The RSA Cryptosystem and Key Generation

T-79.5501 Cryptology

Lecture 7
April 1, 2008

Kaisa Nyberg

The RSA Cryptosystem

- A public-key cryptosystem presented by R. Rivest, A. Shamir and L. Adleman in 1978.
- Let p and q be two distinct odd primes, and $n = pq$. Then $\Phi(n) = (p-1)(q-1)$. Let $\mathcal{P} = \mathcal{C} = \mathbb{Z}_n$, and define

$$\mathcal{K} = \{(n, p, q, a, b) \mid ab \equiv 1 \pmod{\phi(n)}\}.$$

For $K = (n, p, q, a, b) \in \mathcal{K}$, $x \in \mathcal{P}$ and $y \in \mathcal{C}$, define

$$\begin{aligned} e_K(x) &= x^b \bmod n, \text{ and} \\ d_K(y) &= y^a \bmod n. \end{aligned}$$

- The values n and b comprise the public key, and the values p, q and a comprise the private key.

$d_K(e_K(x)) = x$

- Claim: $(x^a)^b = x \pmod{n}$, for all $x \in \mathbb{Z}_n$.
- By the Chinese Reminder Theorem it suffices to show that $(x^a)^b = x \bmod p$, for all $x \in \mathbb{Z}_p$, for any p that divides n such that $\gcd(p, n/p) = 1$.
- Since $ab = 1 + k(p-1)$ for some integer k, we obtain

$$(x^a)^b = x^{ab} = x^{1+k(p-1)} = x(x^{p-1})^k = x \pmod{p}.$$

RSA is Efficient

- Generate two large primes, p and q, such that $p \neq q$
- Calculate $n = pq$ and $\phi(n) = (p-1)(q-1)$
- Generate random b, $1 < b < \phi(n)$, such that $\gcd(b, \phi(n)) = 1$
- Calculate $a = b^{-1} \bmod \phi(n)$
- Note. Sometimes a is generated first, and then b is calculated as its inverse $\bmod \phi(n)$.
- Note. The parameters can be generated efficiently.
- Note. The encryption and decryption operations can be computed efficiently using the *Square and Multiply Algorithm*.

Decision Problem: Composites

- **Composites:** Given a positive integer $n \geq 2$, is n composite?
- The problem **Composites** (and **Primes**) is in **P** (2004). The best known algorithm is not efficient enough for practical applications.
- **A Monte Carlo Algorithm:** a non-deterministic algorithm, which always gives an answer (in polynomial time).
- A Monte Carlo algorithm is yes-biased if the “yes” answer is always correct, but the “no” answer may be incorrect.
- A Monte Carlo algorithm is no-biased if the “no” answer is always correct, but the “yes” answer may be incorrect.
- The error probability is computed over all possible random choices made by the algorithm when it is run.
- Next two yes-biased Monte Carlo algorithm for solving the “Composites” problem will be presented.

Quadratic Residues and Euler's Criterion

- **Definition:** (Quadratic Residue mod odd integer) Suppose that n is an odd integer and x is an integer, $1 \leq x \leq n-1$. If there is $y \in \mathbb{Z}_n$ such that $y^2 \equiv x \pmod{n}$ the x is called a **quadratic residue** $\bmod n$. Otherwise x is called a **quadratic non-residue** $\bmod n$.

- Theorem (Euler's criterion) Let p be an odd prime. Then x is a quadratic residue $\bmod p$ if and only if

$$x^{\frac{p-1}{2}} \equiv 1 \pmod{p}.$$

- *Proof.* See the textbook.

