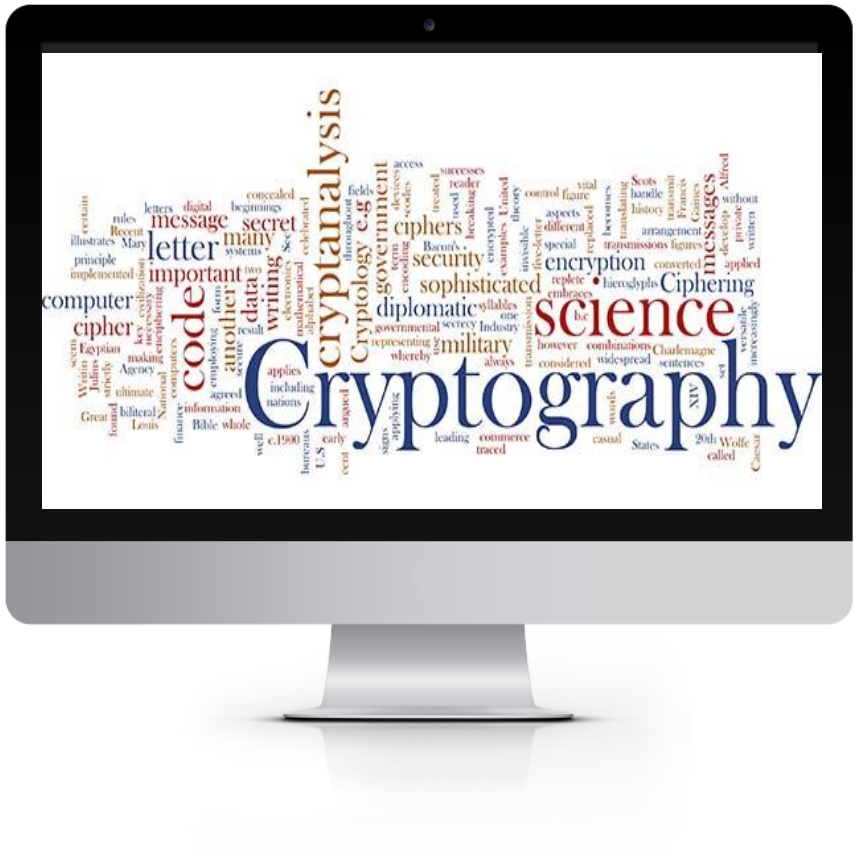
NHẬP MÔN MẬT MÃ HỌC

NỘI DUNG

CHƯƠNG 05

VẤN PHÂN PHỐI KHÓA & THỎA THUẬN KHÓA

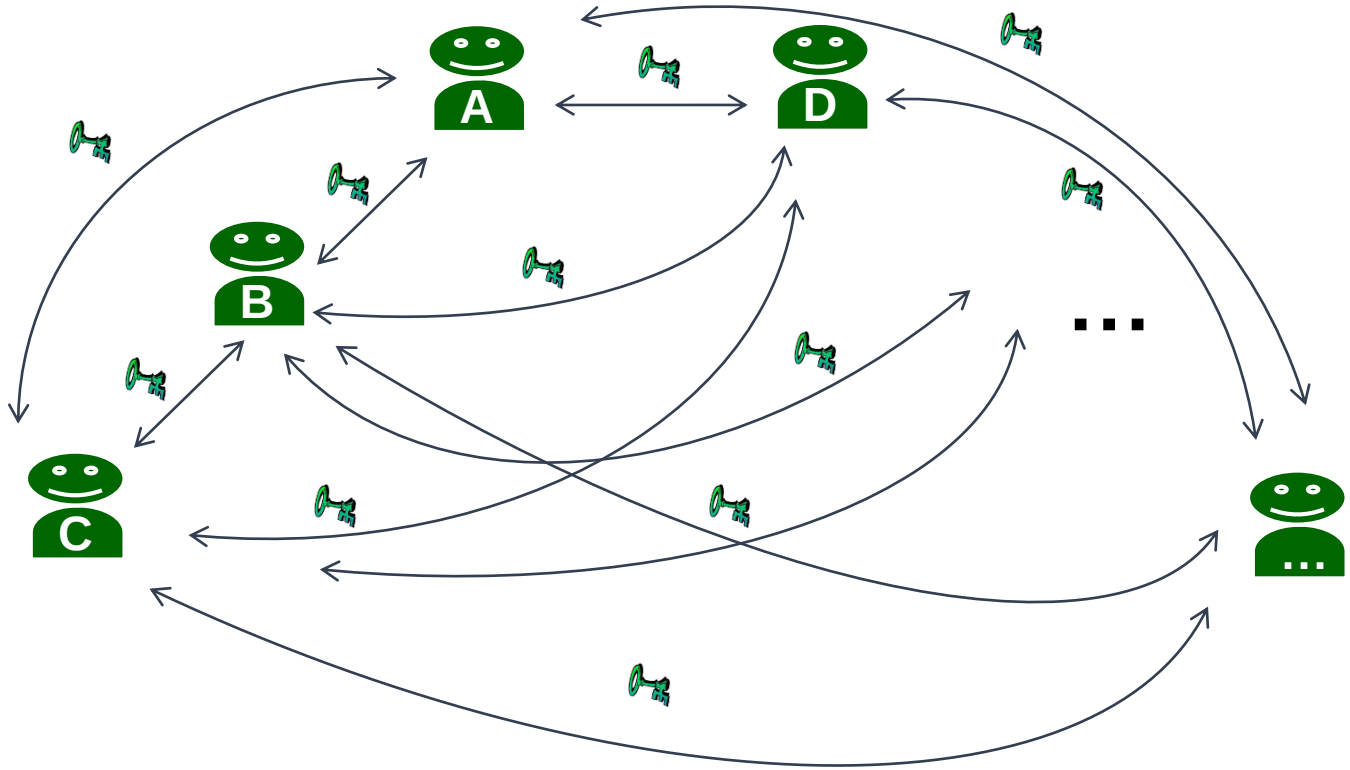
VẤN ĐỀ PHÂN PHỐI VÀ THỎA THUẬN KHÓA



- 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

Quản trị khóa trong các mạng truyền tin

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



