CS 6550: Randomized Algorithms **Spring 2019**

Lecture 12: RSA Encryption and Primality Testing

February 19, 2019

Lecturer: Eric Vigoda *Scribes: Shengding Sun and Yuanyuan Yang*

12.1 Preliminaries in number theory

The RSA public key encryption scheme relies on certain important results in number theory, in particular Fermat's little theorem and Euler's theorem.

Theorem 12.1 (Fermat's little theorem) *Let p be any prime number. Then for any a relatively prime to p, i.e. $\gcd(a,p)=1$, we have $a^{p-1} \equiv 1 \mod p$.*

Proof: Let $S = \{1, ..., p-1\}$. We let aS denote the set obtained from multiplying each element of S by a and then mod p , i.e. $aS = \{a \mod p, 2a \mod p, ..., (p-1)a \mod p\}$. We claim that $aS = S$.

First, we show that any two elements in aS are distinct. Suppose not, given i, j with $ai \equiv aj$, since a is relatively prime to p, its multiplicative inverse in $\mathbb{Z}_p$ exists. In other words, there exists b such that $ba \equiv 1 \mod p$. So we have $i \equiv bai \equiv baj \equiv j \mod p$. A contradiction.

Next we show that $0 \notin aS$. Suppose otherwise, then there exists $i \in \{1, ..., p-1\}$ such that $ai \equiv 0 \mod p$. But this is impossible since a and p are relatively prime.

Therefore $aS = S$, and in particular we have $\prod_{i \in S} i = \prod_{i \in aS} i$. In other words,

$$(p-1)! \equiv a^{n-1}(p-1)! \mod p$$

Since $(p-1)!$ is not 0 in $\mathbb{Z}_p$, its multiplicative inverse exists, and we have $a^{n-1} \equiv 1 \mod p$. ■

The generalization of this theorem for non-prime numbers is called the Euler's theorem, which is closely related to the Euler totient function.

Definition 12.2 *Given any integer $n \geq 2$, we define the Euler totient function $\phi(n)$ to be the number of elements in $\{1, ..., n-1\}$ that is relatively prime to n.*

The main properties we need for Euler totient function is that $\phi(p) = p - 1$ for any prime p, and $\phi(pq) = pq - p - q + 1 = (p-1)(q-1)$ for any prime p, q. The Euler's theorem is the following.

Theorem 12.3 (Euler's theorem) *Given $n \geq 2$ and a relatively prime to n. Then for any a relatively prime to n we have $a^{\phi(n)} \equiv 1 \mod n$.*

Proof: We omit the proof since it is very similar to the one of Fermat's little theorem. The set S in this case is the elements in $\{1, ..., n-1\}$ that are relatively prime to n. ■

12.2 RSA encryption algorithm

The RSA encryption is based on the hardness of factorizing large numbers. In this public key encryption scheme, Alice encrypts the message using the public key and send encrypted it to Bob, who possesses the private key that decrypts the message. This algorithm is designed in such a way that it is difficult for any adversary Eve to decrypt the ciphertext even if she knows the public key used in encryption.

Algorithm 1: RSA key generation

input : size N
output: public key $\{M, e\}$ and private key $\{M, d\}$

1 Choose p, q to be random N bit prime ;
2 $M = pq$;
3 Choose e relatively prime to $\phi(M) = pq - p - q + 1$;
4 Compute d satisfying $ed \equiv 1 \mod \phi(M)$;
5 **return** public key $\{M, e\}$, private key $\{M, d\}$;

Algorithm 2: RSA encryption

input : public key $\{M, e\}$, plaintext m
output: ciphertext c

1 **return** ciphertext $c = m^e \mod M$;

Algorithm 3: RSA decryption

input : private key $\{M, d\}$, ciphertext c
output: plaintext m

1 **return** plaintext $m = c^d \mod M$;

12.2.1 Correctness

For the correctness of this algorithm, we need to show that $m^{ed} \equiv m \mod M$, where m is any plaintext and M, e, d are the numbers in public and private keys.

Since $ed \equiv 1 \mod \phi(M)$, we have $ed = 1 + k\phi(M)$ for some integer k. Then $m^{ed} \equiv m^{k\phi(M)}m \equiv m \mod M$, since $m^{\phi(M)} \equiv 1 \mod M$ from Euler's theorem.

