RSA Cryptosystem, Number Theory, Primality Testing, and Security of RSA

Douglas Wikström
KTH Stockholm
dog@csc.kth.se

February 5

- The RSA Cryptosystem
- Number Theory
- Random Primes

The RSA Cryptosystem (1/2)

Key Generation.

- Choose n-bit primes p and q randomly and define $N = pq$.
- Choose e randomly in $\mathbb{Z}^*_{\phi(N)}$ and compute $d = e^{-1} \bmod \phi(N)$.
- Output the key pair $((N, e), (p, q, d))$, where (N, e) is the public key and (p, q, d) is the secret key.

The RSA Cryptosystem (2/2)

Encryption. Encrypt a plaintext m by computing

$$c = m^e \bmod N \enspace .$$

Decryption. Decrypt a ciphertext c by computing

$$m = c^d \bmod N \enspace .$$

Why Does It Work?

$$(m^e \bmod N)^d \bmod N = m^{ed} \bmod N$$

Why Does It Work?

$$\begin{aligned}(m^e \bmod N)^d \bmod N &= m^{ed} \bmod N \\ &= m^{1+t\phi(N)} \bmod N\end{aligned}$$

Why Does It Work?

$$
\begin{aligned}
(m^e \bmod N)^d \bmod N &= m^{ed} \bmod N \\
&= m^{1+t\phi(N)} \bmod N \\
&= m^1 \cdot \left(m^{\phi(N)}\right)^t \bmod N
\end{aligned}
$$

Why Does It Work?

$$
\begin{aligned}
(m^e \bmod N)^d \bmod N &= m^{ed} \bmod N \\
&= m^{1+t\phi(N)} \bmod N \\
&= m^1 \cdot \left(m^{\phi(N)}\right)^t \bmod N \\
&= m \cdot 1^t \bmod N
\end{aligned}
$$

Why Does It Work?

$$
\begin{aligned}
(m^e \bmod N)^d \bmod N &= m^{ed} \bmod N \\
&= m^{1+t\phi(N)} \bmod N \\
&= m^1 \cdot \left(m^{\phi(N)}\right)^t \bmod N \\
&= m \cdot 1^t \bmod N \\
&= m \bmod N
\end{aligned}
$$

Implementing RSA

- Modular arithmetic.
- Primality test.

Modular Arithmetic (1/2)

Basic operations on $O(n)$-bit integers using "school book" implementations.

Operation	Running time
Addition	$O(n)$
Subtraction	$O(n)$
Multiplication	$O(n^2)$
Modular reduction	$O(n^2)$

What about modular exponentiation?

Modular Arithmetic (2/2)

Square-and-Multiply.

$\mathit{SquareAndMultiply}(x, e, N)$

$z \leftarrow 1$
$i \leftarrow \lfloor \log_2 e \rfloor - 2$
while $i \geq 0$
  do
    $z \leftarrow z \cdot z \bmod N$
    if $e_i = 1$
      then $z \leftarrow z \cdot x \bmod N$
return z

Legendre Symbol (1/2)

Definition. Given an odd integer $b \geq 3$, an integer a is called a **quadratic residue** modulo b if there exists an integer x such that $a = x^2 \bmod b$.

Definition. The **Legendre Symbol** of an integer a modulo an odd prime p is defined by

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

Legendre Symbol (2/2)

Theorem. If p is an odd prime, then

$$\left(\frac{a}{p}\right) = a^{(p-1)/2} \bmod p \ .$$

Legendre Symbol (2/2)

Theorem. If p is an odd prime, then

$$\left(\frac{a}{p}\right) = a^{(p-1)/2} \bmod p \enspace .$$

Proof.

- If $a = y^2 \bmod p$, then $a^{(p-1)/2} = y^{p-1} = 1 \bmod p$.

Legendre Symbol (2/2)

Theorem. If p is an odd prime, then

$$\left(\frac{a}{p}\right) = a^{(p-1)/2} \bmod p \enspace .$$

Proof.

- If $a = y^2 \bmod p$, then $a^{(p-1)/2} = y^{p-1} = 1 \bmod p$.
- If $a^{(p-1)/2} = 1 \bmod p$ and b generates $\mathbb{Z}_p^*$, then $a^{(p-1)/2} = b^{x(p-1)/2} = 1 \bmod p$ for some x. Since b is a generator, $(p-1) \mid x(p-1)/2$ and x must be even.

