Mã hóa đối xứng và bảo mật thông tin

Nội dung

- Tổng quan về mã hóa
- Mã hóa đối xứng
- Các thuật toán mã hóa

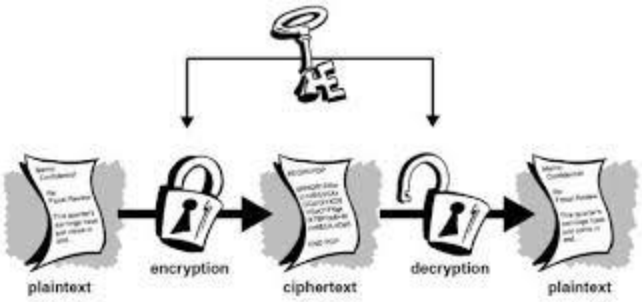
Tổng quan về mã hóa

Khái niệm:

Mã hóa là **phương thức biến đổi thông tin** từ định dạng thông thường thành một dạng khác (mã hóa) không giống như ban đầu nhưng có thể khôi phục lại được (giải mã)

Mục đích:

- Đảm bảo tính bảo mật của thông tin khi truyền trong môi trường có độ an toàn thấp.
- Trong quá trình mã hóa sử dụng giá trị đặc biệt gọi là khóa mã (key)



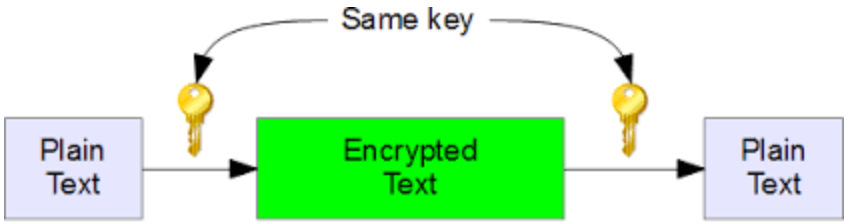
Một số thuật ngữ

- **Plaintext:** bản rõ (bản gốc)
- **Ciphertext**: bản mã (bản mật), là kết quả của bản rõ sau khi mã hóa
- **Encryption**: mã hóa, là quá trình chuyển đổi bản rõ thành bản mã
- **Decryption:** giải mã, là quá trình biến đổi bản mã thành bản rõ.
- **Cryptosystem**: hệ mã, là phương pháp ngụy trang bản rõ
- **Cryptanalysis**: phá mã, là quá trình cố gắng chuyển đổi bản mã thành bản rõ mà không có khóa.

Mã hóa đối xứng

Khái niệm:

- Hệ thống mã hóa mà bên gửi và bên nhận cùng sử dụng chung một khóa, nghĩa là quá trình mã hóa và giải mã đều dùng một khóa chung.
- Còn gọi là mã hóa khóa riêng, khóa bí mật
- Kỹ thuật mã hóa duy nhất trước 1970 và hiện rất phổ biến



