Chapter 6: Public-key Cryptography

COMP 7120-8120
Lih-Yuan Deng
lihdeng@memphis.edu

Overview

- ElGamal Cryptosystem
- Discrete Logarithm Problem
- Algorithms for Discrete Logarithm Problem (skip)
- Finite Field
- Elliptic Curves (skip)
- Security of ElGamal Systems

ElGamal Cryptosystem

- Based on the difficulty of Discrete Logarithm Problem.
- Named after its inventor Taher El Gamal
- Used the same idea that we deal with real numbers:
  \[ y = \log_b x \leftrightarrow x = b^y, \text{ b=base, y=index.} \]
- Applied to a cyclic group. (how?)
Logarithm function for reals

- Suppose for the moment that we deal with real numbers:
  - $y = \log_b x \Leftrightarrow x = b^y$, $b=$base, $y=$index.
- Properties of logarithm function?
- Applications of logarithm function?
- How to define discrete logarithm (DL) function? Similarity/difference?

Property of logarithm function

- When $b=10$, $y = \log_{10} x = \log x$. (common log)
- When $b=e$, $y = \log_e x = \ln x$. (natural log)
- When $b=2$, $y = \log_2 x$ (number of binary bits)
- Formula for logarithm function?

Logarithm function formula

- $\log_b x = (\log_c x)/(\log_c b)$
- $\log_b (x_1 \cdot x_2) = \log_b x_1 + \log_b x_2$
- $\log_b \left(\frac{x_1}{x_2}\right) = \log_b x_1 - \log_b x_2$
- $\log_b x^a = a (\log_b x)$
- $\log_b b = 1$
- $\log_b 1 = 0$. 
Application of logarithm function

- \( \log_{10} (x_1 \times x_2) = \log_{10} x_1 + \log_{10} x_2 \)
- Before the popularity of calculator, the above formula is very useful to find the multiplication result of two real numbers. (why?)
- For real numbers, \( \log_b x \) is a continuous function of \( x \). That is, when \( x_1 \approx x_2 \), \( \log_b x_1 \approx \log_b x_2 \)

Group and subgroup

- \( G = \) multiplicative group of finite elements.
- Let an element \( g \in G \), the order of \( g \) is \( n \). That is, \( n = \min \{ c > 0 \mid g^c = 1 \} \).
- Define sub-group of \( G \):
  \[ <g> = \{ g^i : 0 \leq i \leq n-1 \} \]

Cyclic Group

- \( G \) is a cyclic group if there exists an element \( g \in G \) such that \( \text{order}(g) = \text{order}(G) \). Such a \( g \) is called a “generator” or “primitive element”.
- \( \mathbb{Z}_p^* = \{ 1, 2, \ldots, p-1 \} \) is a cyclic group, if \( p \) is a prime number.
- If \( g \) is a generator, then \( <g> = \mathbb{Z}_p^* \)
- If \( g \) is a not generator, then \( <g> \subset \mathbb{Z}_p^* \)
Example: \( Z_7^* = \{1, 2, 3, 4, 5, 6\} \)

<table>
<thead>
<tr>
<th>g</th>
<th>g^2</th>
<th>g^3</th>
<th>g^4</th>
<th>g^5</th>
<th>g^6</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>4</td>
<td>1</td>
<td>2</td>
<td>4</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>2</td>
<td>6</td>
<td>4</td>
<td>5</td>
<td>1</td>
</tr>
<tr>
<td>4</td>
<td>2</td>
<td>1</td>
<td>4</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>5</td>
<td>4</td>
<td>6</td>
<td>2</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>6</td>
<td>1</td>
<td>6</td>
<td>1</td>
<td>6</td>
<td>1</td>
</tr>
</tbody>
</table>

\( g = 2, \langle 2 \rangle = \{1, 2, 4\}; \quad g = 3, \langle 3 \rangle = \langle 1, 2, 3, 4, 5, 6 \rangle. \)

### Discrete Logarithm Problem

- \( G = \) multiplicative group of finite elements.
- Define sub-group of \( G: \langle \alpha \rangle = \{\alpha^i : 0 \leq i \leq n-1\}. \)
- For an element \( \beta \in \langle \alpha \rangle, \) find \( i \) such that \( \beta = \alpha^i \)
  - i.e. find discrete logarithm \( i = \log_\alpha \beta. \)

### Difference between real and discrete logarithm

- For real numbers, \( \log_b x \) is a continuous function of \( x. \) That is, when \( x_1 \approx x_2, \) \( \log_b x_1 \approx \log_b x_2. \)
- The above property is not true for discrete logarithm problem.
- There are many algorithms to find discrete logarithm, but no known algorithm is polynomial time in \( \log_2(n) \) when \( n \) is large.
Cryptosystem 6.1 (page 235)

