Number Theory and Cryptographic Hardness Assumptions (数论与密码学困难度假设)-1

Sheng Zhong Yuan Zhang

Computer Science and Technology Department
Nanjing University

Outline

1. Where we are now

2. Preliminaries and Basic Group Theory
   - Primes and Divisibility
   - Modular Arithmetic
   - Groups

1. Where we are now
2. Preliminaries and Basic Group Theory

Private-key cryptography: a top-to-down view

A picture shows where we are:

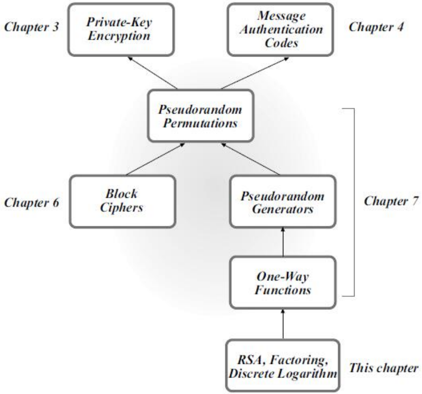

图 1: Private-key cryptography: a top-down approach

1. Where we are now

2. Preliminaries and Basic Group Theory
   - Primes and Divisibility
   - Modular Arithmetic
   - Groups

Some basic notations

- $\mathbb{Z}$: the set of integers.
- $a|b$ or a *divides* b $\Leftrightarrow$ For $a, b \in \mathbb{Z}$, there exists an integer c such that $ac = b$.
- $a \nmid b \Leftrightarrow a$ cannot divide b.
- a is a *divisor* or a *factor* of $b \Leftrightarrow a|b$ and $a > 0$.

Some basic notations

- $\mathbb{Z}$: the set of integers.
- $a|b$ or a *divides* b $\Leftrightarrow$ For $a, b \in \mathbb{Z}$, there exists an integer c such that $ac = b$.
- $a \nmid b \Leftrightarrow a$ cannot divide b.
- a is a *divisor* or a *factor* of $b \Leftrightarrow a|b$ and $a > 0$.
- a is called a *nontrivial divisor* of $b \Leftrightarrow a$ is a factor of b, AND $a \neq 1, b$.

Some basic notations (Contd.)

- $a > 1$ is a *prime* $\Leftrightarrow$ a has NO nontrivial divisor (i.e. it has only two divisors 1 and a.).
- $a > 1$ is a *composite* $\Leftrightarrow$ a is not a prime.[1]
- *gcd(a,b)*: the greatest common divisor of two integers a and b.
- a and b are *coprime* $\Leftrightarrow$ $gcd(a, b) = 1$.

[1] By convention, 1 is neither prime nor composite.

Unique representation of division-with-remainder

We have done lots of division with remainder in elementary school:

PROPOSITION 8.1: Uniqueness of division-with-remainder representation

Let a be an integer and let b be a positive integer. Then there exists unique integers q, r for which $a = qb + r$ and $0 \leq r < b$.

- Given integers $a, b \in [1, N]$, it is possible to compute q and r in polynomial time of $||N||$, where $||N|| = \lfloor \log N \rfloor + 1$.

Computing the greatest common divisor

A very useful result about the greatest common divisor is:

PROPOSITION 8.2

Let a, b be positive integers. Then there exist integers X, Y such that $Xa + Yb = gcd(a, b)$. Furthermore, $gcd(a, b)$ is the smallest positive integer that can be expressed in this way.

- The representation is not unique.
  e.g. Xa+Yb= (X+b)a+(Y-a)b=(X+2b)a+(Y-2a)b=...
- Given a and b, $gcd(a, b)$ can be computed using the Euclidean algorithm within polynomial time. And (X, Y) can be computed using the extended Euclidean algorithm within polynomial time.

Euclidean Algorithm

The Euclidean algorithm can be described as follows.

$gcd_{\text{loop}}(a, b)$

1. set r = 0;
2. **while** $(b \neq 0)$ {
3. $\quad r = a \mod b;$
4. $\quad a = b;$
5. $\quad b = r;$
6. }
7. **return** a;

or described using a recursion structure as

$gcd_{\text{recursion}}(a, b)$

1. **if** b=0, **return** a;
2. **else return** $gcd_{\text{recursion}}(b, a \mod b)$;

Examples of Euclidean algorithm

Q: Compute gcd(385, 245).

