Discrete Mathematics

DLOG, CDH, Diffie-Hellman key exchange, cardinality

Liangfeng Zhang
School of Information Science and Technology
ShanghaiTech University

DLOG and CDH

DEFINITION: Let $G = \langle g \rangle$ be a cyclic group of order q. For every $h \in G$, there exists $x \in \{0,1,\dots,q-1\}$ such that $h = g^x$. The integer x is called the **discrete logarithm (DLOG) of** h **with respect to** g. Notation: $x = \log_g h$

DLOG Problem**:** $G = \langle g \rangle$ is a cyclic group of order q

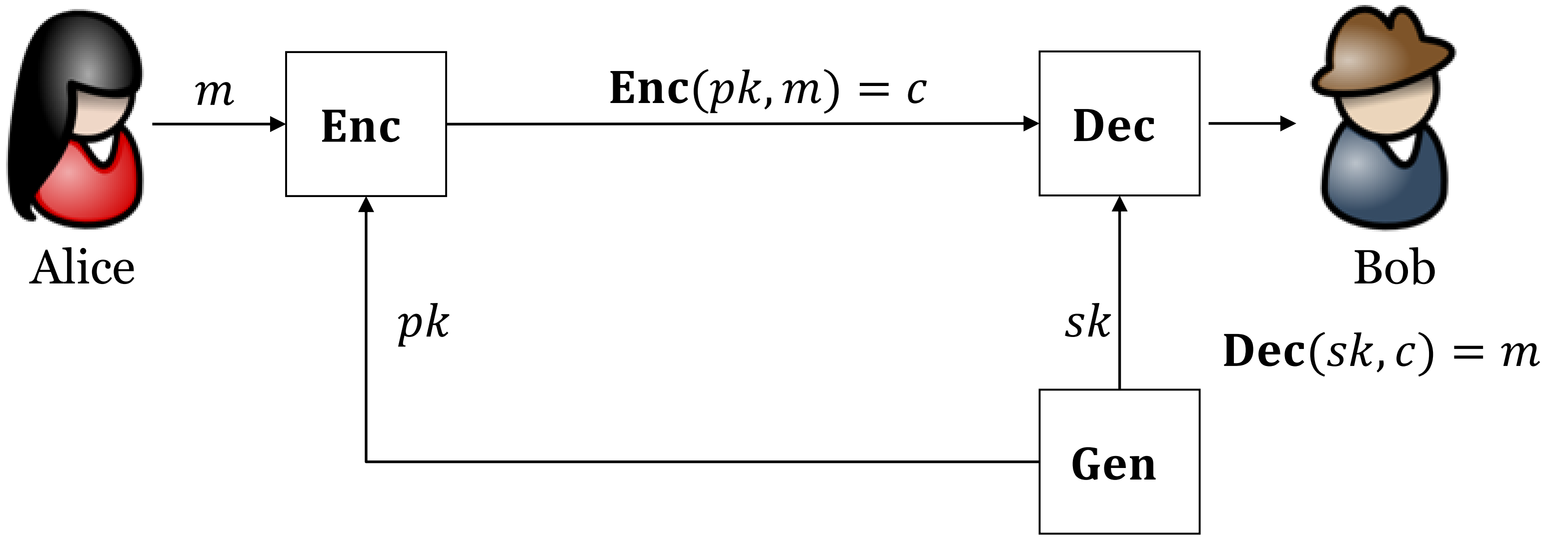
- **Input**: q, G, g and $h \in G$; **Output**: $\log_g h$

CDH Problem**: Computational Diffie-Hellman**

- **Input**: q, G, g and $A = g^a, B = g^b$ for $a, b \leftarrow \{0,1,\dots,q-1\}$; **Output**: g^{ab}