- ElGamal Public-key Cryptosystem in $\mathbb{Z}_p^*$
- Plaintext space $P = \mathbb{Z}_p^*$,
- Ciphertext space $C = \mathbb{Z}_p^* \times \mathbb{Z}_p^*$
- key space $K = \{(p, a, \beta): \beta = a^a \mod p\}$
  - public keys: $p, a, \beta$
  - secret key: $a$

ElGamal Public-key Cryptosystem in $\mathbb{Z}_p^*$

- key space $K = \{(p, a, a, \beta): \beta = a^a \mod p\}$
  - secret key: $a$
- choose another random number $k \in \mathbb{Z}_p^*$
- Encryption: $e_k(x, k) = (y_1, y_2)$ where $y_1 = a^k \mod p$, $y_2 = x \beta^k \mod p$
- Decryption: (why?)
  $d_k(y_1, y_2) = y_2 \cdot (y_1^{-1})^k \mod p$. 

Example 6.1 (page 234)

- $p = 2579$. $(p-1)/2 = 1289$ is also a prime.
- $a = 2$ is a primitive root (why?)
  - $a^{(p-1)/q} \neq \mod p$, for prime $q | (p-1)$.
  - $a^{1289} = 2578 \mod 2579$.
  - $a^2 = 4 \mod 2579$.
- secret key $a = 765$. $\beta = a^{765} = 949 \mod p$.
- choose $k = 853$ randomly. $x = 1299$.
- $y_1 = 2^{853} = 435 \mod 2579$.
- $y_2 = 1299 \cdot 435 = 2396 \mod 2579$. 
Example 6.1 (page 235)
Decryption

- \( p = 2579 \).
- secret key \( a = 765 \). \( x = 1299 \).
- public key \( \beta = 949 \).
- \( y_1 = 435 \), \( y_2 = 2396 \).
- \( x = y_2 (y_1^a)^{-1} \mod p = 2396 (435^{765})^{-1} \mod 2579 = 1299 \).

Parameters for secure ElGamal Public-key Cryptosystem

- \( p \) must be a large prime (300 digits).
- \( p-1 \) should have at least one large prime factor.
  - e.g. \( (p-1)/2 \) is also a prime.
- \( \alpha \) is a primitive element in \( \mathbb{Z}_p^* \).
- exponent “\( a \)” should not be too small.
  - why?

Algorithms for Discrete Logarithm (DL) Problem

- DL Problem: Find \( \log_\alpha \beta \mod n \)
  1. Shanks’ Algorithm
  2. Pollard Rho DL Algorithm
  3. Pohlig-Hellman Algorithm
  4. Index Calculus Method
- Complexity lower bound of any generic DL algorithm is \( O(n^{0.5}) \).
Finite Field

- \( f(x) = \text{k-th degree polynomial over} \ Z_2=\{0,1\}. \) [Can also be defined over \( Z_p \)]
- Finite field \( F_{2^k} \) can be defined via an irreducible polynomial with coefficient in \( Z_2 \) of degree=\( k \).
- Q: how to determine \( f(x) \) is irreducible?

Finite Field \( F_{2^2} \)

- \( f(x)=x^2 + x + 1 \) is only irreducible 2nd degree polynomial. (why?)
  - \( f(x) = x^2 + 1 = (x+1)^2 \)
- \( a(x), b(x) \) are 1st degree polynomials.
- \( a(x) \oplus b(x) = a(x) + b(x) \) (mod \( f(x) \))
- \( a(x) \otimes b(x) = a(x) \times b(x) \) (mod \( f(x) \))

Finite Field \( F_{2^3} \)

- Find irreducible polynomial \( f(x)=x^3 + c_2 x^2 + c_1 x + 1. \) (how?)
  1. \( f(x) = x^3 + x^2 + x + 1 = (x+1)(x^2+1) = (x+1)^2. \) (why?)
  2. \( f(x) = x^3 + x + 1 \)
  3. \( f(x) = x^3 + x^2 + 1 \)
  4. \( f(x) = x^3 + 1 = (x+1)(x^2+x+1) \)
- \( f(x) = x^3 + x + 1 \) or \( x^3 + x^2 + 1. \)
Finite field: $F_{23}$

- $F_{23}^* = \{1, x, x+1, x^2, x^2 +1, x^2 +x, x^2 +x +1\}$ is a cyclic group under irreducible $f(x) = x^3+x+1$.
- $x$ is a primitive element (generator).
- It is easy to see (why?) $(3)^{6}=x^{18}=x^3$.
- We can easily construct a multiplication table. (how?)

