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

Pred pedesetimi leti je imel le malokdo doma telefon, danes pa redko kateri učenec med poukom še ni pogledal s svojim mobilcem na Facebook ali katero podobno omrežje. Na ta način se nam vsaj navidezno zdi, da smo obkroženi s stotinami prijateljev. Pa vendar so ljudje že daleč nazaj prišli do zaključka, da so človeški možgani sposobni res dobro razumeti največ 150 posameznikov in odnosov med njim. (npr. Robin Dunbar iz univerze v Liverpoolu). Tudi v podjetjih in vojski se je število 150 izkazalo za kritično, ko se obravnava najmanjšo neodvisno enoto. Ko se npr. z neko disciplino ukvarja več kot 200 raziskovalcev, se običajno 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 bolj pogosto prihajalo do komuniciranja med ljudmi (oziroma celo napravami), ki se ne poznajo. Kako si lahko torej 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 (slednji je bil takrat še študent!). Ob njem smo predstavili tudi idejo **digitalnega podpisa**. V tem sestavku bomo predstavili konkreten kriptografski protokol, ki omenjeno idejo spravi v prakso. Po razmisleku o lastnostih lastnoročnega in digitalnega podpisa bomo opisali ElGamalovo shemo za digitalni podpis, ki je poleg RSA sheme [5] najbolj razširjena v praksi.

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 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 od kopij 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 pri zaščiti 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 predstavimo, nekaj potrdimo, nekoga pooblastimo,...

> *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

vplivate na tok zgodovine, saj ni rečeno, da ne bi mogli dodati še kakšno novo lastnost, na katero doslej še nihče ni pomislil, le-ta pa bi posledično vsem nam spremenila življenja oziroma vsaj navade.

(STARI) LASTNOROČNI PODPIS

Na podiplomskem študiju sem moral dajati svojemu mentorju na začetku vsakega semestra za podpisat formular na katerem so bili vpisani predmeti, ki sem si jih izbral za tisti semester. Kakšen dan potem, ko sem že dobil podpis, sem na seznamu sosednjega oddelka (računalništvo) zagledal še dva zanimiva predmeta. Opazil sem, da je v formularju prostor ravno še za dva predmeta in ju hitro vpisal. Pa vendar sem pomislil tudi na to, da čeprav v načelu že imam mentorjev podpis, tak način vseeno ni pravi in ga obvestiti o spremembi. Izkazalo pa se je, da bi ga moral v resnici še enkrat prositi za odobritev, ne pa samo obvestiti. In res, ni bil nič kaj zadovoljen, da lahko do takšnih zapletov sploh pride. Kakšno leto kasneje sem zaznal, 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 lahko, namesto da bi šel v šolo."

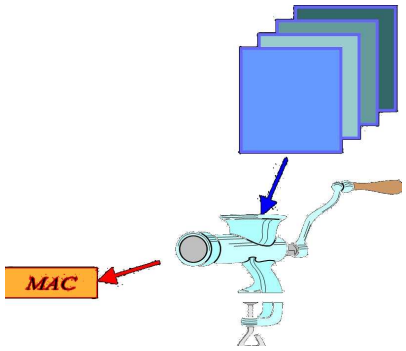
Janezek to naredi in mama pod digitalno obvestilo o smučarskem dnevu pripne svoj "digitalni" podpis. Preden pa ga na ključku odnese v šolo, Janezek zopet zamenja obvestilo o športnem dnevu s starim tekstom. V resnici je škoda za starše še večja, saj ima sedaj Janezek mamin "digitalni" podpis in ga bo odslej lahko uporabljal po mili volji. V času elektronskih medijev je zato izredno nevarno podpis skenirati (posneti) oziroma sprejemati skenirane podpise, ki so v resnici le njihovi posnetki. Kot kaže, mora biti postopek digitalnega podpisa 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 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:

- navadni podpis je fizično del podpisanega dokumenta;
- navadni 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 in nato podpišemo le-tega. Tokrat se ne bomo spuščali v podrobnosti teh postopkov, ki jim rečemo *zgoščevalne funkcije*, pač pa omenimo le da se da priti do izvlečka z bločnimi simetričnimi šiframi, ki smo jih spoznali v prvem delu [1].



(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 $\texttt{sgn}_A$, ki sporočilo podpiše (angl. sign), imenujemo *funkcija za podpis* osebe A. Ključ zanjo varuje oseba A in jo uporablja za podpisovanje dokumentov.
- Pravilu $\texttt{ver}_A$, ki za dokument in njegov podpis preveri oz. verificira (angl. verify), tj. priredi vrednost "veljaven" oziroma "neveljaven", rečemo *funkcija za preverjanje podpisov* osebe A. Ključ zanjo pripada osebi A, a je vseeno javno znan. Uporablja se za preverjanje podpisov, ki jih je opravila oseba A.

Postopek pošiljanja digitalno podpisanega sporočila med Anito in Bojanom je sledeč.

1. Najprej si Bojan izbere svoj zasebni ključ ter sporoči Aniti ustrezni javni ključ.
2. Da bi podpisal sporočilo x, Bojan uporabi algoritem za generiranje digitalnega podpisa s svojim zasebnim ključem in izračuna podpis $\texttt{sgn}_B(x)$.
3. Nato pošlje sporočilo skupaj z njegovim digitalnim podpisom Aniti.
4. Če Anita pozna Bojanov javni ključ, lahko uporabi algoritem za preverjanje digitalnega podpisa $\texttt{ver}_B$ ter tako preveri pristnost podpisa.

