Information Security, Fall 2007

Instructors:

- **Prof.Dr. Ferucio Laurentiu Tiplea**
- **Asist.Prof.Dr. Cătălin Bîrjoveanu**

Department of Computer Science
"Al.I.Cuza" University of Iaşi
C 301
Tel: (0232) 201538

Date: Jan 28, 2008

Examen final – Soluţii

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

   `function` $\bar{h}(x)$
   `input:` $x \in \bigcup_{i \geq t+1} \mathbf{Z}_2^i$
   `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`.

   (30p)

   Soluţie: Presupunem, prin contradicţie, că $\bar{h}$ nu este tare rezistentă la coliziuni. Fie deci (x_1, x_2) o coliziune pentru $\bar{h}$. Vom arăta că putem determina uşor o coliziune pentru h.

   Fie $y(x_1) = y_1 \cdots y_k$, $g_i := h(g_{i-1}y_i)$ pentru $1 \leq i \leq k$, $y(x_2) = y'_1 \cdots y'_l$ şi $g'_i := h(g'_{i-1}y'_i)$ pentru $1 \leq i \leq l$.

   Relaţia $g_k = g'_l$ conduce la $h(g_{k-1}y_k) = h(g'_{l-1}y'_l)$. Dacă $g_{k-1}y_k \neq g'_{l-1}y'_l$, atunci am obţinut o coliziune pentru h; altfel, $y_k = y'_l$ şi $g_{k-1} = g'_{l-1}$. Repetăm procedeul cu egalitatea $g_{k-1} = g'_{l-1}$ etc. Se observă imediat că nu putem avea $k = l$ fără a determina nici o coliziune deoarece, altfel, am avea $x_1 = x_2$ ceea ce ar constitui o contradicţie. Dacă presupunem că $k < l$, atunci procedeul de mai sus se va încheia cu determinarea unei coliziuni deoarece prefixul 11 al şirului $y(x_1)$ nu coincide cu nici un subşir de lungime 2 şi diferit de 11 al şirului $y(x_2)$.

   Ca urmare, presupunerea făcută este falsă, ceea ce ne spune că $\bar{h}$ este tare rezistentă la coliziuni.

   Notă: termenul de "calcul uşor" este înţeles în sensul discutat asupra primitivelor criptografice.

   Notă: funcţia f are scopul de a separa grupuri compacte de 1 prin inserarea unui bit 0 între oricare doi biţi 1 consecutivi.

2. Presupunem că în IPsec modul de criptare CBC se înlocuieşte cu unul din celelalte moduri de criptare predate in cadrul cursului. Studiaţi securitatea protocolului obţinut în acest mod (pentru fiecare din modurile de criptare diferite de CBC). **(20p)**

   Soluţie: Celelalte 2 moduri de operare discutate la curs, în afara modului CBC, sunt OFB şi CFB:

   - în cadrul modului OFB, blocul de criptotext y_i este dat prin:

     $$y_i = e_K^i(x_0) \oplus x_i,$$

     pentru orice i, unde $x = x_1 \cdots x_n$ este textul sursă împărţit în n blocuri cu dimensiunea cerută de criptosistem, iar x_0 este vectorul de iniţializare. Ca urmare,

     $$x_3 = y_3 \oplus e_K^3(x_0),$$

     ceea ce arată că exact acelaşi atac ca în modul CBC poate fi aplicat şi în acest caz (operându-se asupra lui y_3);

   - în cadrul modului CFB, blocul de criptotext y_i este dat prin:

     $$y_i = e_K(y_{i-1}) \oplus x_i,$$

     pentru orice i, unde $x = x_1 \cdots x_n$ este textul sursă împărţit în n blocuri cu dimensiunea cerută de criptosistem, iar $y_0 = x_0$ este vectorul de iniţializare. Ca urmare,

     $$x_3 = y_3 \oplus e_K(y_2),$$

     ceea ce arată că exact acelaşi atac ca în modul CBC poate fi aplicat şi în acest caz (operându-se asupra lui y_3).

   Notă: Reamintesc mai jos atacul asupra modului CBC discutat complet în cadrul cursului. In acest mod,

   $$x_3 = y_2 \oplus d_K(y_3).$$

   Deci, dacă alterăm un bit în y_2, exact acelaşi bit va fi alterat în x_3. Cum primii 32 biţi din x_3 vor trebui să conţină adresa destinaţie, atacantul poate modifica primii 32 biţi ai lui y_2 astfel încât, prin decriptare, primii 32 de biţi ai lui x_3 să conţină adresa atacantului.

Punctajul minim la proba scrisă, pentru promovarea examenului, este de 20p.