Group Theory in Cryptography

Alissa Tan Kel Zin

November 18, 2021

Table of Contents

Basics

Introduction

A group is a set of elements with a binary operation that satisfy certain properties.

Examples

1. Group of integer under addition $(\mathbb{Z}, +)$
   1.1 Adding 2 integers will result in an integer.
   1.2 Addition in $\mathbb{Z}$ is associative.
   1.3 There is an identity element 0 in the group.
   1.4 Every integer has a negative counterpart.
2. Group of rational number excluding 0 under multiplication $(\mathbb{Q} \setminus \{0\}, \times)$
   2.1 Multiplying 2 rational number will result in a rational number.
   2.2 Multiplication in $\mathbb{Q}$ is associative.
   2.3 There is an identity element 1 in the group.
   2.4 Every rational number other than 0 has an inverse.

Introduction

Applications

- Group is one of the algebraic structure in the studies of abstract algebra.
- There are many applications of group theory and mathematicians have used them to solve hard math problems.

Fermat's last theorem

No three positive integers a, b, and c satisfy the equation $a^n + b^n = c^n$ for any integer value of n greater than 2

Abel–Ruffini theorem

There is no solution in radicals to general polynomial equations of degree five or higher with arbitrary coefficients.

Definition and Axioms

A group denoted by $(G, \diamond)$ is a set G together with a binary operation $\diamond$ and satisfies four group axioms

1. Closure
   1.1 For all element a, b in G, $a \diamond b \in G$.
   1.2 $\forall a, b \in G, a \diamond b \in G$
2. Associativity
   2.1 For all element a, b, c in G, $(a \diamond b) \diamond c = a \diamond (b \diamond c)$.
   2.2 $\forall a, b, c \in G, (a \diamond b) \diamond c = a \diamond (b \diamond c)$
3. Identity
   3.1 There exists an unique identity element e such that for all element a in G, $a \diamond e = a$ and $e \diamond a = a$.
   3.2 $\exists! e \in G, \forall a \in G, (a \diamond e = a) \wedge (e \diamond a = a)$
4. Inverse
   4.1 For each element a in G, there exists an unique element a^{-1} in G such that $a \diamond a^{-1} = e$ and $a^{-1} \diamond a = e$.
   4.2 $\forall a \in G, \exists! a^{-1} \in G, (a \diamond a^{-1} = e) \wedge (a^{-1} \diamond a = e)$

Definition and Axioms

Abelian Group

Abelian/Commutative group are groups that satisfy one more axiom.

- Commutativity
  1. For all element a, b in G, $a \diamond b = b \diamond a$.

Finite Group

Finite group are groups that has finite amount of elements in the sets.

- One example is the integer group under addition modulo n $(\mathbb{Z}/n\mathbb{Z}, +)$
- Most of the groups commonly used in cryptography are finite group.

Definition and Axioms

Prove that Integer under addition $(\mathbb{Z}, +)$ is an abelian group

1. Closure
   1.1 Adding two integers will always result in another integer
2. Associativity
   2.1 Take any 3 arbitrary integers a, b, c, $(a + b) + c = a + (b + c)$
3. Identity
   3.1 Take any integer a, $a + 0 = a$ and $0 + a = a$
4. Inverse
   4.1 Take any integer a, $a + (-a) = 0$ and $(-a) + a = 0$
5. Commutativity
   5.1 Take any integer a,b, $a + b = b + a$

Definition and Axioms

Prove that rational number excluding 0 under multiplication $(\mathbb{Q} \setminus \{0\}, \times)$ is an abelian group

1. Closure
   1.1 Multiplying two rational number will always result in another rational number
2. Associativity
   2.1 Take any 3 arbitrary rational numbers a, b, c, $(a \times b) \times c = a \times (b \times c)$
3. Identity
   3.1 Take any rational number a, $a \times 1 = a$ and $1 \times a = a$
4. Inverse
   4.1 Take any rational number a, $a \times (\frac{1}{a}) = 1$ and $(\frac{1}{a}) \times a = 1$
5. Commutativity
   5.1 Take any integer a,b, $a \times b = b \times a$

Pop Quiz

Which of the following are groups?

