Discrete Mathematics
Lecture 6

Liangfeng Zhang
School of Information Science and Technology
ShanghaiTech University

Summary of Lecture 5

Extended Euclidean Algorithm:

- **Input**: a, b $(a \geq b > 0)$
- **Output**: $d = \gcd(a, b)$, s, t such that $d = as + bt$

Linear congruence equation: $ax \equiv b (\bmod n)$

- **Solvable** if and only if $\gcd(a, n) \mid b$
- **Solution**: $x \equiv \frac{b}{d} t \left(\bmod \frac{n}{d}\right),\ t = \left(\frac{a}{d}\right)^{-1} \bmod \frac{n}{d}$

System of linear congruences:

$$\begin{cases} a_1 x \equiv b_1 \pmod{n_1} \\ a_2 x \equiv b_2 \pmod{n_2} \\ \vdots \\ a_k x \equiv b_k \pmod{n_k} \end{cases}$$

System of Linear Congruences

Sun-Tsu's Question: There are certain things whose number is unknown. When divided by 3, the remainder is 2; when divided by 5, the remainder is 3; and when divided by 7, the remainder is 2. What will be the number of things?

- $x \equiv 2 \pmod 3$; $x \equiv 3 \pmod 5$; $x \equiv 2 \pmod 7$

DEFINITION: A **system of linear congruences** is a set of linear congruence equations of the form

$$\begin{cases} a_1 x \equiv b_1 \pmod{n_1} \\ a_2 x \equiv b_2 \pmod{n_2} \\ \qquad \vdots \\ a_k x \equiv b_k \pmod{n_k} \end{cases}.$$

- $x \in \mathbb{Z}$ is a **solution** if it satisfies all k equations.

Chinese Remainder Theorem

两两互素，一对

THEROEM: Let $n_1, \ldots., n_k \in \mathbb{Z}^+$ be pairwise relatively prime and let $\boxed{n = n_1 \cdots n_k}$. Then for any $b_1, \ldots, b_k \in \mathbb{Z}$, then the system

$$x \equiv \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_k \end{pmatrix} \bmod \begin{pmatrix} n_1 \\ n_2 \\ \vdots \\ n_k \end{pmatrix}$$

$$\begin{cases} x \equiv b_1 \pmod{n_1} \\ x \equiv b_2 \pmod{n_2} \\ \qquad \vdots \\ x \equiv b_k \pmod{n_k} \end{cases}$$

$\gcd(n_i, n_j) = 1 \quad i \neq j$

always has a solution. Furthermore, if $b \in \mathbb{Z}$ is a solution, then any solution x must satisfy $x \equiv b \pmod{n}$.

- Let $N_i = n/n_i$ for every $i \in [k]$.
  - 两两互质 → $\gcd(N_i, n_i) = 1$ for every $i \in [k]$.
  - $\exists s_i, t_i, N_i s_i + n_i t_i = 1.$
- Let $b = b_1(\overset{x_1}{N_1 s_1}) + \cdots + b_k(\overset{x_k}{N_k s_k})$.
  - Then $b \equiv b_i \pmod{n_i}$ for every $i \in [k]$.

逆元

- $x \equiv b_i \pmod{n_i}$ for all i

$\Rightarrow x \equiv b \pmod{n_i}$ for all i

$\Rightarrow n_i | (x - b)$ for all i

$\Rightarrow (n_1 n_2 \cdots n_k) | (x - b)$

$\Rightarrow x \equiv b \pmod{n}$

$$x \equiv \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_k \end{pmatrix} \bmod \begin{pmatrix} n_1 \\ n_2 \\ \vdots \\ n_k \end{pmatrix}$$

$$\left.\begin{aligned}
x_1 &\equiv \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \bmod \begin{pmatrix} n_1 \\ n_2 \\ \vdots \\ n_k \end{pmatrix} \\
x_2 &\equiv \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix} \bmod \begin{pmatrix} n_1 \\ n_2 \\ \vdots \\ n_k \end{pmatrix} \\
&\vdots \\
x_k &\equiv \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix} \bmod \begin{pmatrix} n_1 \\ n_2 \\ \vdots \\ n_k \end{pmatrix}
\end{aligned}\right\} \text{有解（需证）} \longrightarrow b_1 x_1 \equiv \begin{pmatrix} b_1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \bmod \begin{pmatrix} n_1 \\ n_2 \\ \vdots \\ n_k \end{pmatrix}$$

$$\cdots$$

$$\Rightarrow b_1 x_1 + b_2 x_2 + \cdots + b_k x_k \equiv \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_k \end{pmatrix} \bmod \begin{pmatrix} n_1 \\ n_2 \\ \vdots \\ n_k \end{pmatrix}$$

$$x_1 \equiv \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \bmod \begin{pmatrix} n_1 \\ n_2 \\ \vdots \\ n_k \end{pmatrix} \Longrightarrow \begin{cases} x_1 \equiv 1 \bmod n_1 \\ x_2 \equiv 0 \bmod n_2 \\ \vdots \\ x_k \equiv 0 \bmod n_k \end{cases}$$