Mã hóa đối xứng

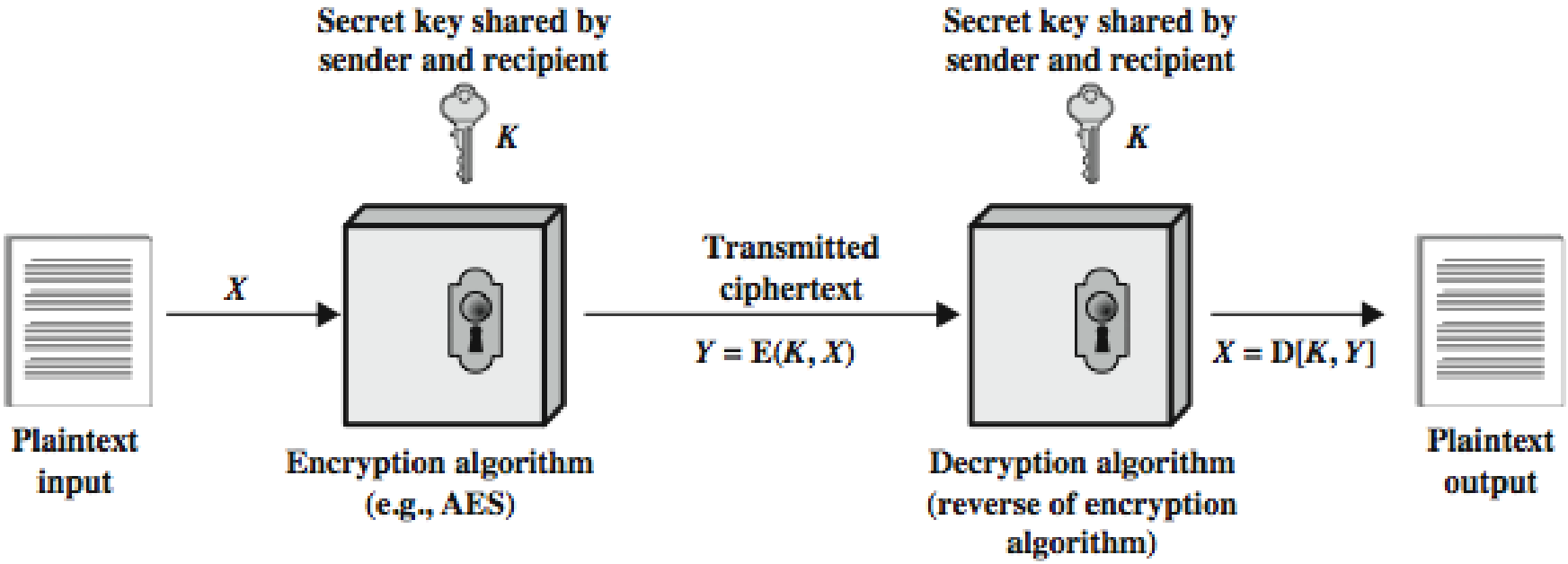
- Khi có bản rõ X và khóa mật K, nhờ thuật toán mã hóa mà bản mã Y = $[Y_1, Y_2,\ldots, Y_m]$.

$$Y=E_k(X)$$

- Người nhận tin tức, giả thiết rằng bằng một cách nào đó, cũng có khóa mật K, cần phải có khả năng biến đổi ngược:

