HỌC VIỆN KỸ THUẬT MẬT MÃ
KHOA AN TOÀN THÔNG TIN
****

GIAO THỨC AN TOÀN MẠNG

Bài 1. Mở đầu

Giảng viên: ThS Nguyễn Ngọc Toàn
SĐT: 096.159.7667
Email: ngoctoan.hvan@gmail.com

1. Giới thiệu học phần
2. Cơ sở mật mã cho an toàn mạng
3. Tổng quan về giao thức an toàn mạng

Mục tiêu bài học

❑Kiến thức

- Hình dung tổng thể về học phần, bao gồm việc hiểu rõ nhiệm vụ làm bài tập lớn
- Củng cố kiến thức về cơ sở lý thuyết mật mã
- Tổng quan về các giao thức an toàn mạng

Tài liệu tham khảo

1. Chương 1 - Giáo trình "Giao thức an toàn mạng", Học viện KTMM, 2013
2. Giáo trình Cơ sở lý thuyết mật mã, Học viện KTMM, 2013

1. Giới thiệu học phần
2. Cơ sở mật mã cho an toàn mạng
3. Tổng quan về giao thức an toàn mạng

Nội dung học phần

1. Một số kiến thức nền tảng
2. Giao thức xác thực
3. Giao thức đảm bảo an toàn cho dữ liệu tầng ứng dụng
4. Giao thức mạng riêng ảo
5. Giao thức an toàn mạng không dây

So sánh với "An toàn mạng máy tính"

❑Giống

- Xem xét cơ chế chống lại các hiểm họa an toàn mạng máy tính

❑Khác

- Tập trung vào phần giao thức (phần mật mã), ít chú trọng vấn đề công nghệ

➔ *Mục đích cuối cùng là cần phải hiểu được các giao thức*

Cấu trúc học phần

- **Thời lượng**: 2tc = 36 tiết
  - 24 tiết lý thuyết
  - 12 tiết bài tập
- **Đánh giá kết quả học tập**
  - Điểm chuyên cần
    - Đi học đầy đủ, đúng giờ
    - Tham gia xây dựng bài
  - Điểm bài tập
  - Điểm thi kết thúc học phần

Giáo trình

1. Nguyễn Quốc Toàn, Hoàng Sỹ Tương, Giáo trình "**Giao thức an toàn mạng máy tính**", Học viện KTMM, 2013.
2. Nguyễn Bình, Hoàng Thu Phương, "**Cơ sở lý thuyết mật mã**", Học viện KTMM, 2013
3. Nguyễn Ngọc Cương, Trần Thị Lượng, "**Mật mã ứng dụng trong an toàn thông tin**", Học viện KTMM, 2013
4. (và các tài liệu khác)