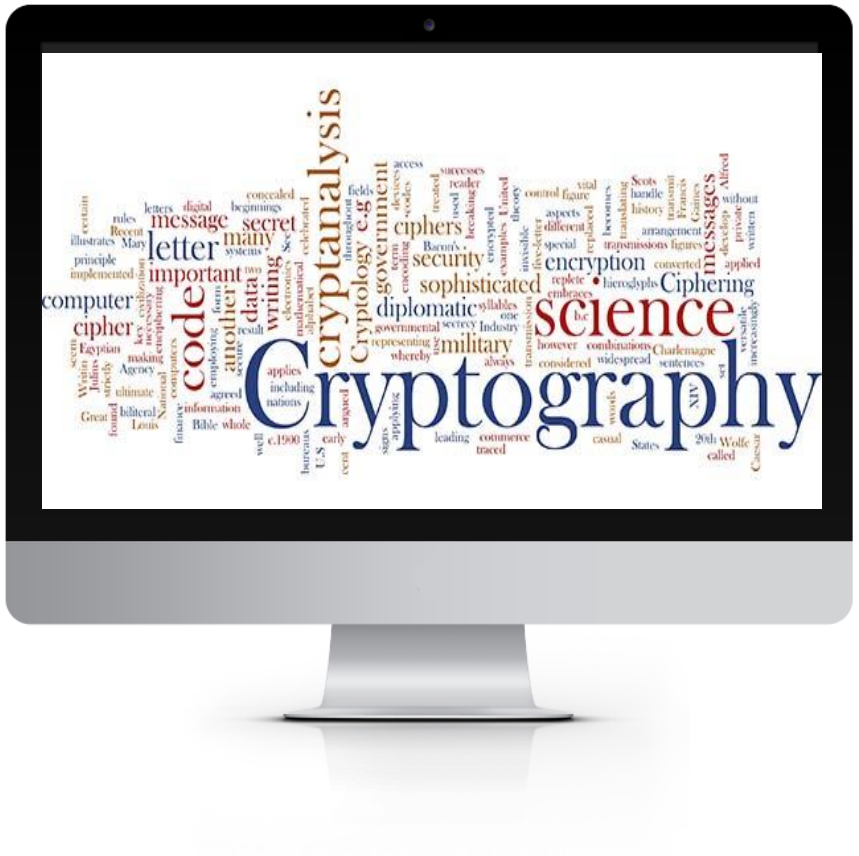
Quản trị khóa trong các mạng truyền tin

- **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

Quản trị khóa trong các mạng truyền tin

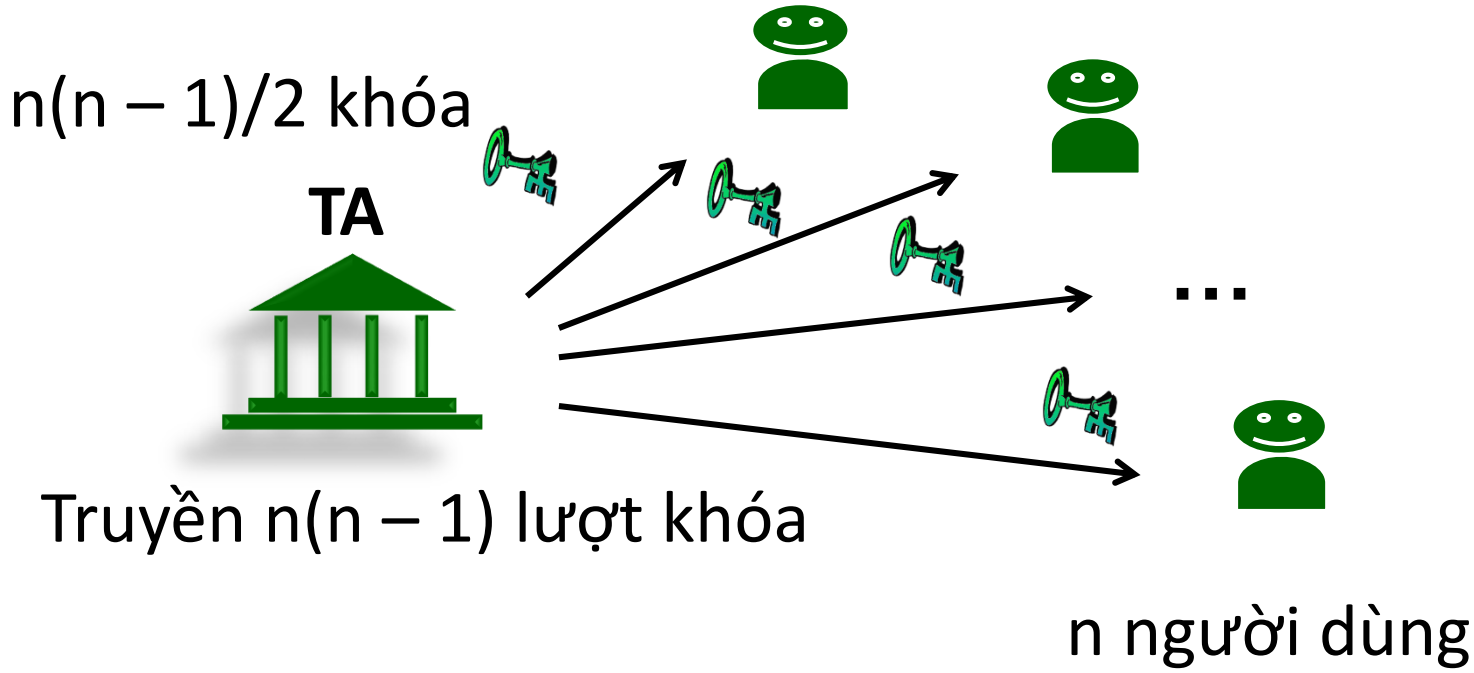
- **Việc trao đổi khóa giữa các chủ thể trong một cộng đồng nào đó có thể:**
  - Được thiết lập một cách tự do giữa bất cứ hai người nào khi có nhu cầu trao đổi thông tin
  - Được thiết lập một cách tương đối lâu dài trong một thời hạn nào đó trong cả cộng đồng với sự điều phối của một cơ quan được ủy 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 $r_A \in Z_p$. (p, r_A) được công khai
- Chọn ngẫu nhiên $a, b, c \in Z_p$, và lập 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: $a_A = a + br_A \bmod p$, $b_A = b + cr_A \bmod p$