$$X=D_k(Y)$$

Mô hình mã hóa đối xứng

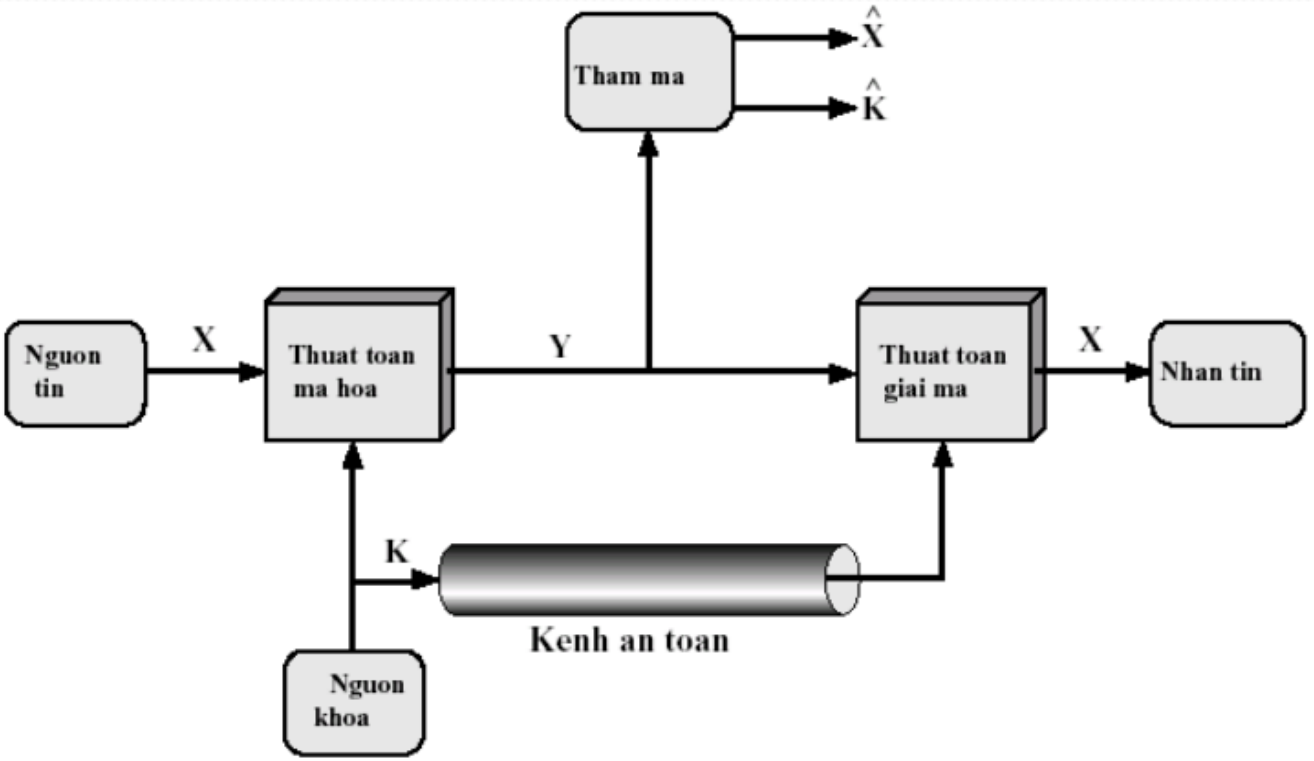


- plaintext – bản rõ
- encryption algorithm – thuật toán mã hóa
- secret key – khóa mật
- ciphertext – bản mã
- decryption algorithm – thuật toán giải mã

Độ tin cậy của mật mã truyền thống

- Thuật toán mật mã cần phải phức tạp để không có khả năng giải mã khi có văn bản mã
- Yếu tố cơ bản độ tin cậy của mật mã truyền thống là khóa bí mật, trong khi đó chính thuật toán mật mã không cần bí mật.

Mô hình của mật mã truyền thống



Phân loại mật mã khóa đối xứng

- **Mã khối:**

thực hiện biến đổi khối dữ liệu với một kích thước không đổi.

- **Mã dòng**

Thực hiện biến đổi tuần tự từng bit hoặc byte riêng lẻ

Thám mã

- Quá trình khôi phục giá trị X hoặc K, hoặc cả hai được gọi là thám mã
- Chiến thuật thám mã được sử dụng phụ thuộc vào sơ đồ mã hóa và vào những thông tin có được trong khi tiến hành

Các dạng thám mã

Dạng thám mã	Các số liệu cần biết
Khi chỉ có bản mã (ciphertext only)	• Thuật toán mã hóa • Bản mã
Khi biết bản rõ	• Thuật toán mã hóa • Bản mã • Có một hoặc một vài cặp tương ứng của bản mã và bản rõ được tao ra từ cùng một khóa bí mật
Phân tích với bản mã chọn lựa	• Thuật toán mã hóa • Bản mã • Văn bản mã chọn lựa phù hợp với bản rõ, được mã hóa cùng một khóa bí mật, được thực hiện bởi người thám mã
Phân tích với bản rõ chọn lựa	• Thuật toán mã hóa • Bản mã • Văn bản rõ chọn lựa phù hợp với bản mã, được mã hóa cùng một khóa bí mật, được thực hiện bởi người thám mã
Phân tích với văn bản chọn lựa	• Thuật toán mã hóa • Bản mã • Văn bản rõ chọn lựa phù hợp với bản mã, được mã hóa cùng một khóa bí mật, được thực hiện bởi người thám mã • Văn bản mã chọn lựa phù hợp với bản rõ, được mã hóa cùng một khóa bí mật, được thực hiện bởi người thám mã

