Chapter 9

The Discrete Logarithm (DL) Problem

- DL is the underlying one-way function for:

    1. Diffie-Hellman key exchange.
    2. DSA (digital signature algorithm).
    3. ElGamal encryption/digital signature scheme.
    4. Elliptic curve cryptosystems.
    5. ......

- DL is based on finite groups.

9.1 Some Algebra

Further Reading: [Big85].

9.1.1 Groups

Definition 9.1.1 *A group is a set $\mathcal{G}$ of elements together with a binary operation "$\circ$" such that:*

1. *If $a, b \in \mathcal{G}$ then $a \circ b = c \in \mathcal{G} \rightarrow$ (closure).*
2. *If $(a \circ b) \circ c = a \circ (b \circ c) \rightarrow$ (associativity).*
3. *There exists an identity element $e \in \mathcal{G}$:*
   $e \circ a = a \circ e = a \rightarrow$ (identity).
4. *There exists an inverse element $\tilde{a}$, for all $a \in \mathcal{G}$:*
   $a \circ \tilde{a} = e \rightarrow$ (inverse).

Examples:

1. $\mathcal{G}= Z = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$
   $\circ$ = addition
   $(Z, +)$ is a group with $e = 0$ and $\tilde{a} = -a$
2. $\mathcal{G}= Z$
   $\circ$ = multiplication
   $(Z, \times)$ is NOT a group since inverses $\tilde{a}$ do not exist except for $a = 1$
3. $\mathcal{G}=\mathcal{C}$ (complex numbers $u + iv$)
   $\circ$ = multiplication
   $(\mathcal{C}, \times)$ is a group with $e = 1$ and

$$\tilde{a} = a^{-1} = \frac{u - iv}{u^2 + v^2}$$

Definition 9.1.2 *"Z_n^*" denotes the set of numbers i, $0 \le i < n$, which are relatively prime to n.*

Examples:

1. $Z_9^* = \{1, 2, 4, 5, 7, 8\}$

2. $Z_7^* = \{1, 2, 3, 4, 5, 6\}$

Multiplication Table

$*$ mod 9	1	2	4	5	7	8
1	1	2	4	5	7	8
2	2	4	8	1	5	7
4	4	8	7	2	1	5
5	5	1	2	7	8	4
7	7	5	1	8	4	2
8	8	7	5	4	2	1

Theorem 9.1.1 *Z_n^* forms a group under modulo n multiplication. The identity element is $e = 1$.*

Remark:

The inverse of $a \in Z_n^*$ can be found through the extended Euclidean algorithm.

9.1.2 Finite Groups

Definition 9.1.3 *A group $(\mathcal{G}, \circ)$ is **finite** if it has a finite number of g elements. We denote the cardinality of $\mathcal{G}$ by $|\mathcal{G}|$.*

Examples:

1. $(Z_m, +)$: $a + b = c \bmod m$

   Question: What is the cardinality $\rightarrow |Z_m| = m$

   $Z_m = \{0, 1, 2, \ldots, m-1\}$

2. $(Z_p^*, \times)$: $a \times b = c \bmod p$; p is prime

   Question: What is the cardinality $\rightarrow |Z_p^*| = p - 1$

   $Z_p^* = \{1, 2, \ldots, p-1\}$

Definition 9.1.4 *The **order** of an element $a \in (\mathcal{G}, \circ)$ is the smallest positive integer o such that $a \circ a \circ \ldots \circ a = a^o = 1$.*

Example: $(Z_{11}^*, \times)$, $a = 3$

Question: What is the order of $a = 3$?