$n_2 \mid x_1,\ n_3 \mid x_1,\ \dots,\ n_k \mid x_1$

$\because n_2, \text{—}, n_k$ 两两互质 $\Longrightarrow n_2 n_3 \cdots n_k \mid x_1$

$x_1 = s\cdot(n_2 n_3 \cdots n_k) \Longrightarrow s(n_2 n_3 \cdots n_k) \equiv 1 \pmod{n_1}$

$\because \gcd(n_2 n_3 \cdots n_k, n_1) = 1 \quad \therefore \exists s_1, t_1 \in \mathbb{Z}$ s.t. $(n_2 n_3 \cdots n_k) s_1 + n_1 t_1 = 1$

$\therefore$ 取 $s = s_1 \Longrightarrow x_1 = s_1 n_2 \cdots n_k$

$\downarrow$

N_1 的逆元

Solution to Sun-Tsu's Question

EXAMPLE: Solve the system $\begin{cases} x \equiv 2 \pmod 3 \\ x \equiv 3 \pmod 5. \\ x \equiv 2 \pmod 7 \end{cases}$

- $n_1 = 3, n_2 = 5, n_3 = 7;\ n = n_1 n_2 n_3 = 105;\ b_1 = 2, b_2 = 3, b_3 = 2$
  - $N_1 = n_2 n_3 = 35, N_2 = n_1 n_3 = 21, N_3 = n_1 n_2 = 15$
  - $12\, n_1 - N_1 = 1; -4n_2 + N_2 = 1; -2\, n_3 + N_3 = 1$
  - $t_1 = 12, s_1 = -1; t_2 = -4, s_2 = 1; t_3 = -2, s_3 = 1$
- $b = b_1(N_1 s_1) + b_2(N_2 s_2) + b_3(N_3 s_3)$

  $= 2\,(-35) + 3\,(21) + 2(15)$

  $= 23$
- $x \in \mathbb{Z}$ is a solution of the system iff $x \equiv 23 \pmod{105}$
  - Solutions: $[23]_{105}$

CRT Map

THEOREM: Let $n_1, \ldots, n_k \in \mathbb{Z}^+$ and $\gcd(n_i, n_j) = 1$ for all $i \neq j$.

Let $n = n_1 \cdots n_k$. The **CRT map** $\theta([x]_n) = ([x]_{n_1}, \ldots, [x]_{n_k})$ is 双射（一一对应） a well-defined bijection from $\mathbb{Z}_n$ to $\mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}$.

- ***θ* is well-defined**: show that $[x]_n = [y]_n \Rightarrow \theta([x]_n) = \theta([y]_n)$
  - $[x]_n = [y]_n$
  - $x \equiv y \pmod{n}$
  - $x \equiv y \pmod{n_i}$ for every $i \in [k]$;
  - $[x]_{n_i} = [y]_{n_i}$ for every $i \in [k]$
  - $\theta([x]_n) = ([x]_{n_1}, \ldots, [x]_{n_k})$
    $= ([y]_{n_1}, \ldots, [y]_{n_k})$
    $= \theta([y]_n)$

$[x]_n = [y]_n \iff \theta([x]_n) = \theta([y]_n)$

CRT Map

THEOREM: Let $n_1, \dots, n_k \in \mathbb{Z}^+$ and $\gcd(n_i, n_j) = 1$ for all $i \neq j$.

Let $n = n_1 \cdots n_k$. The **CRT map** $\theta([x]_n) = ([x]_{n_1}, \dots, [x]_{n_k})$ is a well-defined bijection from $\mathbb{Z}_n$ to $\mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}$.