12.2.2 Implementation

When we choose e in step 3 of RSA key generation, we can try small primes $3, 5, 7, 11, 13$, etc to see whether any of it is a factor of $\phi(M)$. After a fixed number of trials, redo step 1 and 2 if all these small prime numbers fail.

In step 4, d can be effectively computed using Extended Euclidean algorithm. Notice that the runtime of step 3 and 4 is polynomial in N, which is the bit size of public key.

Now for step 1, for each p, q we are going to choose a random N bit number and test its primality. We will show, using the Prime number theorem, that the expected number of trials needed for the chosen number to be prime is linear in N.

Theorem 12.4 (Prime number theorem) *Let $X \geq 55$. Then*

$$\pi(X) > \frac{X}{\ln X + 2}$$

where $\pi(X)$ is the number of prime numbers less than or equal to X.

Therefore, the probability that a random N bit number is prime is at least

$$\frac{2^X/(\ln X + 2)}{2^X} = \frac{1}{2 + N \ln 2} = \Theta(1/N)$$

Therefore in expectation, $\Theta(N)$ trials suffices. In the next section, we will describe a randomized algorithm that tests whether a given number is prime.

12.3 Primality testing

12.3.1 Fermat witness

Due to Fermat's little theorem, if a number n is prime, then for any $1 \leq a < n$, we have $a^{n-1} \equiv 1 \mod n$. Therefore, if there exists an $a \in [1, n-1]$ with $a^{n-1} \not\equiv 1 \mod n$, then n is certified to be not prime. This is called a Fermat witness. Now if a and n have a common factor, then obviously $a^{n-1} \not\equiv 1 \mod n$ since it will be a multiple of $\gcd(a, n)$. Such a Fermat witness will be called trivial. These concepts are formalized in the following definition.

Definition 12.5 *Let n be a composite number. A number $a \in [1, n-1]$ is a Fermat witness if $a^{n-1} \not\equiv 1 \mod n$. A nontrivial Fermat witness is a Fermat witness a such that $\gcd(a, n) = 1$.*

Definition 12.6 (Carmichael Number) *A Carmichael Number is a composite n with no nontrivial Fermat witness.* [1]

For example, the first and smallest Charmichael Number is $561 = 3 \cdot 11 \cdot 17$

Lemma 12.7 *If n has ≥ 1 nontrivial Fermat witness, then the number of $g \in \{1, \ldots, n-1\}$ which are Fermat witness is $\geq (n-1)/2$.*

Proof:
We prove by showing the size of non-Fermat witnesses of n is $\leq$ that of Fermat witnesses of n:
Let a be a non-trivial Fermat witness for n, and we define B and G as follows:

$$B = \{b \in \{1, \ldots, n-1\} : b^{n-1} \equiv 1 \mod n\}$$

$$G = \{g \in \{1, \ldots, n-1\} : g^{n-1} \not\equiv 1 \mod n\}$$

Then, we denote a nontrivial Fermat witness of n as a and we use a to construct an injective function $f : B \to G$ as follows:

- From the definition of a, we have:

$$gcd(a, n) = 1,\ a^{n-1} \not\equiv 1 \mod n$$

- Then, for every $b \in B$, we construct $f(b)$ as follows:

$$f(n) \equiv ba \mod n$$

$$f^{n-1}(n) \equiv b^{n-1}a^{n-1} \equiv a^{n-1} \not\equiv 1 \mod n$$

  Hence, we have $f(b) \in G$.

- Now, let's prove that f is an injective function. Suppose we have $b,\ b'$ satisfies the following:

$$f(b) \equiv f(b') \mod n$$

  Then we have the following:

$$ba \mod b'a \mod n$$

  Notice that for non-trivial Fermat witness a, it has a multiplicative inverse, multiply this number for both sides of the equation, and then we have the following:

$$b \equiv b' \mod n$$

  Since $b,\ b' \in [n]$, it immediately follows that $b = b'$. Hence f is an injective function and $|B| \leq |G|$

[1] Ignoring *Charmichaels*, then every composite n has ≥ 1 nontrivial Fermat witness.

