Coduri şi Criptografie
Oct 2011 - Ian 2012
Prof.dr. F. L. Ţiplea
Lect.dr. S. Iftene
Facultatea de Informatică
Universitatea "Al.I.Cuza", Iaşi

Data: 23.11.2011

Examen [1]

Modul CFB de criptare simetrică a unei secvenţe binare x cu un criptosistem pentru care lungimea cheii de criptare, a blocului de intrare şi a celui de ieşire este m, funcţionează astfel:

- se imparte x în blocuri de lungime r, $x = x_1 \cdots x_n$, unde $1 \leq r \leq m$ (presupunând că $|x|$ este multiplu de r; altfel se padează x convenabil);
- se consideră un vector de iniţializare IV de lungime m;
- se aplică următorul algoritm ce produce criptotextul y asociat lui x cu cheia K:

$I_0 := IV$;
$y_0 := \lambda$; (λ este şirul vid)
$y := \lambda$;
`for` $j := 1$ `to` n `do`
    $I_j :=$ ultimii m bits ai lui $I_{j-1}y_{j-1}$;
    $z_j :=$ primii r bits ai lui $e_K(I_j)$;
    $y_j := x_j \oplus z_j$;
    $y := yy_j$;
`end_for`

Răspundeţi la următoarele:

1. Explicaţi cum se face decriptarea în modul CFB. **1p**
2. Discutaţi cazurile $r < m$ şi $r = m$ atât pentru criptare cât şi pentru decriptare. **1p**
3. Presupunem că x se criptează în modul CFB cu vectorul de iniţializare IV, conducând la $y = y_1 \cdots y_n$, şi apoi cu vectorul de iniţializare IV' diferit de IV, conducând la $y' = y'_1 \cdots y'_n$. Arătaţi că $y \neq y'$ (atenţie: funcţia de criptare este injectivă). **2p**
4. Arătaţi că alterarea unui bit în y_j afectează decriptarea corectă a lui y_j cât şi a următoarelor $\lceil m/r \rceil$ blocuri de criptotext. **2p**
5. Arătaţi că dacă bitul de pe poziţia p este modificat în y_j, atunci prin decriptare, exact bitul de pe poziţia p va fi modificat în x_j. Este această proprietate adevărată şi pentru următoarele $\lceil m/r \rceil$ blocuri de criptotext? **2p**
6. Poate fi folosit modul CFB cu un criptosistem cu chei publice? Justificaţi răspunsul arătând cum poate fi folosit sau de ce nu poate fi folosit într-o astfel de situaţie. **1p**

[1] Baza de notare: 1p