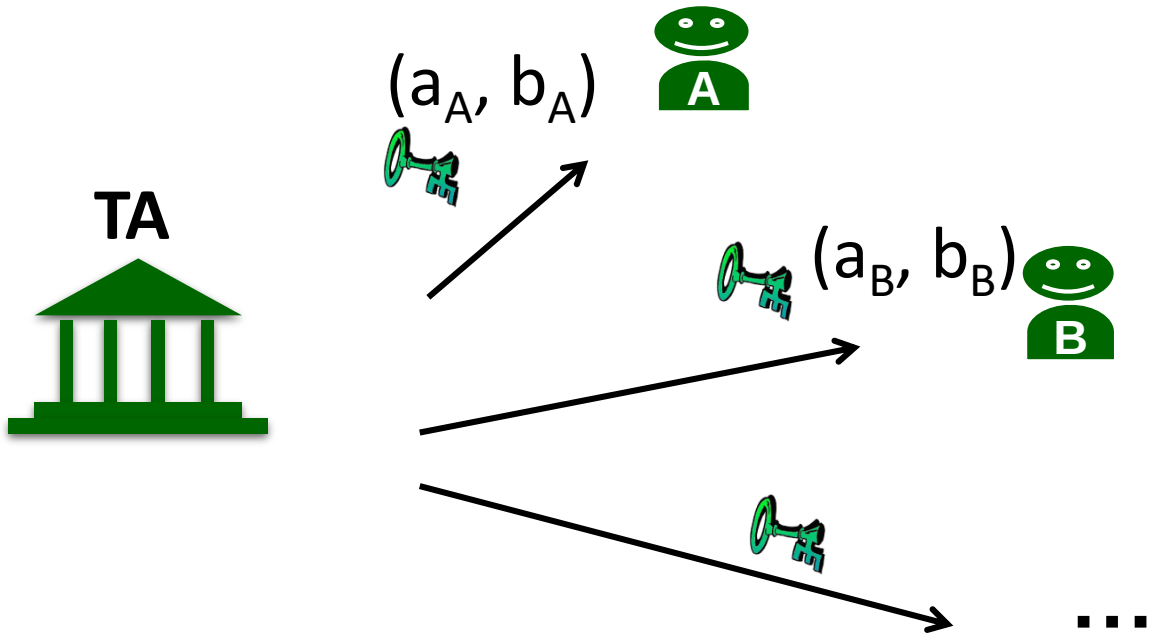
- TA chuyển bí mật cặp số (a_A, b_A) cho A
- Như vậy, A biết $g_A(x) = a_A + b_A x \bmod p$

Với sơ đồ Blom TA 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) không 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?

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:

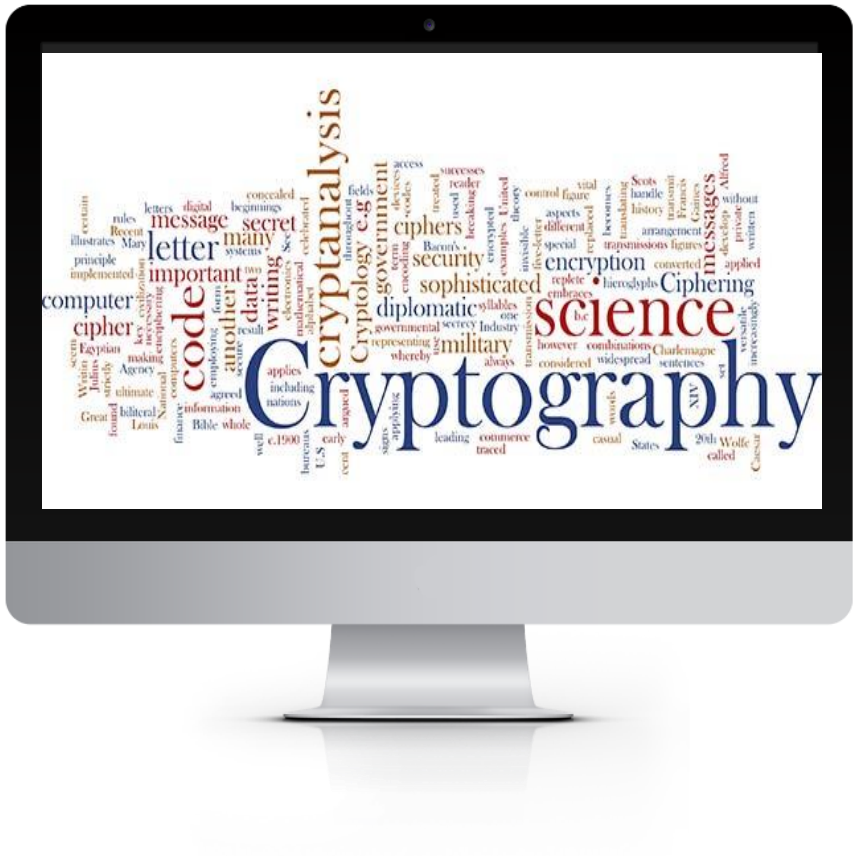
$$f(x, y) = a + b(x + y) + cxy \bmod p$$

