6. poglavje

Sheme za digitalne podpise

- uvod (podpis z RSA sistemom)
- ElGamalov sistem za digitalno podpisovanje
- Digital Signature Standard
- napadi
- enkratni podpis
- podpisi brez možnosti zanikanja
- Fail-stop podpisi

Digitalni podpis je nadomestek za lastnoročni podpis pri elektronski izmenjavi in digitalnemu hranjeju podatkov.

Konceptualno se način zapisovanja informacij ni dramatično spremenil.

Medtem ko smo prej shranjevali in prenašali informacije na papirju, jih sedaj hranimo na magnetnih in drugih medijih ter jih prenašamo preko telekomunikacijskih sistemov (tudi brezžičnih).

Bistveno pa se je spremenila možnost kopiranja in spreminjanja informacij.

Zlahka naredimo na tisoče kopij neke informacije, ki je shranjena digitalno, pri tem pa se nobena ne razlikuje od originala.

Z informacijo na papirju je to precej težje.

Družba, v kateri so informacije spravljene in prenašane v digitalni obliki, mora poskrbeti za to, da ne bo varnost informacij odvisna od fizičnega medija, ki jih je zapisal ali prenesel.

Varnost informacij mora temeljiti izključno na digitalni informaciji.

Eno izmed osrednjih orodij pri zaščiti informacij je **podpis**. Le-ta preprečuje poneverjanje, je dokaz o izvoru, identifikaciji, pričanju.

Podpis naj bi bil unikat vsakega posameznika, z njim se predstavimo, potrdimo, pooblastimo.

Z razvojem digitalne informacije moramo ponovno obdelati tudi koncept podpisa.

Ni več unikat, ki enolično določa podpisnika, kajti elektronsko kopiranje podpisa je tako lahko, da je skoraj trivialno na nepodpisan dokument pripeti poljuben podpis.

Potrebujemo protokole, ki imajo podobne lastnosti kot trenutni "papirni protokoli".

Družba ima enkratno priložnost, da vpelje nove in učinkovitejše načine, ki nam bodo zagotovili varnost informacij.

Veliko se lahko naučimo iz dosedanjih sistemov, obenem pa moramo odpraviti tudi številne pomanjkljivosti.

Primerjava digitalnega in navadnega (lastnoročnega) podpisa:

- navadni podpis je fizično del podpisanega dokumenta;
- navadni podpis preverjamo s primerjanjem, digitalnega z algoritmom, katerega rezultat je odvisen od ključa in dokumenta;
- kopija digitalnega podpisa je identična originalu;
- digitalni podpis je odvisen od dokumenta, ki ga podpisujemo.

Sistem za digitalno podpisovanje je peterka $(\mathcal{P}, \mathcal{A}, \mathcal{K}, \mathcal{S}, \mathcal{V})$, za katero velja

1. $\mathcal{P}$ je končna množica sporočil,
2. $\mathcal{A}$ je končna množica podpisov,
3. $\mathcal{K}$ je končna množica ključev,
4. $\forall$ ključ $K \in \mathcal{K}$ obstaja algoritem za podpisovanje
$$\mathrm{sig}_K \in \mathcal{S}, \quad \mathrm{sig}_K : \mathcal{P} \to \mathcal{A}$$
in algoritem za preverjanje podpisa
$$\mathrm{ver}_K \in \mathcal{V}, \quad \mathrm{ver}_K : \mathcal{P} \times \mathcal{A} \to \{\mathrm{true}, \mathrm{false}\}.$$

Funkciji sig_K in ver_K imata to lastnost, da za vsako sporočilo $x \in \mathcal{P}$ in vsak podpis $y \in \mathcal{A}$ velja

$$\mathrm{ver}_K(x, y) = \begin{cases} \text{true}, & \text{če } y = \mathrm{sig}_K(x) \\ \text{false}, & \text{če } y \neq \mathrm{sig}_K(x) \end{cases}$$

Zahteve:

- algoritma sig_K in ver_K imata polinomsko časovno zahtevnost
- sig_K je znan le podpisniku
- ver_K je splošno znan
- računsko mora biti nemogoče ponarediti podpis

Primer: Algoritem RSA lahko uporabimo tudi za podpisovanje. Naj bo $n = pq$, kjer sta p in q praštevili.

