# COMPSCI 4CR3 - Applied Cryptography

Jake Doliskani

McMaster University

# Public-Key Schemes Based on the Discrete Logarithm Problem

# This lecture

- The Diffie-Hellman key exchange
- Cyclic groups
- The discrete logarithm problem
- Security of the Diffie-Hellman Key Exchange
- The Elgamal encryption scheme

# The Diffie-Hellman Key Exchange

- Proposed by Whitfield Diffie and Martin Hellman in 1976
- The first asymmetric scheme published in the open literature
- Widely used, e.g., SSH, TLS, IPSec.

Set-up:

1. Choose a large prime $p$
2. Choose $\alpha \in \{2, 3, \ldots, p-2\}$
3. Publish $p, \alpha$

# The Diffie-Hellman Key Exchange

$p, \alpha \in \mathbb{Z}_p$

Choose $a \in \{2, 3, \ldots, p-2\}$
Compute $k_A = \alpha^a \bmod p$

Choose $b \in \{2, 3, \ldots, p-2\}$
Compute $k_B = \alpha^b \bmod p$

$$\xrightarrow{\quad k_A \quad}$$

$$\xleftarrow{\quad k_B \quad}$$

Compute $k_{AB} = k_B^a \bmod p$

Compute $k_{AB} = k_A^b \bmod p$

The shared key is $k_{AB}$

# The DH Key Exchange (example)

$p = 31, \alpha = 19$

Choose $a = 8$
Compute $k_A = 19^8 = 9 \bmod 31$

Choose $b = 12$
Compute $k_B = 19^{21} = 4 \bmod 31$

$$\xrightarrow{\quad 9 \quad}$$

$$\xleftarrow{\quad 4 \quad}$$

Compute $k_{AB} = 4^8 = 2 \bmod 31$

Compute $k_{AB} = 9^{12} = 2 \bmod 31$

The shared key is $2 \in \mathbb{Z}_{31}$

# Groups

A group $G$ is a set of elements equipped with a binary operation $*$ that satisfies the following properties:

1. Closure: for every $a, b \in G$ it holds that $a * b \in G$.
2. Associativity: $a, b, c \in G$ it holds that $(a * b) * c = a * (b * c)$.
3. Neutral element: there exists an element $e \in G$ such that $a * e = e * a = a$ for all $a \in G$.
4. For every $a \in G$, there exists an element $a \in G$ such that $a * b = b * a = e$; $b$ is called the inverse of $a$ and is denoted by $a^{-1}$.

A group $G$ is called abelian if $a * b = b * a$ for all $a, b \in G$.

# Groups (examples)

- $(\mathbb{Z}, +)$: The group of integers $\{\dots, -2, -1, 0, 1, 2, \dots\}$ with the usual addition operations. The neutral element is $e = 0$, and $-a$ is the inverse of $a$.
- $(\mathbb{C}^\times, \times)$: The set of nonzero complex numbers under multiplication. The identity element is $e = 1$.
- The set of invertible $2 \times 2$ matrices over the real numbers under matrix multiplication:

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \text{ such that } ad - bc \neq 0, \quad e = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad a, b, c, d \in \mathbb{R}$$

The first two groups are abelian, but the last one is not.

# Groups

Let $\mathbb{Z}_n^\times$ be the set of all integers $x \in \{1, 2, \ldots, n-1\}$ that are coprime to $n$, i.e., $\gcd(x, n) = 1$. Then $\mathbb{Z}_n^\times$ is an abelian group under multiplication modulo $n$. The identity element is $e = 1$.

Example: multiplication table for $\mathbb{Z}_8^\times$

| $\times$ | 1 | 3 | 5 | 7 |
|---|---|---|---|---|
| 1 | 1 | 3 | 5 | 7 |
| 3 | 3 | 1 | 7 | 5 |
| 5 | 5 | 7 | 1 | 3 |
| 7 | 7 | 5 | 3 | 1 |

# Cyclic groups

A group $G$ is finite if it has a finite number of elements. We denote by $|G|$ the cardinality (or the order) of $G$.

Example: The order of $\mathbb{Z}_n^\times$ is $\varphi(n)$. So, $\mathbb{Z}_8^\times$ has $\varphi(8) = 4$ elements.