- ***θ* is bijective**: it suffices to show that θ is injective //why?
  - $\theta([x]_n) = \theta([y]_n)$
  - $([x]_{n_1}, \dots, [x]_{n_k}) = ([y]_{n_1}, \dots, [y]_{n_k})$
  - $[x]_{n_i} = [y]_{n_i}$ for every $i \in [k]$
  - $\underline{n_i}|(x - y)$ for every $i \in [k]$
  - $\underline{n}|(x - y)$
  - $[x]_n = [y]_n$

CRT Map

THEOREM: Let $n_1, \ldots, n_k \in \mathbb{Z}^+$ and $\gcd(n_i, n_j) = 1$ for all $i \neq j$.

Let $n = n_1 \cdots n_k$. The CRT map $\theta([x]_n) = ([x]_{n_1}, \ldots, [x]_{n_k})$ is a well-defined bijection from $\mathbb{Z}_n^*$ to $\mathbb{Z}_{n_1}^* \times \cdots \times \mathbb{Z}_{n_k}^*$.

- ***θ* is well-defined**:
  - show that $\theta([x]_n) \in \mathbb{Z}_{n_1}^* \times \cdots \times \mathbb{Z}_{n_k}^*$ for every $[x]_n \in \mathbb{Z}_n^*$
    - $[x]_n \in \mathbb{Z}_n^*$
    - $\gcd(x, n) = 1$
    - $\gcd(x, n_i) = 1$ for every $i \in [k]$
    - $[x]_{n_i} \in \mathbb{Z}_{n_i}^*$ for every $i \in [k]$
  - show that $[x]_n = [y]_n \Rightarrow \theta([x]_n) = \theta([y]_n)$
    - see the previous theorem
- ***θ* is injective**: see the previous theorem

CRT Map

THEOREM: Let $n_1, \dots, n_k \in \mathbb{Z}^+$ and $\gcd(n_i, n_j) = 1$ for all $i \neq j$.

Let $n = n_1 \cdots n_k$. The CRT map $\theta([x]_n) = ([x]_{n_1}, \dots, [x]_{n_k})$ is a well-defined bijection from $\mathbb{Z}_n^*$ to $\mathbb{Z}_{n_1}^* \times \cdots \times \mathbb{Z}_{n_k}^*$.

满射 原像

- ***θ* is surjective**: Let $([b_1]_{n_1}, \dots, [b_k]_{n_k}) \in \mathbb{Z}_{n_1}^* \times \cdots \times \mathbb{Z}_{n_k}^*$. Preimage?
  - Solve the system $x \equiv b_i \pmod{n_i}$, $1 \leq i \leq k$
  - Due to CRT, there is a solution b
  - $b \equiv b_i \pmod{n_i}$ for all $i \in [k]$
  - $\gcd(b, n_i) = 1$ for all $i \in [k]$
    - Otherwise, $\gcd(b_i, n_i) > 1$, contradiction.
  - $\gcd(b, n_1 n_2 \cdots n_k) = 1$
  - $\theta([b]_n) = ([b]_{n_1}, \dots, [b]_{n_k})$
    $= ([b_1]_{n_1}, \dots, [b_k]_{n_k})$
  - $[b]_n$ is a preimage of $([b_1]_{n_1}, \dots, [b_k]_{n_k})$

Euler's Phi Function

THEOREM: Let $n_1, \ldots, n_k \in \mathbb{Z}^+$ be pairwise relatively prime.
Let $n = n_1 \cdots n_k$. Then $\phi(n) = \phi(n_1) \cdots \phi(n_k)$.

- $\theta\colon \mathbb{Z}_n^* \to \mathbb{Z}_{n_1}^* \times \cdots \times \mathbb{Z}_{n_k}^*$ is bijective
- $\phi(n) = \phi(n_1) \times \cdots \times \phi(n_k)$

推论

COROLLARY: If $n = p_1^{e_1} \cdots p_k^{e_k}$ for distinct primes $p_1, \ldots, p_k$ and integers $e_1, \ldots, e_k \geq 1$, then $\phi(n) = n(1 - p_1^{-1}) \cdots (1 - p_k^{-1})$.

