TRUYỀN VÀ BẢO MẬT THÔNG TIN

Bài 6:

Mã hóa đối xứng hiện đại (phần III)

VŨ THỊ TRÀ

Nội dung

- Bản tin, mã ASCII, biểu diễn nhị phân
- Mã dòng (Stream Cipher)
- Mã khối (Block Cipher)
- Mã DES (Data Encryption Standard)
- Mã AES (Advanced Encryption Standard); Các mô hình ứng dụng của mã khối
- Một số thuộc tính hệ MHĐXHĐ; Trao đổi khóa bí mật bằng TT phân phối khóa KDC

Một số phương pháp mã khối khác

- **Mã Triple DES, Double DES** : khắc phục khóa ngắn trong DES, sử dụng mã DES nhiều lần với các khóa khác nhau cho cùng một bản tin.
  - **Mã Double DES** :

$$C = E(E(P, K_1), K_2)$$

    - ✓ *Tương tự DES với khóa 112 bít*
    - ✓ *Tốc độ chậm hơn DES*
    - ✓ *Tấn công Double DES theo choosen-plaintext: gặp-nhau-ở-giữa (meet-in-the-middle)*
  - **Mã Triple DES** :

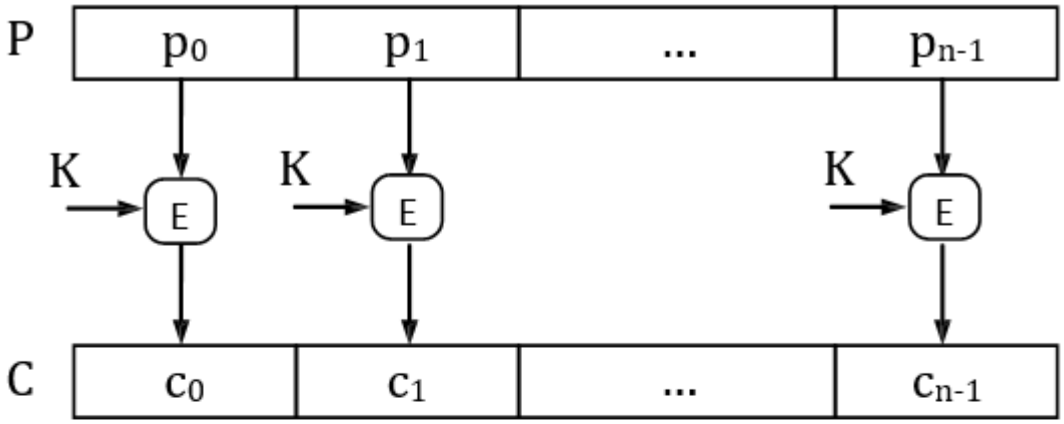
$$C = E(E(E(P, K_1), K_2), K_3)$$

Một số phương pháp mã khối khác

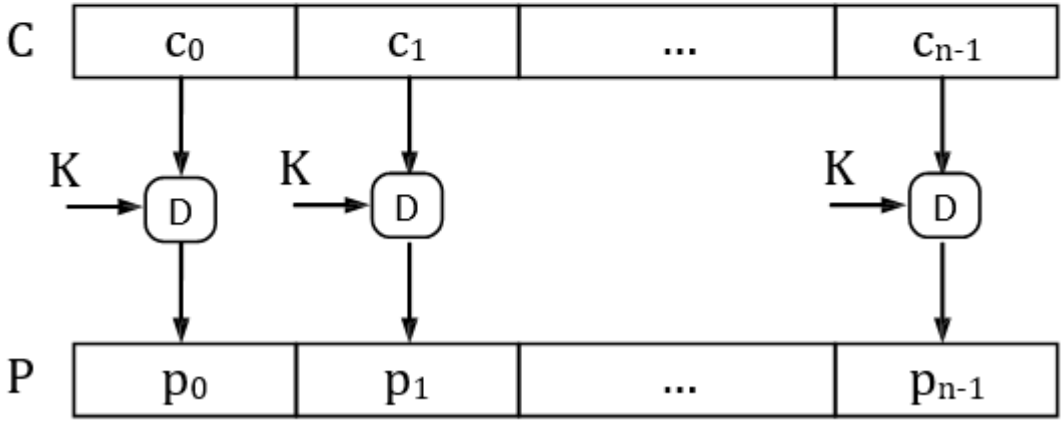
- **Mã AES (Advanced Encryption Standard):** 1990, Cục tiêu chuẩn QG Hoa Kỳ kêu gọi xây dựng pp mã hóa mới. Rijndael được chọn và đổi tên AES. Mã hóa AES với khóa có kích thước 256 bít là "an toàn mãi mãi" bất kể những tiến bộ trong ngành kỹ thuật máy tính. Đặc tính chính của AES
  - Cho phép lựa chọn kích thước khối mã hóa là 128, 192 hay 256 bít
  - Cho phép lựa chọn kích thước của khóa một cách độc lập với kích thước khối: là 128, 192 hay 256 bít
  - Số lượng vòng có thể thay đổi từ 10 đến 14 vòng tùy thuộc vào kích thước khóa