1. $(\{x | x \in \mathbb{R}^{4\times 4} \wedge det(x) \neq 0\}, \times)$
   - Yes this is indeed a group and it is called the general linear group
   - It is denoted by $GL_n(\mathbb{R})$ or $GL(n, \mathbb{R})$ where n is the dimension of the matrix
   - Special linear group $SL_n(\mathbb{R})$ is general linear group but with determinant 1
2. $(\mathbb{C}, \times)$
   - Nope, this is not a group because 0 is in $\mathbb{C}$ but it does not have inverse
   - However, $(\mathbb{C} \setminus \{0\}, \times)$ is a valid group
3. $(\{ax^2 + bx + c | a, b, c \in \mathbb{Q}\}, +)$
   - Yes this is also a group

Finite Group

Infinite Groups are generally useful in the studies of mathematics. But finite groups are more popular and applicable in cryptography.

Example

Group of integer under addition modulo n $(\mathbb{Z}/n\mathbb{Z}, +)$

1. $(\mathbb{Z}/3\mathbb{Z}, +)$

$$\mathbb{Z}/3\mathbb{Z} = \{0, 1, 2\}$$

$$0 + 0 \equiv 0 \pmod 3$$
$$0 + 1 \equiv 1 \pmod 3$$
$$0 + 2 \equiv 2 \pmod 3$$
$$1 + 1 \equiv 2 \pmod 3$$
$$1 + 2 \equiv 0 \pmod 3$$
$$2 + 2 \equiv 1 \pmod 3$$

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

Table: Cayley Table

Finite Group

2. $(\mathbb{Z}/5\mathbb{Z}, +)$

$+$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

Multiplicative Finite Group

Group of integer under multiplication modulo n $(\mathbb{Z}/n\mathbb{Z} \setminus \{0\}, \times)$

- n must be a prime number
- The inverse of 2 modulo 4 does not exists

Finite Group

1. $(\mathbb{Z}/3\mathbb{Z} \setminus \{0\}, \times)$ or $(\mathbb{Z}/3\mathbb{Z})^\times$

$$1 \times 1 \equiv 1 \pmod 3$$
$$1 \times 2 \equiv 2 \pmod 3$$
$$2 \times 2 \equiv 1 \pmod 3$$

$\times$	1	2
1	1	2
2	2	1

Table: Cayley Table

2. $(\mathbb{Z}/5\mathbb{Z} \setminus \{0\}, \times)$ or $(\mathbb{Z}/5\mathbb{Z})^\times$

$\times$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

Subgroup

Definition

let $(G, \diamond)$ be a group.
let H be a subset of G.
$(H, \diamond)$ is a subgroup if H also forms a group under $\diamond$
This is denoted by $H \leq G$

Trivial Subgroup

The trivial subgroup of any group is the subgroup $\{e\}$ consisting of just the identity element.

Proper Subgroup

A proper subgroup of a group G is a subgroup H which is a proper subset of G (that is, $H \neq G$). This is usually represented notationally by $H < G$

Simple Group

Simple group are groups that only has 2 subgroup (Trivial Subgroup and itself)

Subgroup

Examples

1. $\mathbb{Z}/8\mathbb{Z}$ or $(\{0,1,2,3,4,5,6,7\},+)$
   1.1 $(\{0,1,2,3,4,5,6,7\},+)$
   1.2 $(\{0,2,4,6\},+)$
   1.3 $(\{0,4\},+)$
   1.4 $(\{0\},+)$
2. $\mathbb{Z}/10\mathbb{Z}$ or $(\{0,1,2,3,4,5,6,7,8,9\},+)$
   2.1 $(\{0,1,2,3,4,5,6,7,8,9\},+)$
   2.2 $(\{0,2,4,6,8\},+)$
   2.3 $(\{0,5\},+)$
   2.4 $(\{0\},+)$
3. $(\mathbb{Z}/7\mathbb{Z})^{\times}$ or $(\{1,2,3,4,5,6\},\times)$
   3.1 $(\{1,2,3,4,5,6\},\times)$
   3.2 $(\{1\},\times)$

Subgroup

Cosets

let $(G, \diamond)$ be a group.
let H be a subgroup of G.

The left cosets of H in G are the sets
$g \diamond H = \{g \diamond h \mid h \in H\}$ for each $g \in G$

Similarly for right cosets,
$H \diamond g = \{h \diamond g \mid h \in H\}$ for each $g \in G$

Properties

- Cosets of H are equal size and disjoint.
- left cosets is identical with right cosets in abelian group.

