Bài tập 11
Giao thức Diffie-Hellman và hệ mật ElGamal

1 Giao thức trao đổi khoá

Câu 1

Xét giao thức trao đổi khoá với bên thứ ba trực tuyến (như trong Slide 5). Giả sử Alice, Bob, và Carol cả ba cùng sử dụng hệ thống (cùng với những người khác); và mỗi người có một khoá bí mật với TTP. Các khoá này được ký hiệu bởi k_a, k_b, k_c tương ứng. Cả ba muốn sinh một khoá phiên cho nhóm k_{ABC}. Khoá này cả Alice, Bob, và Carol đều biết nhưng không ai nghe trộm có thể biết được. Ta nên sửa giao thức thế nào để cho phép trao đổi khoá nhóm?

1. Alice liên hệ với TTP. TTP sinh một số ngẫu nhiên k_{ABC} và gửi cho Alice

$$E(k_a, k_{ABC}), \quad \text{ticket}_1 \leftarrow k_{ABC}, \quad \text{ticket}_2 \leftarrow k_{ABC}$$

Alice gửi ticket_1 cho Bob và ticket_2 cho Carol.

2. Alice liên hệ với TTP. TTP sinh một số ngẫu nhiên k_{ABC} và gửi cho Alice

$$E(k_a, k_{ABC}), \quad \text{ticket}_1 \leftarrow E(k_b, k_{ABC}), \quad \text{ticket}_2 \leftarrow E(k_c, k_{ABC}).$$

Alice gửi ticket_1 cho Bob và ticket_2 cho Carol.

3. Alice liên hệ với TTP. TTP sinh một số ngẫu nhiên k_{ABC} và gửi nó cho Alice

$$E(k_a, k_{ABC}), \quad \text{ticket}_1 \leftarrow E(k_b, k_{ABC}), \quad \text{ticket}_2 \leftarrow E(k_c, k_{ABC})$$

Alice sends k_{ABC} to Bob and k_{ABC} to Carol.

4. Alice liên hệ với TTP. TTP sinh một số ngẫu nhiên k_{AB} và một số ngẫu nhiên k_{AC}. Nó gửi cho Alice

$$E(k_a, k_{AB}), \quad \text{ticket}_1 \leftarrow E(k_b, k_{AB}), \quad \text{ticket}_2 \leftarrow E(k_c, k_{AC}).$$

Alice gửi ticket_1 cho Bob và ticket_2 cho Carol.

Câu 2

Xét G là một nhóm vòng (v.d. $G = \mathbb{Z}_p^*$) với phần tử sinh là g. Giả sử hàm Diffie-Hellman $\text{DH}_g(g^x, g^y) = g^{xy}$ là khó tính toán trong G. Hàm nào dưới đây cũng khó tính toán? *Gợi ý:* bạn nên xác định hàm f nào dưới đây để mệnh đề phản chứng sau đúng: nếu $f(\cdot,\cdot)$ là dễ tính toán thì $\text{DH}_g(\cdot,\cdot)$ cũng dễ. Nếu bạn có thể chỉ ra mệnh đề này, vậy thì nếu DH_g là khó trong G thì f cũng phải khó trong G.

1. $f(g^x, g^y) = g^{xy+1}$

2. $f(g^x, g^y) = g^{x(y+1)}$

3. $f(g^x, g^y) = (g^2)^{x+y}$

4. $f(g^x, g^y) = (\sqrt{g})^{x+y}$

Câu 3

Giả sử ta sửa đổi giao thức Diffie-Hellman như sau:

- Alice thao tác như thông thường, tức là chọn một số ngẫu nhiên a trong $\{1, \ldots, p-1\}$ và gửi $A \leftarrow g^a$ cho Bob.
- Bob, tuy nhiên, lại chọn một số ngẫu nhiên b thuộc $\{1, \ldots, p-1\}$ và gửi cho Alice $B \leftarrow g^{1/b}$.

Giá trị bí mật nào họ có thể sinh được và họ làm thế nào?

1. giá trị bí mật $= g^{ab}$. Alice tính giá trị bí mật B^a và Bob tính A^b.

