Bài toán logarit rời rạc và Diffie-Hellman

Nội dung

- **Bài toán Logarit rời rạc**
- Bài toán Diffie-Hellman

Định nghĩa Nhóm

Một nhóm Abel $(G,\cdot)$ thoả mãn các tính chất sau:

1. Có phần tử đơn vị: $1 \in G$ thoả mãn
   $$\forall a \in G,\ a \cdot 1 = 1 \cdot a = a$$
2. Mọi phần tử đều khả nghịch:
   $\forall a \in G,\ \exists b \in G$ thoả mãn $a \cdot b = 1$
3. Kết hợp: $\forall a, b, c \in G$ ta có $a \cdot (b \cdot c) = (a \cdot b) \cdot c$
4. Giao hoán: $\forall a, b \in G$ ta có $a \cdot b = b \cdot a$

Cấp của một phần tử trong nhóm

- Cấp của phần tử a, ký hiệu ord(a), là số $u > 0$ nhỏ nhất thoả mãn
$$a^u = 1 \in G.$$

- **Định lý Lagrange**: Trong nhóm hữu hạn G với lực lượng t, ta có
$$\forall a \in G, \quad \mathrm{ord}(a) \mid t.$$

- **Hệ quả:** Trong nhóm hữu hạn G với lực lượng t, ta có
$$\forall a \in G, \quad a^t = 1.$$

- Ký hiệu: $\langle a \rangle = \{a^i \mid i \geq 0\}$ là nhóm con sinh bởi a.

Nhóm vòng

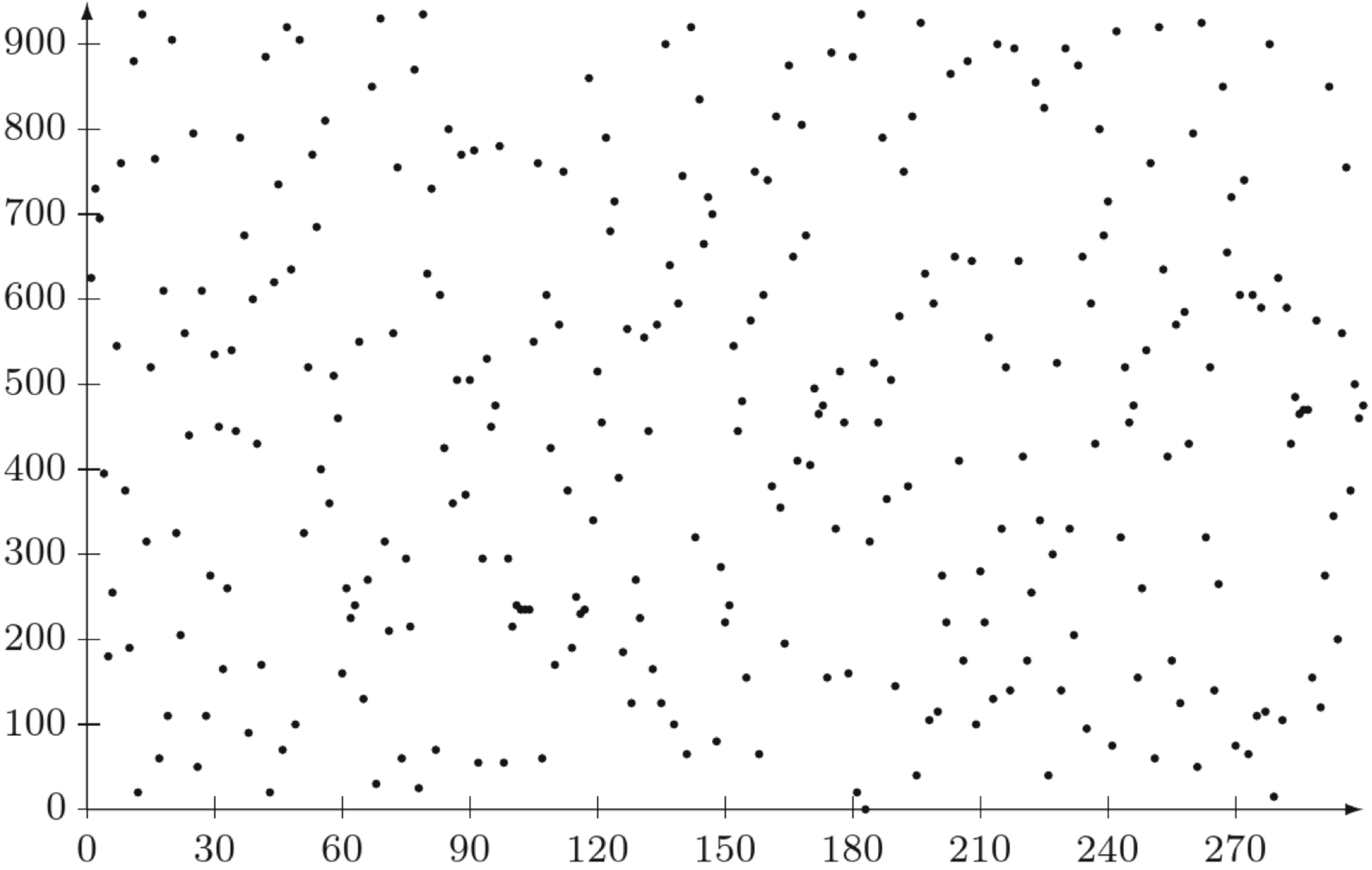
- Ký hiệu $\langle a \rangle = \{a^i \mid i \geq 0\}$ là nhóm con sinh bởi a.
- Nếu $\langle a \rangle = G$ thì a là một phần tử sinh của G.
- **Khẳng định:** $|\langle a \rangle| = \text{ord}(a)$.
- Định nghĩa: G là nhóm vòng nếu có g thoả mãn $\langle g \rangle = G$