Bài tập lớn

Hình thức làm bài tập lớn

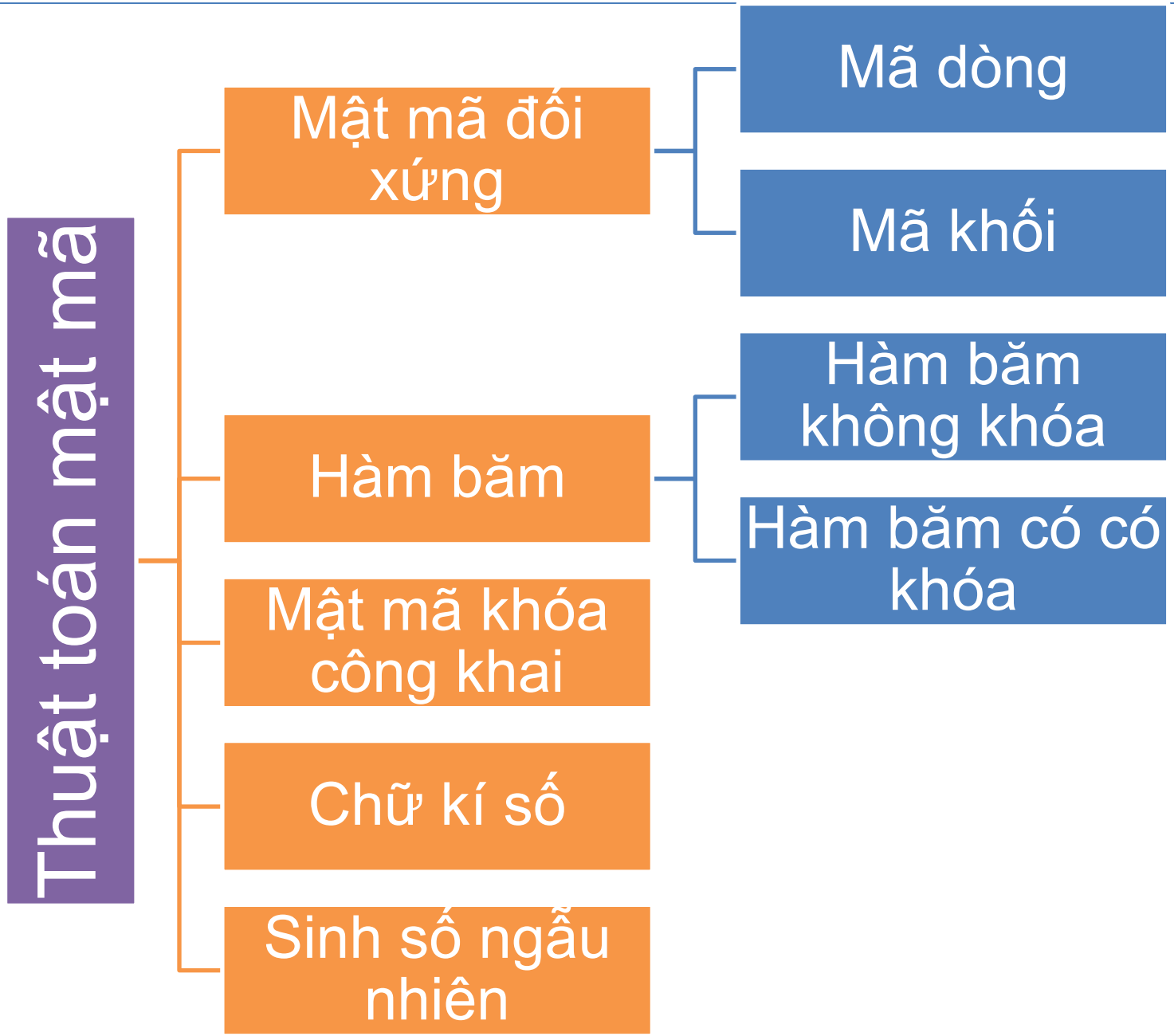
Danh sách chủ đề bài tập lớn

Hình thức báo cáo kết quả bài tập lớn

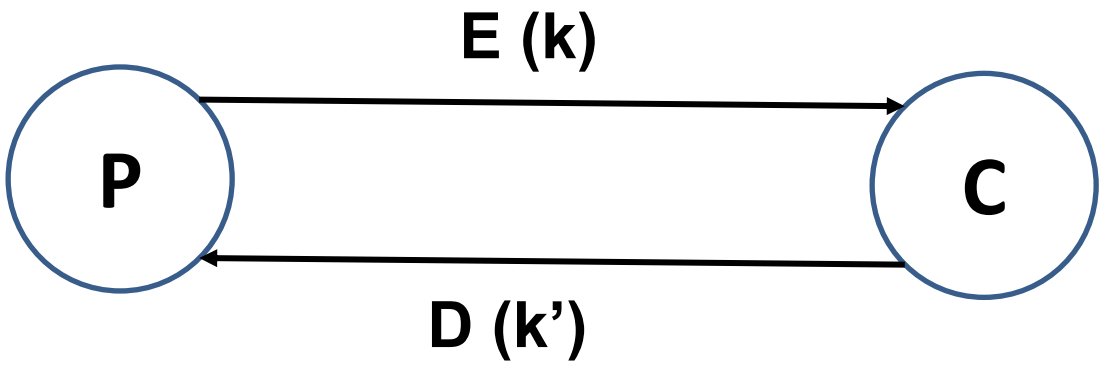
Thời hạn nộp kết quả

1. Giới thiệu học phần
2. Cơ sở mật mã cho an toàn mạng
3. Tổng quan về giao thức an toàn mạng

Thuật toán mật mã

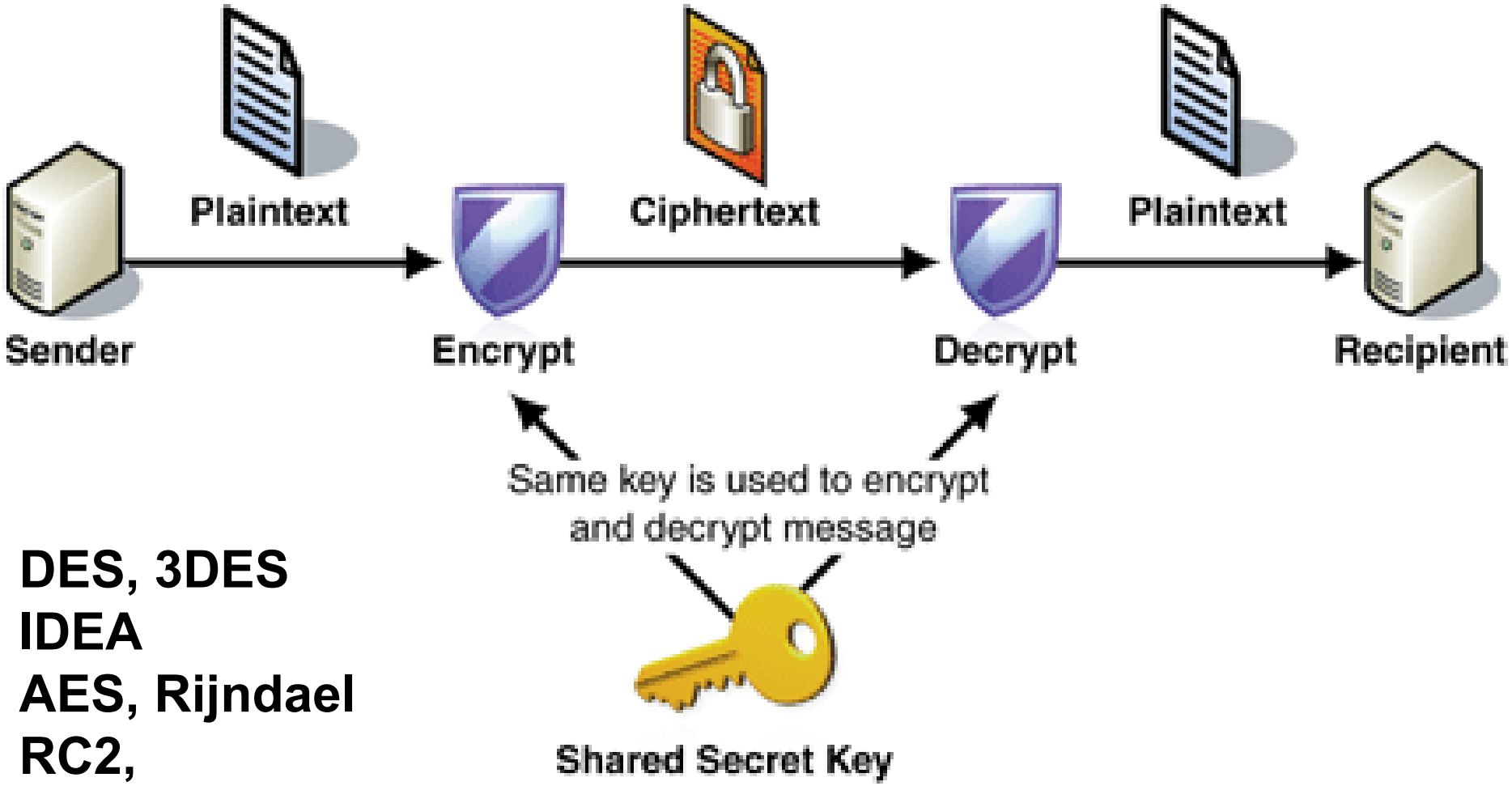


Mật mã



- **P (Paintext):** Bản rõ
- **C (Cipher):** Bản mã
- **K (Key):** Không gian khoá
- **E (Encrypt):** Mã hoá
- **D (Decrypt):** Giải mã

Mật mã đối xứng



DES, 3DES
IDEA
AES, Rijndael
RC2,
RC4
SEAL

Mật mã đối xứng

❑Khóa mật mã

- Là chuỗi bít ngẫu nhiên độ dài xác định
- Được chia sẻ bởi các bên liên quan
- Các bên đều có nghĩa vụ đảm bảo bí mật

❑Hiệu năng

- Tương đối cao so với mật mã khóa công khai
- Thích hợp để mã dữ liệu

❑Phân loại

- Mã khối (block cipher)
- Mã dòng (stream cipher)