- $\phi(n) = \phi(p_1^{e_1}) \cdots \phi(p_k^{e_k})$
  $= n(1 - p_1^{-1}) \cdots (1 - p_k^{-1})$

EXAMPLE: $\phi(10) = \phi(2)\phi(5) = 4; n = 10; n_1 = 2, n_2 = 5$

- $\theta\colon \mathbb{Z}_n^* \to \mathbb{Z}_{n_1}^* \times \mathbb{Z}_{n_2}^*$
  - $1 \mapsto (1,1); 3 \mapsto (1,3); 7 \mapsto (1,2); 9 \mapsto (1,4)$

Group 群

集合

DEFINITION: Let $\star$ be a binary operation on G. The pair $(G,\star)$ is called an **group** if the following are satisfied:

二元运算

- 封闭性 **Closure**: $\forall a, b \in G, a \star b \in G$
- 结合律 **Associative**: $\forall a, b, c \in G, a \star (b \star c) = (a \star b) \star c$
- 必须唯一的
- 单位元 **Identity**: $\exists e \in G, \forall a \in \mathbb{G}, a \star e = e \star a = a$
- 逆元 **Inverse**: $\forall a \in \mathbb{G}, \exists b \in G\ , a \star b = b \star a = e$

阿贝尔群(交换群)

DEFINITION: A group is said to be an **Abelian group** if it additionally satisfies the following property:

- 交换率 **Commutative**: $\forall a, b \in G, a \star b = b \star a$
  - 交换群
  - An Abelian group is also called a **commutative group**.

EXAMPLE: $(\mathbb{Z}, +), (n\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{Q}^*,\times), (\{\pm 1\},\times)$

实数集的乘法不是群

0无逆元 $\longrightarrow$ 去除0就是了

Group $\mathbb{Z}_n$ Z_n的加法

THEOREM: $\mathbb{Z}_n$ is an Abelian group for any $n \in \mathbb{Z}^+$.

- **Closure**: $[a]_n + [b]_n \in \mathbb{Z}_n$
  - $[a]_n + [b]_n = [a+b]_n \in \mathbb{Z}_n$
- **Associative**: $([a]_n + [b]_n) + [c]_n = [a]_n + ([b]_n + [c]_n)$
  - $$\begin{aligned}([a]_n + [b]_n) + [c]_n &= [a+b]_n + [c]_n = [(a+b)+c]_n \\ &= [a+(b+c)]_n = [a]_n + [b+c]_n \\ &= [a]_n + ([b]_n + [c]_n)\end{aligned}$$
- **Identity**: $[a]_n + [0]_n = [0]_n + [a]_n = [a]_n$
  - $[a]_n + [0]_n = [a+0]_n = [0+a]_n = [0]_n + [a]_n$
- **Inverse**: $[a]_n + [-a]_n = [-a]_n + [a]_n = [0]_n$
  - $[a]_n + [-a]_n = [a+(-a)]_n = [0]_n$

群

- **Commutative**: $[a]_n + [b]_n = [b]_n + [a]_n$
  - $[a]_n + [b]_n = [a+b]_n = [b+a]_n = [b]_n + [a]_n$

阿贝尔群

Group $\mathbb{Z}_n^*$

$\mathbb{Z}_n^*$关于乘法

THEOREM: $\mathbb{Z}_n^*$ is an Abelian group for any integer $n > 1$.

- **Closure**: $\forall\ [a]_n, [b]_n \in \mathbb{Z}_n^*, [a]_n \cdot [b]_n = [ab]_n \in \mathbb{Z}_n^*$

  $\gcd(a,n)=1$, $\gcd(b,n)=1 \Rightarrow \gcd(ab,n)=1$
- **Associative**:$\forall [a]_n, [b]_n, [c]_n \in \mathbb{Z}_n^*, [a]_n \cdot ([b]_n \cdot [c]_n) = [abc]_n = ([a]_n \cdot [b]_n) \cdot [c]_n$
- **Identity element**: $\exists [1]_n \in \mathbb{Z}_n^*, \forall [a]_n \in \mathbb{Z}_n^*, [a]_n \cdot [1]_n = [1]_n \cdot [a]_n = [a]_n$
- **Inverse**: $\forall [a]_n \in \mathbb{Z}_n^*, \exists [s]_n \in \mathbb{Z}_n^*$ such that $[a]_n \cdot [s]_n = [s]_n \cdot [a]_n = [1]_n$
- **Commutative**: $\forall [a]_n, [b]_n \in \mathbb{Z}_n^*, [a]_n \cdot [b]_n = [ab]_n = [ba]_n = [b]_n \cdot [a]_n$

REMARK: we are interested in two types of Abelian groups

- **Additive Group**: binary operation $+$; identity 0
  - Example: $(\mathbb{Z}, +), (n\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{Z}_n, +)$
- **Multiplicative Group**: binary operation $\cdot$; identity 1 $//(\mathbb{Z}_n^*, \cdot)$
  - Example: $(\mathbb{Q}^*, \times), (\{\pm 1\}, \times), (\mathbb{Z}_n^*, \cdot)$

2类交换群

加法 $e=0$

乘法 $e=1$

Order

DEFINITION: The **order** of a group G is the cardinality of G.