Legendre Symbol (2/2)

Theorem. If p is an odd prime, then

$$\left(\frac{a}{p}\right) = a^{(p-1)/2} \bmod p \enspace .$$

Proof.

- If $a = y^2 \bmod p$, then $a^{(p-1)/2} = y^{p-1} = 1 \bmod p$.
- If $a^{(p-1)/2} = 1 \bmod p$ and b generates $\mathbb{Z}_p^*$, then $a^{(p-1)/2} = b^{x(p-1)/2} = 1 \bmod p$ for some x. Since b is a generator, $(p-1) \mid x(p-1)/2$ and x must be even.
- If a is a non-residue, then $a^{(p-1)/2} \neq 1 \bmod p$, but $\left(a^{(p-1)/2}\right)^2 = 1 \bmod p$, so $a^{(p-1)/2} = -1 \bmod p$.

Jacobi Symbol

Definition. The **Jacobi Symbol** of an integer a modulo an odd integer $b = \prod_i p_i^{e_i}$, with p_i prime, is defined by

$$\left(\frac{a}{p}\right) = \prod_i \left(\frac{a}{p_i}\right)^{e_i} \quad .$$

Properties of the Jacobi Symbol

Basic Properties.

$$\left(\frac{a}{b}\right) = \left(\frac{a \bmod b}{b}\right)$$
$$\left(\frac{ac}{b}\right) = \left(\frac{a}{b}\right)\left(\frac{c}{b}\right) \quad .$$

Law of Quadratic Reciprocity. If a and b are odd integers, then

$$\left(\frac{a}{b}\right) = (-1)^{\frac{(a-1)(b-2)}{4}} \left(\frac{b}{a}\right) \quad .$$

Supplementary Laws. If b is an odd integer, then

$$\left(\frac{-1}{b}\right) = (-1)^{\frac{b-1}{2}}$$
$$\left(\frac{2}{b}\right) = (-1)^{\frac{b^2-1}{8}} \quad .$$

Computing the Jacobi Symbol (1/2)

The following assumes that $a \geq 0$ and that $b \geq 3$ is odd.

$\textsc{Jacobi}(a, b)$
(1) **if** $a < 2$
(2) **return** a
(3) $s \leftarrow 1$
(4) **while** a is even
(5) $s \leftarrow s \cdot (-1)^{\frac{1}{8}(b^2-1)}$
(6) $a \leftarrow a/2$
(7) **if** $a < b$
(8) $\textsc{Swap}(\mathrm{a,b})$
(9) $s \leftarrow s \cdot (-1)^{\frac{1}{4}(a-1)(b-1)}$
(10) **return** $s \cdot \textsc{Jacobi}(a \bmod b, b)$

Prime Number Theorem

The primes are relatively dense.

Prime Number Theorem

The primes are relatively dense.

Theorem. Let $\pi(n)$ denote the number of primes $0 < p \leq n$. Then

$$\lim_{n\to\infty} \frac{\pi(n)}{\frac{n}{\ln n}} = 1 \enspace .$$

Prime Number Theorem

The primes are relatively dense.

Theorem. Let $\pi(n)$ denote the number of primes $0 < p \leq n$. Then

$$\lim_{n\to\infty} \frac{\pi(n)}{\frac{n}{\ln n}} = 1 \ .$$

To generate a random prime, we repeatedly pick a random integer and check if it is prime!

Solovay-Strassen Primality Test (1/2)

The following assumes that $n \geq 3$.

$\textsc{SolovayStrassen}(n, r)$

for $i = 1$ **to** r
    Choose $0 < a < n$ randomly.
    if $\left(\frac{a}{n}\right) = 0$ or $\left(\frac{a}{n}\right) \neq a^{(n-1)/2} \bmod n$
        return *composite*
return *probably prime*

Solovay-Strassen Primality Test (2/2)

Analysis.

- If n is prime, then $0 \neq \left(\frac{a}{n}\right) = a^{(n-1)/2} \bmod n$ for all $0 < a < n$.
- If $\left(\frac{a}{n}\right) = 0$, then $\left(\frac{a}{p}\right) = 0$ for some prime factor p of n. Thus, $p \mid a$ and n is composite.
- If n is composite, then at most half of all elements a in $\mathbb{Z}_n^*$ have the property that

$$\left(\frac{a}{n}\right) = a^{(n-1)/2} \bmod n \enspace .$$