Các mô hình ứng dụng mã khối

1/.Mô hình ECB (Electronic Codebook)



a) Quá trình mã hóa

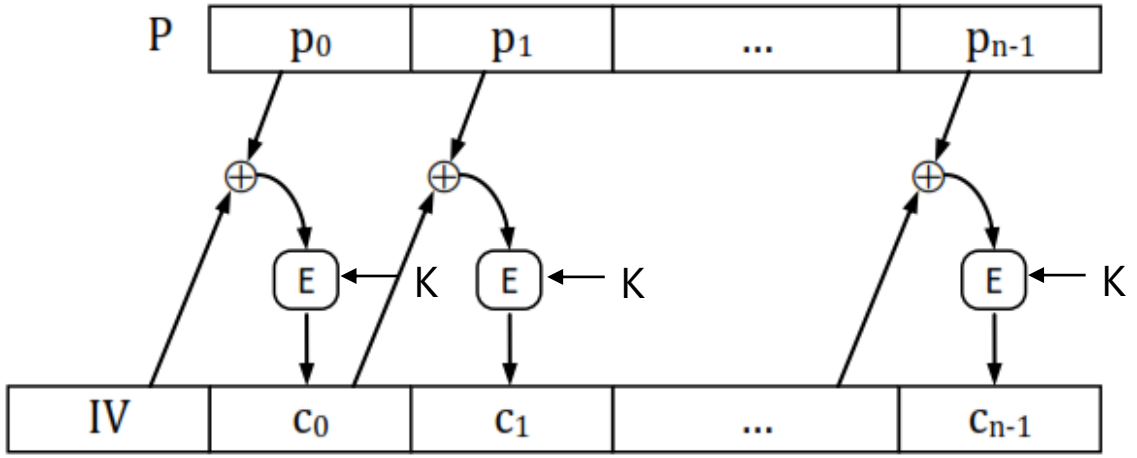


b) Quá trình giải mã

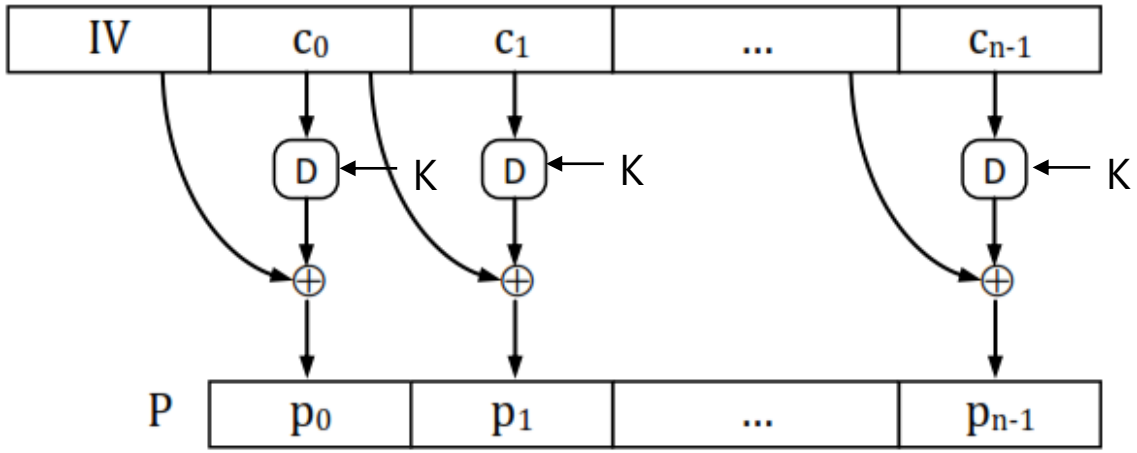
Ảnh sau khi mã hóa dùng mô hình ECB

✓ *Mã hóa dùng mô hình ECB không che dấu hết thông tin*

2/.Mô hình CBC (Cipher Block Chaining)