Subgroup

Examples

1. $\mathbb{Z}/8\mathbb{Z}$

   let $H = \{0, 2, 4, 6\}$
   The cosets of H are

   - $0 + \text{H} = \{0, 2, 4, 6\}$
   - $1 + \text{H} = \{1, 3, 5, 7\}$

   let $H = \{0, 4\}$
   The cosets of H are

   - $0 + \text{H} = \{0, 4\}$
   - $1 + \text{H} = \{1, 5\}$
   - $2 + \text{H} = \{2, 6\}$
   - $3 + \text{H} = \{3, 7\}$

2. $\mathbb{Z}/9\mathbb{Z}$

   let $H = \{0, 3, 6\}$
   The cosets of H are

   - $0 + \text{H} = \{0, 3, 6\}$
   - $1 + \text{H} = \{1, 4, 7\}$
   - $2 + \text{H} = \{2, 5, 8\}$

Subgroup

Generating set of a group

If S is a subset of a group G, then $\langle S \rangle$, the subgroup generated by S, is the smallest subgroup of G containing every element of S

Let $S = \{0, 3\}, G = \mathbb{Z}/9\mathbb{Z}$, $\langle S \rangle = \{0, 3, 6\}$

Cyclic Group

A cyclic group or monogenous group is a group that is generated by a single element

$(\mathbb{Z}/5\mathbb{Z})^{\times}$ is a cyclic group because 2 can be the generator

$\mathbb{Z}/n\mathbb{Z}$ is also a cyclic group because 1 can be the generator

Subgroup

Group Order

For any finite group G, the order of a group is the number of elements in the group

Order of an element

For any group $(G, \diamond)$, the order of an element g in the group is the smallest positive integer k such that $\underbrace{g \diamond g \diamond \cdots \diamond g}_{k \text{ times}} = g^k \equiv e$. The order is infinite if there is no such k.

The order of every element of a finite group is finite. The order of the element also equal to the order of the subgroup generated by the element.

Examples

1. $(\mathbb{Z}/5\mathbb{Z})^\times$
   1.1 $1^4 = 1 \equiv 1 \pmod 5$
   1.2 $2^4 = 16 \equiv 1 \pmod 5$
   1.3 $3^4 = 81 \equiv 1 \pmod 5$
   1.4 $4^4 = 256 \equiv 1 \pmod 5$

Subgroup

The order of every element of a finite group is finite.
The order of the element is equal to the order of the subgroup generated by the element

$$\begin{tikzcd} g^0 & g^1 & g^2 & \cdots & g^{n-1} \arrow[llll, bend right] \end{tikzcd}$$

$$\begin{tikzcd} g^0 & g^1 & g^2 & \cdots & g^m & \cdots & g^{n-1} \arrow[ll, bend right] \end{tikzcd}$$

Prove

1. Let $g \in G$ and consider the set $S = \{g^0 = e, g^1, g^2, \ldots\}$
2. Since G is a finite group, S must also be a finite group. $S = \{e, g^1, g^2, \ldots, g^{n-1}\}$
3. Let n be the number of elements in S and $g^n = g^m$, where $n > m$
4. $g^{n-m} = g^0 = e$. Since $n > m$, Therefore $n - m > 0$
5. Hence, there exists a positive integer k such that $g^k \equiv e$

Subgroup

Lagrange's Theorem

For any finite group G, the order (number of elements) of every subgroup of G divides the order of G.

Corollary

For any finite group G, let $g \in G$, n be the order of the group, k be the order of the element g
$g^k \equiv g^{ak} \equiv g^n \equiv e$, where $ak = n$

Fermat's Little Theorem

$a^{p-1} \equiv 1 \pmod{p}$, where p is a prime number

Euler's Theorem

$a^{\varphi(n)} \equiv 1 \pmod{n}$
Where $\varphi(n)$ is the Euler's totient function i.e the number of positive integers up to a given integer n that are relatively prime to n.