a, b, c $\in Z_p$ bằng một đa thức đối xứng bậc 2k sau:

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

Trong đó, $a_{ij} \in Z_p$, $0 \le i, j \le k$, $a_{ij} = a_{ij}\ \forall i, j$

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

Giao thức trao đổi khóa Diffie - Hellman

- Giả sử A và B muốn liên lạc sử dụng hệ mật khoá bí mật. Để thoả thuận mật khoá 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 thoả thuận khoá Diffie -Hellman

Giao thức trao đổi khóa Diffie - Hellman

Chọn trước số nguyên tố p thích hợp và phần tử sinh α của Z_p^* ($2 \le \alpha \le p - 2$).
Công khai giá trị **p và α**

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

Giao thức trao đổi khóa Diffie - Hellman

- **Ví dụ:**
  - Giả sử A và B chọn p = 11 và α = 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 khoá chung $k = 5^7 \bmod 11 = 3$
  - A nhận được 7 và tính khoá chung $k = 7^4 \bmod 11 = 3$

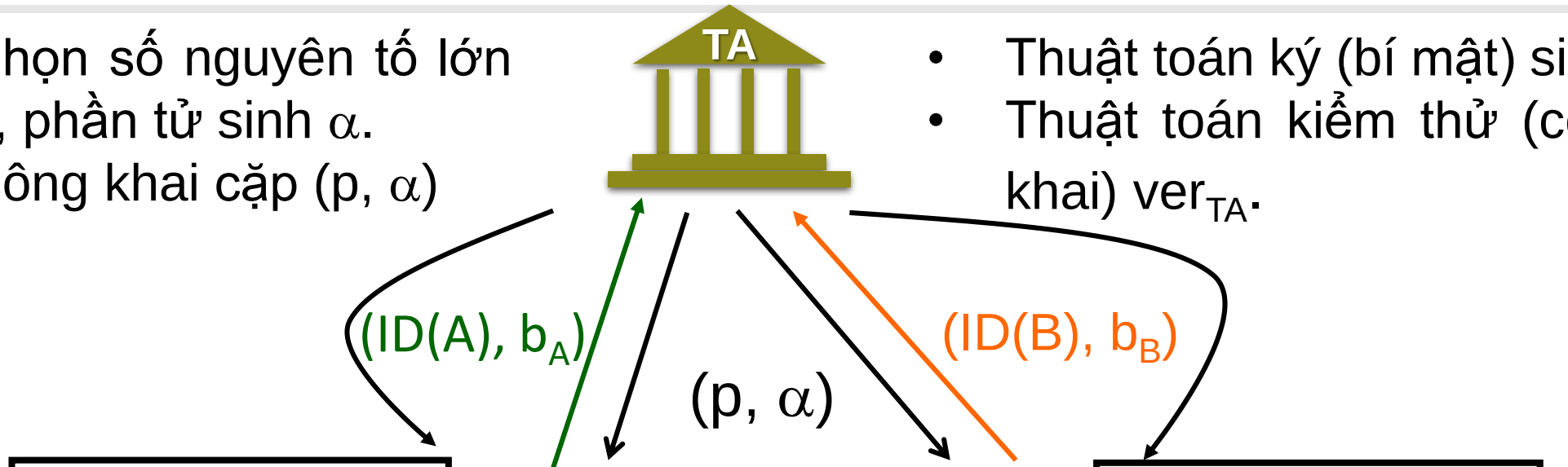
Giao thức trao đổi khóa Diffie - Hellman

- **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 α mod p, sao cho bài toán tính $\log_{\alpha}$ trong Z_p^* là rất khó.

