EE 720: An Introduction to Number Theory and Cryptography (Spring 2018)

Lecture 22 — April 11, 2018

Instructor: Saravanan Vijayakumaran *Scribe: Saravanan Vijayakumaran*

1 Lecture Plan

- Primality Testing Algorithms

2 Recap

- Instance of a group-generation algorithm $\mathcal{G}$ with input being the security parameter 1^n
  1. Generate a uniform n-bit prime
  2. Generate an l-bit prime p such that q divides $p-1$
  3. Choose a uniform $h \in \mathbb{Z}_p^*$ with $h \neq 1$
  4. Set $g = h^{(p-1)/q} \bmod p$
  5. Return p, q, g.
- Let `GenRSA` be 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 $ed = 1 \bmod \phi(N)$.
- But how to randomly generate n-bit primes? Generate a random n-bit odd integer and check whether it is prime.

3 Primality Testing

- **Fermat's Little Theorem:** Let p be a prime. Then for every integer a, we have $a^p = a \bmod p$.
- 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 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. □

- 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.

3.1 Miller-Rabin Primality Test

- **Lemma:** We say that $x \in \mathbb{Z}_n^*$ is a **square root of 1 modulo** n if $x^2 = 1 \bmod n$. If n is an odd prime, then the only square roots of 1 modulo n are $\pm 1 \bmod n$.[1]
- The Miller-Rabin primality test is based on the above lemma.
- By Fermat's little theorem, if n is an odd prime $a^{n-1} = 1 \bmod n$ for all $a \in \{1, 2, \ldots, n-1\}$. Suppose $n - 1 = 2^r u$ where $r \geq 0$ is an integer and u is an odd integer. Then

  $$a^u \bmod n,\ a^{2u} \bmod n,\ a^{2^2 u} \bmod n,\ a^{2^3 u} \bmod n,\ \ldots,\ a^{2^r u} \bmod n$$

  is a sequence where each element is the square of the previous element. In other words, each element is the square root modulo n of the next element. Since the last element in the sequence is a 1, by the above lemma the previous elements should feature a -1 somewhere. So one of two things can happen:

[1] Note that $-1 \bmod n = n - 1 \in \mathbb{Z}_n^*$

  - Either $a^u = 1 \bmod n$. In this case, the whole sequence has only ones.
  - Or one of $a^u \bmod n,\ a^{2u} \bmod n,\ a^{2^2 u} \bmod n,\ a^{2^3 u} \bmod n,\ \ldots,\ a^{2^{r-1}u} \bmod n$ is equal to -1.

- We say that $a \in \mathbb{Z}_n^*$ is a **strong witness that** n **is composite** if both the above conditions do not hold.

- We say that a integer n is a prime power if $n = p^r$ where $r \geq 1$.

- **Theorem:** Let n be an odd number that is not a prime power. Then at least half the elements of $\mathbb{Z}_n^*$ are strong witnesses that n is composite.

4 References and Additional Reading

- Sections 8.2.1, 8.2.2 from Katz/Lindell