$$\mathtt{ver}_\beta(x, \gamma, \delta) = \text{veljaven} \iff \beta^\gamma \gamma^\delta \equiv \alpha^x \pmod p.$$

Taher Elgamal (iz Egipta).

Pierre de Fermat je poznan tudi po naslednjemu izrek [4]:

Za praštevilo p in $a \in \mathbb{Z}_p^*$ velja $a^{p-1} \equiv 1 \pmod p$.

Za pravilnost preverjanja glej 5. nalogo. Zgornji podpis je nedeterminističen (odvisen od naključnega števila k), torej sploh ni natanko določen. Če torej isti dokument podpišemo vsaj dvakrat, bo z veliko verjetnostjo podpis vsakič drugačen. Poudarimo tudi, da podpisnik izračuna podpis z uporabo tako tajne vrednosti a, ki je del ključa, kot tajnega naključnega števila k, ki se sme uporabiti samo za podpis *enega* sporočila x (preverjanje pa je opravljeno samo z uporabo javnih informacij). Če namreč naključno število k ne ostane skrito, ali pa se isto število k uporabi v podpisih dveh različnih sporočil (v tem primeru ga je možno zlahka izračunati), lahko napadalec iz druge enačbe algoritma za podpisovanje izračuna tajno vrednost a in ponaredi podpis. Glej 6. in 7. nalogo. Elgamalovo shemo za podpis smatramo za varno. Do danes namreč še nikomur ni uspelo učinkovito izračunati par (γ, δ) brez računanja diskretnega logaritma. Lahko pa se zgodi, da bomo nekoč ugotovili, da se pri iskanju para (γ, δ) problemu diskretnega logaritma sploh ne moremo izogniti.

Kako bi lahko ponaredili podpis, ne da bi vedeli za vrednost skritega števila a?

(a) Za dano sporočilo x poišči tak par (γ, δ), da bo veljalo $\beta^\gamma \gamma^\delta \equiv \alpha^x \pmod p$:

- če izberemo γ, rabimo $\delta = \log_\gamma \alpha^x \beta^{-\gamma} \pmod p$,
- če izberemo δ, je potrebno rešiti enačbo $\beta^\gamma \gamma^\delta \equiv \alpha^x \pmod p$ po γ,
- hkrati računamo γ in δ

  (zaenkrat ni še nihče odkril hitrega postopka za reševanje zgornje enačbe).

(b) Za podpis (γ, δ) poišči ustrezno sporočilo x, tj. izračunaj: $x = \log_\alpha \beta^\gamma \gamma^\delta \pmod p$.

Omenimo še, da so Elgamalov digitalni podpis temeljito preučili tudi v ZDA, kjer na državnem nivoju neradi plačujejo patente (RSA je bil namreč takrat še patentiran). Na njegovi osnovi so sestavili Digital Signature Algorithm (DSA), ki ga je National Institute of Standards and Technology (NIST) sprejel za ameriški standard: Digital Signature Standard (DSS). Danes je vključen v večino varnostnih standardov.

NALOGE

1. RSA-podpis, ki je opisan v [5], je za razliko od Elgamalovega deterministični. Kako bi ga lahko spremenili v nedeterminističnega? Varnostno analiziraj svoj predlog.
2. Kakšne lastnosti naj ima zgoščevalna funkcija, da ne bo ogrožena varnost podpisa?
3. S prijateljem drug drugemu predlagajta način, s katerim bi iz dokumenta poljubne dolžine z bločno šifro skonstruirali izvleček fiksne dolžine, nato pa poskusita prijateljeve predloge analizirati.
4. V razdelku o digitalnem podpisu smo omenili šifrirno funkcijo $e_{J(B)}$, ki jo uporabi Anita, in Bojanovo odšifrirno funkcijo $d_{Z(B)}$. Elgamal je predlagal taki funkciji na osnovi DLP. Če je sporočilo m iz grupe G, ki je generirana z α, potem Anita izbere naključno naravno število k, ki je manjše od števila elementov v grupi G, ter z njim in Bojanovim javnim ključem $\beta = \alpha^b$ izračuna par $(\alpha^k, m\beta^k)$ ter ga pošlje Bojanu. Opiši odšifrirno funkcijo.
5. Prepričaj se, da je opisano preverjanje Elgamalovega podpisa pravilno. (Namig: pomagaj si s Fermatovim izrekom, da bo jasno, zakaj računamo δ po modulu $p-1$.)
6. Podpisovalec ni bil pazljiv in je ponesreči izgubil naključno število k, ki ga je uporabil pri Elgamalovem podpisu. Uporabi njegovo napako za izračun zasebnega ključa a.
7. Generator naključnih števil je tako počasen, da se je podpisovalec odločil uporabiti število k dvakrat. Ali lahko uporabiš njegovo napako za izračun zasebnega ključa a?
8.* Predlagaj novo varianto Elgamalovega podpisa, kjer ne bomo več potrebovali računanja inverza (k^{-1}), ki ga ponavadi izračunamo z razširjenim Evklidovim algoritmom.
9. Hkratno računanje vrednosti x, γ in δ: naj bosta i in j takšni števili, da velja $0 \le i, j \le p-2$ in $D(j, p-1) = 1$. Prepričaj se, da potem števila

$$\gamma \equiv \alpha^i \beta^j \pmod{p}, \qquad \delta \equiv -\gamma j^{-1} \pmod{p-1} \quad \text{in} \quad x \equiv -\gamma i j^{-1} \pmod{p-1}$$

   zadoščajo enačbi za preverjanje Elgamalovega podpisa: $\beta^\gamma \gamma^\delta \equiv \alpha^x \pmod{p}$.
10.* Ali lahko pri veljavnem podpisu (γ, δ) za x najdemo še kakšen podpis za kakšno drugo sporočilo x'?

   (Postaviti na konec Preseka.) Odg. je "DA". Naj bodo h, i in j takšna števila, da velja $0 \le h, i, j \le p-2$ in $D(h\gamma - j\delta, p-1) = 1$. Potem se prepričaj, da je par (λ, μ) veljaven podpis za x', kjer je

$$\lambda = \gamma^h \alpha^i \beta^j \bmod p, \quad \mu = \delta\lambda(h\gamma - j\delta)^{-1} \bmod p-1 \quad \text{in} \quad x' = \lambda(hx + i\delta)(h\gamma - j\delta)^{-1} \bmod p-1.$$

V drugem razdelku je v tretji točki "ČE", zaradi katerega še nismo povsem rešili problema identifikacije Bojana. Ta se je le prenesla na prepoznavanje Bojanovega javnega ključa. Če se morata Anita in Bojan prej sestati, da bi si izmenjala javna ključa, potem bi se lahko ob tej priložnosti dogovorila za skupen ključ za kakšno simetrično šifro. Več o tem, kako lahko s certifikati in z infrastrukturo javnih ključev rešimo ta problem, pa v zadnjem (5.) delu.

Aleksandar Jurišić in Jasmina Veselinović