Če je (n, d) skriti ključ, (n, e) pa javni, pri čemer je $de \equiv 1 \pmod{\varphi(n)}$, potem definiramo:

$$\mathrm{sig}_K(x) = d_K(x) = x^d \bmod n$$

$$\mathrm{ver}_K(x, y) = \text{true} \iff x = e_K(y) = y^e \bmod n$$

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

Z zgornjim algoritmom je mogoče ponarediti podpis naključnih sporočil.

Ponarejevalec najprej izbere podpis y in nato izračuna

$$x \equiv y^e \pmod{n}.$$

Možnosti takega ponarejanja se izognemo z

- enosmernimi zgoščevalnimi funkcijami ali
- zahtevo, da ima sporočilo x določen pomen.

Pošiljanje podpisanih tajnih sporočil

Vrstni red šifriranja in digitalnega podpisovanja je pomemben.

1. Najprej podpisovanje:
$$x, \mathrm{sig}_{\mathrm{Anita}}(x) \rightarrow e_{\mathrm{Bojan}}((x, \mathrm{sig}_{\mathrm{Anita}}(x))).$$
2. Najprej šifriranje $z = e_{\mathrm{Bojan}}(x)$, potem podpis $y = \mathrm{sig}_{\mathrm{Anita}}(z)$:

   Bojan prejme (z, y), odšifrira tajnopis $x = d_{\mathrm{Bojan}}(z)$ ter preveri podpis $\mathrm{ver}_{\mathrm{Anita}}(z, y)$.

V drugem primeru lahko napadalec Cene zamenja Anitin podpis s svojim:

$$y' = \mathrm{sig}_{\mathrm{Cene}}(z) \rightarrow (z, y') \rightarrow x = d_{\mathrm{Bojan}}(z), \quad \mathrm{ver}_{\mathrm{Cene}}(z, y')$$

in Bojan bo mislil, da je sporočilo prišlo od Ceneta.

Zato se priporoča najprej podpisovanje in nato šifriranje.

V primeru algoritma RSA je potrebno pri zaporednem podpisovanju in šifriranju paziti na velikosti modulov (*reblocking problem*).

Če je $n_{\mathrm{Anita}} > n_{\mathrm{Bojan}}$, se lahko zgodi, da Bojan ne bo mogel razvozlati sporočila. Naj bo

$$(n_{\mathrm{Anita}}, e_{\mathrm{Anita}}, d_{\mathrm{Anita}}) = (62894113, 5, 37726937),$$
$$(n_{\mathrm{Bojan}}, e_{\mathrm{Bojan}}, d_{\mathrm{Bojan}}) = (55465219, 5, 44360237).$$

Anita podpiše sporočilo $x = 1368797$ in podpis zašifrira:

1. $s = x^{d_{\mathrm{Anita}}} \bmod n_{\mathrm{Anita}} = 59847900$,
2. $y = s^{e_{\mathrm{Bojan}}} \bmod n_{\mathrm{Bojan}} = 38842235$.

Bojan izračuna

1. $\widehat{s} = y^{d_{\mathrm{Bojan}}} \bmod n_{\mathrm{Bojan}} = 4382681$,
2. $\widehat{x} = \widehat{s}^{e_{\mathrm{Anita}}} \bmod n_{\mathrm{Anita}} = 54383568$.

Ker je $s > n_{\mathrm{Bojan}}$, je $\widehat{x} \neq x = 1368797$.

Verjetnost tega dogodka je

$$\frac{n_{\mathrm{Anita}} - n_{\mathrm{Bojan}}}{n_{\mathrm{Anita}}}.$$