a) Quá trình mã hóa



b) Quá trình giải mã

Mô hình chuỗi khối mã CBC

- Bản mã của một lần mã hóa được dùng cho lần mã hóa tiếp theo

$$C_i = E(P_i \oplus C_{i-1}, K),\ với\ i = 1,2, \dots, n-1$$

$$C_0 = E(P_0 \oplus IV, K),\ với\ i = 0\ và$$

$$IV - initialization\ vector\ được\ khởi\ tạo\ ngẫu\ nhiên$$

- Để giải mã, tiến hành ngược lại:

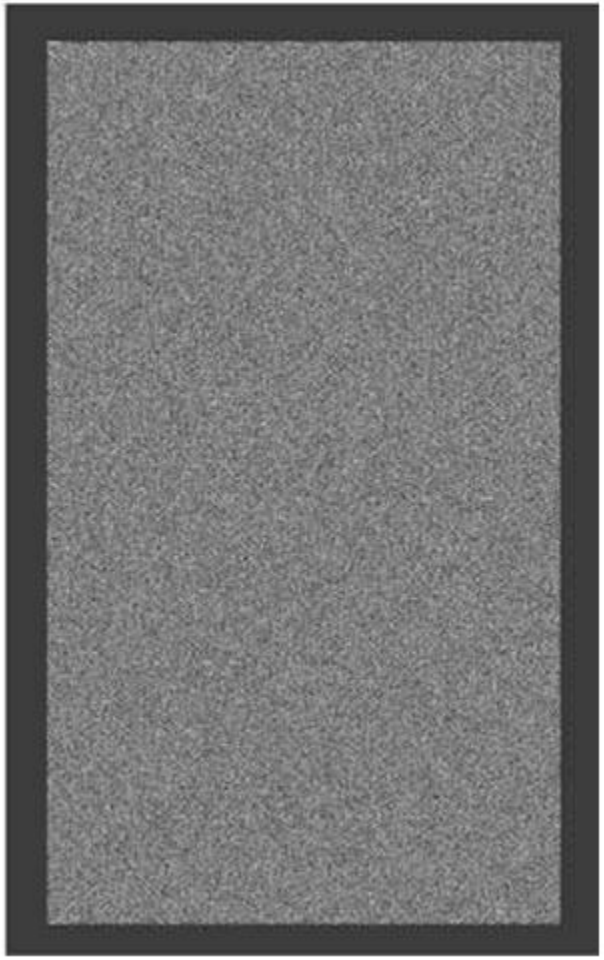
$$P_0 = D(C_0, K) \oplus IV$$

$$P_i = D(C_i, K) \oplus C_{i-1}\ với\ i = 1,2, \dots, n-1$$

Đặc tính của mô hình CBC

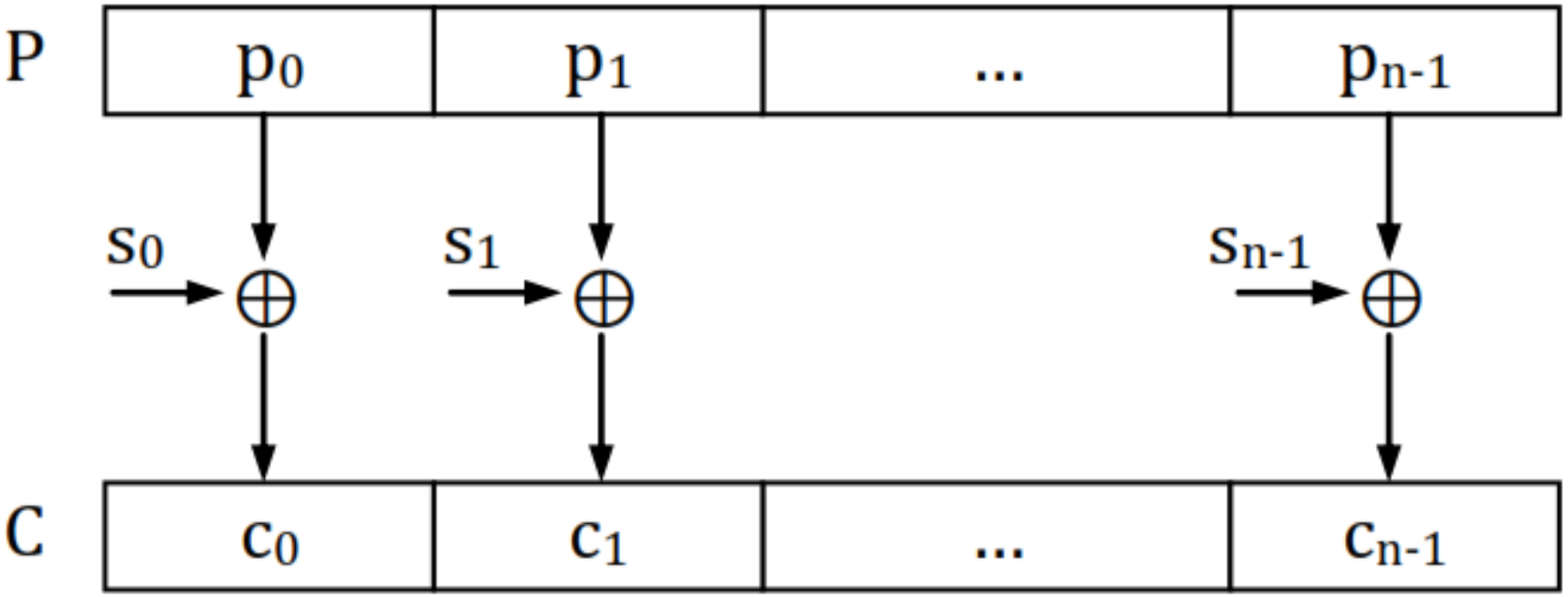
- **Ưu:** Bản mã C_i không chỉ phụ thuộc vào bản rõ P_i mà còn phụ thuộc vào tất cả các bản rõ đứng trước và IV. Do đó nếu có hai bản rõ giống nhau thì hai bản mã sẽ khác nhau (do *IV* ngẫu nhiên). Điều này khắc phục được hạn chế của mô hình ECB, từ bản mã người phá mã không thể phát hiện ra những đặc tính thống kê của dữ liệu.