Then, we have $B \cap G = \emptyset$, $B \cup G = \{1, \ldots, n-1\}$ and $|B| \leq |G|$. Hence, we have:

$$|G| \geq (n-1)/2$$

The number of $g \in \{1, \ldots, n-1\}$ which are Fermat witness is $\geq (n-1)/2$. ■

Definition 12.8 (Square Root) *If $a^2 \equiv 1 \mod n$, then a is a square root of $1 \mod n$. Moreover, 1 and -1 are always square roots of $1 \mod n$*

Lemma 12.9 *For prime p, 1 and -1 are the only square roots of $1 \mod p$.*

Proof: Suppose $a^2 \equiv 1 \mod p$, then there exists $k \in \mathbb{Z}^+$, such that:

$$a^2 = 1 + kp$$

It immediately follows that:

$$(a+1)(a-1) = kp$$

Hence, $a \equiv \pm 1 \mod p$. ■

12.3.2 Primality Test when n is not *Carmichael*

Algorithm 4: Primality Test (not *Carmichael*)

input : N-bit number x, number of rounds k
output: x is prime/composite

```
1 Choose a_1, ..., a_k uniformly at random from {1, ..., x-1} ;
2 if for i = 1...k, (a_i)^{x-1} ≡ 1 mod x then
3 |  return x is prime;
4 else
5 |  return x is composite;
```

12.3.2.1 Correctness

For x is not *Carmichael*, from *Lemma 12.7*, we know that for a random chosen a_i, its probability of being a Fermat witness is ≥ 0.5 by the following:

$$\begin{aligned}
&Pr(\textit{output composite}|\ x \textit{ is composite and not Carmichael}) \\
=&Pr(a_i \textit{ is a Fermat witness of } x\ |x \textit{ is composite and not Carmichael}) \\
\geq&\frac{0.5(x-1)}{x-1} = \frac{1}{2}
\end{aligned}$$

Thus, for fixed k, the probability that our algorithm will output prime when x is composite and not *Carmichael* is:

$$\begin{aligned}
&Pr(\textit{output prime}|\ x \textit{ is composite and not Carmichael}) \\
=&\prod_{i=1}^{k} Pr(a_i \textit{ is not a Fermat witness of } x\ |x \textit{ is composite and not Carmichael}) \\
\leq&\frac{1}{2^k}
\end{aligned}$$

12.3.3 MillerRabin Primality Test

While computing each modular exponentiation, the algorithm looks for a nontrivial square root of 1, modulo n, during the final set of squarings. If it finds one, it stops and returns "x is composite". [1]

Algorithm 5: Primality Test(*Carmichael*)

input : N-bit number x, number of rounds k
output: x is prime/composite

```
Write x as 2^l · m + 1 with m odd (by factoring out powers of 2 from n − 1) ;
Choose a_1, ..., a_k uniformly at random from {1, ..., x − 1} ;
for i=1,...,k do
    x_0 = a_i^m mod x ;
    for j = 1, ..., l, do
        x_j = x_{j−1}^2 mod x ;
        if x_j == 1 and x_{j−1} ≠ 1 and x_{j−1} ≠ −1 then
            return x is composite
        if x_l ≠ 1 then
            return x is composite
return x is prime ;
```

For the sake of efficiency, we list out a few lemmas below without proving it, the proof ot lemmas can be found in [1].

12.3.3.1 Correctness

Lemma 12.10 *The equation $ax \equiv b \mod p$ is solvable for the unknown x iff $d|b$, where $d = gcd(a, n)$.*

Lemma 12.11 *If S' is a proper subgroup of a finite group S, then $|S'| \leq |S|/2$.*

Lemma 12.12 (A nonempty closed subset of a finite group is a subgroup) *If $(S, \oplus)$ is a finite group and S' is any nonempty subset of S such that $a \oplus b \in S'$ for all $a, b \in S'$, then $(S', \oplus)$ is a subgroup of $(S, \oplus)$.*

Lemma 12.13 *The values of $n > 1$ for which $\mathbb{Z}_n^*$ is cyclic are $2, 4, p^e$, and $2p^e$, for all primes $p > 2$ and all positive intergers e.*

Lemma 12.14 (Discrete logarithm theorem) *If g is a primitive root of $\mathbb{Z}_n^*$, then the equation $g^x \equiv g^y \mod n$ holds if and only if the equation $x \equiv y \mod \phi(n)$ holds.*