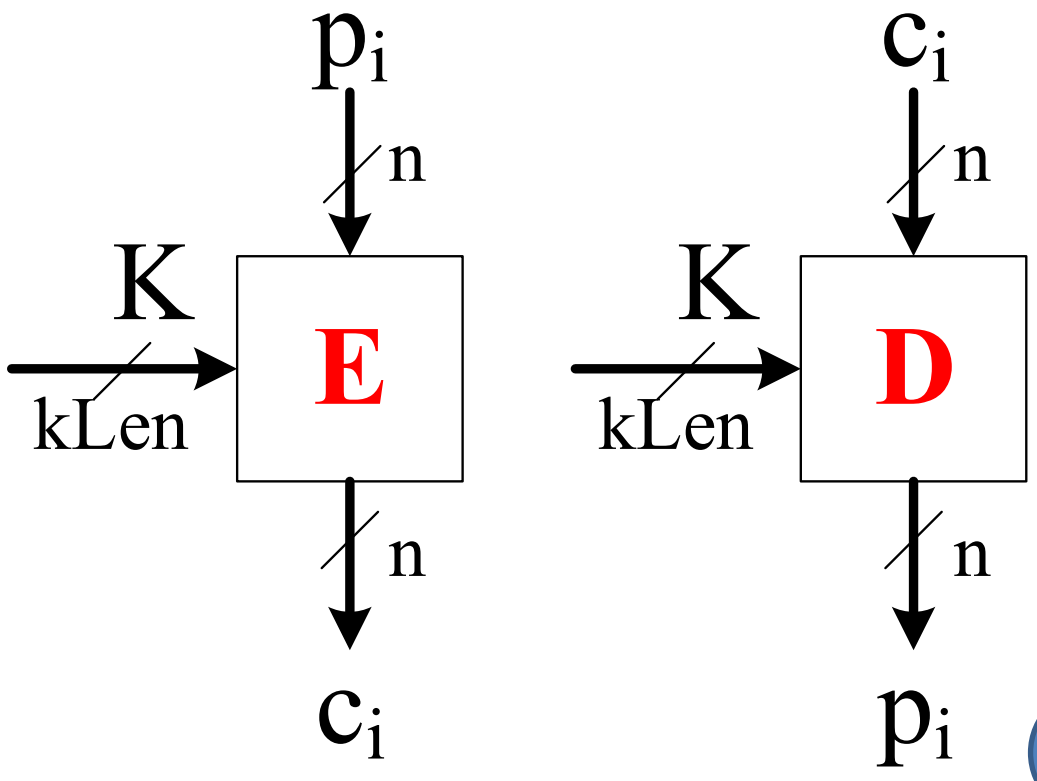
Mã khối

$BlockCipher = \{E, D, \mathbb{K}, \mathbb{P}, \mathbb{C}\}$

Việc mã hóa (bởi hàm E), giải mã (bởi hàm D) được thực hiện theo từng khối

$c_i = \mathbf{E}_K(p_i)$

$p_i = \mathbf{D}_K(c_i)$



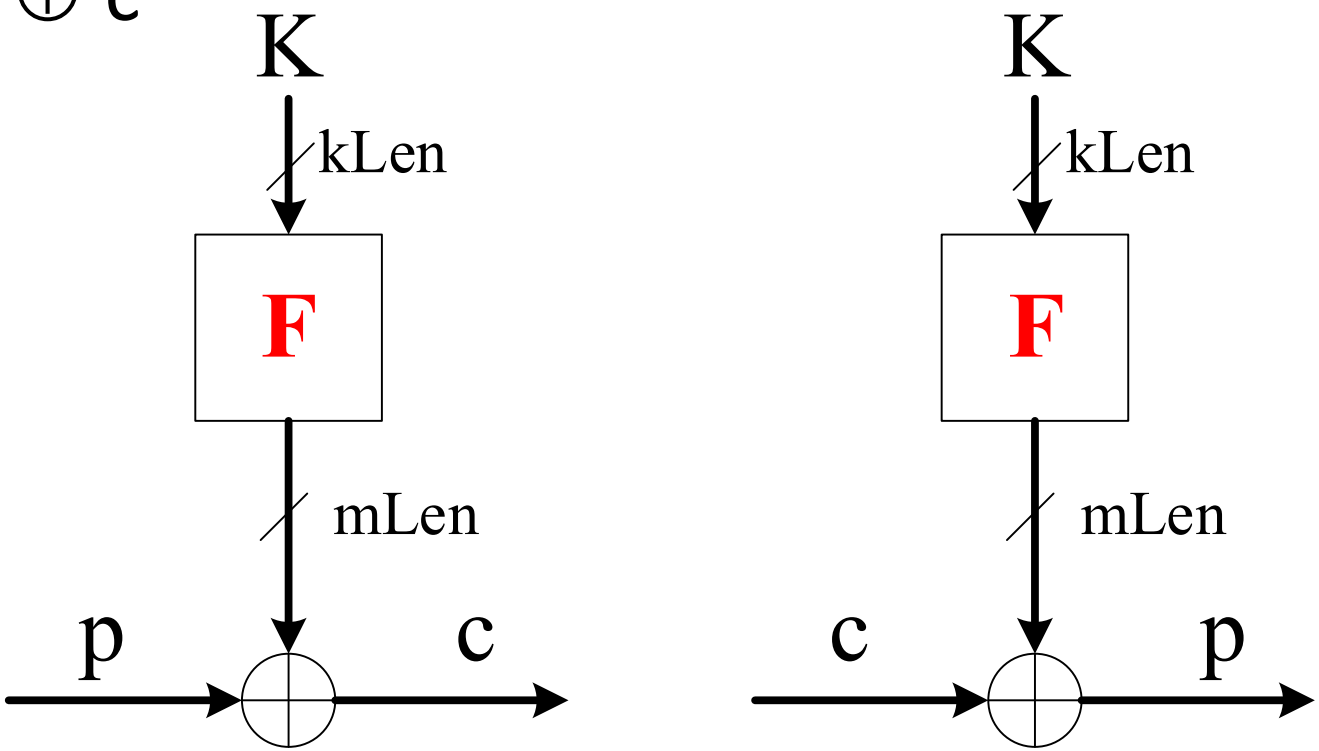
Mã dòng

$StreamCipher = \{F, \mathbb{K}, \mathbb{P}, \mathbb{C}\}$

Việc mã hóa, giải mã là tương tự nhau và được thực hiện theo từng ký tự