Subgroup

Prove

1. Let g be an element in G, H be a subgroup of G with a binary operation $\diamond$
2. Prove that g must be in one of the coset of H
   2.1 Since H contains the identity element, $g \in g \diamond H$
3. Prove that every coset that contains g are the same
   3.1 Let $A = g_1 \diamond H, B = g_2 \diamond H$ be 2 cosets that contains g
   3.2 Let $h_1, h_2 \in H$ such that $g_1 \diamond h_1 = g_2 \diamond h_2 = g$
   3.3 $g_1 = g_2 \diamond h_2 \diamond h_1^{-1}$
   3.4 let $h \in H$, $g_1 \diamond h = g_2 \diamond h_2 \diamond h_1^{-1} \diamond h$
   3.5 $A \subset B$
   3.6 Similarly for other direction, $B \subset A$, therefore $A = B$
4. The cosets of H partition G into disjoint sets of equal size, so the order of coset divides order of G.
5. Since the order of H equal to the order of coset, Lagrange's theorem is true.

Homomorphism

Definition

Given 2 Groups $(G, \diamond)$ and $(H, *)$, a group homomorphism is a function $f : G \to H$ such that $f(a \diamond b) = f(a) * f(b)$ where $a, b \in G$

Properties

- f maps the identity e_G to e_H. $f(e_G) = e_H$
- f maps the inverses to inverses $f(a^{-1}) = f(a)^{-1}$

Types

- Monomorphism (Injective)
- Epimorphism (Surjective)
- Isomorphism (Bijective)
- Endomorphism (Same domain and codomian)
- Automorphism (Endomorphism and Bijective)

Homomorphism

Examples

1. $f : \mathbb{Z} \to \mathbb{Z}/5\mathbb{Z}$
   1.1 $f(x) = x \bmod 5$
   1.2 $f(x+y) = (x+y) \bmod 5 = x \bmod 5 + y \bmod 5 = f(x) + f(y)$
   1.3 f is a group Epimorphism

2. $f : \mathbb{Z}/2\mathbb{Z} \to (\mathbb{Z}/3\mathbb{Z})^{\times}$
   2.1 $f(x) = x + 1$
   2.2 Cayley Table

$+$	0	1
0	0	1
1	1	0

Table: $\mathbb{Z}/2\mathbb{Z}$

$\times$	1	2
1	1	2
2	2	1

Table: $(\mathbb{Z}/3\mathbb{Z})^{\times}$

   2.3 f is a Group Isomorphism

Homomorphism

Properties

- By homomorphism, you can transfer group from one to other. Sometimes a problem can be easier to solve in other group
- All the groups that has prime order are isomorphic with the additive group $\mathbb{Z}/p\mathbb{Z}$
- All the groups that has order less than 3 are isomorphic with each other
- Every infinite cyclic group is isomorphic to the additive group of $\mathbb{Z}$.
- Every finite cyclic group of order n is isomorphic to the additive group of $\mathbb{Z}/n\mathbb{Z}$.

Kernel Group

Let $f : G \to H$ be a group homomorphism.
The kernel group is the set of elements from G which maps to the identity element in H
i.e. $f(g) = e_H$

Ring

Groups are set of elements with one operation.
Rings are set of element with two operations.

Definition

A Ring is a set R with two binary operation $+$ (addition) and $\cdot$ (multiplication) satisfying the axioms. 0 is the additive identity, 1 is the multiplicative identity

1. R is an abelian group under addition
2. Associativity of Multiplication
   2.1 For all element a, b, c in R, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$
3. Multiplicative Identity
   3.1 There exists an unique multiplicative identity 1 such that for all element a in G, $a \cdot 1 = a$ and $1 \cdot a = a$
4. Distributivity
   4.1 For all element a, b, c in R, $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$
   4.2 For all element a, b, c in R, $(b + c) \cdot a = (b \cdot a) + (c \cdot a)$

Ring

Commutative Ring

Commutative Ring is a ring in which the multiplication operation is commutative.

Unit

An element is called a unit of a ring when it has an multiplicative inverse.
The sets of unit from a ring form a group under multiplication.