Theorem 12.15 (Lagranges theorem) *If $(S, \oplus)$ is a finite group and $(S', \oplus)$ is a subgroup of $(S, \oplus)$, then $|S'|$ is a divisor of $|S|$.*

Lemma 12.16 *If $n_1, n_2, \ldots, n_k$ are pairwise relatively prime and $n = n_1 n_2 \ldots n_k$, then for all integers x and a,*

$$x \equiv a \mod n_1 \iff x \equiv a \mod n$$

Lemma 12.17 *If $n_1, n_2, \ldots, n_k$ are pairwise relatively prime and $n = n_1 \ldots n_k$, then for any integers $a_1, a_2 \ldots, a_k$, the set of simultaneous equations $x \equiv a_i \mod n_i$, for $i = 1, 2, \ldots, k$ has a unique solution modulo n for the unknown x.*

Theorem 12.18 (Miller-Robin) [2] [3].
If $n \geq 4$ is composite, then

$$\frac{(n-1)}{2} \leq |Fermat\ Witness\ of\ x|$$

[2] This proof is in [1].
[3] The proof of 3/4 can be found in [2]

Proof:

We prove that the number of nonwitnesses is at most $(n-1)/2$, which implies the theorem.[4]

We start by claiming that any nonwitness must be a member of $\mathbb{Z}_n^*$. Consider any nonwitness a, it must satisfy $a^{n-1} \equiv 1 \mod n$. Thus, the equation $ay \equiv 1 \mod x$ has a solution, namely a^{n-2}. By *Lemma 12.10*, $gcd(a,n)|1 \Longrightarrow gcd(a,n) = 1$. Therefore, a is a member of $\mathbb{Z}_n^*$; all nonwitness belong to $\mathbb{Z}_n^*$.

To complete the proof, we show that not only are all nonwitness contained in $\mathbb{Z}_n^*$, they are all contained in a proper subgroup B of $\mathbb{Z}_n^*$.

By *Lemma 12.11*, we then have $|B| \leq |\mathbb{Z}_n^*|/2$. Since $|\mathbb{Z}_n^*| \leq n-1$, we obtain $|B| \leq (n-1)/2$. Therefore, the number of nonwitnesses is at most $(n-1)/2$, so that the number of witnesses must be at least $(n-1)/2$.

We now show how to find a proper subgroup B of $\mathbb{Z}_n^*$ containing all of the nonwitnesses. We break the proof into two cases.

1. There exists an $x \in \mathbb{Z}_n^*$ such that
$$x^{n-1} \not\equiv 1 \mod n$$
In other words, n is not a *Carmichael* number.
Let $B = \{b \in \mathbb{Z}_n^* : b^{n-1} \equiv 1 \mod n\}$. Clearly, B is nonempty, since $1 \in B$. Since B is closed under multiplication modulo n, we have that B is a subgroup of $\mathbb{Z}_n^*$ by *Lemma 12.12*. Note that every nonwitness belongs to B, since a non-witness a satisfies $a^{n-1} \equiv 1 \mod n$. Since $x \in \mathbb{Z}_n^* - B$, we have that B is a proper subgroup of $\mathbb{Z}_n^*$.

