Coduri şi Criptografie (2015–2016)

Prof.dr. F. L. Ţiplea
Facultatea de Informatică
Universitatea "Al.I.Cuza", Iaşi

Data: 22.01.2016

Examen

1. (Concepte de securitate)
   (a) Ce este o funcţie one-way? **5p**
   (b) Ce este o funcţie rezistentă la coliziuni? **5p**
   (c) Ce legătura este între funcţii one-way şi funcţii rezistente la coliziuni? Justificaţi răspunsul. **15p**
   (d) In ce constă paradoxul zilei de naştere şi care este importanţa lui în construcţia de funcţii candidat la clasa de funcţii rezistente la coliziuni? Justificaţi răspunsul. **10p**

2. Considerăm următorul criptosistem cu chei publice ce criptează un singur bit la un pas de aplicare a lui:
   - $\mathcal{G}(1^\lambda)$: (n,p,q), unde p şi q sunt numere prime ce satisfac $p,q \equiv 3 \bmod 4$, iar $n = pq$. n va fi cheia publică, iar (p,q) va fi cheia privată;
   - $\mathcal{E}(m,n)$: se criptează un bit $m \in \{-1,1\}$ astfel: se generează random $r \in \mathbb{Z}_n^*$ şi se calculează criptotextul $c = r^2 m \bmod n$;
   - $\mathcal{D}(c,p,q)$: dacă c este reziduu pătratic modulo n, atunci $m = 1$; altfel, $m = -1$.

   Arătaţi că schema este corectă (utilizaţi proprietăţile reziduurilor pătratice). **5p**

   Arătaţi apoi că schema este IND-CPA sigură, presupunând că este dificil a distinge între un reziduu pătratic şi un non-reziduu pătratic fără a cunoaşte factorizarea lui n. **10p**

Informaţii ajutătoare pentru subiectul 2

Definition 1 *Let $n > 1$ be an integer and $a \in \mathbb{Z}$ co-prime to n. a is called a* quadratic residue modulo n *if $a \equiv x^2$ mod n for some integer x. Otherwise, a is called a* quadratic non-residue modulo n.

Facts Let p and q be odd primes and $n = pq$. Then:

1. The product of two quadratic residues or two quadratic non-residues (mod p) is a quadratic residue (mod p).
2. The product of a quadratic residue with a quadratic non-residue (mod p) is a quadratic non-residue (mod p).
3. a is a quadratic residue modulo n if and only if a is a quadratic residue both modulo p and modulo q.

Definition 2 *Let $p > 2$ be a prime. The* Legendre symbol *of $a \in \mathbb{Z}$, denoted $\left(\frac{a}{p}\right)$, is*

$$\left(\frac{a}{p}\right) = \begin{cases} 0, & \text{if } p|a \\ 1, & \text{if } p \not| a \text{ and } a \text{ is a quadratic residue modulo } p \\ -1, & \text{if } p \not| a \text{ and } a \text{ is a quadratic non-residue modulo } p \end{cases}$$

Definition 3 *Let $n > 0$ be an odd integer. The* Jacobi symbol *of $a \in \mathbb{Z}$, denoted $\left(\frac{a}{n}\right)$, is*

$$\left(\frac{a}{n}\right) = \begin{cases} 1, & \text{if } n{=}1 \\ \left(\frac{a}{p_1}\right)^{e_1} \cdots \left(\frac{a}{p_k}\right)^{e_k}, & \text{otherwise} \end{cases}$$

where $n = p_1^{e_1} \cdots p_k^{e_k}$ is the prime factorization of n.

Basic rules for computing the Legendre/Jacobi symbol:

1. if $a \equiv b$ *mod* n then $\left(\frac{a}{n}\right) = \left(\frac{b}{n}\right)$
2. $\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$
3. $\left(\frac{1}{n}\right) = 1$
4. $\left(\frac{-1}{n}\right) = \begin{cases} 1, & \text{if } n \equiv 1 \text{ mod } 4 \\ -1, & \text{if } n \equiv 3 \text{ mod } 4 \end{cases}$
5. $\left(\frac{2}{n}\right) = \begin{cases} 1, & \text{if } n \equiv \pm 1 \text{ mod } 8 \\ -1, & \text{if } n \equiv \pm 3 \text{ mod } 8 \end{cases}$
6. $\left(\frac{m}{n}\right) = \begin{cases} -\left(\frac{n}{m}\right), & \text{if } n \equiv m \equiv 3 \text{ mod } 4 \\ \left(\frac{n}{m}\right), & \text{if } n \equiv 1 \text{ mod } 4 \text{ or } m \equiv 1 \text{ mod } 4 \end{cases}$

for any distinct odd integers $n, m > 0$ and $a, b \in \mathbb{Z}$.