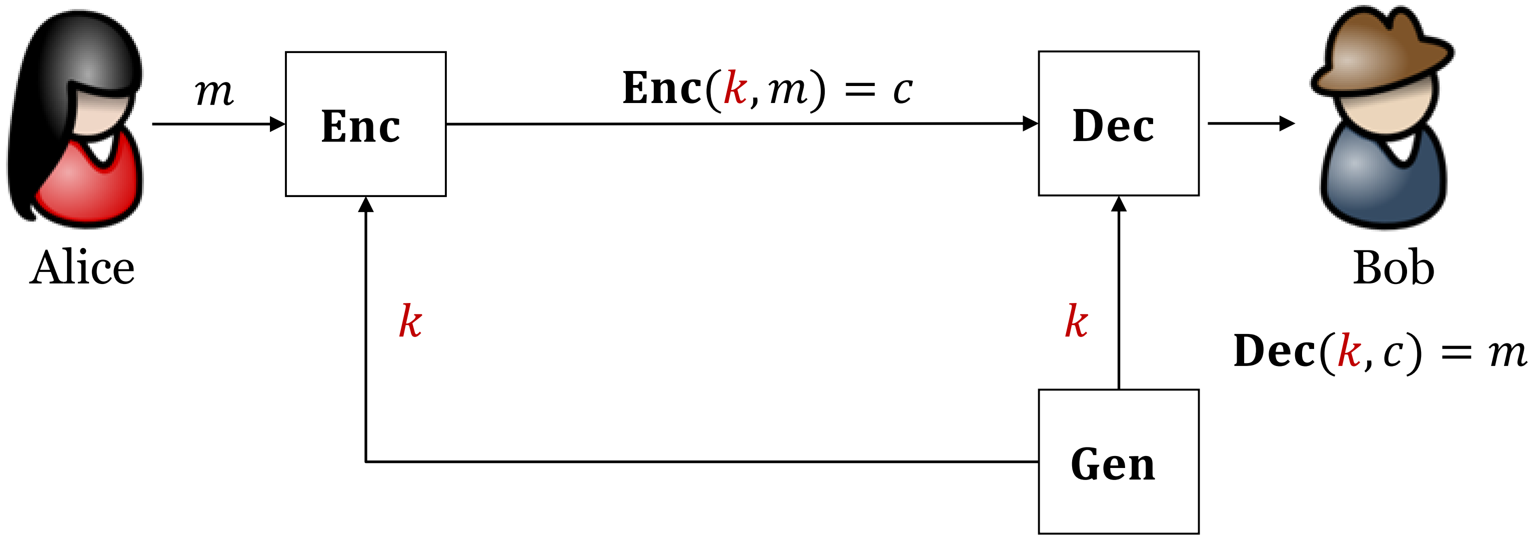
Hardness of DLOG and CDH: If $p = 2q + 1$ is a safe prime and G is the order q subgroup of $\mathbb{Z}_p^*$, then the best known algorithm for DLOG/CDH runs in time $\exp\left(O\left(\sqrt{\ln q \ln \ln q}\right)\right)$. $//q \approx 2^{2048}$

Public-Key Encryption



- **Gen**, **Enc**, **Dec**: key generation, encryption, decryption
- m, c, pk, sk: plaintext (message), ciphertext, public key, private key
- $\mathcal{M}, \mathcal{C}$: plaintext space, ciphertext space
- $\Pi = (\mathbf{Gen}, \mathbf{Enc}, \mathbf{Dec}) + \mathcal{M}, |\mathcal{M}| > 1$
  - **Correctness**: $\mathbf{Dec}\big(sk, \mathbf{Enc}(pk, m)\big) = m$ for any pk, sk, m
  - **Security**: if sk is not known, it's difficult to learn m from pk, c

Private-Key Encryption



- **Gen**, **Enc**, **Dec**: key generation, encryption, decryption
- m, c, k: plaintext (message), ciphertext, secret key
- $\mathcal{M}, \mathcal{C}$: plaintext space, ciphertext space
- $\Pi = (\mathbf{Gen}, \mathbf{Enc}, \mathbf{Dec}) + \mathcal{M}, |\mathcal{M}| > 1$
    - **Correctness**: $\mathbf{Dec}\big(k, \mathbf{Enc}(k, m)\big) = m$ for any k, m
    - **Security**: if k is not known, it's difficult to learn m from c