Hàm logarit rời rạc và hàm mũ

- **Khẳng định:** Nếu G là nhóm vòng cấp t và g là phần tử sinh, thì quan hệ
  $$x \leftrightarrow g^x$$
  là 1-to-1 giữa $\{0,1,\dots,t-1\}$ và G.

- Hàm mũ $x \rightarrow g^x$

- Hàm logarit rời rạc $g^x \rightarrow x$



Tính ngẫu nhiên của lũy thừa $627^x \pmod{941}$

Bài toán Logarit rời rạc

- Xét g là một phần tử sinh của $\mathbb{Z}_p^*$ và $h \in \mathbb{Z}_p^*$.

- Bài toán Logarit rời rạc (DLP) là bài toán tìm một số mũ x thỏa mãn
$$g^x \equiv h \bmod p.$$

- Số x được gọi là logarit rời rạc cơ sở g của h và ký hiệu $\mathrm{Dlog}_g(h)$.

Bài tập

Hãy tính các logarit rời rạc sau.

1. Dlog$_2(13)$ trong modun nguyên tố 23
2. Dlog$_{10}(22)$ trong modun nguyên tố $p = 47$.
3. Dlog$_{627}(608)$ trong modun nguyên tố $p = 941$.

Tính Logarit rời rạc

- Xét số nguyên tố $p = 56509$, và ta có thể kiểm tra $g = 2$ là một căn nguyên thủy modun p.
- Làm thế nào để tính $\log_2(38679)$?
- Một phương pháp là tính

$$2^0,\ 2^1,\ 2^2,\ 2^3,\ \cdots \mod 56509$$

  cho đến khi được lũy thừa bằng 38679.
- Bạn có thể kiểm tra rằng

$$2^{11235} \equiv 38679 \mod 56509.$$

Nội dung

- Bài toán Logarit rời rạc
- **Bài toán Diffie-Hellman**

Bài tập

Hãy tính hai giá trị sau trong $\mathbb{Z}_{13}^*$.

