Coduri şi Criptografie
Sept 2010 - Ian 2011
Curs: Prof.dr. F. L. Ţiplea
Laborator: Lect.dr. S. Iftene
Facultatea de Informatică
Universitatea "Al.I.Cuza", Iaşi

Data: 27.01.2011

Examen

1. *Funcţii hash criptografice*

   (a) Ce este o funcţie hash ? **1.5p**

   (b) Ce este o funcţie hash slab rezistentă la coliziuni ? **1.5p**

   (c) Ce este o funcţie hash tare rezistentă la coliziuni ? **1.5p**

   (d) Ce este o funcţie hash greu inversabilă (one-way) ? **1.5p**

   (e) Care este legătura între funcţii hash slab rezistente la coliziuni, tare rezistente la coliziuni şi funcţii greu inversabile ? **4p**

2. *Criptosistemul ElGamal*
   Criptosistemul ElGamal se formulează astfel. A, entitatea care doreşte să primească mesaje criptate cu un astfel de criptosistem, alege un număr prim mare p şi o rădăcină primitivă modulo p, α. Alege apoi un parametru secret a, $1 \leq a \leq p-2$, şi calculează $\beta = \alpha^a \ mod \ p$; cheia publică va fi (p, α, β), iar cea secretă, a.

   Criptare: B, entitatea care transmite un mesaj criptat lui A, va obţine întâi cheia publică a lui A. Apoi, alege mesajul $x \in \mathbf{Z}_p$, parametrul k, $1 \leq k \leq p-2$, şi calculează $\gamma = \alpha^k \ mod \ p$ şi $\delta = x\beta^k \ mod \ p$. Perechea (γ, δ) este criptotextul asociat lui x, ce se transmite lui A.

   (a) Cum va decripta A mesajul (γ, δ) primit de la B ? Justificaţi corectitudinea decriptării. **2p**

   (b) Care este complexitatea implementării acestui criptosistem ? **3p**

   (c) Pe ce se bazează securitatea acestui criptosistem ? **2p**

   (d) Descrieţi semnătura ElGamal şi faceţi o comparaţie între aceasta şi criptosistemul ElGamal. Se obţine semnătura ElGamal din criptosistemul ElGamal aşa cum se obţine semnatura RSA din criptosistemul RSA? **3p**