Legendre Symbol

- **Definition:** (Legendre Symbol) Suppose p is an odd prime. For any integer $a \geq 0$, we define the Legendre symbol $\left(\frac{a}{p}\right)$ as follows:

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } a \equiv 0 \pmod{p} \\ 1 & \text{if } a \text{ is a quadratic residue } \bmod p \\ -1 & \text{if } a \text{ is a quadratic non-residue } \bmod p. \end{cases}$$

- Putting together this definition and Euler's criterion we get
- **Theorem:** Suppose p is an odd prime. Then

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p} \text{ for all } a,\ 1 \leq a \leq p-1.$$

Jacobi Symbol and Euler Pseudo-Prime

- **Definition:** (Jacobi symbol) Suppose n is an odd positive integer with prime power factorization $p_1^{e_1} \cdots p_k^{e_k}$. Let $a \geq 0$ be an integer. The Jacobi symbol $\left(\frac{a}{n}\right)$ is defined to be

$$\left(\frac{a}{n}\right) = \prod_{i=1}^{k} \left(\frac{a}{p_i}\right)^{e_i}.$$

- The Jacobi symbol can be evaluated efficiently without factorization of n using rules 1-4 given in the textbook.

- Suppose n is composite. Given integer $a \geq 0$, Euler's criterion

$$\left(\frac{a}{n}\right) \equiv a^{\frac{n-1}{2}} \pmod{n}$$

may or may not hold. If it holds, then n is called an *Euler pseudoprime to the base a*.

The Solovay-Strassen Primality Test

- Choose a random integer a, $1 \leq a \leq n-1$
  - if
$$\left(\frac{a}{n}\right) \equiv a^{\frac{n-1}{2}} \pmod{n}$$
    then answer "n is prime"
  - else answer "n is composite".
- The Solovay-Strassen algorithm is a yes-biased Monte Carlo Algorithm for **Composites**, that is, the answer "n is composite" is always correct but the answer "n is prime" may or may not be correct.
- The error probability is less than $\frac{1}{2}$.

The Miller-Rabin Primality Test

- Write $n-1=2^k m$, where m is odd.
- Choose a random integer a, $1 \leq a \leq n-1$.
- Compute $b = a^m \bmod n$.
- If $b \equiv 1 \bmod n$ then answer "n is prime".
- For $i=0$ to $k-1$ do
  - if $b \equiv -1 \pmod{n}$ then answer "n is prime".
  - else $b = b^2 \bmod n$.
- Answer "n is composite".
- The Miller-Rabin primality test is a yes-biased Monte Carlo algorithm for **Composites**. The error probability can be shown to be at most $\frac{1}{4}$.

Square Roots Modulo Prime

- Suppose p is an odd prime and a is a qudratic residue modulo p. Then a has exactly two square roots. If b is one square root, then $p-b$ is the second square root of a.
- Suppose $p \equiv 3 \pmod 4$. Then

  $$b = a^{\frac{p+1}{4}} \bmod$$

  is a square root of a, since then $\frac{p+1}{4}$ is an integer and

  $$b^2 = a^{\frac{p+1}{2}} = a \cdot a^{\frac{p-1}{2}} = a \pmod p$$

  by Euler's criterion.
- For $p \equiv 1 \pmod 4$ no efficient deterministic algorithm is known.

Square Roots Modulo A Composite Integer

- Let $n = pq$, where p and q are distinct primes.
- Let a, $1 \leq a \leq n-1$, be a quadratic residue modulo n.
- Then there is b_p, $0 \leq b_p \leq p-1$, such that $b_p^2 \equiv a \pmod{p}$. Similarly, there is b_q, $0 \leq b_q \leq q-1$, such that $b_q^2 \equiv a \pmod{q}$.
- Using the CRT we can find b, $1 \leq b \leq n$, such that $b \equiv b_p \pmod{p}$ and $b \equiv b_q \pmod{q}$. Then $b^2 \equiv a \pmod{n}$.
- If $a \neq 0 \pmod{p}$ and it has two square roots of $\bmod p$ and two square roots $\bmod q$. Hence a has four square roots $\bmod n$.
- Let ± 1, $\pm w$ be the four square roots of 1 $\bmod n$. If b is one square root of a $\bmod n$, then the four square roots of a are $\pm b$, $\pm wb$.