Coduri şi Criptografie
Oct 2011 - Ian 2012
Prof.dr. F. L. Ţiplea
Lect.dr. S. Iftene
Facultatea de Informatică
Universitatea "Al.I.Cuza", Iaşi

Data: 16.02.2012

Examen [1]

Fie p un număr prim şi a un număr întreg nedivizibil prin p. Spunem că a este *rezidu pătratic modulo p* dacă există r astfel încât $a \equiv r^2\ mod\ p$.

Notăm

$$\left(\frac{a}{p}\right) = \begin{cases} 0, & \text{dacă } p|a \\ 1, & \text{dacă } a \text{ este reziduu pătratic modulo } p \\ -1, & \text{altfel} \end{cases}$$

Fie p şi q numere prime distincte şi $n = pq$. Notăm

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p}\right)\left(\frac{a}{q}\right)$$

Se ştie că dacă $p \equiv 3\ mod\ 4$, $q \equiv 3\ mod\ 4$ şi

$$\left(\frac{a}{n}\right) = 1$$

atunci ori a ori $-a$ este reziduu pătratic modulo n.

Fie p şi q numere prime distincte ce satisfac $p \equiv 3\ mod\ 4$ şi $q \equiv 3\ mod\ 4$, fie $n = pq$ şi fie a un număr întreg cu proprietatea

$$\left(\frac{a}{n}\right) = 1$$

Arătaţi următoarele:

1. 8 divide $\phi(n) + 4$; **1p**

2. Dacă $r = a^{\frac{\phi(n)+4}{8}}\ mod\ n$, atunci $a \equiv r^2\ mod\ n$ sau $-a \equiv r^2\ mod\ n$. **2p**

3. Dacă $b \in \{0, 1\}$, $x = (-1)^b$, $a \equiv r^2\ mod\ n$, iar t_1 este un întreg cu proprietatea

$$\left(\frac{t_1}{n}\right) = x$$

   atunci

$$\left(\frac{s_1 + 2r}{n}\right) = \left(\frac{t_1}{n}\right) = x$$

   unde $s_1 = (t_1 + a/t_1)\ mod\ n$. **2p**

4. Dacă $b \in \{0, 1\}$, $x = (-1)^b$, $-a \equiv r^2\ mod\ n$, iar t_2 este un întreg cu proprietatea

$$\left(\frac{t_2}{n}\right) = x$$

atunci

$$\left(\frac{s_2 + 2r}{n}\right) = \left(\frac{t_2}{n}\right) = x$$

unde $s_2 = (t_2 - a/t_2)\ mod\ n$. **2p**

5. Pornind de la faptul că necunoaşterea factorizării lui n face ca determinarea unui întreg r cu $a \equiv r^2\ mod\ n$ sau $-a \equiv r^2\ mod\ n$ să fie o problemă intractabilă, puteţi concepe o schemă între 2 participanţi prin care un participant să îi trimită în siguranţă celuilalt participant un bit? Schema trebuie să folosească numai elementele de mai sus. **2p**

[1] Baza de notare: 1p