Coduri și Criptografie (2014–2015)

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

Data: 29.01.2015

Examen

- 1. (Concepte de securitate)
 - (a) Ce este un criptosistem cu chei publice?
 - (b) Definiți conceptele de securitate IND-CPA și IND-CCA pentru criptografia cu chei publice, și discutați asupra lor.
 - (c) Arătați că criptosistemele cu chei publice nu pot atinge secret perfect.
 - (d) In ce constă criptarea hibridă?
 - (e) Ce cunoașteți despre securitatea criptării hibride? (doar rezultatul central, fără demonstrație)

20p

- 2. (Criptosistemul RSA)
 - (a) Prezentația versiunea textbook a criptosistemului RSA.
 - (b) Arătați că versiunea textbook a criptosistemului RSA nu este IND-CPA sigură.
 - (c) Discutați securitatea versiunii textbook a criptosistemului RSA pentru valori mici ale exponentului de criptare.
 - (d) Prezentația versiunea padată a criptosistemului RSA.
 - (e) Ce cunoașteți despre securitatea versiunii padate a criptosistemului RSA? (doar rezultatul central, fără demonstrație)

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 $p, q \equiv 3 \mod 4$, 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 $c = r^2 m \mod N$;
 - $\mathcal{D}(c, p, q)$: dacă c este reziduu pătratic modulo N, atunci m = 1; altfel, m = -1.

Arătați că schema este corectă (utilizați proprietățile reziduurilor pătratice).

Arătați apoi că schema este IND-CPA sigură, presupunând că este dificil a distinge între un reziduu pătratic și un non-reziduu pătratic fără a cunoaște factorizarea lui N.

10p

Informații 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 p.

Facts:

- 1. The product of two quadratic residues or two quadratic non-residues \pmod{p} is a quadratic residue \pmod{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

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

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 $a, b \in \mathbb{Z}$.