The order $\operatorname{ord}(a)$ of an element $a \in G$ is the smallest integer $k \geq 1$ such that

$$a^k = \underbrace{a * a * \cdots * a}_{k \text{ times}} = 1.$$

Example: The order of $5 \in \mathbb{Z}_8^\times$ is $2$.

# Cyclic groups

A group $G$ that contains an element $\alpha$ with order $\mathrm{ord}(\alpha) = |G|$ is called cyclic. In this case, $\alpha$ is called a primitive element (or a generator).

Example: The group $\mathbb{Z}_{11}^{\times}$ is cyclic:
$|\mathbb{Z}_{11}^{\times}| = 10$
$\mathrm{ord}(2) = 10$, so, $2$ is a primitive element.

**Theorem**

For every prime $p$, the group $\mathbb{Z}_{p}^{\times}$ us cyclic.

# Order of elements

**Theorem**

Let $G$ be a finite group. For every $a \in G$

1. $a^{|G|} = 1$,
2. $\mathrm{ord}(a)$ divides $|G|$.

Example: $\mathbb{Z}_{11}^{\times}$

$$\begin{aligned} \mathrm{ord}(1) &= 1, & \mathrm{ord}(6) &= 10, \\ \mathrm{ord}(2) &= 10, & \mathrm{ord}(7) &= 10, \\ \mathrm{ord}(3) &= 5, & \mathrm{ord}(8) &= 10, \\ \mathrm{ord}(4) &= 5, & \mathrm{ord}(9) &= 5, \\ \mathrm{ord}(5) &= 5, & \mathrm{ord}(10) &= 2. \end{aligned}$$

# Order of elements

**Theorem**

Let $G$ be a finite cyclic group. Then

1. The number of primitive elements of $G$ is $\varphi(|G|)$,
2. If $|G|$ is prime, then all elements $a \neq 1$ in $G$ are primitive.

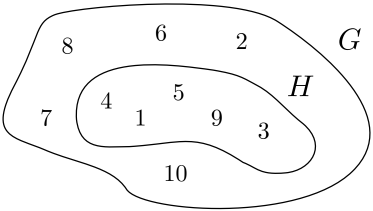
Example 1: $\mathbb{Z}_{11}^{\times}$
$\varphi(|G|) = \varphi(10) = 4$
Primitive elements: $2, 6, 7, 8$.

Example 2: the group $H = \{1, 3, 4, 5, 9\}$ with multiplication modulo $11$
$\varphi(|H|) = \varphi(5) = 4$
Primitive elements: $3, 4, 5, 9$.

# Subgroups

A subgroup $H$ of a group $G$ is a subset of $G$ that is itself a group.

Example: the subgroup $H = \{1, 3, 4, 5, 9\}$ of $\mathbb{Z}_{11}^{\times}$.
Multiplication is done modulo 11, the same as in $\mathbb{Z}_{11}^{\times}$




**Lagrange's Theorem**

For every subgroup $H$ of a group $G$, $|H|$ divides $|G|$.

# Subgroups

Let $G$ be a cyclic group of order $n$ with generator $\alpha$. Then

- For every integer $k$ that divides $n$ there is exactly one cyclic subgroup $H \leq G$ of order $k$.
- The subgroup $H$ is generated by $\alpha^{n/k}$
- There are exactly $k$ element $a \in G$ that satisfy $a^k = 1$.

Example: $\mathbb{Z}_{11}^{\times}$

- has order $n = 10$, and is generated by $\alpha = 8$.
- There is exactly one subgroup of order $2$ generated by

$$\alpha^{n/k} = 8^{10/2} = 32768 = 10 \bmod 11$$

# The Discrete Logarithm Problem (DLP)

DLP in $\mathbb{Z}_p^\times$:

Let $\alpha \in \mathbb{Z}_p^\times$ be a generator. Given any $\beta \in \mathbb{Z}_p^\times$, the DLP is the problem of finding an integer $1 \leq x \leq p-1$ such that

$$\alpha^x = \beta \bmod p.$$

- The integer $x$ is called the discrete logarithm of $\beta$ to the base $\alpha$.
- We write $x = \log_\alpha \beta \bmod p$
- Example: in $\mathbb{Z}_{47}^\times$: $\log_5 41 = 11 \bmod 47$, and $\log_2 36 = 17 \bmod 47$

