Mathematical Cryptography

Kenneth Chu Study Notes September 8, 2013

1 The RSA Cryptosystem

1.1 Mechanism

Goal: Alice wants to send Bob an encrypted message through an insecure channel.

- Bob chooses his public key $(n, e) \in \mathbb{N}^2$ and private key $d \in \mathbb{N}$. Bob publishes his public key.
  - $n \in \mathbb{N}$ is called the modulus, with $n = pq$, where p and q are large distinct prime numbers. Note that Bob publishes n but keeps p and q secret.
  - $e \in \mathbb{N}$ is the called encryption exponent, and satisfies $\gcd(e, (p-1)(q-1)) = 1$.
  - $d \in \mathbb{N}$ is the called decryption exponent, and is determined by e and $n = pq$ via $d = e^{-1} \in \mathbb{Z}_{(p-1)(q-1)}$. Note that $e^{-1} \in \mathbb{Z}_{(p-1)(q-1)}$ exists since $\gcd(e, (p-1)(q-1)) = 1$.
- Alice
  - chooses plaintext $m \in \mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$.
  - encrypts her plaintext m using Bob's public key (n, e) by raising $m \in \mathbb{Z}_n$ to the e^{th} power. In other words, Alice computes her ciphertext $c = m^e \in \mathbb{Z}_n$.
  - sends to Bob through the insecure channel the ciphertext $c \in \mathbb{Z}_n$.
- Bob decrypts the ciphertext $c \in \mathbb{Z}_n$ from Alice by taking the e^{th} root of c in $\mathbb{Z}_n$ using his private key $d \in \mathbb{N}$ as follows:
$$c^d = (m^e)^d = m^{ed} = m^{1+k(p-1)(q-1)} = m \cdot (m^{(p-1)(q-1)})^k = m \cdot (1)^k = m \in \mathbb{Z}_n$$
  - The second last equality follows from $m^{(p-1)(q-1)} \equiv 1 \mod n$, which follows immediately from Euler's Theorem. It can also be justified with Fermat's Little Theorem as follows:
$$\text{Fermat's Little Theorem} \quad \Longrightarrow \quad \begin{cases} m^{(p-1)(q-1)} = \left(m^{p-1}\right)^{q-1} \equiv 1 \mod p, \ \text{and} \\ m^{(p-1)(q-1)} = \left(m^{q-1}\right)^{p-1} \equiv 1 \mod q. \end{cases}$$
    Hence, $m^{(p-1)(q-1)} - 1$ is divisble by both p and q, and hence also by $pq = n$ (since p and q are distinct primes). Thus, $m^{(p-1)(q-1)} \equiv 1 \mod n = pq$.

1.2 Comments

- One-way function (easy): Exponentiation in $\mathbb{Z}_n$.
  - Repeating Squaring Algorithm
- (Difficult) inverse function: Taking roots in $\mathbb{Z}_n$, for $n = pq$, where p and q are large distinct prime numbers.
- Trapdoor: If the factorization of $n = pq$ is known, then we can convert the inverse function (taking roots in $\mathbb{Z}_n$, which is slow) to an exponentiation in $\mathbb{Z}_n$, which is fast.

1.3 How to find large prime numbers?

- Generate random numbers x with $2^{1023} < x < 2^{1024}$.
- The Prime Number Theorem (from Analytic Number Theory) implies that, for large values of N, the probability that a randomly selected integer $x \in (2^{N-1}, 2^N)$ is prime is approximately

$$\frac{1}{\ln(2^N)}$$

- Test for the compositeness or "probable primality" of x using the Miller-Rabin primality test.

A Gibbs' Inequality & Jensen's Inequality

Theorem A.1 (Jensen's Inequality)

Suppose

- $(\Omega, \mathcal{A}, \mu)$ *is a probability space (i.e. measure space with* $\mu(\Omega) = 1$*).*
- $\varphi : (a, b) \longrightarrow \mathbb{R}$ *is a convex function, i.e.*

$$\varphi(t\,x_1 + (1-t)x_2) \leq t\,\varphi(x_1) + (1-t)\,\varphi(x_2), \quad \text{for any } t \in [0,1],\ x_1, x_2 \in (a,b),$$

  where $-\infty \leq a < b \leq \infty$*.*

- $g : \Omega \longrightarrow (a, b)$ *is a* μ*-integrable function.*

Then, the following inequality holds:

$$\varphi\left(\int_\Omega g\,\mathrm{d}\mu\right) \;\leq\; \int_\Omega \varphi \circ g\,\mathrm{d}\mu$$

Corollary A.2 (Jensen's Inequality (Expectation Form))

Suppose

- $X : (\Omega, \mathcal{A}, \mu) \longrightarrow (a, b)$ *is a* $\mathbb{R}$*-valued random variable defined on the probability space* $(\Omega, \mathcal{A}, \mu)$ *with range contained in the open interval* (a, b)*, where* $-\infty \leq a < b \leq \infty$*.*
- $\varphi : (a, b) \longrightarrow \mathbb{R}$ *is a convex function.*

Then, the following inequality holds:

$$\varphi\,(\,E[\,X\,]\,) \;\leq\; E[\,\varphi(X)\,]$$

Theorem A.3 (Gibbs' Inequality)

Suppose

- $(\Omega, \mathcal{A})$ *is a measurable space.*
- $f, g : \Omega \longrightarrow [0, \infty)$ *are two nowhere-vanishing probability density functions defined on* $(\Omega, \mathcal{A})$*.*

Then, the following inequality holds:

$$-\int_\Omega (\log f)\, f\,\mathrm{d}x \;\leq\; -\int_\Omega (\log g)\, f\,\mathrm{d}x$$

PROOF First, note that $\varphi := -\log : (0, \infty) \longrightarrow \mathbb{R}$ is a convex function defined on the open unit interval $(0, 1)$, and that the domain of φ contains the range of f and g. Hence, by Jensen's Inequality, we have:

$$\int_\Omega \left[-\log\left(\frac{g(x)}{f(x)}\right)\right]\cdot f(x)\,\mathrm{d}x \;\geq\; -\log\left(\int_\Omega \frac{g(x)}{f(x)}\cdot f(x)\,\mathrm{d}x\right) = -\log\left(\int_\Omega g(x)\,\mathrm{d}x\right) = -\log\,(\,1\,) = 0$$

The above inequality immediately implies:

$$-\int_\Omega (\log g(x))\cdot f(x)\,\mathrm{d}x \;\geq\; -\int_\Omega (\log f(x))\cdot f(x)\,\mathrm{d}x\,,$$

which completes the proof of Gibbs' Inequality. $\square$