A: Using the Euclidean algorithm, we have

Round	a	b	r=a mod b
1	385	245	140
2	245	140	105
3	140	105	35
4	105	35	0
5	35	0	

Thus, gcd(385,245)=35.

Examples of the extended Euclidean algorithm

Q: Find (X,Y) such that 385X+245Y=35.
A: We record more information about how r is computed in each round in *extended Euclidean algorithm*:

Round	a	b	r=a mod b
1	385	245	140=385-245*1
2	245	140	105=245-140*1
3	140	105	35=140-105*1
4	105	35	0=105-35*3
5	35	0	

Then, we backtrace the computation as:

$$35 = 140 - 105$$
$$=140 - (245 - 140) = 140 \times 2 - 245$$
$$=(385 - 245) \times 2 - 245 = 385 \times 2 - 345 \times 3.$$

Thus, we have one possible $(X, Y) = (2, -3)$.

Examples of Euclidean algorithm

Q: Compute gcd(385, 246).

A: Using the Euclidean algorithm, we have

Round	a	b	r=a mod b
1	385	246	139
2	246	139	107
3	139	107	32
4	107	32	11
5	32	11	9
6	11	9	2
7	9	2	1
8	2	1	0
9	1	0	

We know gcd(385,246)$=$1, thus they are coprime to each other.

Basic notations in modular arithmetic

Let $a, b, N \in \mathbb{Z}$ with $N > 1$.

- $[a \mod N]$: the remainder of a upon division by N.
- Given $a = qN + r$ and $0 \leq r < N$, $[a \mod N] = r$.
- *reduction modulo N*: the process of mapping a to $[a \mod N]$.
- a and b are *congruent modulo N*, written as "$a = b \mod N$" $\Leftrightarrow [a \mod N] = [b \mod N]$.

Basic rules of modular arithmetic

Congruence modulo N obeys standard rules of arithmetic with respect to:

- **Addition**: e.g. $105 = 5 \mod 100, 25 = 25 \mod 100 \Rightarrow 105 + 25 = 5 + 25 \mod 100.$
- **Subtraction**: e.g. $105 = 5 \mod 100, 25 = 25 \mod 100 \Rightarrow 105 - 25 = 5 - 25 \mod 100.$
- **Multiplication**: e.g. $105 = 5 \mod 100, 25 = 25 \mod 100 \Rightarrow 105 \times 25 = 5 \times 25 \mod 100.$

Therefore, remember to "reduce and then add/subtract/multiply" to simplify the computing process.

e.g. try to compute $[109376854434 \times 111124555 \mod 100]$.

Divisions of modular arithmetic

Q: Does Congruence obeys standard rules of arithmetic with respect to **Division**? i.e.

$$a = a' \mod N, b = b' \mod N \overset{?}{\Rightarrow} \text{``}a/b = a'/b' \mod N\text{''}$$

A: Congruence modulo N does NOT (in general) respect division.

Example 1: We know $40 = 5 \mod 35, 5 = 5 \mod 35$. $40/5 = 8 \mod 35$ while $5/5 = 1 \mod 35$.

Similarly, we know
"$ab = cb \mod N$ does NOT necessarily imply that $a = c \mod N$".

Exercise: Try to verify whether the above implication holds for N=24,a=3,b=2,c=15.

To define a meaningful modular division

The inconsistency of arithmetic rules on modular divisions is because "$a/b \mod N$" is not always well-defined. In certain cases, we can define a meaningful notation of division?

- an integer b is *invertible modulo N* $\Leftrightarrow$ there exists an integer c such that $bc = 1 \mod N$. And c is called a (multiplicative) *inverse* of b modulo N.
- b^{-1}: the unique inverse of b that lies in the range $\{1, \ldots, N-1\}$.
- When b is invertible modulo N, we define *division by b modulo N* as multiplication by b^{-1}.

$$[a/b \mod N] \stackrel{def}{=} [ab^{-1} \mod N].$$

An well-defined modular division example

Example: Try to verify whether that

$$\text{“}ab = cb \mod N \text{ implies that } a = c \mod N\text{”}$$

holds for N=24,a=3,b=5,c=27.