Nhận xét

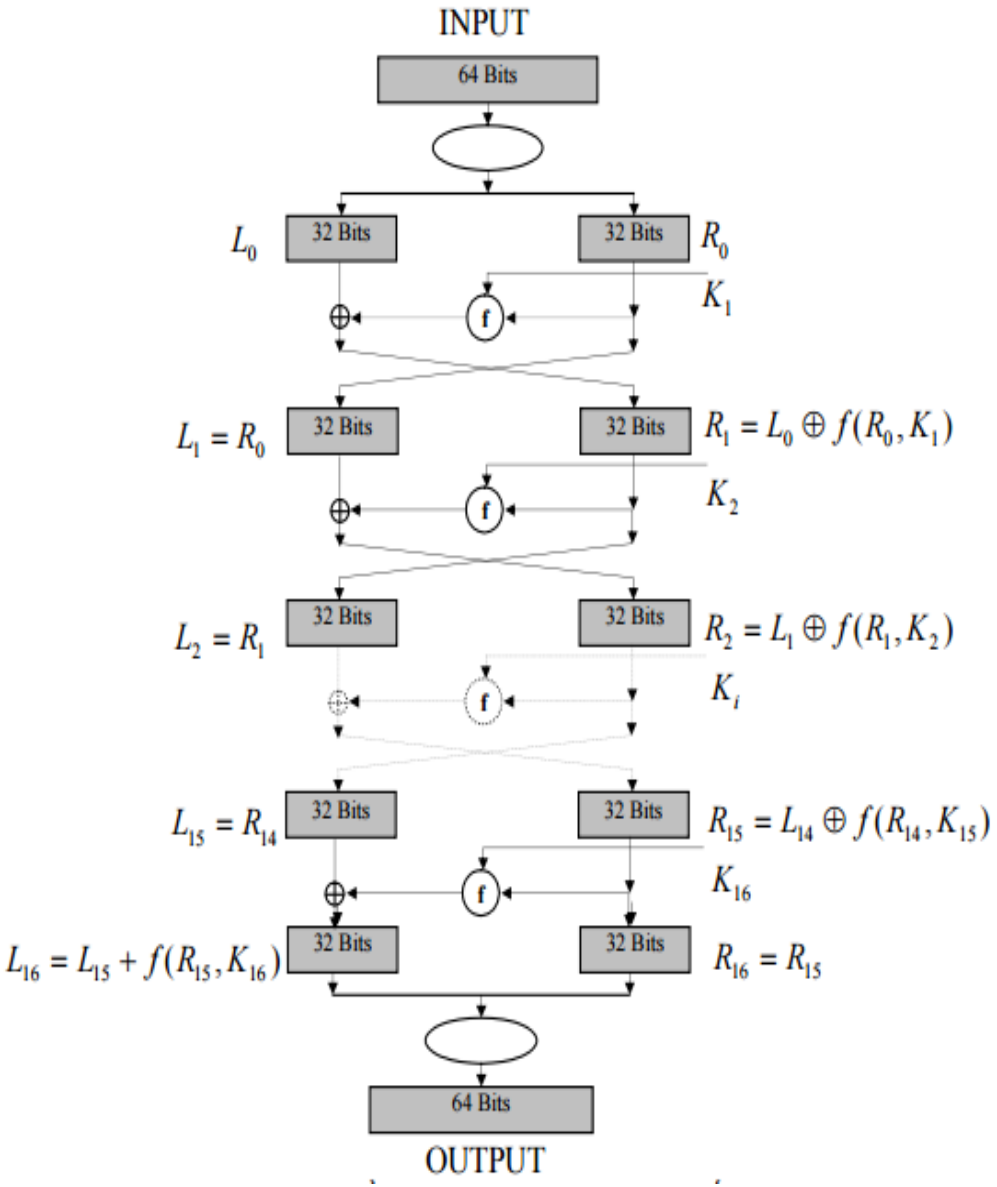
- Bài toán phức tạp nhất từ các bài toán được trình bày trong bảng này là trường hợp khi tiến hành thám mã mà chỉ có văn bản mã
- Một xu thế thám mã là thử chọn tất cả các khả năng của khóa
- Tuy nhiên, nếu không gian khóa rất lớn thì không khả thi.