Giao thức trao đổi khóa Diffie - Hellman

- Chọn số nguyên tố lớn p, phần tử sinh α.
- Công khai cặp (p, α)

- Thuật toán ký (bí mật) sig_{TA}
- Thuật toán kiểm thử (công khai) ver_{TA}.



$C(A) = (ID(A), b_A, sig_{TA}(ID(A), b_A))$

- Chọn a_A ($0 \le a_A \le p - 2$)
- Tính $b_A = \alpha^{a_A} \bmod p$.
- KBM: a_A
- KCK: $(ID(A), b_A)$

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

$C(B) = (ID(B), b_B, sig_{TA}(ID(B), b_B))$

- Chọn a_B ($0 \le a_B \le p - 2$)
- Tính $b_B = \alpha^{a_B} \bmod p$.
- KBM: a_B
- KCK: $(ID(B), b_B)$

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

Giao thức trao đổi khóa Diffie - Hellman

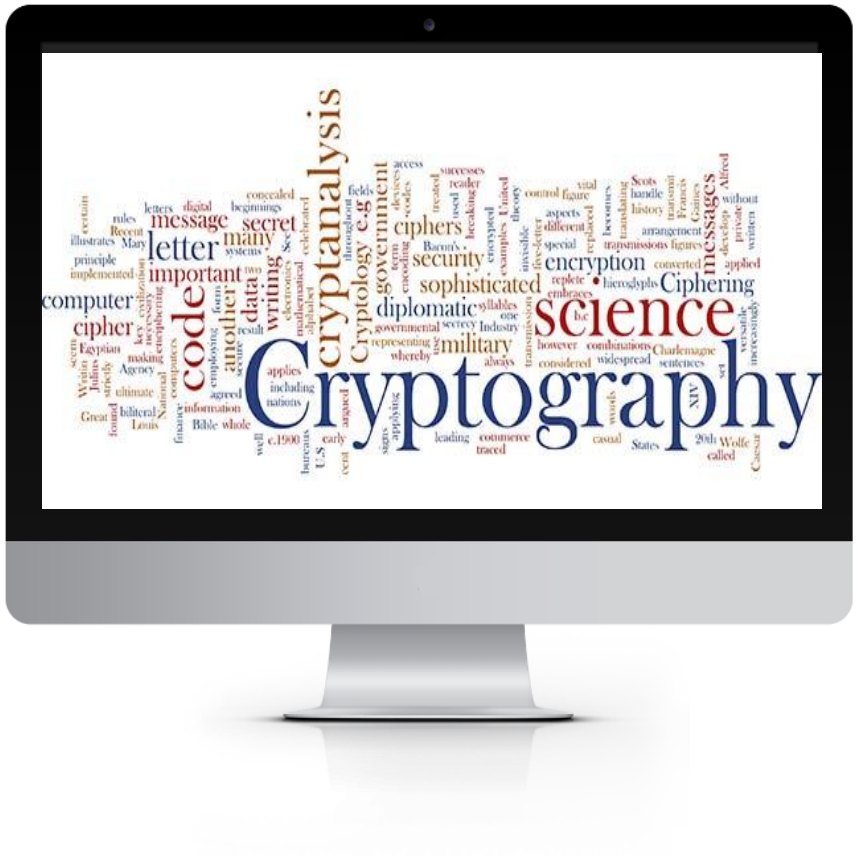
- Khóa chung của A, B:

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

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

- Để đảm bảo được các thông tin về b_B và b_A là chính xác, A và B có thể dùng thuật toán verTA 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 logarit rời rạc.