- $|\mathbb{Z}_n| = n, \left|\mathbb{Z}_p^*\right| = p - 1, |\mathbb{Z}| = \infty$

DEFINITION: when $|G| < \infty$, $\forall a \in G$, the **order** of a is defined as the least integer $l > 0$ s.t. $a^l = 1$ ($la = 0$ for additive group)

EXAMPLE: Determine the orders of all elements of $\mathbb{Z}_7^*$

- $\mathbb{Z}_7^* = \{1,2,3,4,5,6\}$
- $o(1) = 1, o(2) = 3, o(3) = 6, o(4) = 3, o(5) = 6, o(6) = 2$

EXAMPLE: Determine the orders of all elements of $\mathbb{Z}_6$

- $\mathbb{Z}_6 = \{0,1,2,3,4,5\}$
- $o(0) = 1, o(1) = o(5) = 6, o(2) = o(4) = 3, o(3) = 2$

Order of $a \in \mathbb{Z}_{11}^*$

a	a^1	a^2	a^3	a^4	a^5	a^6	a^7	a^8	a^9	a^{10}	$o(a)$
1	1	1	1	1	1	1	1	1	1	1	1
2	2	4	8	5	10	9	7	3	6	1	10
3	3	9	5	4	1	3	9	5	4	1	5
4	4	5	9	3	1	4	5	9	3	1	5
5	5	3	4	9	1	5	3	4	9	1	5
6	6	3	7	9	10	5	8	4	2	1	10
7	7	5	2	3	10	4	6	9	8	1	10
8	8	9	6	4	10	3	2	5	7	1	10
9	9	4	3	5	1	9	4	3	5	1	5
10	10	1	10	1	10	1	10	1	10	1	2

- $a^{10} = 1$ for every $a \in \mathbb{Z}_{11}^*$; $o(a)|10$ for every $a \in \mathbb{Z}_{11}^*$

Euler's Theorem

THEOREM: Let G be a multiplicative Abelian group of order m.
Then for any $a \in G$, $a^m = 1$.

- $G = \{a_1, \ldots, a_m\}$
  - If $i \neq j$, then $aa_i \neq aa_j$.
    - $aa_1 \cdot aa_2 \cdots aa_m = a_1 a_2 \cdots a_m \Rightarrow a^m = 1$

Euler's Theorem: Let $n > 1$ and $\alpha \in \mathbb{Z}_n^*$. Then $\alpha^{\phi(n)} = 1$.

- $\alpha^{\phi(n)}$, 1 are both residue classes modulo n
- Proof: a corollary of the previous theorem for $G = \mathbb{Z}_n^*$

Fermat's Little Theorem: If p is a prime and $\alpha \in \mathbb{Z}_p$.
Then $\alpha^p = \alpha$.

Subgroup

DEFINITION: Let $(G,\star)$ be an Abelian group. A subset $H \subseteq G$ is called a **subgroup** of G if $(H,\star)$ is also a group. $(H \leq G)$

- Multiplicative: $G = \mathbb{Z}_6^* = \{1,5\}, H = \{1\}$
- Additive: $G = \mathbb{Z}_6 = \{0,1,2,3,4,5\}; H = \{0,2,4\}$

THEOREM: Let $(G,\cdot)$ be an Abelian group. Let $\langle g \rangle = \{g^k : k \in \mathbb{Z}\}$ be a subset of G, where $g \in G$. Then $\langle g \rangle \leq G$.

- Closure: $g^a \cdot g^b = g^{a+b} \in \langle g \rangle$
- Associative: $g^a \cdot \left(g^b \cdot g^c\right) = g^{a+b+c} = \left(g^a \cdot g^b\right) \cdot g^c$
- Identity element: $g^0 \cdot g^a = g^a \cdot g^0 = g^a$
- Inverse: $g^a \cdot g^{-a} = g^{-a} \cdot g^a = g^0$
- Communicative: $g^a \cdot g^b = g^{a+b} = g^{b+a} = g^b \cdot g^a$

Cyclic Group

DEFINITION: Let $(G,\cdot)$ be an Abelian group. G is said to be **cyclic** if there exists $g \in G$ such that $G = \langle g \rangle$.

- g is called a **generator** of G.