Mã hóa đối xứng

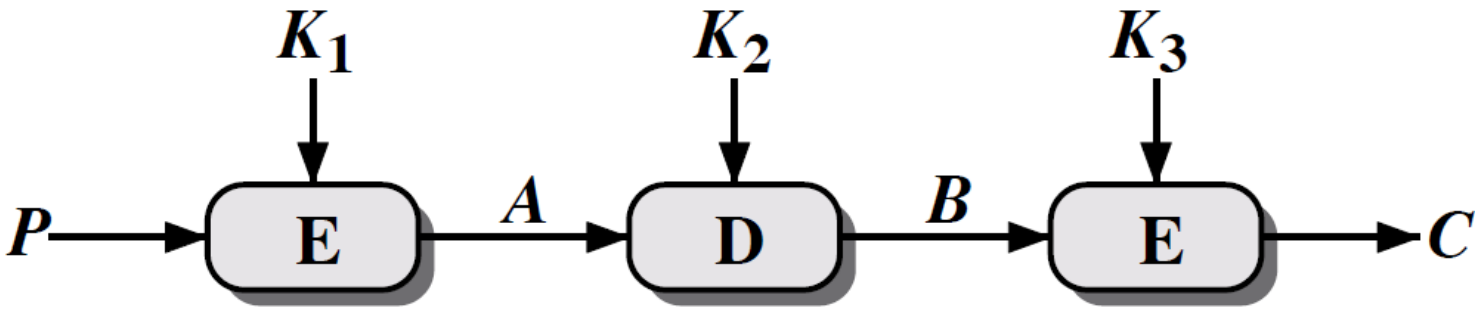
- Các phép toán sử dụng trong mật mã khóa bí mật:
  - Phép hoán vị
  - Phép thay thế
  - Các phép toán số học: dịch vòng, XOR,..
- Các kỹ thuật mã hóa đối xứng thông dụng: DES, 3DES, AES

Mã hóa DES

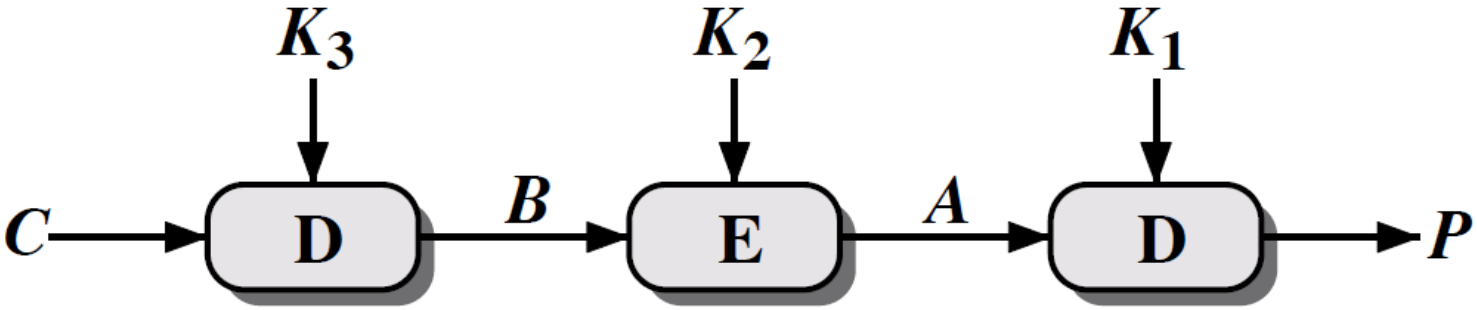
- Xây dựng theo nguyên tắc các vòng lặp
- Mỗi vòng lặp thực hiện một phép toán f
- Đầu ra của vòng lặp trước là đầu vào của vòng lặp sau
- Giải thuật DES sử dụng 16 vòng lặp
  - Độ dài khối: 64 bit
  - Độ dài khóa: 56 bit
  - Đầu ra: 64 bit



