Information Security, Fall 2007

- **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. Considerăm următoarea schemă de distribuţie a cheii pentru n utilizatori. Administratorul (TA) alege un număr prim $p > n$, trei coeficienţi $a, b, c \in \mathbf{Z}_p$ (distincţi doi câte doi) şi formează polinomul

$$f(x, y) = a + b(x + y) + cxy \ mod \ p.$$

TA distribuie fiecărui utilizator U polinomul

$$g_U(x) = f(x, r_U) \ mod \ p = a_U + b_U x \ mod \ p,$$

unde $r_U \in \mathbf{Z}_p$ este un parametru public ales aleator de U. Polinomul g_U este secret al lui U.

Doi utilizatori U şi V vor comunica prin intermediul cheii

$$K_{UV} = g_U(r_V) = f(r_U, r_V) = f(r_V, r_U) = g_V(r_U) = K_{VU}.$$

In cadrul cursului s-a arătat că schema este rezistentă la atac de coaliţie 1. Modificaţi schema astfel încât aceasta să fie rezistentă la atac de coaliţie $1 < k < n$. **(30p)**

Soluţie: Fie polinomul simetric

$$f(x, y) = \sum_{i=0, j=0}^{\alpha} a_{i,j} x^i y^j$$

unde $a_{i,j} = a_{j,i} \ mod \ p$, iar în rest coeficienţii sunt distincţi doi câte doi (calculul va fi peste tot modulo p).

Acest polinom are $\frac{(\alpha+1)(\alpha+2)}{2}$ coeficienţi. Un utilizator U va primi polinomul g_U ce are gradul α şi, deci, $\alpha + 1$ coeficienţi. Deci, dacă dorim ca schena să fie rezistentă la atac de coaliţie k, atunci trebuie să avem satisfăcute cerinţele:

$$\begin{cases} k(\alpha+1) & < & (\alpha+1)(\alpha+2)/2 \\ (k+1)(\alpha+1) & \geq & (\alpha+1)(\alpha+2)/2 \end{cases}$$

Aceste relaţii conduc imediat la $\alpha = 2k - 1$ sau $\alpha = 2k$. Ca urmare, alegându-se $\alpha = 2k - 1$ (de exemplu), obţinem o schemă rezistentă la coaliţii de dimensiune k, dar nu la coaliţii de dimensiune $k + 1$.

Notă: nestabilirea faptului că determinantul sistemului este nenul (în cazul unei coaliţii de dimensiune $k + 1$) nu va diminua punctajul stabilit (de 30p).

2. Descrieţi o modalitate prin care componenta IKE a protocolului IPsec poate fi modificată prin includerea schemei de la punctul precedent, şi studiaţi securitatea ei. Discutaţi apoi avantajele şi dezavantajele acestei noi metode în comparaţie cu metoda IKE standard. **(20p)**

Solutie: Schema de la 1 poate fi folosită în IKE în cel puţin două moduri:

- în prima fază: dat un TA, fiecare utilizator U va comunica cu TA printr-un canal sigur pentru a obţine g_U. Se poate trece apoi direct la faza 2 din IKE cu utilizarea cheilor $K_{U,V}$ între U şi V.
  - securitate: dată de canalul sigur dintre U şi TA;
  - avantaje: lipsa fazei 1 din IKE care poate fi costisitoare;
  - dezavantaje: necesitatea unui TA; canale sigure între U şi TA pot exista doar în cazuri particulare;
- în a doua fază: se derulează prima fază din IKE pentru a se obţine o cheie secretă cu care apoi în faza 2 IKE se transportă polinomul g_U de la TA către fiecare utilizator U (plus alte informaţii necesare). $K_{U,V}$ se utilizează pentru criptarea payload-urilor între U şi V.
  - securitate: dată de faza 1 IKE;
  - avantaje: evaluare polinom în locul exponenţierii modulare;
  - dezavantaje: necesitatea unui TA.

Notă: Pot exista variaţii a acestor 2 soluţii, precum şi modalităţi diverse de realizare a protocoalelor corespunzătoare. Orice abordare rezonabilă va fi punctată.

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