Examples

1. $\mathbb{Z}$
2. $\mathbb{Z}/n\mathbb{Z}$
3. $\mathbb{Z}[x]$
4. $\mathbb{R}$
5. $\mathbb{R}[x]$

Ring

Properties

1. Additive identity 0 multiply any other element equals additive identity 0
   1.1 Let additive identity be e_a
   1.2 Let a be another element in the ring.
   1.3 $a \cdot e_a = e_a + e_a + \cdots + e_a = e_a$
2. Additive identity does not have an multiplicative inverse
   2.1 Let additive identity be e_a, multiplicative identity be e_m
   2.2 From 1, we know that e_a multiply with any element will result back in e_a
   2.3 Therefore, it is impossible that there exist e_a^{-1} such that $e_a \cdot e_a^{-1} = e_m$
3. If additive identity is the same as multiplicative identity. Then the ring only has the identity element.
   3.1 Let identity be e
   3.2 Suppose there exist another element a in the ring
   3.3 $e \cdot a = e = a$

Ring

Zero Divisor

An element a of a ring R is called a left zero divisor if there exists a nonzero $x \in R$ such that $a \cdot x = 0$. Similarly for right zero divisor.

Examples

1. $\mathbb{Z}/6\mathbb{Z}$
   1.1 $2 \cdot 3 = 6 \equiv 0 \pmod 6$
   1.2 2 and 3 are the zero divisors of $\mathbb{Z}/6\mathbb{Z}$
2. $\mathbb{Z}/10\mathbb{Z}$
   2.1 $2 \cdot 5 = 10 \equiv 0 \pmod{10}$
   2.2 2 and 5 are the zero divisors of $\mathbb{Z}/10\mathbb{Z}$

Domain

A domain is a ring which has no zero divisor.

Integral Domain

A commutative domain is also called an integral domain.

Field

Definition

A Field is a Set F with two binary operation $+$ (addition) and $\cdot$ (multiplication) satisfying the axioms.

1. Closure in both addition and multiplication
2. Associativity in both addition and multiplication
3. Commutative in both addition and multiplication
4. Exist both additive and multiplicative identity
5. Every element has additive inverse
6. Every element other than the additive identity has multiplicative inverse
7. Distributivity of multiplication over addition

Other Interpretation

1. Fields are Rings with multiplicative inverses and no zero divisors.
2. Field are combination of groups which relates through distributivity.

Field

Properties

1. Every field must have order of p^m where p is a prime number. p is also the characteristic of the field
2. All field with the same order are isomorphic with each other
3. We denote a finite field of order q with $GF(q)$

Examples

1. $\mathbb{Z}/5\mathbb{Z}$ or $GF(5)$

$+$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\times$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Field

Cauchy's Theorem

Let G be a finite group and p be a prime. If p divides the order of G, then G has an element of order p.

Prove

1. Take a non-identity element a from G and generate the subgroup $H = \langle a \rangle$
2. Since p divides $|G|$, p must either divides $|H|$ or $|G|/|H|$
3. Case 1 : p divides $|H|$
   3.1 Construct $k = a^{|H|/p}$
   3.2 k has order of p since $k^p = a^{|H|} = 1$
4. Case 2 : p divides $|G|/|H|$
   4.1 $\ldots$
5. Therefore, Cauchy's Theorem is True

Field

Order of Finite Field

Every field must have order of p^m where p is a prime number. p is also the characteristic of the field

Prove

1. Let a, b be two non-identity element from the field F
2. Let $h : \langle a \rangle \to \langle b \rangle$ such that $h(x) = b \cdot a^{-1} \cdot x$
3. $h(a + a) = b \cdot a^{-1} \cdot (a + a) = b + b$
4. The additive group of Finite Field are automorphic with each other and have the same order.
5. By Cauchy's theorem, if G does not have an element of order p, then p does not divides the order of G
6. Since every element of G has the same order, the order of every element must be a prime and $|G| = p^m$

Field

Prime Field

Field with prime order is isomorphic with $\mathbb{Z}/p\mathbb{Z}$, where p is a prime

Extension Field

Field with order p^m where $m > 1$ and p is prime

- Is $\mathbb{Z}/p^m\mathbb{Z}$ a field?
  1. $\mathbb{Z}/4\mathbb{Z}$
  2. 2^{-1} mod (4) does not exists
  3. p will not have an multiplicative inverse
- How do we construct a field with order p^m?
  1. Since we need $p \cdot p \cdot \ldots \cdot p$ elements, the simplest way is to use polynomial.
  2. $GF(p^m) = a_{m-1} \cdot x^{m-1} + a_{m-2} \cdot x^{m-2} + \cdots + a_1 \cdot x + a_0$, where $a_i \in GF(p)$
  3. Instead of number arithmetic, we now use polynomial arithmetic.

