ĐẠI HỌC BÁCH KHOA HÀ NỘI
VIỆN CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

Nhập môn An toàn thông tin

Hệ mật mã dựa trên Bài toán logarit rời rạc và Diffie-Hellman

---

Nội dung

- **Bài toán Logarit rời rạc**
- Giao thức trao đổi khoá Diffie-Hellman
- Hệ mật mã ElGamal

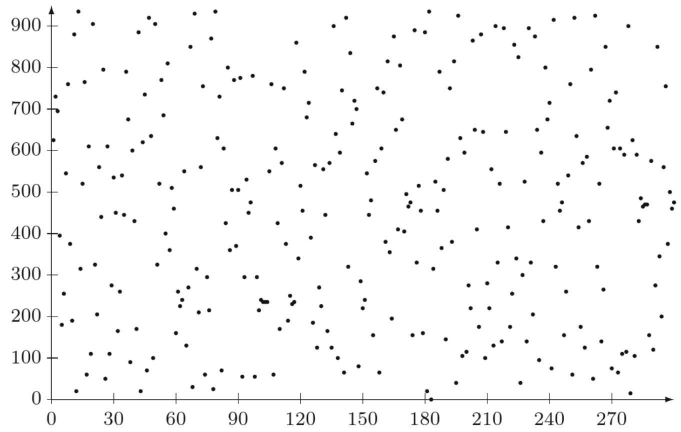
Nhắc lại: Cấp của một phần tử trong nhóm

- 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.

Nhắc lại: 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:** $|\langle a \rangle| = \mathrm{ord}(a)$.
- Định nghĩa: G là nhóm vòng nếu có g thoả mãn $\langle g \rangle = G$

Tính ngẫu nhiên của lũy thừa **627^x (mod 941)**



Bài tập

Hãy tính các logarit rời rạc sau.

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

Hàm logarit rời rạc và hàm mũ

- **Khẳng định:** Nếu G là nhóm vòng cấp t và g là phần tử sinh, thì ánh xạ

$$x \leftrightarrow g^x$$

là 1-to-1 giữa $\{0,1,\dots,t-1\}$ và G.

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

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 $\mathrm{Dlog}_g(h)$.

Nội dung

- Bài toán Logarit rời rạc
- **Giao thức trao đổi khoá Diffie-Hellman**
- Hệ mật mã ElGamal

Giao thức Diffie-Hellman

Chọn một số nguyên tố lớn p (v.d. 600 chữ số)

Chọn một số nguyên g thuộc {1, …, p}

Alice **Bob**

Chọn ngẫu nhiên **a** thuộc {1,…,p-1} Chọn ngẫu nhiên **b** thuộc {1,…,p-1}

"Alice", $A \leftarrow g^a \pmod{p}$ →

← "Bob", $B \leftarrow g^b \pmod{p}$

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

Tính Logarit rời rạc

- Xét số nguyên tố $p = 56509$, và ta có thể kiểm tra $g = 2$ là một phần thử sinh của Z_p.
- Làm thế nào để tính Dlog$_2(38679)$?
- Một phương pháp là tính

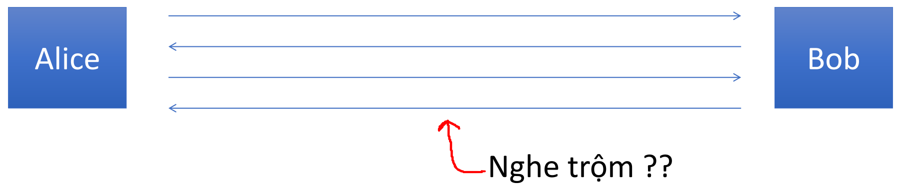
  $$2^0,\ 2^1,\ 2^2,\ 2^3,\ \cdots \text{ mod } 56509$$

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

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

Trao đổi khoá không cần bên thứ ba

Mục đích: Alice và Bob muốn chia sẻ khoá bí mật, mà kẻ nghe trộm không biết



Tính an toàn

Kẻ nghe trộm nhìn thấy: p, g, A=g^a (mod p), và B=g^b (mod p)

Liệu có thể tính g^{ab} (mod p) ??

