Information Security, Fall 2012

- **Prof.Dr. Ferucio Laurenţiu Ţiplea**
- **Lect.Dr. Cătălin Bîrjoveanu**
- **Lect.Dr. Sorin Iftene**

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

Date: Feb 06, 2013

Examen Final (timp de lucru: 1h40')

1. (IPsec – timp estimat: 30')
   (a) Ce este o asociere de securitate în IPsec şi care sunt mecanismele de securitate fundamentale din IPsec? **1p**
   (b) Descrieţi, succint dar clar, protocolul AH în cele două moduri de utilizare pentru datagrame IPv4. **1p**
   (c) Descrieţi, succint dar clar, protocolul ESP în cele două moduri de utilizare pentru datagrame IPv4. **1p**
   (d) Descrieţi câteva combinaţii de asocieri de securitate in IPsec (end-to-end, VPN, end-to-end cu VPN). **1p**

2. (DNSsec – timp estimat: 40')
   (a) Descrieţi, succint dar clar, modul de funcţionare a protocolului DNS. **1.5p**
   (b) Descrieţi, succint dar clar, modul de funcţionare a protocolului $DNSsec$. **1.5p**
   (c) Prezentaţi şi discutaţi 2 argumente pentru care credeţi că $DNSsec$ asigură securitate. **1p**

3. (Protocolul Woo-Lam – timp estimat: 30')
   Protocolul de mai jos are scopul de a mijloci autentificarea unui client A către un alt client B prin intermediul unui server S (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). **0.5p**
   - Se ştie că acest protocol este vulnerabil la atac prin interpunerea unui intrus între participanţii la protocol. Prezentaţi un astfel de atac. **1.5p**