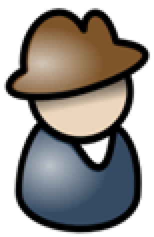
Diffie-Hellman Key Exchange

CONSTRUCTION: $G = \langle g \rangle$ is a cyclic group of prime order q

- Alice: $a \leftarrow \mathbb{Z}_q, A = g^a$; send (q, G, g, A) to Bob
- Bob: $b \leftarrow \mathbb{Z}_q, B = g^b$; send B to Alice; output $k = A^b$
- Alice: output $k = B^a$

Alice

Correctness: $A^b = g^{ab} = B^a$
Wiretapper: view $= (q, G, g, A, B)$
Security: view $\nrightarrow$ g^{ab} (CDH problem)



Bob

(q, G, g)
$a \leftarrow \mathbb{Z}_q$
$A = g^a$

$$\xrightarrow{\quad (q, G, g, A) \quad}$$

$b \leftarrow \mathbb{Z}_q$
$B = g^b$

$$\xleftarrow{\quad B \quad}$$

$k = B^a$ $\qquad$ $k = A^b$

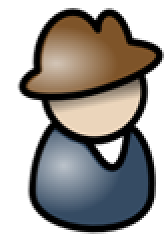
Whitfield Diffie, Martin E. Hellman: New directions in Cryptography, IEEE Trans. Info. Theory, 1976
Turing Award 2015

Diffie-Hellman Key Exchange

EXAMPLE: $p = 23$; $\mathbb{Z}_p^* = \langle 5 \rangle; G = \langle 2 \rangle, q = |G| = 11, g = 2$

Alice

Adversary: $q = 11, p = 23, g = 2, A = 8, B = 13, k = ?$



Bob

(q, G, g)

$a = 3$

$A = g^a = 8$

(q, G, g, A) $\longrightarrow$

$b = 7$

$B = g^b = 13$

$\longleftarrow$ B

$B^a = 12$

$A^b = 12$

Combinatorics

1666, Leibniz (1646-1716), **De Arte Combinatoria**

Enumerative combinatorics

- permutations, combinations, partitions of integers, generating functions, combinatorial identities, inequalities ......

Designs and configurations

- block designs, triple systems, Latin squares, orthogonal arrays, configurations, packing, covering, tiling ......

Graph theory

- graphs, trees, planarity, coloring, paths, cycles, ...

Extremal combinatorics

- extremal set theory, probabilistic method......

Algebraic combinatorics

- symmetric functions, group, algebra, representation, group actions......

Sets and Functions

DEFINITION: A **set** is an unordered collection of **elements**

- $a \in A$; $a \notin A$; roster method, set builder; empty set $\emptyset$, universal set
- $A = B$; $A \subseteq B$; $A \subset B$; $A \cup B$; $A \cap B$; $\bar{A}$

DEFINITION: Let $A, B \neq \emptyset$ be two sets. A **function (map)** $f: A \to B$ assigns a unique element $b \in B$ for all $a \in A$.

- **injective**: $f(a) = f(b) \Rightarrow a = b$
- **surjective**: $f(A) = B$
- **bijective**: injective and surjective

Cardinality of Sets

DEFINITION: Let A be a set. A is a **finite set** if it has finitely many elements; Otherwise, A is an **infinite set**.

- The **cardinality** $|A|$ of a finite set A is the number of elements in A.

EXAMPLE: $\emptyset, \{1\}, \{x: x^2 - 2x - 3 = 0\}, \{a, b, c, \dots, z\}$ are all finite sets; $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ are all infinite sets

DEFINITION: Let A, B be any sets. We say that A, B **have the same cardinality** ($|A| = |B|$) if there is a bijection $f: A \to B$

- We say that $|A| \le |B|$ if there exists an injection $f: A \to B$.
    - If $|A| \le |B|$ and $|A| \ne |B|$, we say that $|A| < |B|$

