

Cryptography CS 555

Lecture 14



Primality Testing and Attacks on RSA

Announcements

- Today's office hour cancelled
- For HW4, Problem 2 & 3
 - show knowledge of the extended Euclidean algorithm, i.e., either write a program, or compute by hand, with help from calculators
- Project due date
 - November 29(?)

Review of RSA

Public key: (e, n)

Secret key: d

where $n=pq$ and $ed \equiv 1 \pmod{\Phi(n)}$

Encrypting M: $M^e \pmod n$

Decrypting C: $C^d \pmod n$

Lecture Outline

- Number of prime numbers
- Cyclic groups
- Quadratic residues
- Primality testing
- Factorization
- Attacks on RSA



Number of Prime Numbers

Theorem

The number of prime numbers is infinite.

Proof: For the sake of contradiction, assume that the number of prime numbers is finite. Let p_1, p_2, \dots, p_k be all primes. Let $n = p_1 p_2 \dots p_k + 1$, then n must be composite.

Then there exists a prime p s.t. $p \mid n$ (fundamental theorem of arithmetic), and p cannot be any of the p_1, p_2, \dots, p_k . (Why?)

Therefore, p_1, \dots, p_k were not all the prime numbers.

Distribution of Prime Numbers

Theorem (Gaps between primes)

For every positive integer n , there are n or more consecutive composite numbers.

Proof Idea:

The consecutive numbers

$$(n+1)! + 2, (n+1)! + 3, \dots, (n+1)! + n+1$$

are composite.

(Why?)

Distribution of Prime Numbers

Definition

Given real number x , let $\pi(x)$ be the number of prime numbers $\leq x$.

Theorem (prime numbers theorem)

$$\lim_{x \rightarrow \infty} \frac{\pi(x)}{x / \ln x} = 1$$

For a very large number x , the number of prime numbers smaller than x is close to $x / \ln x$.

Generating large prime numbers

- Randomly generate a large odd number and then test whether it is prime.
- How many random integers need to be tested before finding a prime?
 - the number of prime numbers $\leq p$ is about $N / \ln p$
 - roughly every $\ln p$ integers has a prime
 - for a 512 bit p , $\ln p = 355$. on average, need to test about $177=355/2$ odd numbers
- Need to solve the Primality testing problem
 - the decision problem to decide whether a number is a prime

{ Complexity }

- **Complexity theory**: mathematical discipline that classifies problems based on the difficulty to solve them.
- **P-class** (polynomial-time): number of steps needed to solve a problem is bounded by some power of the problem's size.
- **NP-class** (nondeterministic polynomial-time): it permits a nondeterministic solution and the number of steps to verify the solution is bounded by some power of the problem's size.

Testing for Primality

Theorem

Composite numbers have a divisor below their square root.

Proof idea:

n composite, so $n = ab$, $0 < a \leq b < n$, then $a \leq \sqrt{n}$, otherwise we obtain $ab > n$ (contradiction).

Algorithm 1

```
for (i=2, i < sqrt(n) + 1; i++) {  
    If i a divisor of n {  
        n is composite  
    }  
}  
n is prime
```

Running time is $O(\sqrt{n})$, which is exponential in the size of the binary representation of n

More Efficient Algorithms for Primality Testing

- Primality testing is easier than prime factorization, and is in P-class.

How can we tell if a number is prime or not without factoring the number?

- The most efficient algorithms are randomized.
 - Solovay-Strassen
 - Rabin-Miller

More Number Theory First

- **Definition:** Given a group (G, \bullet) ,
 - the **order of G** is $|G|$
 - the **order of an element a** in G is the smallest positive integer such that $a^m=1$
 - $\{a, a^2, \dots, a^m\}$ is a subgroup of G
 - (why?)
- **Definition:** a group (G, \bullet) is a **cyclic group** if there exists $g \in G$ such that $G = \{g, g \bullet g, g^3, \dots, g^{|G|}\}$
 - g is known as a generator
 - the order of g is $|G|$
 - (why?)

Z_p^* is a Cyclic Group

- **Fact:** Given a prime p , Z_p^* is a cyclic group.
 - we won't prove it here.
- There exists $g \in Z_p^*$ s.t. $\{g^j \mid 1 \leq j \leq p-1\} = Z_p^*$
 - g is a generator of Z_p^* ,
 - g is also known as the primitive element modulo p
 - what is the order of g
- For example, 2 is a generator for Z_{11}^*
 - $\{2^j \mid 1 \leq j \leq p-1\} = \{2, 4, 8, 5, 10, 9, 7, 3, 6, 1\}$
 - what is the order of $4=2^2$? what is the order of $8=2^3$?
- Let g be a generator of Z_p^* , and let $a=g^j$
 - the order of a is $(p-1)/\gcd(p-1, j)$
 - what are the primitive elements in Z_{11}^* ?

To be Continued

- See Lecture 14-b