- **Nhược:** Bản mã C_i không chỉ phụ thuộc vào bản rõ P_i mà còn phụ thuộc vào bản mã C_{i-1} đứng trước. Do đó nếu xảy lỗi trên đường truyền, chỉ cần một bít bị hỏng thì dẫn đến không thể giải mã được bản mã đó và bản mã tiếp theo sau.

Ảnh sau khi mã hóa dùng mô hình CBC



✓ *Mã hóa dùng mô hình CBC che dấu hết thông tin*

3/.Mô hình sinh số CTR (Counter)



→ s_i *được sinh ra từ bộ sinh số ngẫu nhiên*

Một số thuộc tính hệ MHĐXHĐ

Tính chứng thực (authentication) của mã hóa đối xứng

Xét tình huống 1: vấn đề mạo danh

1. Alice và Bob quyết định dùng mã Vigenere để trao đổi dữ liệu, với khóa bí mật K_{AB} là „DECEPTIVE“
2. Khi Alice gửi cho Bob một bản mã C, Bob dùng K_{AB} để giải mã cho ra bản rõ. Ví dụ, Alice gửi bản mã: „ZICVTWQNGRZGVTWAVZHCQYGLMGJ“. Bob giải mã có được bản rõ: „wearediscoveredsaveyourself“. Đây là một bản tin tiếng Anh có ý nghĩa.