c = **F**(K) ⊕ p

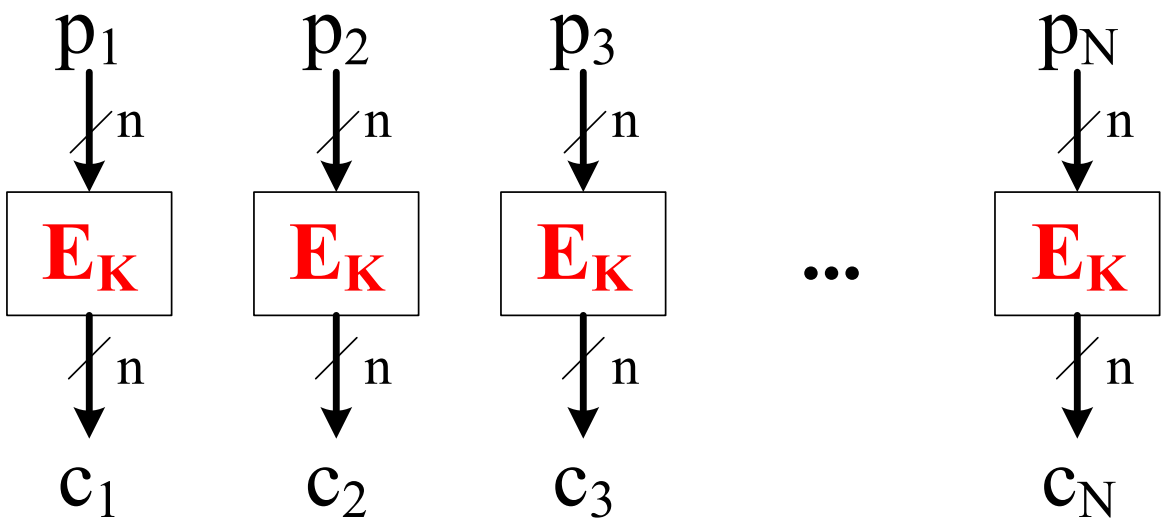
p = **F**(K) ⊕ c



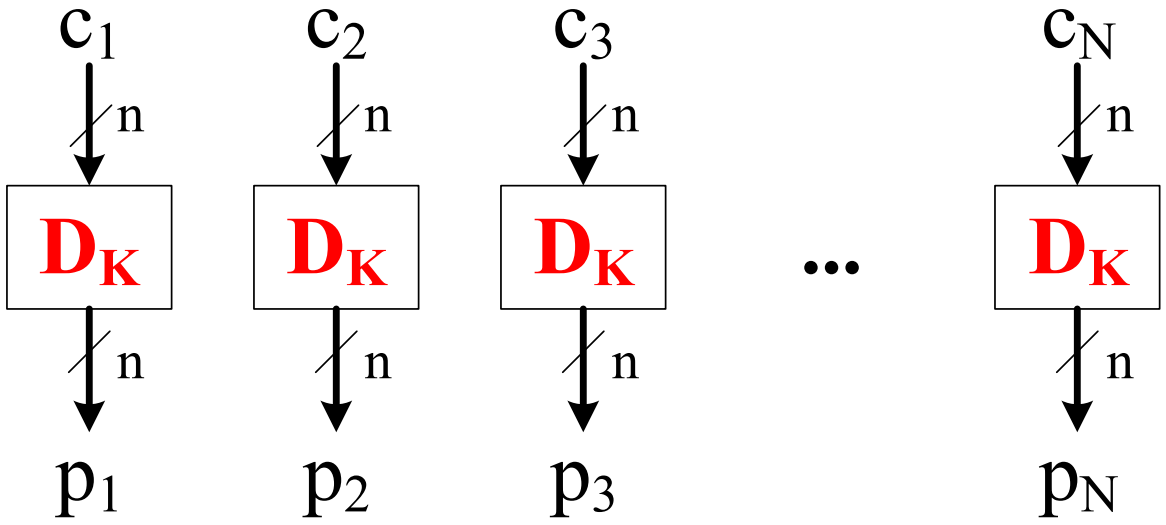
Chế độ hoạt động của mã khối

- Mã khối có nhiều chế độ làm việc khác nhau: ECB, CBC, OFB, CFB, CTR, GCM...
- Một số chế độ là thuần túy mã khối: ECB, CBC, CTS
- Một số chế độ là tương tự như mã dòng: OFB, CFB, CTR...
- Một số chế độ cho phép kết hợp mã hóa và xác thực (dữ liệu)