# Generalized DLP

DLP in any cyclic group:

Let $G$ be a cyclic group of order $n$ and let $\alpha \in G$ be a generator. Given any $\beta \in G$, the DLP is the problem of finding an integer $1 \leq x \leq n$ such that

$$\alpha^x = \beta.$$

- Here $\alpha^x = \alpha * \cdots * \alpha \text{ (}x\text{ times)}$
- Example: in $\mathbb{Z}_{47}^{\times}$: $\log_5 41 = 11 \bmod 47$, and $\log_2 36 = 17 \bmod 47$

# Is DLP hard in all groups?

- $\mathbb{Z}_p^+$ is cyclic of order $p$.
- The operation is normal addition $\bmod p$.
- A generator $\alpha \in \mathbb{Z}_p^+$ is an element such that every $\beta \in \mathbb{Z}_p^+$ is a repeated sum of $\alpha$.
- DLP: given $\beta \in \mathbb{Z}_p^+$, find $1 \leq x \leq p-1$ such that
$$x\alpha = \underbrace{\alpha + \cdots + \alpha}_{x \text{ times}} = \beta.$$

Solution: compute $x = \alpha^{-1}\beta$
Computing inverses $\bmod p$ is easy.

# Is DLP hard in all groups?

(Hard) DLP groups that have been proposed for cryptography:

- The multiplicative group $\mathbb{Z}_p^\times$
  - Classical DHKE, Elgamal encryption, the Digital Signature Algorithm
- The cyclic group formed by an Elliptic Curve.
- The multiplicative subgroups of the Galois Field $\mathrm{Gal}(2^n)$
  - Not as popular as $\mathbb{Z}_p^\times$, because attacks against them are more efficient
- Hyperelliptic Curves or algebraic varieties
  - Generalization of elliptic curves

# Attacks against DLP

- Generic algorithms
  - Brute-Force Search
  - Shanks' Baby-Step Giant-Step Method
  - Pollard's Rho Method
  - Pohlig-Hellman Algorithm
- Nongeneric algorithms
  - The Index-Calculus Method

Brute-Force Search: try all values of $1 \leq x \leq n$ until you find an $x$ such that

$$\alpha^x = \beta$$

# Shanks' Baby-Step Giant-Step method

Let $n = |G|$ and $m = \lfloor \sqrt{n} \rfloor$. To find $x$ such that $\alpha^x = \beta$, we write

$$x = x_g m + x_b, \qquad \text{for } \; 0 \leq x_g, x_b < m.$$

Then

$$\beta = \alpha^{x_g m + x_b} \Rightarrow \beta \cdot (\alpha^{-m})^{x_g} = \alpha^{x_b}$$

1. Compute $\gamma = \alpha^{-m}$
2. Compute all the values $\gamma^i$ for $i = 0, 1, \ldots, m-1$, and store them. (Giant step)
3. For each value $0 \leq x_b < m$ check if there is an $i$ such that

$$\beta \cdot \gamma^i = \alpha^{x_b} \qquad \text{(Baby step)}$$

Complexity: $O(\sqrt{n})$ time, and $O(\sqrt{n})$ memory

# Pollard's Rho method

1. Let $n = |G|$. Consider the sequence $\{x_i\}$ given by $x_i = \alpha^{a_i}\beta^{b_i}$, where the pairs $(a_i, b_i)$ are computed in a way that the sequence "looks random".
2. Use a cycle finding algorithm to find $(a, b)$ and $(c, d)$ such that
$$\alpha^a\beta^b = \alpha^c\beta^d.$$
3. Substituting $\beta = \alpha^x$ gives $a + bx = c + dx \bmod n$.
4. The discrete logarithm is
$$x = \frac{a-c}{d-b} \bmod n$$

- Complexity: $O(\sqrt{n})$ time, and $O(1)$ memory
- Much better than Shanks' Baby-Step Giant-Step Method

# Pohlig-Hellman algorithm

1. Let $n = |G|$. Factor $n$ into prime factors: $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$.
2. Compute the discrete logarithm in the subgroups $G_i \leq G$ of size $|G_i| = p_i^{e_i}$.
3. Use the Chinese Remainder Theorem to recover the discrete logarithm in $G$.