Tổng quát: định nghĩa $DH_g(g^a, g^b) = g^{ab}$ (mod p)

Hàm DH theo môđun p liệu có khó tính?

Hàm DH theo modun p

Giả sử p là số nguyên tố n dài bits long.

Thuật toán tốt nhất (GNFS): có thời gian ch exp($\tilde{O}(\sqrt[3]{n})$)

khoá bí mật	kích thước modun	Kích thước Elliptic Curve
80 bits	1024 bits	160 bits
128 bits	3072 bits	256 bits
256 bits (AES)	**15360** bits	512 bits

Hệ quả: chuyển từ (mod p) sang đường cong Elliptic

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?

Bài tập

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

- $DH_7(10,5)$
- $DH_2(12,9)$

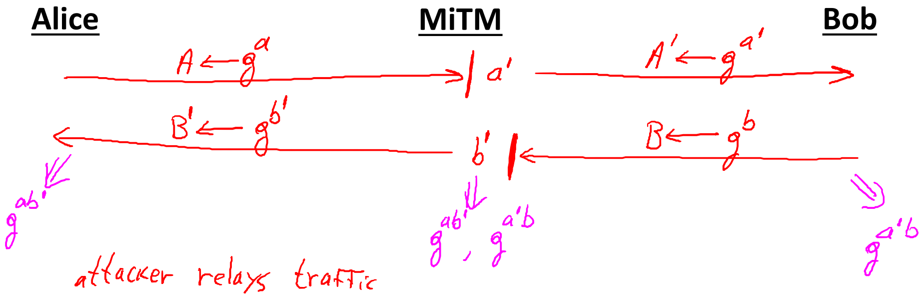
biết rằng

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

$$DH_g(g^a, g^b) = g^{ab} \quad (\text{mod } p)$$

Không an toàn chống lại man-in-the-middle

Giao thức này không an toàn chống lại kẻ tấn công chủ động

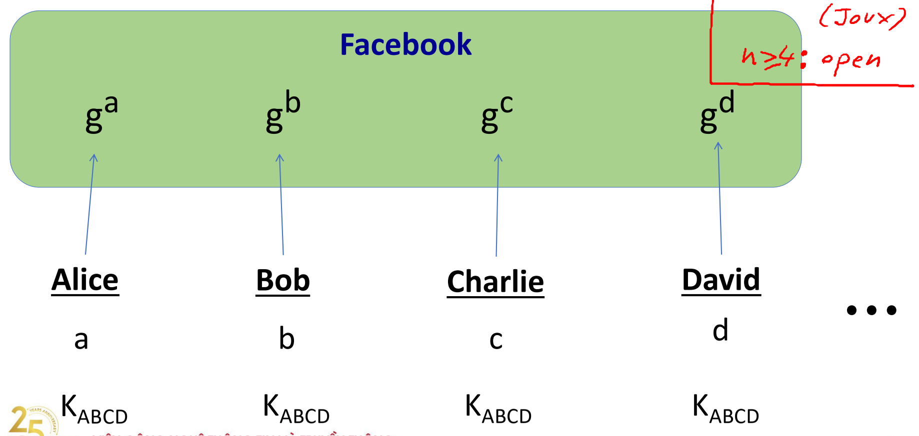


attacker relays traffic from Alice to Bob and reads it in the clear

---

Một bài toán mở

n=2 : DH
n=3 : Known (Joux)
n≥4 : open



www.google.com

The identity of this website has been verified by Thawte SGC CA.

Certificate Information

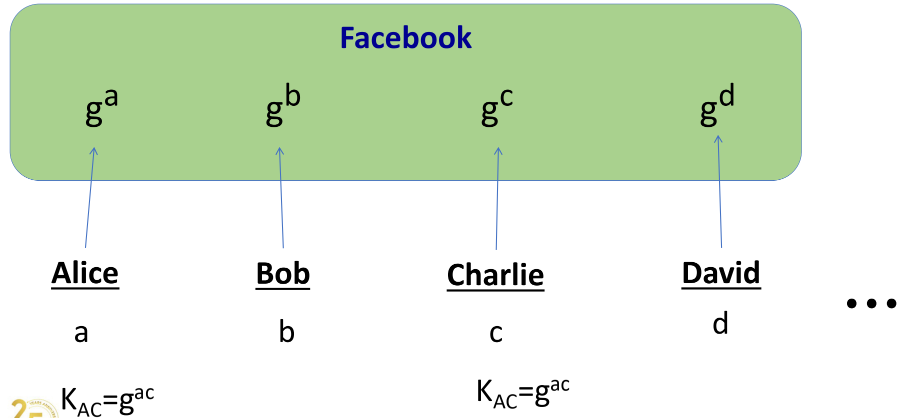
Your connection to www.google.com is encrypted with 128-bit encryption.