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

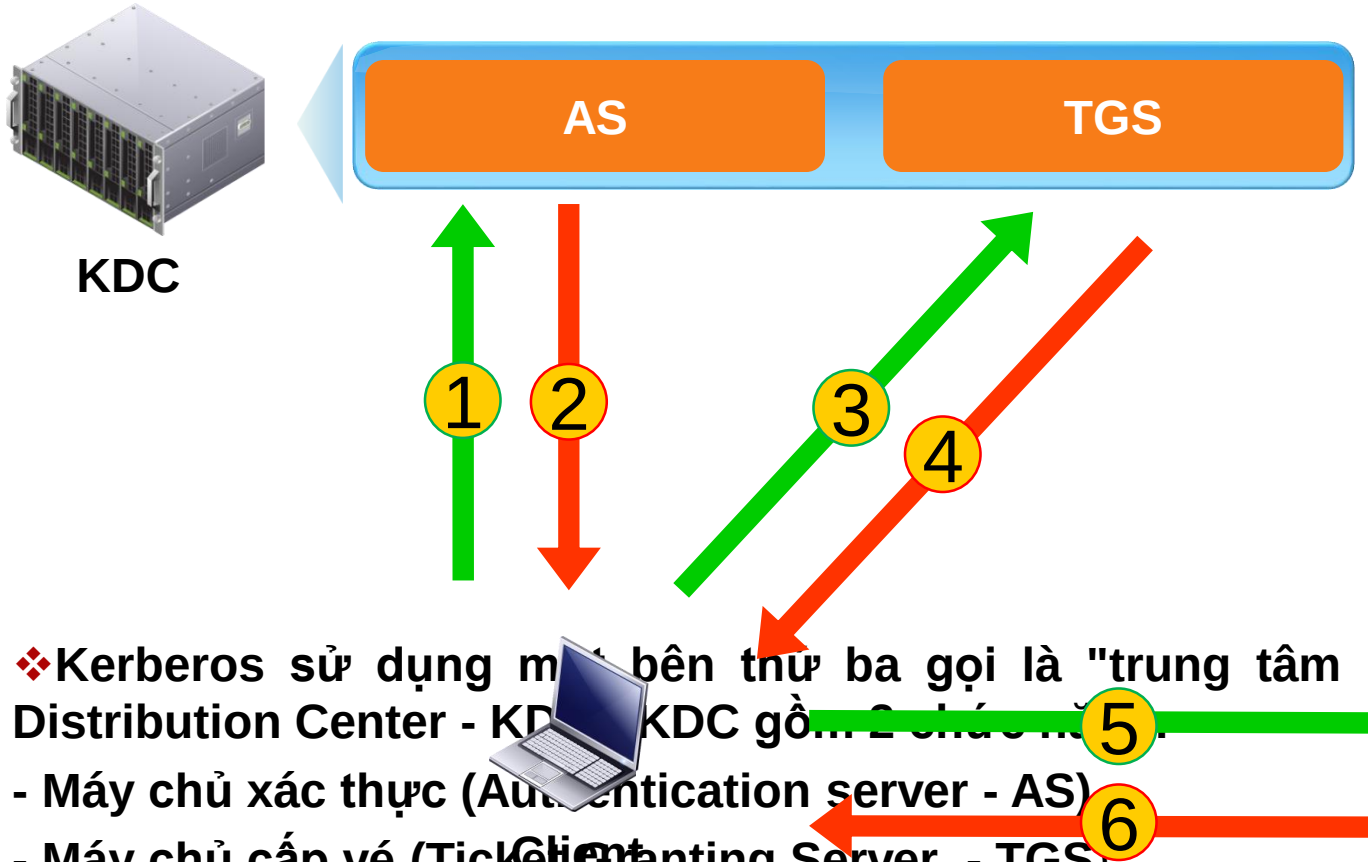
Hệ phân phối khóa Kerberos

- **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

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.

