

NHẬP MÔN MẬT MÃ HỌC



Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin

6 September 2022 | Page 1

NỘI DUNG



01. TỔNG QUAN VỀ MẬT MÃ HỌC
Tổng quan về mật mã học
02. CÁC HỆ MẬT KHÓA BÍ MẬT
Các hệ mật khóa bí mật
03. CÁC HỆ MẬT KHÓA CÔNG KHAI
Các hệ mật khóa công khai
04. HÀM BẮM, XÁC THỰC VÀ CHỮ KÍ SỐ
Hàm băm, toàn vẹn và chữ ký số
05. VẤN ĐỀ PHÂN PHỐI & THỎA THUẬN KHÓA
Vấn đề phân phối & thỏa thuận khóa

6 September 2022 | Page 2

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin

CHƯƠNG 05

VẤN PHÂN PHỐI KHÓA & THỎA THUẬN KHÓA



Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin

6 September 2022 | Page 3



VẤN ĐỀ PHÂN PHỐI VÀ THỎA THUẬN KHÓA



- ✓ Quản trị khóa trong các mạng truyền tin
- ✓ Sơ đồ phân phối khóa Blom
- ✓ Giao thức trao đổi khóa Diffie - Hellman
- ✓ Hệ phân phối khóa Kerberos

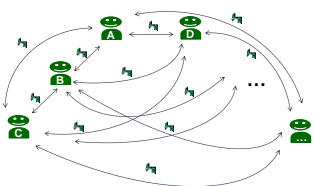
Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin

6 September 2022 | Page 4



Quản trị khóa trong các mạng truyền tin

Sơ đồ phân phối khóa bí mật với mạng gồm n người dùng



Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin

6 September 2022 | Page 5



Quản trị khóa trong các mạng truyền tin

- ❖ **Hệ mật khóa bí mật:** đòi hỏi kênh bí mật để chuyển khóa hoặc trao đổi khóa giữa các đối tác
- ❖ **Hệ mật khóa công khai (KCK):** về nguyên tắc hệ mật KCK không cần có những kênh bí mật như vậy. Tuy nhiên, trên thực tế để đảm bảo cho các hoạt động thông tin thực sự an toàn, không phải bất cứ thông tin nào về các KCK của một hệ mật mã, của một thuật toán kiểm thử chữ ký, của một giao thức xác nhận thông báo hay xác nhận danh tính, vv.. cũng phát công khai một cách tràn lan trên mạng công cộng, chỉ những ai cần biết thì mới nên biết mà thôi.
- ❖ Do đó, cần có những giao thức thực hiện việc trao đổi khóa giữa những đối tác thực sự có nhu cầu trao đổi thông tin với nhau, kể cả trao đổi khóa công khai

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin

6 September 2022 | Page 6



Quản trị khóa trong các mạng truyền tin

- ❖ **Việc trao đổi khóa giữa các chủ thể trong một cộng đồng nào đó có thể:**
 - ❑ Được thiết lập một cách tự do giữa bất cứ hai người nào khi có nhu cầu trao đổi thông tin
 - ❑ Được thiết lập một cách tương đối lâu dài trong một thời hạn nào đó trong cả cộng đồng với sự điều phối của một cơ quan được ủy thác (TA – Trusted Authority)



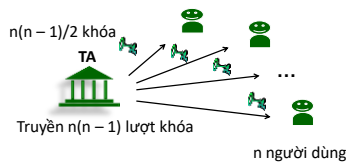
VẤN ĐỀ PHÂN PHỐI VÀ THỎA THUẬN KHÓA



- ❌ Quản trị khóa trong các mạng truyền tin
- ✅ Sơ đồ phân phối khóa Blom
- ❌ Giao thức trao đổi khóa Diffie - Hellman
- ✅ Hệ phân phối khóa Kerberos



Sơ đồ phân phối khóa Blom



- ❖ Sơ đồ phân phối khóa với mạng gồm n người dùng



Sơ đồ phân phối khóa Blom

- Chọn số nguyên tố $p \geq n$
 - Chọn cho mỗi người dùng A một số $r_A \in \mathbb{Z}_p$. (p, r_A) được công khai
 - Chọn ngẫu nhiên $a, b, c \in \mathbb{Z}_p$, và lặp đa thức

$$f(x, y) = a + b(x + y) + cxy \bmod p$$
 - Với mỗi người dùng A. TA tính:

$$g_A(x) = f(x, r_A) = a_A + b_A x \bmod p$$
- Trong đó: $a_A = a + br_A \bmod p$, $b_A = b + cr_A \bmod p$
- TA chuyển bí mật cặp số (a_A, b_A) cho A
 - Như vậy, A biết $g_A(x) = a_A + b_A x \bmod p$
- Với sơ đồ Blom TA truyền n lượt cặp số

