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: Feb 3, 2008

Final Exam (ID)

1. Protocolul de mai jos (datorat lui Woo şi Lam) are scopul de a mijloci autentificarea unui client către un alt client prin intermediul unui server (în protocol, $\{x\}_K$ înseamnă x criptat cu K, iar K_{XY} reprezintă cheia partajată de X şi Y):

$$\begin{array}{lcl} 1.\ A{\rightarrow}B & : & A \\ 2.\ B{\rightarrow}A & : & N_b \\ 3.\ A{\rightarrow}B & : & \{A,B,N_b\}_{K_{AS}} \\ 4.\ B{\rightarrow}S & : & \{A,B,\{A,B,N_b\}_{K_{AS}}\}_{K_{BS}} \\ 5.\ S{\rightarrow}B & : & \{A,B,N_b\}_{K_{BS}} \end{array}$$

   - Explicaţi modul în care funcţionează protocolul (furnizaţi cât mai multe detalii convingătoare asupra realizării obiectivului acestuia). **30p**
   - Se ştie că acest protocol este vulnerabil la atac prin interpunerea unui intrus între participanţii la protocol. Prezentaţi un astfel de atac. **30p**

2. 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 $1 < k < n$. **(40p)**

Punctajul minim la proba scrisă, pentru promovarea examenului, este de 30p.