Mã hóa 3DES



(a) Encryption



(b) Decryption

Three-key: key length = 56*3 = 168 bits

Thuật toán AES

- DES và các thuật toán cải tiến (DES-X, G-DES, T_DES,…) không đáp ứng được nhu cầu hiện tại và tương lai
- NIST mở cuộc thi nhằm tìm kiếm thuật toán mới thay thế cho DES (AES – Advanced Encryption Standard)
  - Có tốc độ nhanh hơn DES
  - Độ an toàn không kém hơn T_DES
  - Có khả năng tối ưu trên cả phần cứng và phần mềm
  - Khối dữ liệu có độ dài 128 bit, có khả năng làm việc với các khóa có độ dài khác nhau – 128, 192, 256 bit

Mã hóa AES

- AES – Advanced Encryption Standard
- Là bộ mã khối gồm nhiều vòng
- AES còn gọi là Rijndael (tên của 2 nhà thiết kế Daemen và Rijmen)
- Cho phép lựa chọn kích thước khối mã hóa là 128, 192, 256 bit.
- Số lượng vòng có thể thay đổi từ 10, 12, đến 14 vòng (phụ thuộc vào độ dài khối dữ liệu và khóa 128, 192, hoặc 256 bit)

Một số vấn đề lưu ý

- Hệ mật mã khóa đối xứng: **vai trò bên gửi** và nhận tin đều **như nhau** vì đều sở hữu chung một khóa bí mật.
- Một số cách gọi khác:
  - Hệ mã khóa riêng (Private Key Cryptosystem)
  - Hệ mã khóa bí mật (Secret key Cryptosystem)
  - Hệ mã truyền thống (Conventional Cryptosystem)

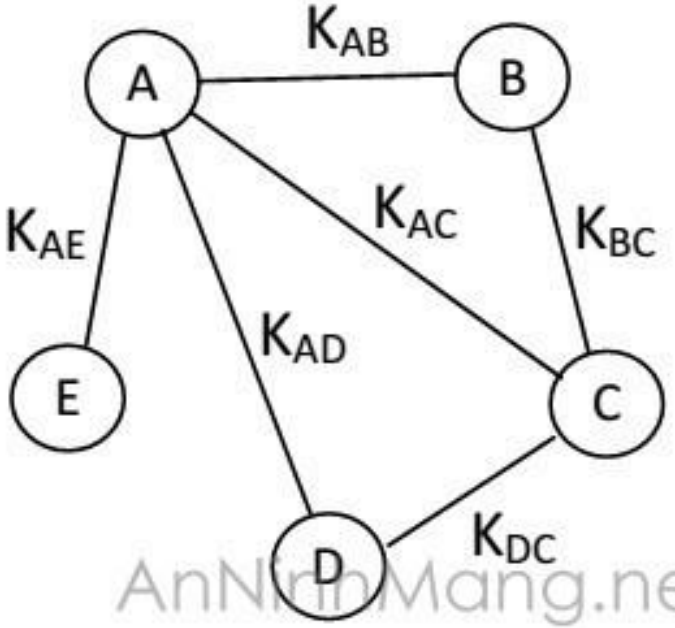
Các tính chất bảo mật của mã hóa đối xứng

