2009 m. sausio 29 d.
10:45

UNDENIABLE Signature -- NEPANEIGIAMAS Parašas

Sistemos parametrai: p - pirminis
generatorius $g \in \mathcal{I}_p^* = \{1, 2 \dots, p-1\}$

$\mathcal{A}$: $PR \equiv x$; $VR \equiv g^x \bmod p = \alpha$

$\mathcal{A}$ - parduoda $\mathcal{B}$ progr. įrangą Π ir ją pasirašo
$m = H(\Pi)$, sudaro H-funkciją įrangai Π
$\sigma \equiv m^x \bmod p$ Legali be virusų progr. įr.

$\mathcal{A} \longrightarrow \mathcal{B} : (\Pi, \sigma)$

$\mathcal{B}$? Ar $\mathcal{A}$ parašas teisingas ?

1. $\mathcal{B}$ - atsit. parenka $a, b \in_R \mathcal{I}_p^*$ ir apsk.
$c \equiv \sigma^a (g^x)^b \bmod p$; $c \longrightarrow \mathcal{A}$

2. $\mathcal{A}$ - apsk. $t \equiv x^{-1} \bmod (p-1)$ ir $\forall y : y^{p-1} \equiv 1 \bmod p-1$
$d \equiv c^t \bmod p$; $d \longrightarrow \mathcal{B}$

3. $\mathcal{B}$: tikrina ? $d \equiv m^a g^b \bmod p$?

$d \equiv c^t \bmod p = \left(\sigma^a (g^x)^b\right)^t \bmod p =$

$= \sigma^{at} g^{xbt} \bmod p = m^{xat} g^{xbt} \bmod p =$

$= m^{xa\cancel{x^{-1}}} g^{x b \cancel{x^{-1}}} \bmod p = m^a g^b \bmod p$

$\mathcal{B}$ nori perparduoti Π kokiam nors $\mathcal{D}$irektoriui
$\mathcal{B} \longrightarrow \mathcal{D} : (\Pi, \sigma)$ ir prašo sumokėti.

$\mathcal{D}$ - netiki, nes jis negali atskirti (Π, σ) nuo (Π', σ'), kurie yra prz. iš $\mathcal{L}$osės.

$\mathcal{B}$ vykdant protokolą su $\mathcal{L}$, jis gaus (Π', σ')

kurie tenkins (3) patikrinimo sąlyga : x', m'

$d' \equiv (m')^{a'} g^{b'} \bmod p$ PATIKRINKITE

ar gal $\mathcal{B} \equiv \mathcal{L}$?

? Ką turi daryti $\mathcal{D}$, kad patikrinti $\mathcal{B}$ sąžiningumą?