Coduri şi Criptografie (2013–2014)

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

Data: 31.01.2014

Examen

1. (Concepte de securitate)

   (a) Ce este un criptosistem cu chei publice?

   (b) Definiţi conceptele de securitate IND-CPA şi IND-CCA pentru criptografia cu chei publice, şi discutaţi asupra lor.

   (c) Arătaţi că criptosistemele cu chei publice nu pot atinge secret perfect.

   (d) In ce constă criptarea hibridă?

   (e) Ce cunoaşteţi despre securitatea criptării hibride? (doar rezultatul central, fără demonstraţie)

   20p

2. (Criptosistemul RSA)

   (a) Prezentaţia versiunea textbook a criptosistemului RSA.

   (b) Arătaţi că versiunea textbook a criptosistemului RSA nu este IND-CPA sigură.

   (c) Discutaţi securitatea versiunii textbook a criptosistemului RSA pentru valori mici ale exponentului de criptare.

   (d) Prezentaţia versiunea padată a criptosistemului RSA.

   (e) Ce cunoaşteţi despre securitatea versiunii padate a criptosistemului RSA? (doar rezultatul central, fără demonstraţie)

   20p

3. Considerăm următorul criptosistem cu chei publice ce criptează un singur bit la un pas de aplicare a lui:

   - $\mathcal{G}(1^n)$: (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).

   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 3

Definition 1 *Let $p > 2$ be a prime and $a \in \mathbb{Z}$ non-divisible by p. a is called a* quadratic residue modulo p *if $a \equiv x^2 \ mod \ n$ for some integer x. If a is neither divisible by p nor a quadratic residue modulo p then a is called a* quadratic non-residue modulo n.

Facts:

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).

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

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