$a^1 = 3$

$a^2 = 3^2 = 9$

$a^3 = 3^3 = 27 \equiv 5 \bmod 11$

$a^4 = 3^4 = 3^3 \cdot 3 = 5 \cdot 3 = 15 \equiv 4 \bmod 11$

$a^5 = a^4 \cdot a = 4 \cdot 3 = 12 \equiv 1 \bmod 11$

$\Rightarrow \text{ord}(3) = 5$

Definition 9.1.5 *A group $\mathcal{G}$ which contains elements α with maximum order ord$(\alpha) = |\mathcal{G}|$ is said to be* ***cyclic****. Elements with maximum order are called* ***generators*** *or* ***primitive elements****.*

Example: 2 is a primitive element in Z_{11}^*

$|Z_{11}^*| = |\{1,2,3,4,5,6,7,8,9,10\}| = 10$

$a = 2$

$a^2 = 4$

$a^3 = 8$

$a^4 = 16 \equiv 5$

$a^5 = 10;$

$a^6 = 20 \equiv 9$

$a^7 = 18 \equiv 7$

$a^8 = 14 \equiv 3;$

$a^9 = 6$

$a^{10} = 12 \equiv 1$

$\underline{a^{11} = 2 = a}.$

$\Rightarrow$ ord$(a = 2) = 10 = |Z_{11}^*|$

$\Rightarrow$ (1) $|Z_{11}^*|$ is cyclic

$\Rightarrow$ (2) $a = 2$ is a primitive element

Observation (important): 2^i; $i = 1, 2, \ldots, 10$ **generates** all elements of Z_{11}^*

i	1	2	3	4	5	6	7	8	9	10
2^i	2	4	8	5	10	9	7	3	6	1

Some properties of cyclic groups:

1. The number of primitive elements is $\Phi(\lvert\mathcal{G}\rvert)$.
2. For every $a \in \mathcal{G}$: $a^{\lvert\mathcal{G}\rvert} = 1$.
3. For every $a \in \mathcal{G}$: $\mathrm{ord}(a)$ divides $\lvert\mathcal{G}\rvert$.

Proof only for (2): $a = \alpha^i$

$a^{|\mathcal{G}|} = (\alpha^i)^{|\mathcal{G}|} = (\alpha^{|\mathcal{G}|})^i \doteq 1^i = 1.$

Example: Z_{11}^*; $|Z_{11}^*| = 10$

1. $\Phi(10) = (2-1)(5-1) = 1 \cdot 4 = 4$
2. $a = 3 \rightarrow 3^{10} = (3^5)^2 = 1^2 = 1$
3. homework ...

9.2 The General DL Problem

Given a cyclic subgroup $(\mathcal{G}, \circ)$ and a primitive element α. Let

$$\beta = \underbrace{\alpha \circ \alpha \ldots \alpha}_{i \quad times} = \alpha^i$$

be an arbitrary element in $\mathcal{G}$.

General DL Problem:

$$\boxed{\begin{array}{l}\text{Given } \mathcal{G},\ \alpha, \beta = \alpha^i, \text{ find } i. \\ \\ \qquad\qquad i = \log_\alpha(\beta)\end{array}}$$

Examples:

1. $(Z_{11}, +)$; $\alpha = 2$; $\beta = \underbrace{2 + 2 + \ldots + 2}_{i \quad times} = i \cdot 2$

i	1	2	3	4	5	6	7	8	9	10	11
2i	2	4	6	8	10	1	3	5	7	9	0

   Let $i = 7$: $\beta = 7 \cdot 2 \equiv 3 \bmod 11$

   Question: given $\alpha = 2$, $\beta = 3 = i \cdot 2$, find i

   Answer: $i = 2^{-1} \cdot 3 \bmod 11$

   Euclid's algorithm can be used to compute i thus this example is NOT a one-way function.

2. $(Z_{11}^*, \times)$; $\alpha = 2$; $\beta = \underbrace{2 \cdot 2 \cdot \ldots \cdot 2}_{i \quad times} = 2^i$

   $\beta = 3 = 2^i \bmod 11$

   Question: $i = \log_2(3) = \log_2(2^i) = ?$

   Very hard computational problem!