2. giá trị bí mật $= g^{a/b}$. Alice tính giá trị bí mật B^a và Bob tính $A^{1/b}$.

3. giá trị bí mật $= g^{a/b}$. Alice tính giá trị bí mật $B^{1/b}$ và Bob tính A^a.

4. giá trị bí mật $= g^{ab}$. Alice tính giá trị bí mật $B^{1/a}$ và Bob tính A^b.

Câu 4

Cấp của phần tử 2 trong $\mathbb{Z}_{35}^*$ là gì?

Câu 5

Phần tử nào dưới đây là phần tử sinh của $\mathbb{Z}_{13}^*$?

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

2. 5, $\langle 5 \rangle = \{1, 5, 12, 8\}$

3. 9, $\langle 9 \rangle = \{1, 9, 3\}$

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

5. 3, $\langle 3 \rangle = \{1, 3, 9\}$

Câu 6

Nếu p là số nguyên tố, có bao nhiêu phần tử sinh trong $\mathbb{Z}_p^*$?

1. $(p-1)/2$

2. $p-1$

3. $\varphi(p)$

4. $\varphi(p-1)$

Câu 7

Xét giao thức trao đổi khoá sau đây:

- Alice chọn số ngẫu nhiên $k, r \in \{0,1\}^n$ và gửi $s = k \oplus r$ cho Bob
- Bob chọn số ngẫu nhiên $t \in \{0,1\}^n$, và gửi $u = s \oplus t$ cho Alice.
- Alice tính $w = u \oplus r$ và gửi w cho Bob.
- Alice output k và Bob output $w \oplus t$.

Chứng minh rằng Alice và Bob output cùng khoá. Hãy phân tích tính an toàn của sơ đồ này. (cụ thể, hãy chứng minh sơ đồ này là an toàn hoặc chỉ ra một tấn công cụ thể).

2 Hệ mật mã ElGamal

1. Xét $\mathbb{G}$ là nhóm vòng cấp (nguyên tố) q sinh bởi $g \in \mathbb{G}$. Xét một sửa đổi đơn giản của hệ mật ElGamma $\mathscr{E}_{\text{MEP}}(G, E, D)$ định nghĩa trên $(\mathbb{G}, \mathbb{G}^2)$. Thuật toán sinh khoá G như thông thường, nhưng mã hoá và giải mã thay đổi như sau:

- với khoá công khai $\text{pk} = u \in \mathbb{G}$ và thông điệp $m \in \mathbb{G}$:

$$E(\text{pk}, m) := \qquad \beta \xleftarrow{\text{R}} \mathbb{Z}_q, \quad v \leftarrow g^\beta, \quad c \leftarrow m \cdot u^\beta, \quad \text{output } (v, c)$$

- với khoá bí mật $\text{sk} = \alpha \in \mathbb{Z}_q$ và bản mã $(v, e) \in \mathbb{G}^2$:

$$D(\text{sk}, (v, c)) := \qquad \text{output } c/v^\alpha.$$

Hãy chứng minh rằng $\mathscr{E}_{\text{MEP}}$ có tính chất sau: cho khoá công khai pk, và hai bản mã $c_1 \xleftarrow{\text{R}} E(\text{pk}, m_1)$ và $c_2 \xleftarrow{\text{R}} E(\text{pk}, m_2)$, ta có thể tạo ra bản mã c là mã hoá của $m_1 \cdot m_2$. Tính chất này gọi là **đồng cấu nhân tính**.

2. Giả sử hệ mã sử dụng là $\mathscr{E}_{\text{MEP}}$ ở Bài tập 1 với $\mathbb{G} = \mathbb{Z}_{467}^*$ và phần tử sinh $g = 2$. Hãy mã hoá các thông điệp sau:

(a) $\text{sk} = \alpha = 105, \beta = 213, m = 33$

(b) $\text{sk} = \alpha = 105, \beta = 123, m = 33$

(c) $\text{sk} = \alpha = 300, \beta = 45, m = 248$

(d) $\text{sk} = \alpha = 300, \beta = 47, m = 248$

Bây giờ hãy giải mã các thông điệp trên và chỉ rõ từng bước.