ECB: Electronic Codebook

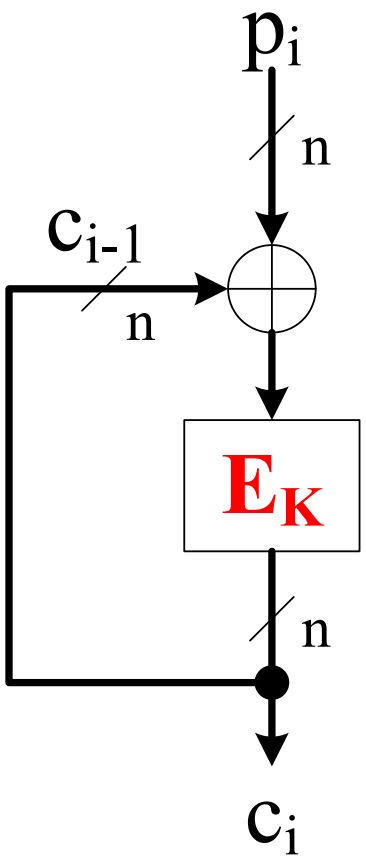


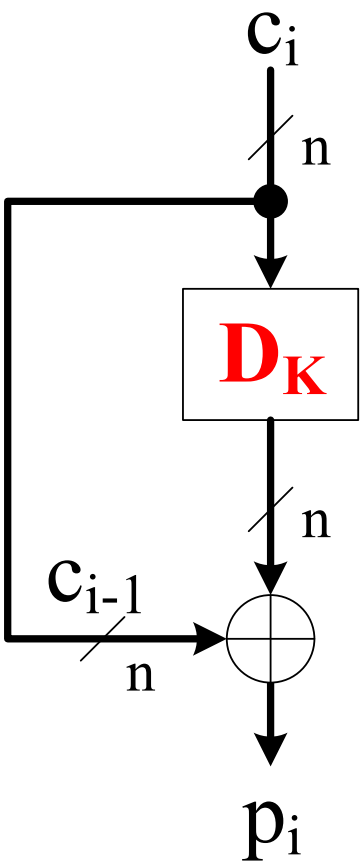
$c_i = E_K(p_i)$



$p_i = D_K(c_i)$

CBC: Cipher Block Chaning





$c_i = \mathbf{E}_K(p_i \oplus c_{i-1})$

$c_0 = IV$

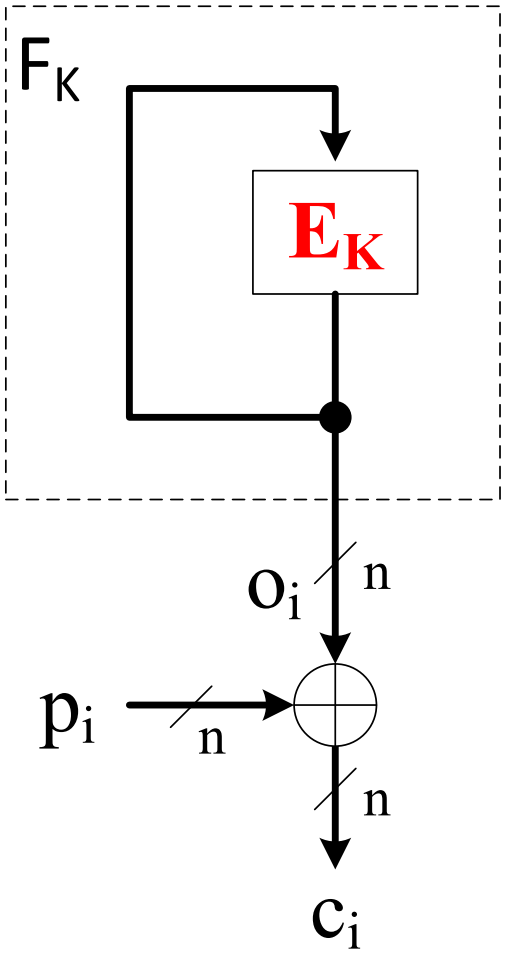
$i = 1..N$

$p_i = \mathbf{D}_K(c_i) \oplus c_{i-1}$

$c_0 = IV$

$i = 1..N$

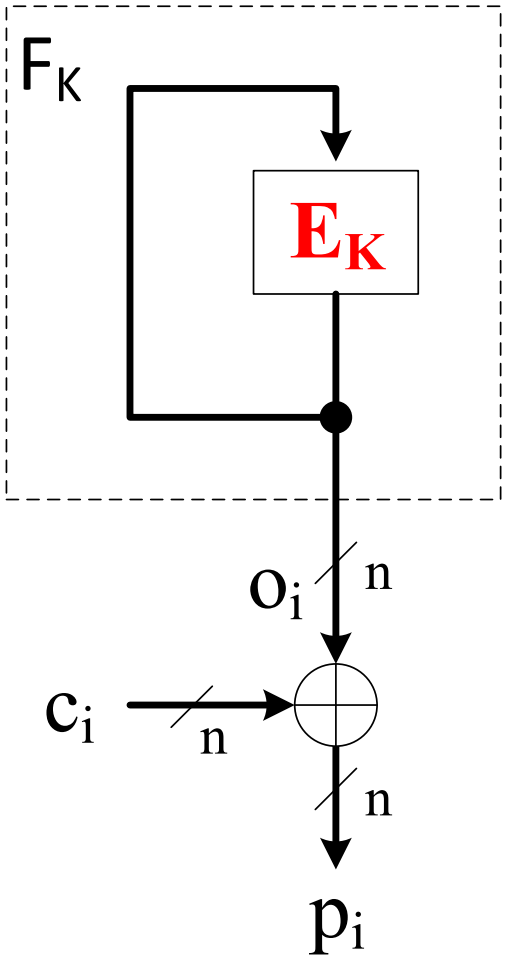