9.3 Attacks for the DL Problem

1. **Brute force**:

   check:

   $\alpha^1 \stackrel{?}{=} \beta$

   $\alpha^2 \stackrel{?}{=} \beta$

   $\vdots$

   $\alpha^i \stackrel{?}{=} \beta$

   Complexity: $\mathcal{O}(|\mathcal{G}|)$ steps.

   Example: DL in $Z_p^* \approx \frac{p-1}{2}$ tests

   minimum security requirement $\Rightarrow p-1 = |\mathcal{G}| \geq 2^{80}$

2. **Shank's algorithm (Baby-step giant-step) and Pollard's-ρ method**:

   Further reading: p. 165 in [Sti95].

   Complexity: $\mathcal{O}(\sqrt{|\mathcal{G}|})$ steps (for both algorithms).

   Example: DL in $Z_p^* \approx \sqrt{p}$ steps

   minimum security requirement $\Rightarrow p-1 = |\mathcal{G}| \geq 2^{160}$

3. **Pohlig-Hellman algorithm**:

   Let $|\mathcal{G}| = p_1 \cdot p_2 \cdots \underbrace{p_l}_{largest \quad prime}$

   Complexity: $\mathcal{O}(\sqrt{p_l})$ steps.

   Example: DL in Z_p^*: p_l of $(p-1)$ must be $\geq 2^{160}$

   minimum security requirement $\Rightarrow p_l \geq 2^{160}$

4. **Index-Calculus method**:

   Further reading: [AM97].

   Applies only to Z_p^* and Galois fields GF(2^k)

   Complexity: $\mathcal{O}\ (e^{(1+\mathcal{O}(1))\sqrt{\ln(p)\ln(\ln(p))}})$ steps.

   Example: DL in Z_p^*: minimum security requirement $\Rightarrow p \geq 2^{1024}$

Remark: Index-Calculus is more powerful against DL in Galois Fields GF(2^k) than against DL in Z_p^*.

9.4 Diffie-Hellman Key Exchange

Remarks:

- Proposed in 1976 in Diffie-Hellman paper.
- Used in many practical protocols.
- Can be based on any DL problem.

9.4.1 Protocol

Set-up:

1. Find a large prime p.
2. Find a primitive element α of Z_p^* or of a subgroup of Z_p^*.

Protocol:

Alice		Bob
pick $k_{prA} = a_A \in \{2, 3, \ldots, p-1\}$		pick $k_{prB} = a_B \in \{2, 3, \ldots, p-1\}$
compute $k_{pubA} = b_A = \alpha^{a_A} \bmod p$		compute $k_{pubB} = b_B = \alpha^{a_B} \bmod p$
	$\xrightarrow{b_A}$	
	$\xleftarrow{b_B}$	
$k_{AB} = b_B^{a_A} = (\alpha^{a_B})^{a_A}$		$k_{AB} = b_A^{a_B} = (\alpha^{a_A})^{a_B}$

Session key $k_{ses} = k_{AB} = \alpha^{a_B \cdot a_A} = \alpha^{a_A \cdot a_B} \bmod p$.

9.4.2 Security

Question: Which information does Oscar have?

Answer: α, p, b_A, b_B.

Diffie-Hellman Problem:

$$\boxed{\text{Given } b_A = \alpha^{a_A} \bmod p, b_B = \alpha^{a_B} \bmod p, \text{ and } \alpha \text{ find } \alpha^{a_A \cdot a_B} \bmod p.}$$

One solution to the D-H problem:

1. Solve DL problem: $a_A = \log_\alpha(b_A) \bmod p$.
2. Compute: $b_B^{a_A} = (\alpha^{a_B})^{a_A} = \alpha^{a_A \cdot a_B} \bmod p$.

   Choose $p \geq 2^{1024}$.

Note:

> There is no proof that the DL problem is the only solution to the D-H problem!
>
> However, it is conjectured.