<table>
<thead>
<tr>
<th>$i$</th>
<th>$x^i \mod f(x)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>$x$</td>
</tr>
<tr>
<td>2</td>
<td>$x^2$</td>
</tr>
<tr>
<td>3</td>
<td>$x+1$</td>
</tr>
<tr>
<td>4</td>
<td>$x^2 +x$</td>
</tr>
<tr>
<td>5</td>
<td>$x^2 +x +1$</td>
</tr>
<tr>
<td>6</td>
<td>$x^2 +1$</td>
</tr>
<tr>
<td>7</td>
<td>1</td>
</tr>
</tbody>
</table>

Another Finite field: $F_{23}$

- $F_{23}^* = \{1, x, x+1, x^2, x^2 +1, x^2 +x, x^2 +x +1\}$ is a cyclic group under irreducible $f(x) = x^3+x^2+1$.
- $x$ is a primitive element (generator).
- E.g. $(3)x(7)=? (1)$

<table>
<thead>
<tr>
<th>$i$</th>
<th>$x^i \mod f(x)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>$x$</td>
</tr>
<tr>
<td>2</td>
<td>$x^2$</td>
</tr>
<tr>
<td>3</td>
<td>$x^2 +1$</td>
</tr>
<tr>
<td>4</td>
<td>$x^2 +x +1$</td>
</tr>
<tr>
<td>5</td>
<td>$x +1$</td>
</tr>
<tr>
<td>6</td>
<td>$x^2 +x$</td>
</tr>
<tr>
<td>7</td>
<td>1</td>
</tr>
</tbody>
</table>

Elliptic Curves

- $y^2 = x^3 + a \cdot x + b$, where $4a^3 + 27b^2 \neq 0$.
- EC Curve over real (Fig 6.1, page 256)
- Result of $P_1 + P_2$ is shown.
Elliptic Curves Over $\mathbb{Z}_p$

- $y^2 = x^3 + a x + b$, where
  - $4a^3 + 27b^2 \neq 0$.
- EC Curve over $\mathbb{Z}_p$ or a finite field can be similarly defined. We can show that it is a group in which DL problem is also intractable. (skip)

Security of ElGamal Systems

- Bit-security of DL
- Semantic security of El Gamal Systems
- Diffie-Hellman Key Problem

Bit-security of DL

Problem 6.2 DL i-th Bit
- $K=\{(p, a, a, \beta): B= a^\beta \mod p\}$
- $L_i(\beta) = i$-th least significant bit of “$a” = log_{a}\beta$.
- It is easy to check “$a” is odd/even. (how? $\beta^{(p-1)/2} \mod p = \pm 1$, why?)
- “$a” is odd, then $L_i(\beta) = 1$, else $L_i(\beta) = 0$
Finding $L_i(\beta)$, $i \geq 2$.

- $L_i(\beta) =$ $i$-th least significant bit of “a” = $\log_\alpha \beta$.
- Q: Can we find $L_i(\beta)$ for $i=2$?
- If we can find an algorithm to find $L_i(\beta)$, then we can use it to solve the DL problem. [Algorithm 6.6, page 271]
- Implication?

Diffie-Hellman Key Exchange Problem

- Q: How to decide symmetric key between two parties over insecure channel?
- Choose a large prime $p$ and $g$=generator of $\mathbb{Z}_p^*$. (public key)
- A to B: A choose randomly “a” compute $g_a = g^a \mod p$. Send $g_a$ to B.
- B to A: B choose randomly “b” compute $g_b = g^b \mod p$. Send $g_b$ to A.
- Both A and B can compute the same key as $k = g_a b = g_b a \mod p$.

Computational Diffie-Hellman Problem (CDH)

- Let $\beta, \gamma \in <a>$. Find $\delta \in <a>$. such that
  $\log_\alpha \delta = \log_\alpha \beta \times \log_\alpha \gamma$
  i.e. Given $a^\alpha$ and $a^\gamma$, find $a^\delta$
- DDH (Decision Diffie-Hellman Problem)
  - decide whether the above situation holds or not.
  - $\text{DDH} \prec \text{CDH} \prec \text{DL}$. 
Summary
- ElGamal Cryptosystem
- Discrete Logarithm Problem
- Algorithms for Discrete Logarithm Problem (skip)
- Finite Field
- Elliptic Curves (skip)
- Security of ElGamal Systems

HW 6
- Chapter 6: 6.9, 6.10, 6.11, 6.12.