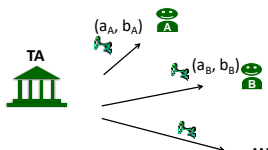
Với sơ đồ Blom TA chỉ phải truyền n lượt cặp số (a_A, b_A) thay vì $n(n-1)$ lượt khóa



Sơ đồ phân phối khóa Blom

- ❖ Khóa chung $K_{A,B}$:

$$K_{A,B} = g_A(r_B) = g_B(r_A) = f(r_A, r_B)$$



Sơ đồ phân phối khóa Blom

- ❖ **Nhận xét:**
 - ❑ Theo sơ đồ phân phối Blom, TA phân phối cho mỗi người dùng một phần bí mật của khóa, hai người dùng bất kỳ phối hợp phần bí mật của riêng mình với phần công khai của người kia để cùng tạo nên khóa bí mật dùng chung cho hai người.
 - ❑ Độ an toàn?



Sơ đồ phân phối khóa Blom

- ❖ **Sơ đồ Blom là an toàn theo nghĩa sau:**
 - ❑ Bất kỳ một người thứ ba C nào (kể cả C là một người tham gia trong mạng) có thể phát hiện được khóa bí mật riêng của A và B.
 - ❑ Chứng minh?
- ❖ **Nếu có hai người tham gia C, D khác A, B liên minh với nhau để phát hiện $K_{A,B}$ thì lại rất dễ dàng**
 - ❑ Chứng minh?

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin

6 September 2022 | Page 13



Sơ đồ phân phối khóa Blom

❖ Chứng minh:

- ❑ C là người tham gia trong mạng \Rightarrow C biết a_c, b_c do TA cung cấp. Ta CM với những gì C biết thì bất kì giá trị $l \in \mathbb{Z}_p$ nào cũng có thể được chấp nhận là $K_{A,B}$

$$\begin{aligned} a + b(r_A + r_B) + cr_A r_B &= l \\ a + br_C &= a_C \\ b + cr_C &= b_C \end{aligned}$$

- Hệ phương trình đó nếu xem a, b, c là ẩn số ta có định thức các hệ số như sau:

$$\begin{vmatrix} 1 & r_A + r_B & r_A r_B \\ 1 & r_C & 0 \\ 0 & 1 & r_C \end{vmatrix} = (r_C - r_A)(r_C - r_B)$$
 Theo giả thiết chọn các số r_i định thức đó khác 0, do đó HPT luôn có nghiệm $(a, b, c) \Rightarrow$ việc chấp nhận l là giá trị của $K_{A,B}$ là hoàn toàn có thể!

Bất kì giá trị $l \in \mathbb{Z}_p$ nào cũng có thể được C chấp nhận là $K_{A,B}$, điều này đồng nghĩa với C không biết $K_{A,B}$ là số nào!!!

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin

6 September 2022 | Page 14



Sơ đồ phân phối khóa Blom

❖ Chứng minh:

- ❑ C và D khác A, B liên minh với nhau để phát hiện $K_{A,B}$ thì lại dễ dàng vì C, D đều biết:

$$\begin{aligned} a + br_C &= a_C \\ b + cr_C &= b_C \\ a + br_D &= a_D \\ b + cr_D &= b_D \end{aligned}$$

- 4 phương trình đó đủ để xác định (a, b, c) từ đó tìm được $K_{A,B}$

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin

6 September 2022 | Page 15



Sơ đồ phân phối khóa Blom

- ❖ **Sơ đồ Blom tổng quát:** trong đó mọi khóa chung $K_{A,B}$ của A, B là bí mật hoàn toàn đối với bất kỳ liên minh nào gồm k người ngoài A và B, nhưng không còn là bí mật đối với mọi liên minh gồm $k + 1$ người tham gia trong mạng.

- ❑ Muốn vậy, ta thay đa thức:

$$f(x, y) = a + b(x + y) + cxy \pmod p$$

$a, b, c \in \mathbb{Z}_p$ bằng một đa thức đối xứng bậc 2k sau:

$$f(x, y) = \sum_{i=0}^k \sum_{j=0}^k a_{ij} x^i y^j \pmod p$$

Trong đó, $a_{ij} \in \mathbb{Z}_p, 0 \leq i, j \leq k, a_{ij} = a_{ji} \forall i, j$