Field

Extension Field Arithmetic

- Addition
  1. Let $g, h \in GF(p^m)$
  2. $g + h = (g_0 + h_0) \bmod p + ((g_1 + h_1) \bmod p) \cdot x + \cdots + ((g_0 + h_0) \bmod p) \cdot x^{m-1}$
- Subtraction
  1. Let $g, h \in GF(p^m)$
  2. $g - h = (g_0 - h_0) \bmod p + ((g_1 - h_1) \bmod p) \cdot x + \cdots + ((g_0 - h_0) \bmod p) \cdot x^{m-1}$
- Multiplication
  1. Let $g, h \in GF(p^m)$
  2. Let P be an irreducible polynomial in $GF(p^m)$
  3. $f \equiv (g \cdot h) \bmod (P)$
- Inverse
  1. Let $g \in GF(p^m)$
  2. Let P be an irreducible polynomial in $GF(p^m)$
  3. $g^{-1} \cdot g \equiv 1 \bmod (P)$

Field

Irreducible polynomial

P is an irreducible polynomial in $GF(p^m)$ if P has degree of m and there are no 2 non-constant polynomials $a, b \in GF(p^m)$ such that $a \cdot b = p$

Quiz

1. x in $GF(2)$
   1.1 Yes, this is an irreducible polynomial
2. $x^2 + x + 1$ in $GF(4)$
   2.1 Yes, this is an irreducible polynomial
3. $x^2 + 1$ in $GF(4)$
   3.1 No, this is not an irreducible polynomial
   3.2 $(x+1)^2 = x^2 + 2x + 1 \equiv x^2 + 1$

Field

Examples

1. $GF(2^2)$ with $p = 1 + x + x^2$

+	0	1	x	x + 1
0	0	1	x	x + 1
1	1	0	x + 1	x
x	x	x + 1	0	1
x + 1	x + 1	x	1	0

×	0	1	x	x + 1
0	0	0	0	0
1	0	1	x	x + 1
x	0	x	x + 1	1
x + 1	0	x + 1	1	x

+	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

×	0	1	2	2
0	0	0	0	0
1	0	1	2	3
2	0	2	3	1
3	0	3	1	2

Application in Cryptography

Discrete Logarithm Problem

Definition

Let $(G, \diamond)$ be a group.
Let $g, b \in G$ such that $b = g^k = \underbrace{g \diamond g \diamond \cdots \diamond g}_{k \text{ times}}$

Find $k = \log_g b$

Examples

1. In group $(\mathbb{Z}/13\mathbb{Z})^{\times}$. Find k, where $5 \equiv 2^k \pmod{13}$
   1.1 When $\mathrm{k} = 9$, $2^9 = 512 \equiv 5 \pmod{13}$
2. In group $\mathbb{Z}/13\mathbb{Z}$. Find k, where $5 \equiv k \cdot 2 \pmod{13}$
   2.1 $k \equiv 5 \cdot 2^{-1} \pmod{13}$
   2.2 $k \equiv 5 \cdot 7 \equiv 35 \equiv 9 \pmod{13}$

Discrete Logarithm Problem

Discrete Logarithm Problem (DLP) is generally hard. However, it is easy to compute in a few special groups, such as the additive group modulo n.

Properties

1. A good one-way function
   1.1 It is easy to compute $b = g^k$ given g and k.
   1.2 By using double and add method, we can compute g^k in $O(log(k))$
   1.3 Algorithm that computes $\log_g b$ has a higher time complexity
   1.4 Baby-step giant-step algorithm takes $O(\sqrt{n})$ times to compute the discrete logarithm
2. Applicable to many groups
   2.1 Discrete Logarithm is hard to compute generally.
   2.2 Take any group and you can invent a new cryptographic scheme based on DLP

Discrete Logarithm Problem

Why discrete logarithm is easy for some groups?

Field extension

Given some group $(G, +)$, if there exist some field F which is extended from G, then the DLP in G is just the multiplication in F.

- $\mathbb{Z}$
- $\mathbb{Z}/n\mathbb{Z}$

However, there is no guarantee that multiplication in all fields are easy to compute.

Isomorphism

If we can find a group isomorphism between two groups G, H and given that DLP in H is easy, we can easily solve DLP in G too.