Tính chứng thực (authentication) của mã hóa đối xứng

Xét tình huống 1: vấn đề mạo danh

3. Trudy muốn mạo danh Alice nên tìm một bản mã C_T và gửi C_T cho Bob. Bob nghĩ rằng C_T là từ Alice nên giải mã bằng K_{AB} và có được bản rõ P_T. Vấn đề ở đây là làm sao Bob biết được P_T là của Trudy chứ không phải của Alice?
4. Vì Trudy không biết K_{AB} nên Trudy không thể chọn P_T trước rồi mới có C_T. Do đó Trudy phải chọn ngẫu nhiên một C_T nào đó. Ví dụ Trudy chọn WDTAXRLKY". Như vậy Bob giải mã có được P_T là „tzrwiydpu". Tuy nhiên này không phải là văn bản có nghĩa trong tiếng Anh.
5. Việc Trudy chọn được một C_T nào đó, sao cho sau khi Bob giải mã cho ra P_T là văn bản có nghĩa, thì có xác suất rất bé.

Tính chứng thực (authentication) của mã hóa đối xứng

Xét tình huống 1: vấn đề mạo danh

→ *P_T có nghĩa coi như không thể xảy ra.*

→ *có thể chắc chắn rằng nếu Trudy mạo danh thì P_T sẽ là văn bản vô nghĩa, từ đó Bob biết được C_T là không phải từ Alice.*

Tính chứng thực (authentication) của mã hóa đối xứng

Xét tình huống 2: vấn đề sửa nội dung thông điệp, nếu Trudy chặn được bản mã C của Alice và sửa C thành C_T, thì xác suất để P_T là văn bản có nghĩa cũng rất bé. Và Bob biết được C đã bị sửa đổi.

Trong mã hóa hiện đại, nếu Trudy chọn C_T là một dãy bít bất kỳ thì bản rõ P_T cũng là một dãy bít lộn xộn, không có cấu trúc ý nghĩa. Thực tế, việc xác định như thế nào là dãy bít vô nghĩa là một công việc khó khăn đối với máy tính. Để đảm bảo tính chứng thực, người ta dùng khái niệm mã chứng thực thông điệp – MAC để biến dãy bít ngẫu nhiên thành dãy bít có cấu trúc

Tính chứng thực (authentication) của mã hóa đối xứng

Xét tình huống 3: vấn đề tấn công phát lại thông điệp (replay attack). Alice gửi bản mã C cho Bob, Bob nhận được và giải mã để có bản rõ P. Tuy nhiên Trudy chặn được bản mã C và sau đó mạo danh Alice gửi C cho Bob thêm một lần nữa. Bob giải mã và cũng có được P. Như vậy Bob nhận được cùng một thông điệp P hai lần. Tại lần thứ 2, Bob không có cơ sở xác định là Alice muốn gửi lại hay là do Trudy gửi.

→ Các phương pháp chống lại hình thức tấn công phát lại thông điệp?

Tính không từ chối (non-repudiation) của mã hóa đối xứng

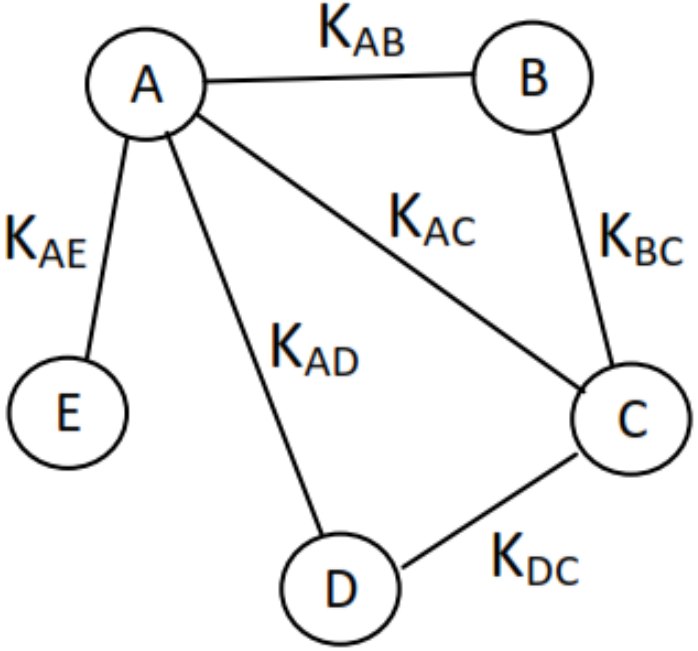
- Mã hóa đối xứng đảm bảo tính bảo mật của hệ truyền tin, tuy nhiên mã hóa đối xứng lại không thực hiện được tính không từ chối. Nguyên nhân ở đây là tính bí mật của khóa. Vì khóa K bí mật có hai người biết, nên nếu K bị tiết lộ thì không có cơ sở để quy trách nhiệm cho Alice hay Bob làm lộ khóa. Do đó Alice có thể từ chối là đã gửi bản tin.

