2009 m. sausio 29 d.
10:45

Designated Confirmer Signatures - Paskirto Patvirtintojo Parašai

Tegul $\mathcal{A}$ pasirašinėja programinę įrangą Π, panaudodama nepaneigiamą parašą σ.

Tačiau ji neturi laiko patvirtinti savo σ.
Patvirtinimų srautas yra labai didelis.

$\mathcal{A}$ paskiria Pavaduotoją, kad šis patvirtintų jos parašą σ visiems Direktoriams.

$\mathcal{B}$ nuperka iš $\mathcal{A}$ įrangą Π ir įsitikina, kad $\mathcal{A}$ parašas σ teisingas.

$\mathcal{B}$ parduoda Π $\mathcal{D}$ kartu su σ

$\mathcal{D} \longleftrightarrow \underset{\mathcal{P}}{\cancel{\mathcal{A}}}$, kad įsitikintų jog Π teisėta.

Viešieji sistemos parametrai:
p - pirminis
g - generatorius $\mathcal{Z}_p^* = \{1, 2 \dots, p-1\}$
$n = p \cdot q$ - pirminių skaičių sandauga.

$PR_{\mathcal{P}} = y$ $\qquad$ $VR_{\mathcal{P}} = v = g^y \bmod p$

$\mathcal{A} \longleftrightarrow \mathcal{B}$: tikrina, ar $\mathcal{A}$ parašas teisingas ir jeigu Taip, tada negali tuo įtikinti $\mathcal{D}$

Proxy Signature - Įgaliotasis Parašas

$\mathcal{A}$ įgalioja $\mathcal{B}$ pasirašyti už ją dokumentus.

Savybės:

1) Atskiriamumas - bet kas gali atskirti įgaliotą parašą

1) **Atskiriamumas** – bet kas gali atskirti įgaliotą parašą nuo originalaus parašo: A parašą nuo B parašo.

2) **Nesuklastojamumas** – įgaliotą parašą gali formuoti tiktai pats įgaliotojas A arba pats įgaliotasis B.

3) **Išskirtinumas** – įgaliotasis B negali suformuoti parašą, kuris būtų suprantamas ne kaip įgaliotas parašas.

4) **Patvirtinamumas** – įgaliotasis B parašas patvirtina tikrintojui D, kad įgaliojimą jam suteikė A.

5) **Identifikuojamumas** – įgaliotojas A gali nustatyti, kad įgaliotasis B parašas suformuotas būtent B.

6) **Neišsiginamumas** – įgaliotasis B negali išsiginti, kad jis pasirašė įgaliotu parašu.

Kriptografinė duomenų bazių apsauga

Pavardė	Vardas	Tarnyba	Pareigos	Atlyginimas

↑ Ind. laukas

$H(\ )$ C_K

$H(\text{Pavardė})$

$H(P_1)$ $E_K(V_1)$ $E_K(T_1)$ $E_K(P_1)$ $E_K(A_1)$

$H(P_2)$ . . . . . .

. . . .

$H(P_n)$

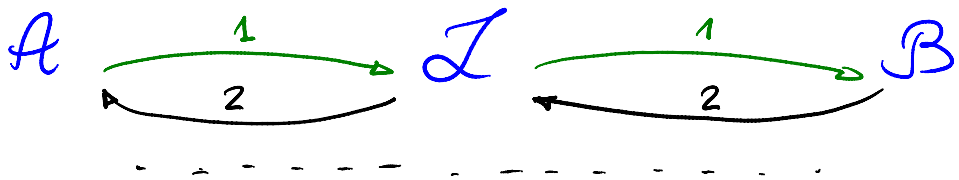
$P_i \longrightarrow H(P_i)$

$H(P_i)$ $E_K(V_i)$ $E_K(T_i)$ . . . . . .

$D_K(E_K(V_i)) = V_i \quad T_i \quad P_i$

A & B Grosmeisterio problema

A & B Grosmeisterio problema



Mafia fraud – Mafijos sukčiavimas

A. Shamir. Lecture at SECURICOM'89: „Aš galiu užeiti į mafijos parduotuvę nors milijoną kartų, bet jie vis tiek nesugebės save pristatyti kaip mane."

$M = \{I_o, I_i\} = ZZ = \mathbb{Z}$

B pietauja restorane „Pas I_o"

I_i ateina į Juvelyrinę parduotuvę J.

Pavalgius:

B paprašo sąskaitos apmokėjimui iš I_o

I_o susisiekia su I_i mob. telefonu

I_i pasirenka auksinių ir ~~sidabrinių~~ juvelyr. d.

1a. B siunčia I_o savo duomenis atsiskaitymui

$B \xrightarrow{d_B} I_o$

1b. $\mathcal{I}_o \xrightarrow{w_B} \mathcal{I}_i$

1c. $\mathcal{I}_i \xrightarrow{d_B} \mathcal{J}$ (stimulas)

2a. $\mathcal{I}_i \xleftarrow{c_J} \mathcal{J}$ (challenge)

2b. $\mathcal{I}_o \xleftarrow{c_J} \mathcal{I}_i$

2c. $\mathcal{B} \xleftarrow{c_J} \mathcal{I}_o$

3a. $\mathcal{B} \xrightarrow{r_B} \mathcal{I}_o$ (reakcija) (response) - - - - -