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

Če pa bi Anita najprej zašifrirala sporočilo x in potem podpisala rezultat, bi izračunala $z = e_{Bojan}(x)$ in $y = \texttt{sgn}_{Anita}(z)$ ter par (z, y) poslala Bojanu. Bojan bi z odšifriranjem tajnopisa z dobil x, nato bi preveril podpis y na x z uporabo funkcije $\texttt{ver}_{Anita}$. V tem primeru pride do problema, če Oskar prestreže takšen par (z, y), saj lahko zamenja Anitin podpis s svojim $y' = \texttt{sgn}_{Oskar}(z)$, čeprav ne pozna čistopisa x. Ko pošlje (z, y') Bojanu, bo ta mislil, da mu je sporočilo x poslal Oskar. Zato se priporoča najprej podpisovanje in nato šifriranje sporočil.

Če veljata naslednji dve lastnosti:

- Anita je edina, ki lahko podpiše sporočilo, torej edina, ki zna pri danem x izračunati y, tako da je $\texttt{ver}_{Anita}(x, y) = \text{veljaven}$,
- 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 si bomo predstavili konkretne opise funkcij `sgn` in `ver`, ki ju smatramo za varne.

ELGAMALOV DIGITALNI PODPIS

Opišimo shemo za podpis, ki temelji na težavnosti problema diskretnega logaritma (tj. da je v končni grupi, ki je generirana z elementom α za dana α in $\beta = \alpha^x$, za neko naravno število x, težko poiskati x) in Diffie-Hellmanovega dogovora o ključu, ki smo ga opisali v drugem delu [2]. Leta 1985 jo je razvil Taher ElGamal.

ElGamalov algoritem. *Naj bo p tako praštevilo, da je v obsegu $\mathbb{Z}_p = (\{0, 1, \ldots, p-1\}, +_p, *_p)$ težko izračunati diskretni logaritem in α generator multiplikativne grupe $\mathbb{Z}_p^* = (\{1, \ldots, p-1\}, *_p)$, tj. množica $\{\alpha^0, \alpha^1, \ldots, \alpha^{p-2}\}$ pokrije vse elemente v $\mathbb{Z}_p^*$. Naj bo še $\mathcal{P} = \mathbb{Z}_p^*$ množica sporočil in*

$$\mathcal{K} = \{(p, \alpha, a, \beta);\ \beta = \alpha^a \bmod p\} \quad \text{množica ključev.}$$

Število a je skrito (zasebno), števila p, α in β pa so javno znana.

Podpisovanje: *podpisnik izbere naključno skrito število $k \in \mathbb{Z}_{p-1}^*$ in s ključem $K = (p, \alpha, a, \beta)$ izračuna $\mathtt{sgn}_K(x, k) = (\gamma, \delta)$, kjer je*

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

Preverjanje podpisa *(samo z javnimi števili p, α in β):*

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

Slika 1: Taher ElGamal.

Slika 2: Pierre de Fermat je poznan tudi po naslednjemu izrek [4]:

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

Zgornji podpis je nedeterminističen (odvisen od naključnega števila k), torej sploh ni natanko določen. Če torej isto stvar 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. 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 enkrat 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 je potrebno najti 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: glede na γ je potrebno rešiti enačbo $\beta^\gamma \gamma^\delta \equiv \alpha^x \pmod p$,
- hkrati računamo γ in δ (zaenkrat ni še nihče odkril hitrega postopka za reševanje zgornje enačbe).

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

NALOGE

1. RSA-podpis, ki je opisan v [5], je za razliko od ElGamalovega deterministično. Kako bi ga lahko spremenili v nedeterminističnega?
2. S prijateljem drug drugemu predlagajta kakšne način s katerim bi iz dokumenta poljubne dolžine z bločno šifro skonstruirali izvleček fiksne dolžine, nato pa poskusita predloge drug drugemu analizirati.
3. Prepričaj se, da je opisano preverjanje ElGamalovega podpisa pravilno! (Namig: pomagaj si s Fermatovim izrekom, da bo jasno zakaj računamo δ po modulu $p-1$.)
4. Podpisovalec ni bil pazljiv in je ponesreči izgubil naključno število k, ki ga je uporabil pri ElGamalovem podpisu. Uporabi njegovo napako za izračun zasebnega kluča a?
5. Generator naključnih števila je tako počasen, da se je podpisovalec odločil uporabiti število k dvakrat. Uporabi njegovo napako za izračun zasebnega kluča a?
6. 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: $\beta^\gamma \gamma^\delta \equiv \alpha^x \pmod{p}$.
7. Predlagaj novo varianto ElGamalovega podpisa, kjer ne bomo potrebovali več računanja inverza k^{-1} (ki ga ponavadi izračunamo z razširjenim Evklidovim algoritmom).
8. Ali lahko pri veljavnem podpisu (γ, δ) za x najdemo še kakšen podpis za neko drugo sporočilo x'?

   Odg. je "DA": Naj bodo h, i in j takšna števila, da zanje 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 četrti točki en "ČE", zaradi katerega še nismo povsem rešili problema identifikacije Bojana - le-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. Kako lahko rešimo ta problem?

Viri in dodatno branje

[1] A. Jurišić in U. Perko, Klasične šifre in zdravstvena kartica, prvi del, *Presek* **33**/1 (2005-06), str. 22–24

[2] A. Jurišić, Diffie-Hellmanov dogovor o ključu, drugi del, *Presek* **34** (2006-07), str. 25–30.

[3] A. Jurišić, Poštni nabiralnik in kriptografski protokoli, kriptosistemi z javnimi ključi, tretji del, *Presek* **36**/2 (2008-09), 22–26.

[4] D. Pagon, Kongruence in Eulerjev izrek, *Presek* **15**/4 (1987/88), str. 194–196.

[5] M. Vencelj, Šifriranje z javnim ključem, *Presek* **22**/6 (1994-05), str. 354-357.

Aleksandar Jurišić in Jasmina Veselinović