→ *Tìm kiếm các phương pháp mã hóa khác, sao cho khóa bí mật chỉ có một người biết* → *Mã hóa khóa công khai*

Trao đổi khóa bí mật bằng TT phân phối khóa KDC

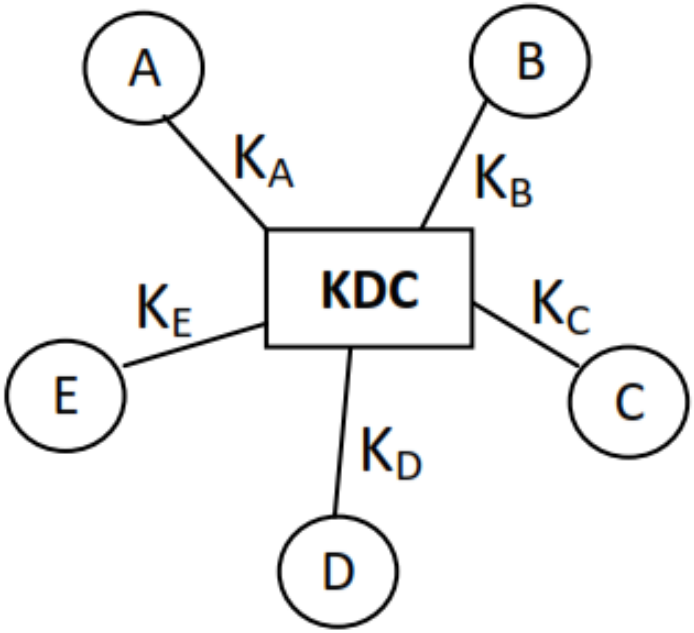
Trao đổi khóa bí mật bằng trung tâm phân phối khóa

- Giả sử có N người sử dụng, trao đổi dữ liệu bằng mã hóa đối xứng, mỗi cặp người sử dụng cần có một khóa bí mật riêng, dẫn đến cần có N(N-1)/2 khóa bí mật. Việc thiết lập các khóa bí mật này sẽ gây ra khó khăn cho các người sử dụng vì mỗi người cần thiết lập N-1 khóa.



Trao đổi khóa bí mật bằng trung tâm phân phối khóa

- Trao đổi khóa bằng trung tâm phân phối khóa (Key Distribution Center – KDC) giúp đơn giản hóa vấn đề này. Trong mô hình sử dụng KDC, mỗi người sử dụng chỉ cần có một khóa bí mật với KDC. Còn khóa dùng để trao đổi dữ liệu giữa các cặp người sử dụng sẽ do KDC cung cấp.