Hệ phân phối khóa Kerberos



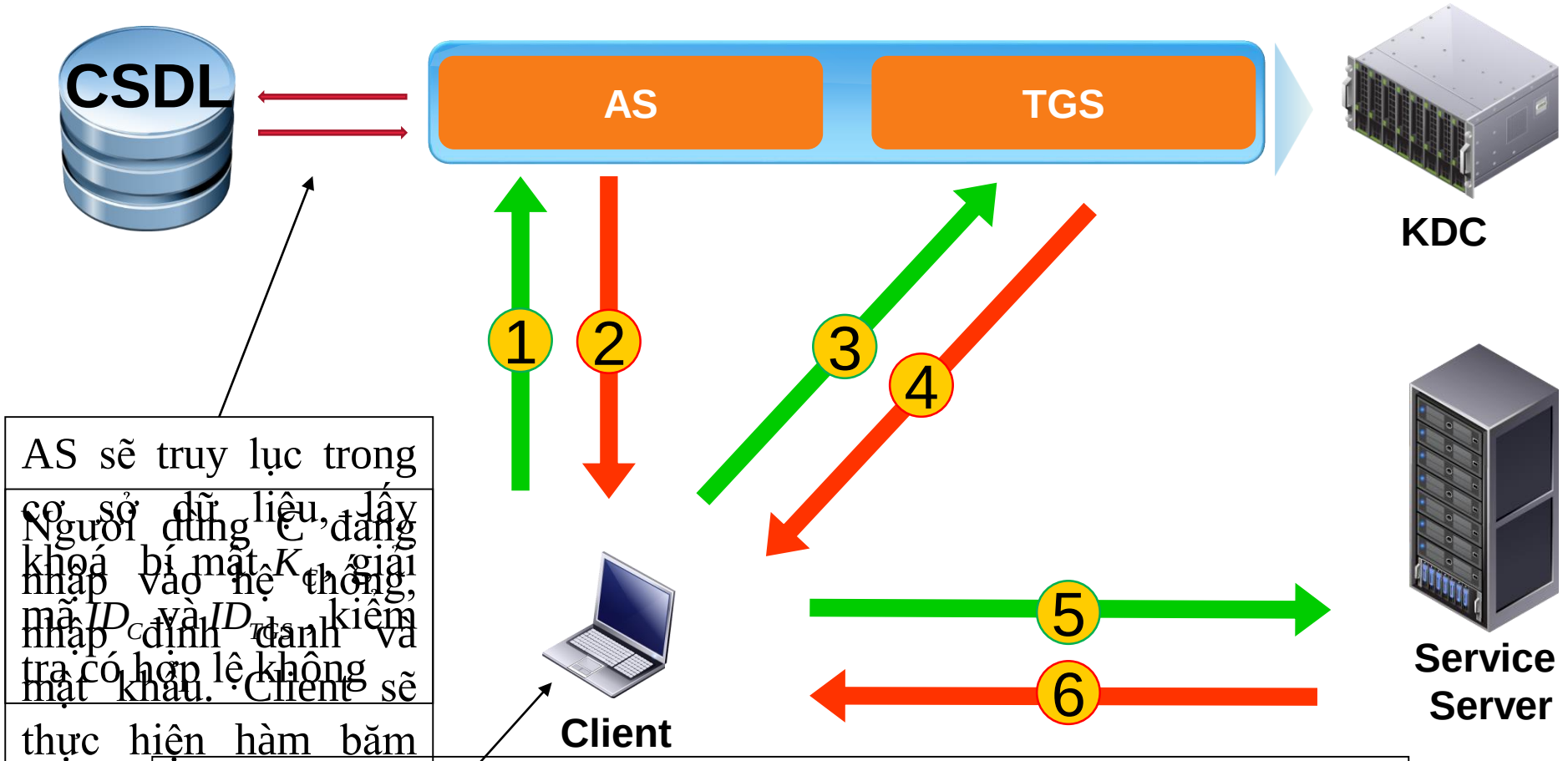
❖**Kerberos sử dụng một bên thứ ba gọi là "trung tâm phân phối khóa" (Key Distribution Center - KDC). KDC gồm 2 chức năng:**

- Máy chủ xác thực (Authentication server - AS).

- Máy chủ cấp vé (Ticket Granting Server - TGS).

1. Người dùng gửi yêu cầu sử dụng dịch vụ S và đưa ra thẻ sử dụng dịch vụ S (ST) đến máy chủ dịch vụ.
2. TGS xác nhận người dùng có thể sử dụng dịch vụ S (ST máy chủ SS) tới máy chủ TGS và gửi tới máy chủ xác thực (AS).
3. AS gửi thông báo chấp nhận yêu cầu sử dụng dịch vụ của người dùng.

Hệ phân phối khóa Kerberos



AS sẽ truy lục trong cơ sở dữ liệu, lấy khoá bí mật K_C, giải mã ID_C và ID_{TGS}, kiểm tra có hợp lệ không

Người dùng C đăng nhập vào hệ thống, nhập định danh và mật khẩu. Client sẽ thực hiện hàm băm một chiều với mật khẩu nhập vào làm khoá, quả thu được chính là mật K_C

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.

CẢM ƠN.