Bài tập
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).