3. Như có thể thấy qua bốn ví dụ từ Bài tập 2, hệ mã của Bài tập 1 là hệ mã xác suất: với mỗi bản rõ m có thể có nhiều bản mã phù hợp.

(a) Tại sao hệ ElGamal là hệ mã xác suất?

(b) Có bao nhiêu bản mã phù hợp ứng với mỗi thông điệp m cụ thể? Hãy viết công thức tường minh.

4. (***Tấn công hệ ElGamal nhân tính***). Xét p và q là hai số nguyên tố lớn sao cho q là ước của $p-1$. Xét $\mathbb{G}$ là nhóm con cấp q của $\mathbb{Z}_p^*$ sinh bởi $g \in \mathbb{G}$. Ta xét hệ ElGamal như trong Bài tập 1 với nhóm $\mathbb{G}$. Tuy nhiên, bản các thông điệp được chọn trong toàn bộ nhóm $\mathbb{Z}_p^*$ sao cho hệ mã được định nghĩa trên $(\mathbb{Z}_p^*, \mathbb{G} \times \mathbb{Z}_p^*)$. Chứng minh rằng hệ mã không an toàn ngữ nghĩa.

5. Máy chủ email BK Mail mã hoá mọi email gửi tới Bob bằng khoá công khai pk_{bob} của Bob. Khi Bob đi nghỉ mát, Bob ra lệnh BK Mail: *với tất cả email được gửi tới Bob, hãy chuyển tiếp cho đồng nghiệp Alice xử lý.* Khóa công khai của Alice là pk_{alice}. Để làm điều này, BK Mail cần một cách để **dịch** một email được mã hóa theo khoá công khai pk_{bob} thành một email được mã hóa theo khoá công khai pk_{alice} của Alice. Việc này có thể thực hiện dễ dàng nếu BK Mail có sk_{bob}, nhưng vấn đề là, sau đó BK Mail có thể đọc tất cả email gửi tới Bob, đây là điều Bob không muốn!

Xét $\mathbb{G}$ là một nhóm cấp nguyên tố q và $g \in \mathbb{G}$ là một phần tử sinh. Ta xét một biến thể của hệ mật ElGamal trong đó khoá công khai là $\text{pk} := u = g^\alpha \in \mathbb{G}$ và hàm mã hoá định nghĩa như sau:

$$E(\text{pk}, m) = \left\{\beta \leftarrow \mathbb{Z}_q,\ v = g^\beta,\ k = H(u^\beta),\ c = E_{\text{sym}}(k, m),\ \text{output } (v, c)\right\}$$

với E_{sym} là hệ mã khoá đối xứng với không gian khoá $\mathcal{K}_{\text{sym}}$, và H là một hàm băm $H : \mathbb{G} \to \mathcal{K}_{\text{sym}}$.

Giả sử rằng pk_{bob} và pk_{alice} là khoá công khai trong sơ đồ mã hoá trên với khoá bí mật tương ứng là $\text{sk}_{\text{bob}} = \alpha \in \mathbb{Z}_q$ và $\text{sk}_{\text{alice}} = \alpha' \in \mathbb{Z}_q$. Để cho phép dịch bản mã từ pk_{bob} cho pk_{alice}, Alice và Bob cùng nhau tính $\tau := \alpha/\alpha' \in \mathbb{Z}_q$. Họ gửi τ tới máy chủ BK Mail.

(a) Hãy giải thích cách mà máy chủ BK Mail dùng τ để dịch bản mã $c \leftarrow E(\text{pk}_{\text{bob}}, m)$ thành bản mã c' cho pk_{alice} cho cùng thông điệp m.

(b) Hãy giải thích cách mà BM Mail dùng τ để dịch bản mã theo hướng ngược lại. Tức là, nếu $c \leftarrow E(pk_{\text{alice}}, m)$ thì BK Mail có thể xây dựng bản mã c' cho pk_{bob} cho cùng thông điệp m.

(c) Liệu máy chủ BK Mail có thể giải mã c hoặc c' khi biết τ hay không? Nếu có hãy chỉ ra cách giải mã; nếu không hãy chứng minh.