

- Prof.Dr. Ferucio Laurențiu Țiplea
- Lect.Dr. Sorin Iftene
- Asist.Prof.Dr. Cătălin Bîrjoveanu

Department of Computer Science
“Al.I.Cuza” University of Iași
Office: C 301
Tel: (0232) 201538

Date: Feb 12, 2009

Examen Final

1. Modul CFB de criptare a unei secvențe binare x funcționează astfel:

- se împarte x în blocuri de lungime r , $x = x_1 \cdots x_n$;
- se consideră un vector de inițializare de lungime m , unde m este lungimea cheii K de criptare;
- se aplică următorul algoritm ce produce criptotextul y asociat lui x cu cheia K :


```
 $I_0 := IV;$   
 $z_0 := \lambda;$  ( $\lambda$  este șirul vid)  
 $y := \lambda;$   
for  $j := 1$  to  $n$  do  
     $I_j :=$  ultimii  $m$  bits ai lui  $I_{j-1}z_{j-1}$   
     $z_j :=$  primii  $r$  bits ai lui  $e_K(I_j)$ ;  
     $y_j := x_j \oplus z_j$ ;  
     $y := yy_j$ ;  
end_for
```

- (a) Cum se realizează decriptarea în modul CFB? 15p
- (b) Dacă în IPsec se utilizează modul de criptare CFB în locul modului CBC, se mai poate monta același atac (ca în cazul modului CBC)? 20p

2. Presupunem că mesajele transmise prin SSL sunt prelucrate astfel:

- mesajul este împărțit în blocuri, B_1, \dots, B_m (fiecare cu cel mult 2^{14} octeți);
- pentru fiecare bloc B_i se realizează:
 - se aplică un MAC blocului B_i rezultând X_i ;
 - se criptează X_i cu un criptosistem simetric în modul CBC rezultând Y_i ;
 - se adaugă un header SSL rezultând Z_i ;
 - se transmite Z_i printr-un segment TCP.

Criptarea primului bloc X_1 se face astfel:

- se împarte X_1 în blocuri de 64 sau 128 bits (în funcție de criptosistem), $X_1 = x_1^1 \cdots x_1^{l_1}$;
- se generează $Y_1 = y_1^1 \cdots y_1^{l_1}$, unde $y_1^1 = e_K(x_1^1 \oplus y_0)$, y_0 este un vector inițial, iar $y_1^j = e_K(x_1^j \oplus y_j^1)$ pentru orice $j > 1$. 

Criptarea celorlalte blocuri $X_i = x_i^1 \cdots x_i^{l_i}$ ($i > 1$) se face ca și pentru X_1 dar cu deosebirea că y_0 este ales ca fiind $y_{i-1}^{l_{i-1}}$ (ultimul criptotext din blocul anterior).

- (a) Arătați că un intrus care are acces la blocurile Y_1 și B_2 dar nu la B_1 , poate decide efectiv dacă un anumit sub-bloc x_1^j coincide sau nu cu un mesaj x^* (de aceeași lungime cu x_1^j) ales de intrus (remarcă: funcția de criptare este injectivă). 15p
- (b) Dacă un sub-bloc x_1^j conține o parolă mică, poate fi utilizat rezultatul anterior pentru montarea unui atac prin ghicirea parolei? (puteți presupune că intrusul poate monta un atac de plaintext ales). 10p
- (c) Cum poate fi îmbunătățit protocolul pentru a nu mai avea loc proprietatea de la (a)? 10p