The connection uses TLS 1.0.

The connection is encrypted using RC4_128, with SHA1 for message authentication and ECDHE_RSA as the key exchange mechanism.

Elliptic curve Diffie-Hellman

Một cách nhìn khác về DH



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 điểm trên đường cong Elliptic

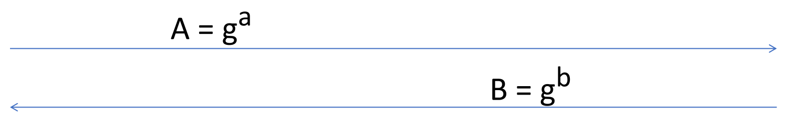
Nhắc lại: Giao thức Diffie-Hellman (1977)

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, … , 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

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

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?

Nội dung

- Bài toán Logarit rời rạc
- Giao thức trao đổi khoá Diffie-Hellman
- **Hệ mật mã ElGamal**

ElGamal: converting to pub-key enc. (1984)

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

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

Alice

Chọn ngẫu nhiên **a** thuộc {1,…,n}

$A = g^a$

Coi A như khoá công khai

Bob

Chọn ngẫu nhiên **b** in {1,…,n}

tính $g^{ab} = A^b$,

Dẫn xuất khoá đối xứng k ,

Mã hoá m với k

ct = [$B = g^b$, Mã hoá m với k]

ElGamal: converting to pub-key enc. (1984)

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

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

Alice

Chọn ngẫu nhiên **a** thuộc {1,…,n}

$A = g^a$

Coi a như khoá công khai

Bob

Chọn ngẫu nhiên **b** in {1,…,n}

tính $g^{ab} = A^b$,

Dẫn xuất khoá đối xứng k ,

Mã hoá m với k

ct = [$B = g^b$, Mã hoá m với k]

Để giải mã:
tính $g^{ab} = B^a$,
Dẫn ra k, và giải mã

Hệ mật ElGamal (cách nhìn hiện đại)

- G: nhóm vòng cấp n
- (E_s, D_s) : mã đối xứng an toàn trên (K,M,C)
- H: $G^2 \longrightarrow K$ hàm băm

Ta xây dung hệ mật khoá công khai (Gen, E, D):

- Sinh khoá Gen:
  - Chọn ngẫu nhiên phần tử sinh g trong G và một số ngẫu nhiên a thuộc Z_n
  - output sk = a , pk = (g, $h=g^a$)

Hệ mật ElGamal

- G: nhóm vòng cấp n

- (E_s, D_s) : mã đối xứng an toàn trên (K,M,C)

- H: $G^2 \longrightarrow K$ hàm băm

<u>E(pk=(g,h), m)</u> :

$b \leftarrow Z_n$, $u \leftarrow g^b$, $v \leftarrow h^b$

$k \xleftarrow{R} H(u,v)$, $c \leftarrow E_s(k, m)$

output (u, c)

<u>D(sk=a, (u,c))</u> :

$v \leftarrow u^a$

$k \leftarrow H(u,v)$, $m \leftarrow D_s(k, c)$

output m

Hiệu năng ElGamal

E(pk=(g,h), m) :

$b \longleftarrow Z_n$, $u \longleftarrow g^b$, $v \longleftarrow h^b$

D(sk=a, (u,c)) :

$v \longleftarrow u^a$

Mã hoá: 2 phép lấy mũ. (cơ sở cố định)

- Có thể tính trước $\left[g^{(2^i)} , h^{(2^i)} \quad \text{for} \quad i=1,\ldots,\log_2 n \right]$
- Tốc độ nhanh gấp 3x (hoặc hơn)

Decryption: 1 phép lấy mũ. (cơ sở thay đổi)