Coduri şi Criptografie (2014–2015)

Prof.dr. F. L. Ţiplea
Facultatea de Informatică
Universitatea "Al.I.Cuza", Iaşi

Data: 29.01.2015

Examen

1. (Concepte de securitate)
   (a) Ce este un criptosistem cu chei simetrice?
   (b) Definiţi conceptele de securitate IND-CPA şi IND-CCA pentru criptografia cu chei simetrice, şi discutaţi asupra lor.
   (c) Arătaţi că criptosistemele cu chei simetrice pot atinge secret perfect.
   (d) In ce constă criptarea hibridă?
   (e) Ce cunoaşteţi despre securitatea criptării hibride? (doar rezultatul central, fără demonstraţie)

   20p

2. (Moduri de criptare înlănţuită)
   Prezentaţi modul de criptare CTR şi arătaţi că este IND-CPA sigur pentru permutări pseudo-random. **20p**

3. Fie $h : \mathbb{Z}_2^{t+1} \to \mathbb{Z}_2^t$ o funcţie hash tare rezistentă la coliziuni. Demonstraţi că funcţia $\bar{h} : \bigcup_{i \geq t+1} \mathbb{Z}_2^i \to \mathbb{Z}_2^t$ dată ca mai jos este tare rezistentă la coliziuni.

   `function` $\bar{h}(x)$
   `input:` $x \in \bigcup_{i \geq t+1} \mathbb{Z}_2^i$
   `begin`
   `let` $f : \{0,1\}^* \to \{0,1\}^*$ be the morphism given by $f(0) = 0$ and $f(1) = 01$;
   $y(x) := 11f(x) = y_1 \cdots y_k$, where $y_i \in \{0,1\}$ for all i;
   $g_0 := 0^t$;
   `for` $i := 1$ `to` k `do` $g_i := h(g_{i-1}y_i)$;
   `return` g_k
   `end`.

   (10p)