A: The implication holds because $b = 5$ is invertible modulo 24 ($b^{-1} = 5$), thus the division is well-defined.

Which integers are invertible modulo N?

PROPOSITION 8.7

Let b, N be integers, with $b \geq 1$ and $N > 1$. Then b is invertible modulo N if and only if $gcd(b, N) = 1$.

证明.

"$\Rightarrow$"

If $gcd(b, N) = 1$, we can find integer X, Y such that $bX + NY = 1 \mod N$ (Prop.8.2). It is easy to see $bX = 1 \mod N$ and X is an inverse of b.

"$\Leftarrow$"

If b is invertible modulo N, let c be its inverse, we know $bc = 1 \mod N$, which implies $bc = \gamma N + 1$ for some $\gamma \in \mathbb{Z}$. Therefore, $bc - N\gamma = 1$. Since $gcd(b, N)$ is the smallest positive integer that can be expressed in this way, we know $1 = gcd(b, N)$. □

How to compute the multiplicative inverse?

Given b and N, how to compute b^{-1} modulo N?

- One method is to use the extended Euclidean algorithm to compute X, Y such that $bX + NY = 1 \mod N$, and $b^{-1} = [X \mod N]$.

Example: Let $b = 11$ and $N = 17$.
We get $(-3) \cdot 11 + 2 \cdot 17 = 1$, so $14 = [-3 \mod 17]$ is the inverse of 11.

The computation complexity of modular arithmetic

Given $a, b, c, N \in \{0,1\}^n$, the following computations can be performed within redpolynomial time of n.

- Addition: $[a + b \mod N]$.
- Subtraction: $[a - b \mod N]$.
- Multiplication: $[a \times b \mod N]$
- Computation of inverses: $a^{-1} \mod N$.
- Exponentiation :$a^c \mod N$.

Groups

Many cryptographic systems are defined on *groups*:

- A group is an algebraic structure consisting of a set of elements $\mathbb{G}$ together with a two-input operation $\circ$ on $\mathbb{G}$.

  e.g. $(\mathbb{Z}, +)$ is a group.
- $\mathbb{G}$ and $\circ$ have to satisfy the following conditions:
  - *Closure*. e.g. $3 + 5 \in \mathbb{Z}$; $x, y \in \mathbb{Z} \Rightarrow x + y \in \mathbb{Z}$.
  - *Existence of an identity*. e.g. $0 + x = x + 0 = x$.
  - *Existence of inverses*. e.g. $5 + (-5) = 0$; $x + (-x) = 0$.
  - *Associativity*. e.g. $(3 + 4) + 5 = 3 + (4 + 5)$.

Definition of a group

Formally, a group can be defined as follows:

DEFINITION 8.9

– A **group** is a set $\mathbb{G}$ along with a binary operation $\circ$ for which the following conditions hold:

- (**Closure**:) For all $g, h \in \mathbb{G}$, $g \circ h \in \mathbb{G}$.
- (**Existence of an identity**:) There exists an identity $e \in \mathbb{G}$ such that for all $g \in \mathbb{G}$, $e \circ g = e = g \circ e$.
- (**Existence of inverses**:) For all $g \in \mathbb{G}$ there exists an element $h \in \mathbb{G}$ such that $g \circ h = e = h \circ g$. Such an h is called an inverse of g.
- (**Associativity**:) For all $g_1, g_2, g_3 \in \mathbb{G}$, $(g_1 \circ g_2) \circ g_3 = g_1 \circ (g_2 \circ g_3)$.

– When $\mathbb{G}$ has a finite number of elements, we say $\mathbb{G}$ is finite and let $|G|$ denote the **order** of the group (that is, the number of elements in $\mathbb{G}$).
– A group $\mathbb{G}$ with operation $\circ$ is **abelian** if the following holds:

- (**Commutativity:**) For all $g, h \in \mathbb{G}$, $g \circ h = h \circ g$.