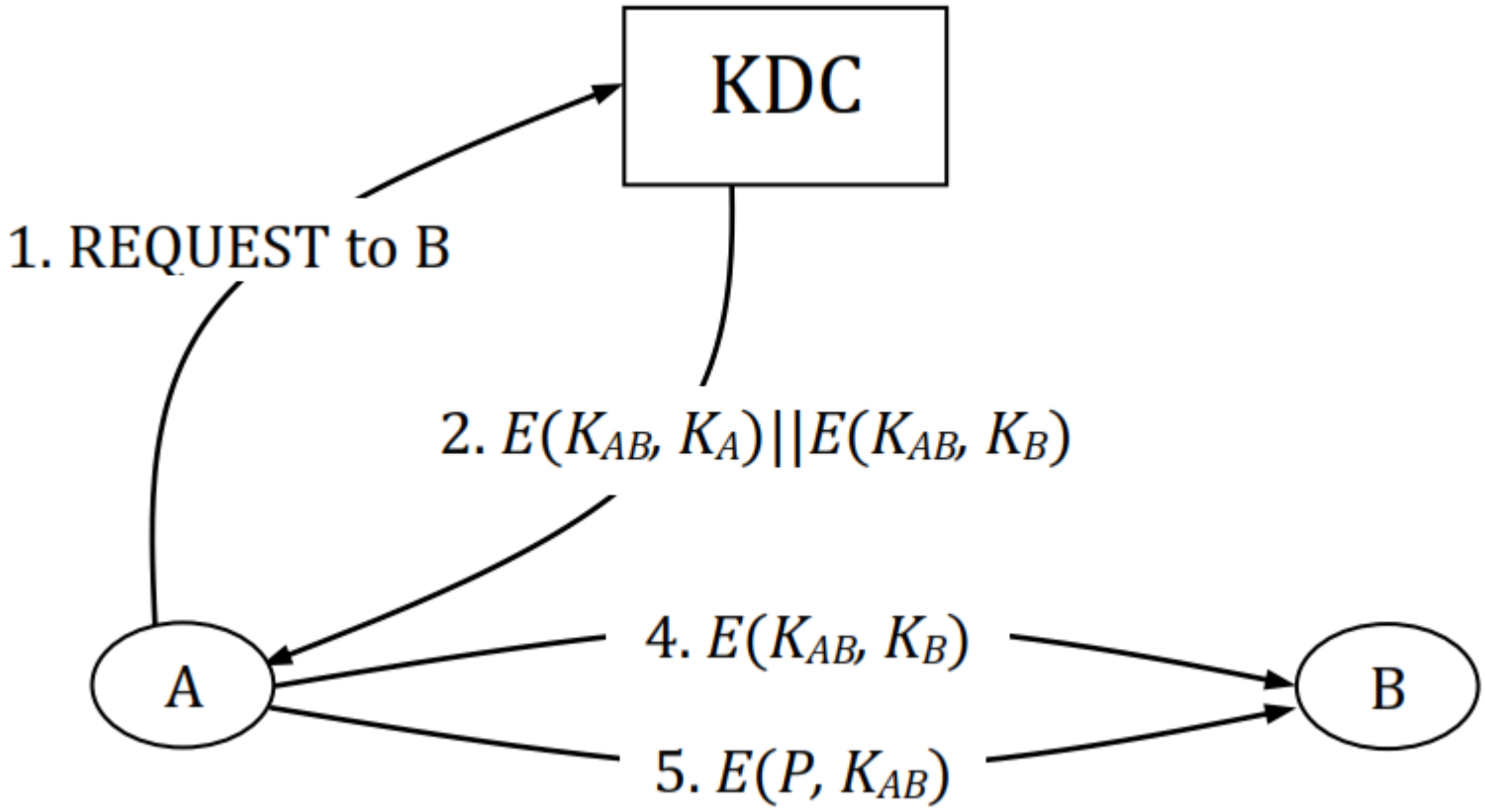


Trao đổi khóa bí mật bằng trung tâm phân phối khóa

- Giả sử Alice có khóa bí mật K_A với KDC và Bob có khóa bí mật K_B với KDC. Bây giờ Alice muốn trao đổi dữ liệu với Bob. Quá trình thiết lập khóa chung K_{AB} giữa Alice và Bob gồm các bước:

    1. Alice gửi yêu cầu muốn trao đổi dữ liệu với Bob cho KDC.
    2. KDC tạo một khóa bí mật K_{AB} và mã hóa thành hai bản mã. Một bản mã được mã hóa bằng khóa bí mật của Alice $E(K_{AB}, K_A)$ và một bản mã được mã hóa bằng khóa bí mật của Bob $E(K_{AB}, K_B)$.
    3. Alice giải mã $E(K_{AB}, K_A)$ để có K_{AB}
    4. Alice gửi $E(K_{AB}, K_B)$ cho Bob, Bob giải mã để có được K_{AB}
    5. Alice và Bob trao đổi dữ liệu qua khóa bí mật K_{AB}

Trao đổi khóa bí mật cùng KDC



Trao đổi khóa bí mật dùng KDC

- Như vậy, khóa K_{AB} chỉ có KDC. Trách nhiệm của KDC là giữ bí mật khóa này. Kết thúc quá trình truyền dữ liệu K_{AB} được hủy bỏ. Lần sau nếu Alice lại truyền số liệu với Bob thì KDC sẽ cung cấp khóa K_{AB} khác.

  → K_A, K_B được gọi là khóa chủ

  → K_{AB} được gọi là khóa phiên