EE 720: An Introduction to Number Theory and Cryptography (Spring 2020)

Lecture 18 — March 27, 2020

Instructor: Saravanan Vijayakumaran *Scribe: Saravanan Vijayakumaran*

1 Lecture Plan

- Plain RSA Numerical Example
- Primality Testing Algorithms

2 Plain RSA Example

- Recall that `GenRSA` is a PPT algorithm that on input 1^n, outputs a modulus N that is the product of two n-bit primes, along with integers $e, d > 1$ satisfying $ed = 1 \bmod \phi(N)$.
- **Example:** Suppose `GenRSA` outputs $(N, e, d) = (391, 3, 235)$. Note that $391 = 17 \times 23$ and $\phi(391) = 16 \times 22 = 352$. Also $3 \times 235 = 1 \bmod 352$.

  The message $m = 158 \in \mathbb{Z}_{391}^*$ is encrypted using public key $(391, 3)$ as $c = 158^3 \bmod 391 = 295$.

  Decryption of m is done as $295^{235} \bmod 391 = 158$.

3 Primality Testing

- But how to randomly generate n-bit primes required by `GenRSA`? Generate a random n-bit odd integer and check whether it is prime.
- **Bertrand's postulate:** For any $n > 1$, the fraction of n-bit integers that are primes is at least $\frac{1}{3n}$.
- So if we choose $3n^2$ random n-bit integers, the probability that a prime is not chosen is at most

$$\left(1 - \frac{1}{3n}\right)^{3n^2} = \left(\left(1 - \frac{1}{3n}\right)^{3n}\right)^n \leq \left(e^{-1}\right)^n = e^{-n}.$$

  We have use the result that for all $x \geq 1$ it holds that $\left(1 - \frac{1}{x}\right)^x \leq e^{-1}$.
- **Fermat's little theorem:** If p is a prime and a is any integer not divisible by p, then $a^{p-1} = 1 \bmod p$.
- For $a \in \{1, 2, \ldots, N-1\}$, if $a \notin \mathbb{Z}_N^*$ then $a^{N-1} \neq 1 \bmod N$, i.e. such an a is a witness for the compositeness of N. This is because $\gcd(a, N) \neq 1$ implies $\gcd(a^{N-1}, N) \neq 1$. Then $a^{N-1} \neq 1 \bmod N$. To see why, recall that the gcd of two integers is the smallest positive integer which can be written as a linear combination of those integers.

- But integers in the range $1, 2, \ldots, N-1$ **not** belonging to $\mathbb{Z}_N^*$ are rare. If N is prime, then there are no such integers as $\mathbb{Z}_N^* = \{1, 2, \ldots, N-1\}$. For composite $N = p_1^{e_1} \cdots p_k^{e_k}$ where $p_1, p_2, \ldots, p_k$ are distinct primes and $e_1, e_2, \ldots, e_k$ are positive integers, the cardinality of $\mathbb{Z}_N^*$ is $\phi(N) = p_1^{e_1-1}(p_1-1) \cdots p_k^{e_k-1}(p_k-1)$. Then the probability that a random element in $\{1, 2, \ldots, N-1\}$ is in $\mathbb{Z}_N^*$ is given by

$$\frac{\phi(N)}{N-1} \approx \frac{\phi(N)}{N} = \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_k}\right).$$

  If $p_1, p_2, \ldots, p_k$ are large primes, then this fraction is close to 1. If they are small primes, then it is easy to check that N is composite and fancy primality testing algorithms are not required.

- With this context, let us focus on the integers in $\mathbb{Z}_N^*$. For an integer N, we say that the integer $a \in \mathbb{Z}_N^*$ is a *witness for compositeness of* N if $a^{N-1} \neq 1 \bmod N$.

- For $a \in \{1, 2, \ldots, N-1\}$, if $a \in \mathbb{Z}_N^*$ then $\gcd(a, N) = 1$ and $\gcd(a^{N-1}, N) = 1$. This implies that $Xa^{N-1} + Yn = 1$ for some integers X, Y. So $Xa^{N-1} = 1 \bmod N$ but $a^{N-1} \bmod N$ may or may not be equal to 1. So the a's in $\mathbb{Z}_N^*$ may or may not be witnesses.

- **Theorem:** If there exists a witness (in $\mathbb{Z}_N^*$) that N is composite, then at least half the elements of $\mathbb{Z}_N^*$ are witnesses that N is composite.

  Proof. Consider the subset H of $\mathbb{Z}_N^*$ which consists of elements $a \in \mathbb{Z}_N^*$ satisfying $a^{N-1} = 1 \bmod N$. In other words, H is the set of elements in $\mathbb{Z}_N^*$ which are **not witnesses**. H is a subgroup of $\mathbb{Z}_N^*$ by the below Proposition. By the hypothesis, $H \neq \mathbb{Z}_N^*$. By Lagrange's theorem, the order of H is a proper divisor of $|\mathbb{Z}_N^*|$. Since the largest proper divisor of an integer m is possibly $m/2$, the size of H is at most $|\mathbb{Z}_N^*/2|$. So at least half the elements of $\mathbb{Z}_N^*$ are witnesses that N is composite. $\square$

- **Proposition 8.36:** Let G be a finite group and $H \subseteq G$. If H is nonempty and for all $a, b \in H$ we have $ab \in H$, then H is a subgroup of G.

- Suppose there is a composite integer N for which a witness for compositeness exists. Consider the following procedure which fails to detect the compositeness of N with probability at most 2^{-t}.

  1. For $i = 1, 2, \ldots, t$, repeat steps 2 and 3.
  2. Pick a uniformly from $\{1, 2, \ldots, N-1\}$.
  3. If $a^{N-1} \neq 1 \bmod N$, return "composite".
  4. If all the t iterations had $a^{N-1} = 1 \bmod N$, return "prime".

- But there exist composite numbers for which $a^{N-1} = 1 \bmod N$ for all integers $a \in \mathbb{Z}_N^*$. These are called *Carmichael numbers.* The number $561 = 3 \cdot 11 \cdot 17$ is one such number.

4 References and Additional Reading

- Sections 8.2.1, 8.2.2 from Katz/Lindell