OFB: Output Feedback



$o_i = \mathbf{E}_K(o_{i-1})$, i=1..N

$o_0 = IV$

$c_i = p_i \oplus o_i$

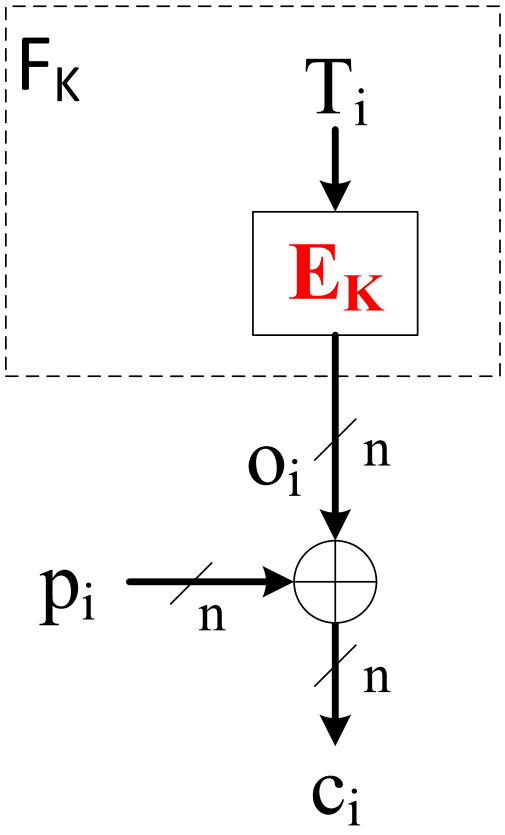


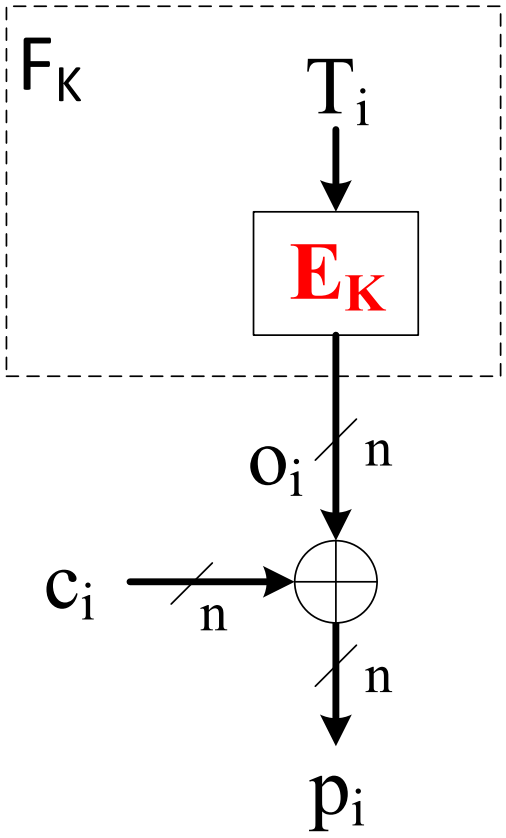
$o_i = \mathbf{E}_K(o_{i-1})$, i=1..N

$o_0 = IV$

$p_i = c_i \oplus o_i$

CTR: Counter





$o_i = \mathbf{E}_K(T_i)$, i=1..N

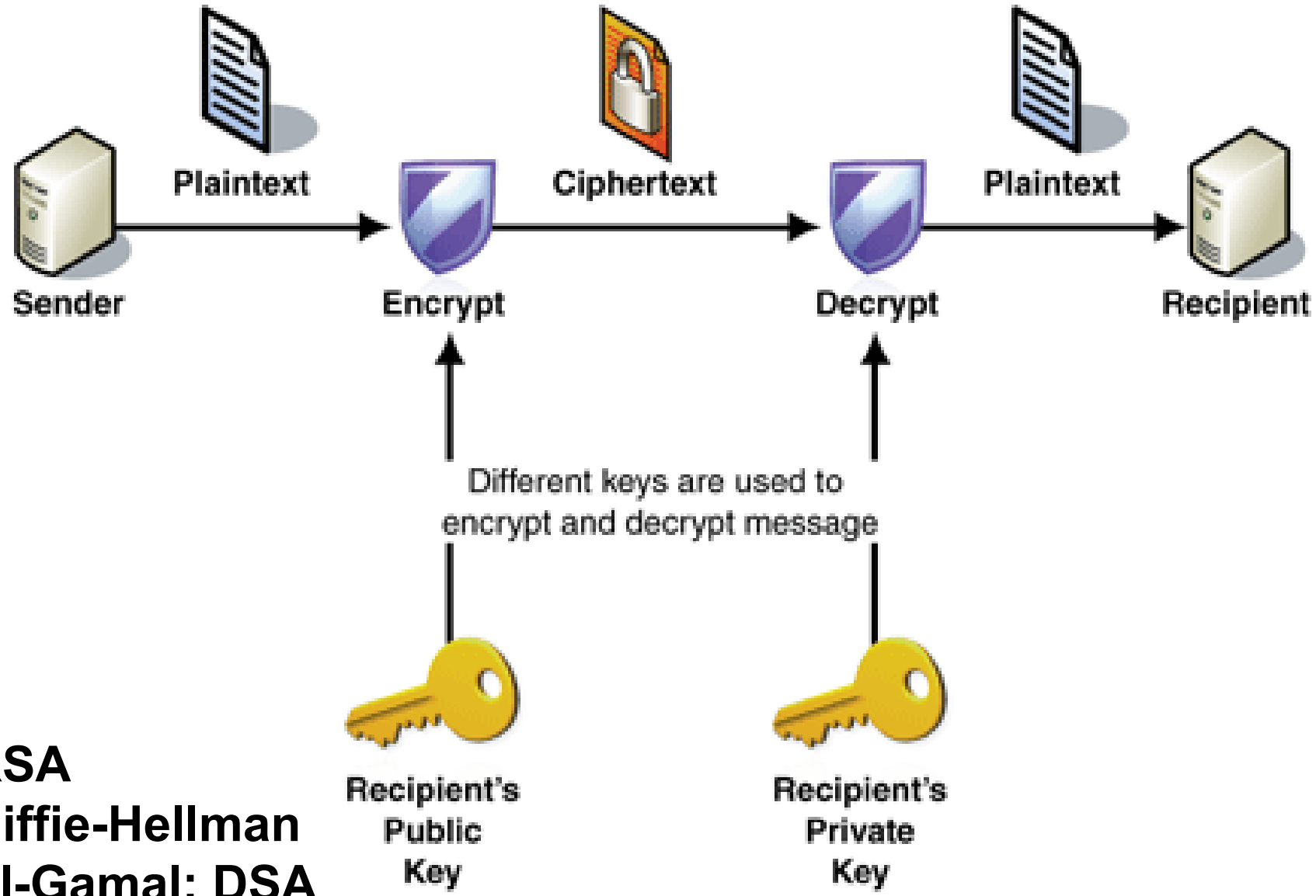
$c_i = p_i \oplus o_i$

$o_i = \mathbf{E}_K(T_i)$, i=1..N