EXAMPLE: $\mathbb{Z}_{10}^{*} = \{[1]_{10}, [3]_{10}, [7]_{10}, [9]_{10}\} = \langle [3]_{10} \rangle$

- $g = [3]_{10}$
- $g^0 = [1]_{10}, g^1 = [3]_{10}, g^2 = [9]_{10}, g^3 = [27]_{10} = [7]_{10}$

REMARK: Let G be a finite group and let $g \in G$. Then $\langle g \rangle$ can be computed as $\{g^1, g^2, \dots\}$

Cyclic Group

EXAMPLE: $\mathbb{Z}_p^*$ is a cyclic group and $G = \langle g \rangle$ is a cyclic subgroup.

- p =1797693134862315907729305190789024733617976978942306572734300811577326758055009631327084773224075360211201138798713933576587897688144166224928474306394741243777678934248654852763022196012460941194530829520850057688381506823424628814739131105408272371633505106845862982399472459384797163048353563296242279988 59
  - p is a prime; $\mathbb{Z}_p^* = \langle 2 \rangle$ is a cyclic group of order $p - 1$
- q =8988465674311579538646525953945123668089884894711532863671504057886633790275048156635423866120376801056005693993569667882939488440720831124642371531973706218888394671243274263815110980062304705972654147604250288441907534117123144073695655527041361858167525534229314911997362296923985815241767816481211 3999429
  - $q = (p-1)/2$ is a prime
  - $g = 3$
  - $G = \langle g \rangle$ is a subgroup of $\mathbb{Z}_p^*$ of order q

DLOG and CDH

DEFINITION: Let $G = \langle g \rangle$ be a cyclic group of order q with generator g. 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 of** h **with respect to** g.

- $x = \log_g h$

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

- **Input**: G and $h = g^x$ for $x \leftarrow \{0,1,\dots,q-1\}$
- **Output**: $f_{\mathrm{DLOG}}(q, G, g; h) = \log_g h$

CDH Problem: computational Diffie-Hellman

- **Input**: $G = \langle g \rangle$ of order q and $A = g^a, B = g^b$ for $a, b \leftarrow \{0,1,\dots,q-1\}$
- **Output**: $f_{\mathrm{CDH}}(q, G, g; A, B) = g^{ab}$

Diffie-Hellman Key Exchange

The Scheme: $G = \langle g \rangle$ 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

Bob

(q, G, g)

$a \leftarrow \mathbb{Z}_q$

$A = g^a$

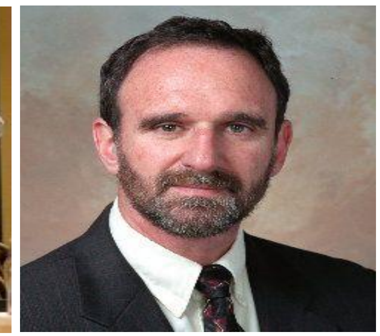
$\xrightarrow{(q, G, g, A)}$

$b \leftarrow \mathbb{Z}_q$

$B = g^b$

$\xleftarrow{B}$

output B^a | output A^b



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

Correctness: $A^b = g^{ab} = B^a$

Wiretapper: view $= (q, G, g, A, B)$

Security: view $\not\rightarrow$ g^{ab}

Diffie-Hellman Key Exchange

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

Alice

$a = 3$

$A = g^a = 8$

Bob

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

$b = 13$

$B = g^b = 4$

$\xleftarrow{B}$

$k = 18$ (Alice)

$k = 18$ (Bob)

Adversary: $q = 11, p = 23, g = 2, A = 8, B = 4, k = ?$

Security

Algorithms for DLOG, CDH: solving the DLOG problem first

- $\boldsymbol{G}$: **the group $\mathbb{Z}_p^*$ of order $q = p - 1$**
  - The best known algorithm runs in $\exp\left(O\left(\sqrt{\ln q \ln\ln q}\right)\right)$
  - $|G| = 2^{1024}$ has been used for many years; now not very safe
  - $|G| = 2^{2048}$ is recommended for today's application
- $\boldsymbol{G}$: **an order q subgroup of $\mathbb{Z}_p^*$, where $p = 2q + 1$ is a safe prime**
  - The best known algorithm runs in $\exp\left(O\left(\sqrt{\ln q \ln\ln q}\right)\right)$
- For specific group G of order q, the best known algorithm runs in
  - $\exp\left(O\left(\sqrt{(\ln q)^{1/3}(\ln\ln q)^{2/3}}\right)\right)$ //multiplicative group $\mathbb{F}_{p^k}^*$
- For specific group G of order q, the best algorithm runs in
  - $O(\sqrt{q})$ // elliptic curves