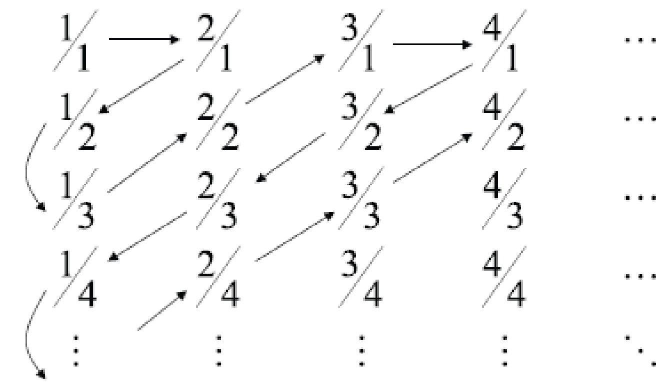
THEOREM: Let A, B, C be any sets. Then

- $|A| = |A|$
- $|A| = |B| \Rightarrow |B| = |A|$
- $|A| = |B| \land |B| = |C| \Rightarrow |A| = |C|$

Cardinality of Sets

EXAMPLE: $|\mathbb{Z}^+| = |\mathbb{N}| = |\mathbb{Z}| = |\mathbb{Q}^+| = |\mathbb{Q}|$

- $f: \mathbb{Z}^+ \to \mathbb{N} \quad x \mapsto x - 1$
- $f: \mathbb{Z} \quad \to \mathbb{N} \quad f(x) = \begin{cases} 2x & x \geq 0 \\ -(2x+1) & x < 0 \end{cases}$



$f: \mathbb{Z}^+ \to \mathbb{Q}^+$

EXAMPLE: $|\mathbb{R}^+| = |\mathbb{R}| = |(0,1)| = |[0,1]|$

- $f: \mathbb{R} \to \mathbb{R}^+ \quad x \mapsto 2^x$
- $f: (0,1) \to \mathbb{R} \quad x \mapsto \tan\big(\pi(x - 1/2)\big)$
- $f: [0,1] \to (0,1)$
  - $f(1) = 2^{-1}, f(0) = 2^{-2}, f(2^{-n}) = 2^{-n-2}, n = 1,2,3,\ldots$
  - $f(x) = x$ for all other x

Cardinality of Sets

THEOREM: $|(0,1)| \neq |\mathbb{Z}^+|$

- Suppose that $|(0,1)| = |\mathbb{Z}^+|$. Then there is a bijection $f: \mathbb{Z}^+ \to (0,1)$

$$
\begin{gathered}
f(1) = 0.b_{11}b_{12}b_{13}b_{14}b_{15}b_{16}b_{17}b_{18}b_{19}\cdots \\
f(2) = 0.b_{21}b_{22}b_{23}b_{24}b_{25}b_{26}b_{27}b_{28}b_{29}\cdots \\
f(3) = 0.b_{31}b_{32}b_{33}b_{34}b_{35}b_{36}b_{37}b_{38}b_{39}\cdots \\
f(4) = 0.b_{41}b_{42}b_{43}b_{44}b_{45}b_{46}b_{47}b_{48}b_{49}\cdots \\
f(5) = 0.b_{51}b_{52}b_{53}b_{54}b_{55}b_{56}b_{57}b_{58}b_{59}\cdots \\
f(6) = 0.b_{61}b_{62}b_{63}b_{64}b_{65}b_{66}b_{67}b_{68}b_{69}\cdots \\
\cdots \\
f(n) = 0.b_{n1}b_{n2}b_{n3}b_{n4}b_{n5}b_{n6}b_{n7}b_{n8}b_{n9}\cdots \\
\cdots
\end{gathered}
$$

- Let $b_i = \begin{cases} 4, & b_{ii} \neq 4 \\ 5, & b_{ii} = 4 \end{cases}$ for $i = 1,2,3,\ldots$
- $b = 0.b_1b_2b_3b_4b_5b_6b_7b_8b_9\cdots$ is in $(0,1)$ but has no preimage
  - $b \neq f(i)$ for every $i = 1,2,\ldots$
- f cannot be a bijection