- $\mathrm{DH}_7(10,5)$
- $\mathrm{DH}_2(12,9)$

biết rằng

$$\begin{aligned}\langle 2\rangle &= \{1, 2, 4, 8, 3, 6, 12, 11, 9, 5, 10, 7\}\\ \langle 7\rangle &= \{1, 7, 10, 5, 9, 11, 12, 6, 3, 8, 4, 2\}\end{aligned}$$

$$\mathrm{DH}_g(g^a, g^b) = g^{ab} \quad (\mathrm{mod}\ p)$$

Nhắc lại: Giao thức Diffie-Hellman (1977)

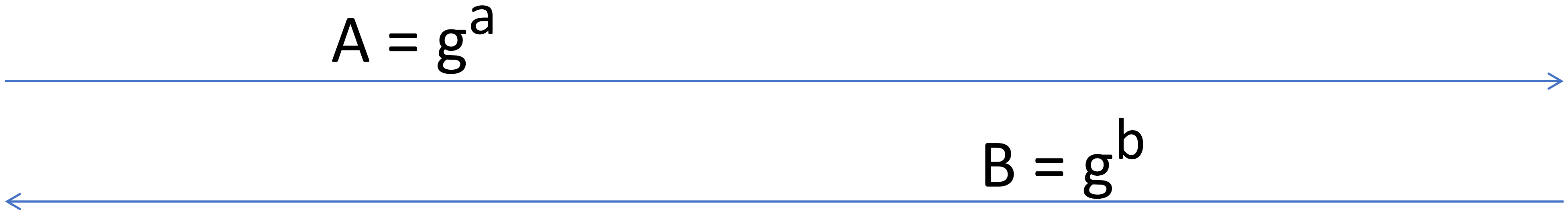
Xét nhóm vòng G (e.g $G = (Z_p)^*$) với cấp n

Lấy một phần tử sinh g thuộc G (i.e. $G = \{1, g, g^2, g^3, \ldots, g^{n-1}\}$)

Alice **Bob**

Chọn ngẫu nhiên **a** in {1,…,n}

Chọn ngẫu nhiên **b** trong {1,…,n}



$A = g^a$

$B = g^b$

$$\mathbf{B^a} = (g^b)^a = \boxed{\mathbf{k_{AB} = g^{ab}}} = (g^a)^b = \mathbf{A^b}$$

Bài tập

- Alice và Bob dùng số nguyên tố $p = 1373$ và cơ sở $g = 2$ để trao đổi khóa.
- Alice gửi Bob giá trị $A = 974$.
- Bob chọn số bí mật $b = 871$.
- Bob nên gửi cho Alice giá trị gì, và khóa bí mật họ chia sẻ là gì?
- Bạn có thể đoán được số bí mật a của Alice không?

Một câu hỏi mở

- Nếu ta có thể giải bài toán Logarit rời rạc, vậy ta có thể giải bài toán Diffie-Hellman. Tại sao?

- Nhưng nếu ta có thể giải được bài toán Diffie-Hellman, vậy liệu ta có thể giải được bài toán logarit rời rạc không?

Một số nhóm hay được dùng

- Nhóm $\mathbb{Z}_p^* = \{1, \dots, p-1\}$ với p nguyên tố
- Nhóm thặng dư bình phương $\mathbb{Q}_p = \{a^2 \mid a \in \mathbb{Z}_p^*\}$
- Nhóm $\mathbb{Z}_n^* = \{a \in \{1, \dots, n-1\} \mid \gcd(a, n) = 1\}$.
  Hệ RSA sử dụng $\mathbb{Z}_{pq}$ với p, q là các số nguyên tố ngẫu nhiên lớn.
- Nhóm $\mathbb{Q}_n = \{a^2 \mid a \in \mathbb{Z}_n^*\}$
- Nhóm điểm trên đường cong Elliptic