Information Security, Fall 2013

Prof.Dr. Ferucio Laurenţiu Ţiplea

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

Date: May 12, 2014

Examen Restanţă Specială (timp de lucru: 1h30')

1. In ce constă paradoxul zilei de naştere şi care este importanţa lui în construcţia de funcţii hash rezistente la coliziuni? **10p**

2. Considerăm următoarea schemă de distribuţie a cheii pentru n utilizatori. Administratorul (TA) alege un număr prim $p > n$, generează random 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 random de U. Polinomul g_U este secret al lui U.
Doi utilizatori U şi V vor comunica prin intermediul cheii
$$K_{UV} = g_U(r_V) = f(r_U, r_V) = f(r_V, r_U) = g_V(r_U) = K_{VU}.$$
Arătaţi următoarele:
   (a) Schema este rezistentă la atac de coaliţie 1 (pentru un utilizator W, cheia utilizată de orice alţi doi utilizatori poate fi oricare din cheile posibile, cu aceeaşi probabilitate). **7p**
   (b) Schema nu este rezistentă la atac de coaliţie 2 (doi utilizatori pot deduce în timp polinomial cheia utilizată de orice alţi doi utilizatori). **8p**

3. Considerăm, în cadrul modelului take-grant, două insule (distincte) I_1 şi I_2 conectate printr-un element extern z.
   - Discutaţi posibilitatea şi modul de transfer a drepturilor de la o insulă la cealaltă. **7p**
   - Studiaţi complexitatea algoritmului prin care o insulă poate obţine toate drepturile celeilalte insule. **8p**