Discrete Logarithm Problem

Prime order

Since all group with prime order are isomorphic with $\mathbb{Z}/n\mathbb{Z}$. If a group G has prime order, then there exist a group isomorphism between G and $\mathbb{Z}/n\mathbb{Z}$.

- Anomalous elliptic curves

However, there is no guarantee that we can find the group isomorphism fast

Smooth order

If G is an abelian group and the order of G is smooth, then the DLP in G is easy to compute using Pohlig–Hellman algorithm.

- A number is said to be smooth if the highest prime factor of the number is small.

Diffie-Hellman Key Exchange

Two parties Alice, Bob wish to exchange a shared key through an public channel.

Preparation

Alice, Bob agree on a group $(G, \diamond)$ a generator $g \in G$ and function $f : G \to k$ that maps the group element to the set of keys

Exchange

1. Alice generate a random secret a and send $A = g^a = \underbrace{g \diamond g \diamond \cdots \diamond g}_{a \text{ times}}$ to Bob
2. Bob generate a random secret b and send $B = g^b = \underbrace{g \diamond g \diamond \cdots \diamond g}_{b \text{ times}}$ to Alice
3. Alice get the shared key by computing $f(B^a)$
4. Bob get the shared key by computing $f(A^b)$

Diffie-Hellman Key Exchange

Correctness

Since $B^a = A^b = g^{a \cdot b}$. Alice and Bob get the same shared key.

Security

The security of DHKE depends on the hardness of DLP in group G

Aftermath

After exchanging keys, two parties Alice and Bob can now communicate securely by encrypting/decrypting their messages using a symmetric encryption system such as AES through an unsecure channel

Diffie-Hellman Key Exchange

Example

1. $(\mathbb{Z}/13\mathbb{Z})^{\times}$, $g = 2$
    1.1 Alice : $a = 5$, $A \equiv 2^a \equiv 6 \pmod{13}$
    1.2 Bob : $b = 7$, $B \equiv 2^b \equiv 11 \pmod{13}$
    1.3 Alice send A to Bob, Bob send B to Alice
    1.4 Alice : $S = B^a \equiv 7 \pmod{13}$
    1.5 Bob : $S = A^b \equiv 7 \pmod{13}$

2. $(\mathbb{Z}/23\mathbb{Z})^{\times}$, $g = 2$
    2.1 Alice : $a = 14$, $A \equiv 2^a \equiv 8 \pmod{23}$
    2.2 Bob : $b = 5$, $B \equiv 2^b \equiv 9 \pmod{23}$
    2.3 Alice send A to Bob, Bob send B to Alice
    2.4 Alice : $S = B^a \equiv 16 \pmod{23}$
    2.5 Bob : $S = A^b \equiv 16 \pmod{23}$

ElGamal Encryption

Alice wish to securely send encrypted messages to Bob through a public channel.

Preparation

Alice, Bob agree on a group $(G, \diamond)$ a generator $g \in G$ and a bijective function $f : M \to G$ that maps the message to a group element

Encryption

1. Bob generate a random secret b and send $B = g^b$ to Alice
2. Alice generate a random secret a and computes $A = g^a$, $S = B^a$.
3. Alice maps the message m to a group element by $f(m) = g_m$
4. Alice computes $k = g_m \diamond S$ and sends A, k to Bob

Decryption

1. Bob compute $S = A^b$ and $g_m = k \diamond S^{-1}$
2. Bob decrypt the message by mapping g_m back to m using $f^{-1}(g_m) = m$

Elliptic Curve Cryptography

Elliptic Curve Cryptography is based on the group structure of elliptic curves over finite fields.

Properties

1. Diffie-Hellman Key Exchange, Elgamal Encryption are both applicable with Elliptic Curve Group.
2. It offers a better bit security compare to multiplicative group modulo n.
3. Discrete Logarithm is hard in well designed Elliptic Curve parameter.
4. It is widely used in modern cryptography and mathematics.

Reading Material

1. The Arithmetic of Elliptic Curves by Joseph H. Silverman
2. Elliptic Tales: Curves, Counting, and Number Theory by Avner Ash, Robert Gross

Challenges

PolyRSA

RSA with polynomial... Is it even possible?

Diagonal

Solving Discrete Logarithm is hard, it should be hard in this matrix group too?