An (modulo addition) group example: $\mathbb{Z}_N$

Let $N > 1$ be an integer. The set $\{0, \dots, N-1\}$ with respect to addition modulo N is an abelian group.

- We denote this group by $\mathbb{Z}_N$ (with respect to modulo addition).
- The order of the group is N.

Q: Is $\mathbb{Z}_N$ with respect to modulo multiplication a group?

A: No.

An (modulo addition) group example: $\mathbb{Z}_N$

Let $N > 1$ be an integer. The set $\{0, \ldots, N-1\}$ with respect to addition modulo N is an abelian group.

- We denote this group by $\mathbb{Z}_N$ (with respect to modulo addition).
- The order of the group is N.

Q: Is $\mathbb{Z}_N$ with respect to modulo multiplication a group?

A: No.

1) Check N=8, $\{0, \ldots, 7\}$ is NOT a group with respect to multiplication, neither is $\{1, \ldots, 7\}$

2) Check N=7 and remove 0 from the set.

The (modulo multiplication) group $\mathbb{Z}_N^*$

For arbitrary integer $N > 0$, can we design a group with respect to multiplication modulo N?

Yes, for example, we can define a group $\mathbb{Z}_N^*$ with respect to (modulo) multiplication as follows.

$$\mathbb{Z}_N^* \stackrel{def}{=} \{b \in \{1, \ldots, N-1\} | gcd(b, N) = 1\};$$

- All elements in $\mathbb{Z}_N^*$ are co-prime to N.
- The set $\mathbb{Z}_N^*$ is called reduced residue class/system modulo N. Correspondingly, $\mathbb{Z}_N$ is called the complete residue class/system modulo N.
- Define $\phi(N) \stackrel{def}{=} |\mathbb{Z}_N^*|$. ($\phi$ is called the **Euler phi function**.)

What is the size of $\mathbb{Z}_N^*$

Regarding the size of $\mathbb{Z}_N^*$ (i.e. $\phi(N)$), we have the following theorem:

THEOREM 8.19

Let $N = \prod_i p_i^{e_i}$, where the p_i are distinct primes and $e_i \geq 1$. Then $\phi(N) = \prod_i p_i^{e_i - 1}(p_i - 1)$.

Example: Take $N = 15 = 5 \cdot 3$. Then

$$Z_{15}^* = \{1, 2, 4, 7, 8, 11, 13, 14\}.$$

And $|Z_{15}^*| = 8 = (5 - 1) \cdot (3 - 1)$.

Group exponentiation

- In many cryptographic systems, we often need to apply the group operations for a certain number of times to a fixed element g, i.e.

$$\underbrace{g \circ \ldots \circ g}_{m-1 \text{ times}}$$

Group exponentiation

- In many cryptographic systems, we often need to apply the group operations for a certain number of times to a fixed element g, i.e.

$$\underbrace{g \circ \ldots \circ g}_{m-1 \text{ times}}$$

When using multiplication notation to denote the group operation, we express the above application by g^m. That is

$$g^m \stackrel{def}{=} \underbrace{g \circ \ldots \circ g}_{m-1 \text{ times}}.$$

- Define $g^0 \stackrel{def}{=} 1$.
- Define $g^{-m} \stackrel{def}{=} (g^{-1})^m$.

A handy result on group exponentiation

THEOREM 8.14

Let $\mathbb{G}$ be a finite group with $m = |G|$, the order of the group. Then for any element $g \in \mathbb{G}$, $g^m = 1$.

Based on Thm 8.14, we have the following corollary:

COROLLARY 8.21 (Fermat-Euler Theorem)

Take arbitrary integer $N > 1$ and $a \in \mathbb{Z}_N^*$. Then $a^{\phi(N)} = 1 \mod N$. For the specific case that $N = p$ is a prime, we have $a^{p-1} = 1 \mod p$.

Fermat-Euler Theorem is quite useful for computing modular exponentiation and testing non-primarity.

Let's try

Q: What's $[2^{19491001} \mod 11]$?

Q: Is 221 a prime number? How about 223?