- Efficient only when the prime factors $p_i$ are not too large.
- The discrete logarithm in the $G_i$ can be computed using the Pollard's Rho Method.
- Complexity: $O(\sum_{i=1}^{k} (\log n + \sqrt{p_i}) e_i)$

# The Index-Calculus method

- Nongeneric algorithm, i.e., works for specific groups.
- Has subexponential running time for the groups $\mathbb{Z}_p^\times$ and $\mathrm{Gal}(2^m)^\times$
- Idea: use the property that a non-negligible fraction of the elements of $G$ can be expressed as products of elements of a small subset of $G$.
- Using this subset we can collect some linear relations and solve a linear system of equations.

Complexity: $L_n[1/2, \sqrt{2} + o(1)]$, where $L_n$ refers to the L-notation.

Better algorithms: Number Field Sieve, Function Field Sieve

# Security of Diffie-Hellman Key Exchange

- Active attaks: the basic version of DHKE is not secure against MITM
- Passive attacks: the security is based on the Diffie–Hellman Problem

The Diffie-Hellman Problem (DHP): Let $G$ be a finite cyclic group and let $\alpha \in G$ be a generator. Given $\alpha^a$ and $\alpha^b$ for some unknown integers $a, b$, compute $\alpha^{ab}$.

- If Trudy knows how to solve DLP, then he can solve DHP.
- In general, we don't know if DLP and DHP are equivalent.

# The Elgamal encryption scheme

Public parameters:
- large prime $p$
- generator $\alpha \in \mathbb{Z}_p^\times$

Choose $b \in \{2, 3, \ldots, p-2\}$
Compute $k_B = \alpha^b \bmod p$

$$\xleftarrow{\quad k_B \quad}$$

Choose $a \in \{2, 3, \ldots, p-2\}$
Compute $k_A = \alpha^a \bmod p$
Compute $k_{AB} = k_B^a \bmod p$
Encrypt plaintext $x \in \mathbb{Z}_p^\times$:
$y = x \cdot k_{AB} \bmod p$

$$\xrightarrow{\quad (k_A, y) \quad}$$

Compute $k_{AB} = k_A^b \bmod p$
Decrypt ciphertext $y \in \mathbb{Z}_p^\times$:
$x = y \cdot k_{AB}^{-1} \bmod p$

# The Elgamal encryption scheme

Public parameters:

- prime $53$
- generator $27 \in \mathbb{Z}_{53}^{\times}$

Choose $12 \in \{2, 3, \ldots, 51\}$
Compute $k_B = 27^{12} = 46 \bmod 53$

$\xleftarrow{46}$

Choose $32 \in \{2, 3, \ldots, 51\}$
Compute $k_A = 27^{32} = 24 \bmod 53$
Compute $k_{AB} = 46^{32} = 42 \bmod 53$
Encrypt plaintext $21 \in \mathbb{Z}_{53}^{\times}$:
$34 = 21 \cdot 42 \bmod 53$

$\xrightarrow{(24, 34)}$

Compute $k_{AB} = 24^{12} = 42 \bmod 53$
Decrypt ciphertext $34 \in \mathbb{Z}_{53}^{\times}$:
$21 = 34 \cdot 42^{-1} \bmod 53$

# Security (passive attacks)

- Security relies on the Diffie-Hellman problem
- The only known attack is through solving DLP

1. Find Bob's secrete key by solving DLP:
$$b = \log_\alpha k_B \bmod p$$
2. Compute the shared key using Alice's $k_A$
$$k_{AB} = k_A^b \bmod p$$
3. Recover the message:
$$x = y \cdot k_{AB}^{-1} \bmod p$$

# Security (active attacks)

- MITM (like any other public-key scheme), public keys should be authenticated
- Alice's secrete exponent should not be reused.

1. Alice reuses the exponent $a$, then there are two ciphertexts $(y_1, k_A), (y_2, k_A)$ over the channel.
2. If Trudy knows the first message $x_1$, he can compute

$$k_{AB} = y_1 x_1^{-1} \bmod p$$

- Like plain RSA, plain Elgamal is malleable

1. Trudy can replace $(k_A, y)$ with $(k_A, sy)$.
2. Bob decrypts $sy \cdot k_{AB}^{-1} = s \cdot (x \cdot k_{AB}) \cdot k_{AB}^{-1} = sx \bmod p$