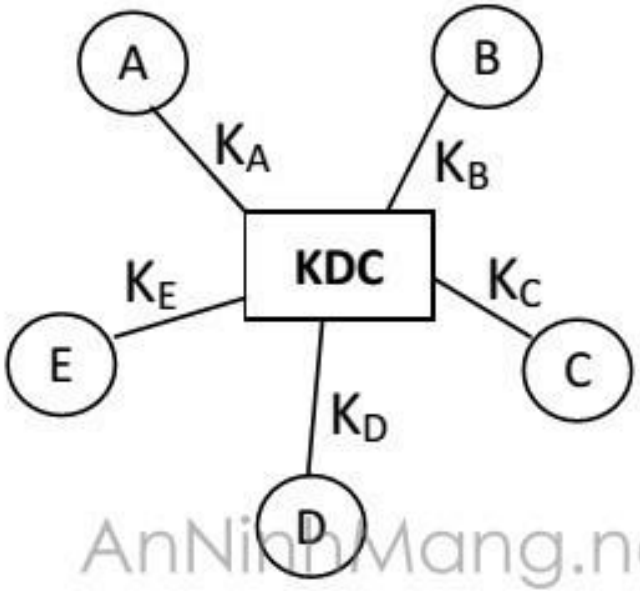
- Tính bí mật (Confidentiality): bản mã được gửi trên kênh truyền, người thứ 3 can thiệp trên kênh truyền chỉ lấy được bản mã (không có ý nghĩa).
- Tính toàn vẹn dữ liệu (integrity): sửa dữ liệu trên kênh truyền → khả năng văn bản sẽ không có ý nghĩa
- Tính xác thực (authentication): có thể chống lại các hình thức tấn công: sửa đổi thông điệp, mạo danh và phát lại thông điệp
- Tính non-repudiation: không có cơ sở quy trách nhiệm

Một số nhược điểm

- **Vấn đề quản lý khóa**: vấn đề trao đổi khóa giữa người gửi và người nhận rất phức tạp trong môi trường nhiều người sử dụng. Với n NSD thì phải tạo n(n-1)/2 khóa. Mỗi người dùng phải lưu (n-1) khóa bí mật để làm việc với n-1 người khác
- **Tính bí mật của khóa**: không có cơ sở quy trách nhiệm nếu khóa bị tiết lộ.

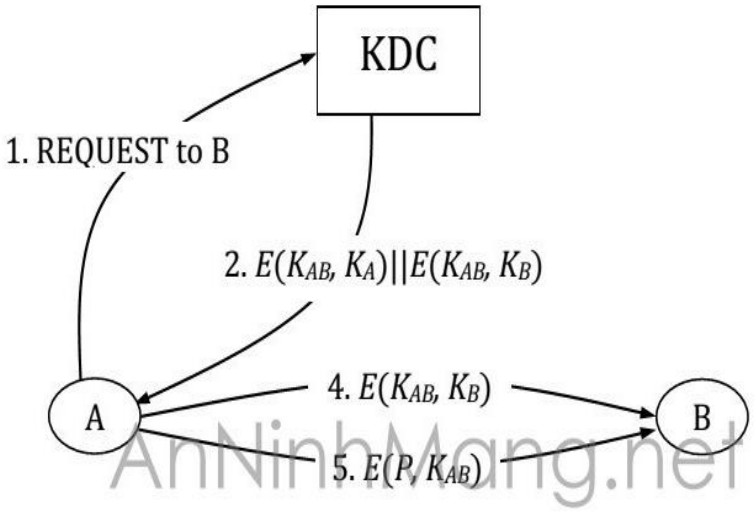
Trao đổi khóa bí mật – trung tâm phân phối khóa (Key distribution Center – KDC)





Trao đổi khóa bí mật – trung tâm phân phối khóa (Key distribution Center – KDC)

- Alice muốn trao đổi với Bob (request to KDC)
- KDC tạo khóa bí mật K_{AB}, mã hóa 2 bản mã $E(K_{AB},K_A)$, $E(K_{AB}, K_B)$
- Alice giải mã $E(K_{AB}, K_A)$ để có K_{AB}
- Bob giải mã $E(K_{AB}, K_B)$ để có K_{AB}
- Alice và Bob trao đổi qua khóa bí mật K_{AB}



Như vậy: chỉ có Alice, Bob và KDC biết K_{AB}. K_{AB} hủy sau khi kết thúc trao đổi dữ liệu