2. For all $x \in \mathbb{Z}_n^*$,
$$x^{n-1} \equiv 1 \mod n$$
In other words, n is a *Carmichael* number. (extremely rare in practice). In this case, n cannot be a prime power. To see why, let us suppose to the contrary that $n = p^e$, where p is a prime and $e > 1$. We derive a contradiction as follows. Since we assume that n is odd, p must also be odd. *Lemma 12.13* implies that $\mathbb{Z}_n^*$ is a cyclic group: it contains a generator g such that $ord_n(g) = |\mathbb{Z}_n^*| = \phi(n)$.Hence, we have $g^{n-1} \equiv 1 \mod n$. Then the discrete logarithm theorem (*Lemma 12.14*, taking $y = 0$) implies that $n - 1 \equiv 0 \mod \phi(n)$, or,
$$(p-1)p^{e-1} | p^e - 1$$
This is a contradiction for $e > 1$, since $(p-1)p^{e-1}$ is divisible by the prime p but $p^e - 1$ is not. Thus, n is not a prime power.
Since the odd composite number n is not a prime power, we decompose it into a product $n_1 n_2$, where n_1 and n_2 are odd numbers greater than 1 that are relatively prime to each other. (There may be several ways to choose $n_1,\ n_2$)
Recall that we define l and m so that $n - 1 = 2^l m$, where m is odd and $l \geq 1$, and that for an input a_i, our process computes the sequence.
$$X = [a_i^m, a_i^{2m}, \ldots, a^{2^l m}] \mod n$$
Let us call a pair (v, j) of integers **acceptable** is $v \in \mathbb{Z}_n^*,\ j \in \{0, \ldots, l\}$, and $v^{2^j m} \equiv -1 \mod n$.
Acceptable pairs certainly exist since u is odd; we can choose $v = n - 1$ and $j = 1$, so that $(n-1, 0)$ is an acceptable pair. Now pick the largest possible j such that there exists an acceptable pair (v, j) and fix v so that (v, j) is an acceptable pair. Let
$$B = \{x \in \mathbb{Z}_\ltimes^* : x^{2^j u \equiv \pm 1 \mod n}\}$$
Since B is closed under multiplication modulo n, it is a subgroup of $\mathbb{Z}_n^*$. By *Lagranges theorem*, therefore, $|B|$ divides $|\mathbb{Z}_n^*|$. Every nonwitness must be a member of B, n since the sequence X produced

[4]The x in algorithm is n in the proof

by a nonwitness must either be all 1's or else contain $a-1$ no later than the jth position, by the maximality of j . (If (a, j') is acceptable, where a is a nonwitness, we must have $j' \leq j$ by how we chose j .)

We now use the existence of v to demonstrate that there exists a $w \in \mathbb{Z}_n^* - B$, and hence that B is a proper subgroup of $\mathbb{Z}_n^*$. Since $v^{2^j m} \equiv -1 \mod n$, we have $v^{2^j m} \equiv -1 \mod n_1$ by *Lemma 12.16* to the Chinese remainder theorem. By *Lemma 12.16*, there exists a w simultaneously satisfying the equations

$$w \equiv v \mod n_1$$

$$w \equiv 1 \mod n_2$$

Therefore,

$$w^{2^j m} \equiv -1 \mod n_1$$

$$w^{2^j m} \equiv 1 \mod n_2$$

By *cor 31.29*, $w^{2^j m} \not\equiv 1 \mod n_1$ implies $w^{2^j m} \not\equiv 1 \mod n$, and $w^{2^j m} \not\equiv -1 \mod n_2$ implies $w^{2^j m} \not\equiv -1 \mod n$. Hence, we conclude that $w^{2^j m} \not\equiv \pm 1 \mod n$, and so $w \notin B$.

It remains to show that $w \in \mathbb{Z}_n^*$, which we do by first working separately modulo n_1 and modulo n_2. Working modulo n_1, we observe that since $v \in \mathbb{Z}_n^*$, we have that $gcd(v, n) = 1$, and so also $gcd(v, n_1) = 1$; if v does not have any common divisors with n, then it certainly does not have any common divisors with n_1. Sicne $w \equiv v \mod n_1$, we see that $gcd(w, n_1) = 1$. Working modulo n_2, we observe that $w \equiv 1 \mod n_2$ implies $gcd(w, n2) = 1$. To combine these results, we use *thm 31.6*, which implies that $gcd(w, n_1 n_2) = gcd(w, n) = 1$. That is, $w \in \mathbb{Z}_n^*$.

Therefore $w \in \mathbb{Z}_n^* - B$, and we finish case 2 with the conclusion that B is a proper subgroup of $\mathbb{Z}_n^*$.

In either case, we see that the number of witnesses to the compositeness of n is at least (n-1)/2.

■

Theorem 12.19 *For any odd integer $n > 2$ and positive integer k, the probability that M-R errors is at most 2^{-k}.*

Proof:

Following the same idea as **12.3.2.1**, it's easy to show that the probability that M-R errors is at most 2^{-k}. ■

References

[1] Cormen, Thomas H and Leiserson, Charles E and Rivest, Ronald L and Stein, Clifford. *Introduction to algorithms*, pages 968–974, 2009.

[2] Rabin, Michael O. Probabilistic algorithm for testing primality *Journal of number theory*, volume 12, pages 128–138, 1980.