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin

6 September 2022 | Page 16



VẤN ĐỀ PHÂN PHỐI VÀ THỎA THUẬN KHÓA



- ☒ Quản trị khóa trong các mạng truyền tin
- ☒ Sơ đồ phân phối khóa Blom
- ☒ Giao thức trao đổi khóa Diffie - Hellman
- ☒ Hệ phân phối khóa Kerberos

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin

6 September 2022 | Page 17



Giao thức trao đổi khóa Diffie - Hellman

- ❖ Giả sử A và B muốn liên lạc sử dụng hệ mật khóa bí mật. Để thỏa thuận mật khóa K chung cho cả hai bên qua một kênh không an toàn mà không ai khác có thể biết được, A và B có thể dùng thủ tục thỏa thuận khóa Diffie - Hellman

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin

6 September 2022 | Page 18



Giao thức trao đổi khóa Diffie - Hellman

Chọn trước số nguyên tố p thích hợp và phân tử sinh α của \mathbb{Z}_p^* ($2 \leq \alpha \leq p-2$).
Công khai giá trị p và α

A chọn số nguyên bí mật x : $1 \leq x \leq p-2$
và gửi B thông báo $\beta_A = \alpha^x \bmod p$
B chọn số nguyên bí mật y : $1 \leq y \leq p-2$
và gửi A thông báo $\beta_B = \alpha^y \bmod p$

B thu được β_A và tính khóa chung $k: k = (\beta_A)^y = (\alpha^x)^y \bmod p$
A thu được β_B và tính khóa chung $k: k = (\beta_B)^x = (\alpha^y)^x \bmod p$

❖ Thủ tục thỏa thuận khóa Diffie – Hellman giữa người A và người B

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin

6 September 2022 | Page 19



Giao thức trao đổi khóa Diffie - Hellman

❖ Ví dụ:

- Giả sử A và B chọn $p = 11$ và $\alpha = 2$
- Giả sử A chọn giá trị ngẫu nhiên $x = 4$ và gửi cho B giá trị $2^4 \bmod 11 = 5$.
- Giả sử B chọn giá trị ngẫu nhiên $y = 7$ và gửi cho A giá trị $2^7 \bmod 11 = 7$.
- B nhận được 5 và tính khóa chung $k = 5^7 \bmod 11 = 3$
- A nhận được 7 và tính khóa chung $k = 7^4 \bmod 11 = 3$

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin

6 September 2022 | Page 20



Giao thức trao đổi khóa Diffie - Hellman

❖ Bài tập áp dụng:

- Cho $p = 211$ và $\alpha = 41$ là các tham số công khai dùng cho thủ tục thỏa thuận khóa Diffie – Hellman. Giả sử A chọn $x = 101$ và B chọn $y = 57$. Hãy tính khóa chung của A và B
 - A tính $\alpha^x \bmod p = 41^{101} \bmod 211 = 155$
 - B tính $\alpha^y \bmod p = 41^{57} \bmod 211 = 27$
 - A tính khóa chung $k = (\alpha^y)^x \bmod p = 27^{101} \bmod 211 = 90$
 - B tính khóa chung $k = (\alpha^x)^y \bmod p = 155^{57} \bmod 211 = 90$

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin

6 September 2022 | Page 21



Giao thức trao đổi khóa Diffie - Hellman

❖ Hệ phân phối khóa Diffie – Hellman:

- Hệ phân phối khóa Diffie – Hellman không đòi hỏi TA phải biết và chuyển bất kỳ thông tin bí mật nào về khóa của các người tham gia trong mạng để họ thiết lập được khóa chung bí mật cho việc truyền tin với nhau.
- Trong hệ phân phối khóa này TA chỉ việc chọn 1 số nguyên tố lớn p và một phần tử nguyên thủy $\alpha \bmod p$, sao cho bài toán tính \log_{α} trong \mathbb{Z}_p^* là rất khó.

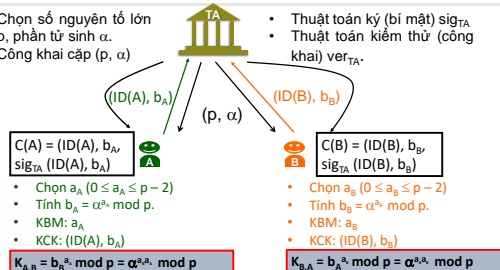
Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin

6 September 2022 | Page 22



Giao thức trao đổi khóa Diffie - Hellman

- Chọn số nguyên tố lớn p , phân tử sinh α .
- Công khai cặp (p, α)
- Thuật toán ký (bí mật) sig_{TA}
- Thuật toán kiểm thử (công khai) ver_{TA} .



Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin

6 September 2022 | Page 23



Giao thức trao đổi khóa Diffie - Hellman

❖ Khóa chung của A, B:

$$K_{A,B} = b_B^{a_A} \bmod p = \alpha^{a_A a_B} \bmod p$$

$$K_{B,A} = b_A^{a_B} \bmod p = \alpha^{a_B a_A} \bmod p$$

- ❖ Để đảm bảo được các thông tin về b_B và b_A là chính xác, A và B có thể dùng thuật toán ver_{TA} để kiểm thử chữ ký xác nhận của TA trong các chứng chỉ $C(B)$ và $C(A)$ tương ứng.
- ❖ Độ an toàn của hệ phân phối khóa Diffie – Hellman dựa trên bài toán khó tương đương với bài toán tính logarithm rời rạc.

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin

6 September 2022 | Page 24



VẤN ĐỀ PHÂN PHỐI VÀ THỎA THUẬN KHÓA



- ✔ Quản trị khóa trong các mạng truyền tin
- ✔ Sơ đồ phân phối khóa Blom
- ✔ Giao thức trao đổi khóa Diffie - Hellman
- ✔ Hệ phân phối khóa Kerberos

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin

6 September 2022 | Page 25



Hệ phân phối khóa Kerberos

- ❖ **Kerberos, RFC 1510:** Là một giao thức mật mã dùng để xác thực trong các mạng máy tính hoạt động trên những đường truyền không an toàn.
- ❖ **Kerberos:** có khả năng chống lại việc nghe lén và đảm bảo tính toàn vẹn của dữ liệu

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin

6 September 2022 | Page 26



Hệ phân phối khóa Kerberos

- ❖ Mục tiêu khi thiết kế giao thức này là nhằm vào mô hình client – server và đảm bảo xác thực cho cả hai chiều.
- ❖ Giao thức được xây dựng dựa trên mật mã khóa đối xứng và cần đến một bên thứ ba gọi là “Trung tâm phân phối khóa” (Key Distribution Center).
- ❖ Hiện có 2 phiên bản là Kerberos v4 và Kerberos v5.

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin

6 September 2022 | Page 27



Hệ phân phối khóa Kerberos

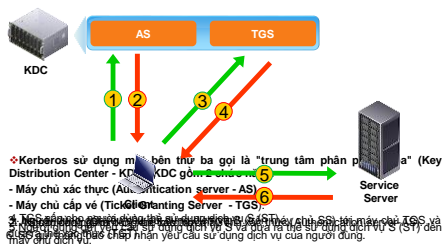
- ❑ **Từ viết tắt**
 - ❑ AS: Authentication Server
 - ❑ TGS: Ticket Granting Server
 - ❑ KDC (= AS+TGS): Key Distribution Center
 - ❑ SS: Service Server
 - ❑ TGT: Ticket Granting Ticket
 - ❑ ST: Service Ticket

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin

6 September 2022 | Page 28



Hệ phân phối khóa Kerberos

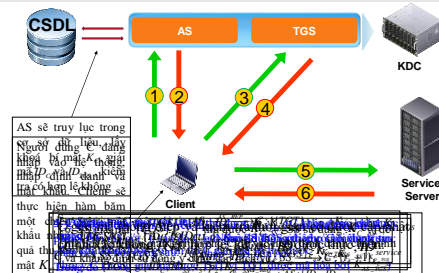


Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin

6 September 2022 | Page 29



Hệ phân phối khóa Kerberos



Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin

6 September 2022 | Page 30



Hệ phân phối khóa Kerberos

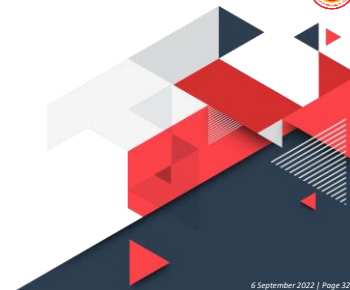
- ❖ **Tồn tại một điểm yếu:** Nếu máy chủ trung tâm ngừng hoạt động thì mọi hoạt động sẽ ngừng lại. Điểm yếu này có thể được hạn chế bằng cách sử dụng nhiều máy chủ Kerberos.
- ❖ **Giao thức đòi hỏi** đồng hồ của tất cả những máy tính liên quan phải được đồng bộ. Nếu không đảm bảo điều này, cơ chế xác thực giữa trên thời hạn sử dụng sẽ không hoạt động. Thiết lập mặc định đòi hỏi các đồng hồ không được sai lệch quá 10 phút. Cơ chế thay đổi mật khẩu không được tiêu chuẩn hóa.

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin

6 September 2022 / Page 31

CẢM ƠN.

Bộ môn Khoa Học An Toàn Thông Tin – Khoa An Toàn Thông Tin



6 September 2022 / Page 32