$p_i = c_i \oplus o_i$

Bộ đếm T phải được thiết kế để mọi Ti là khác nhau (chỉ được phép lặp lại khi thay khóa K mới)

Mật mã khóa công khai



RSA
Diffie-Hellman
El-Gamal; DSA
ECDH, ECDSA

Mật mã khóa công khai

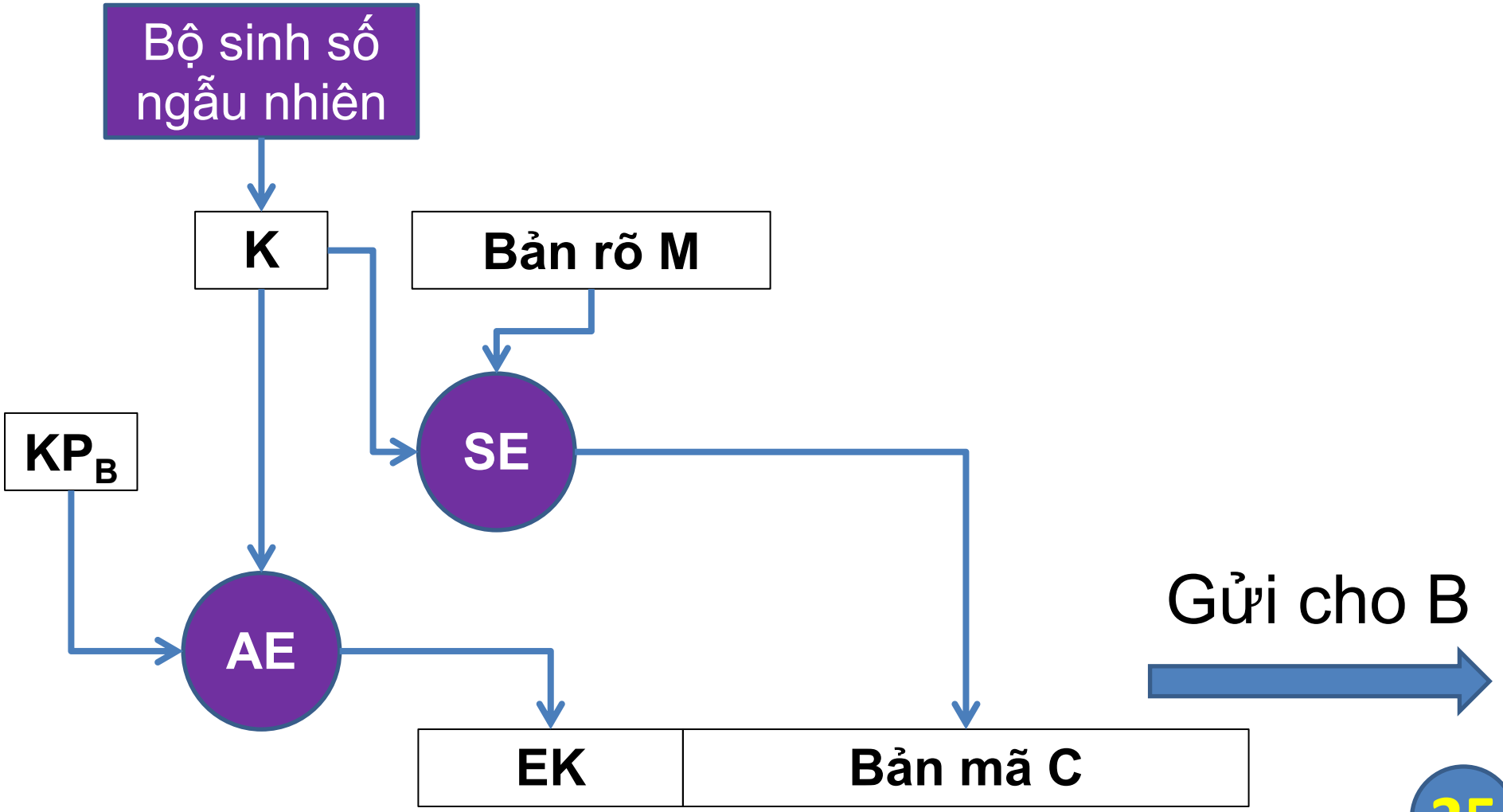
❑Khóa mật mã

- Tồn tại theo cặp
- Là một bộ tham số, có ý nghĩa toán học
- Khóa bí mật phải ngẫu nhiên
- Kích thước khóa luôn phải rất lớn

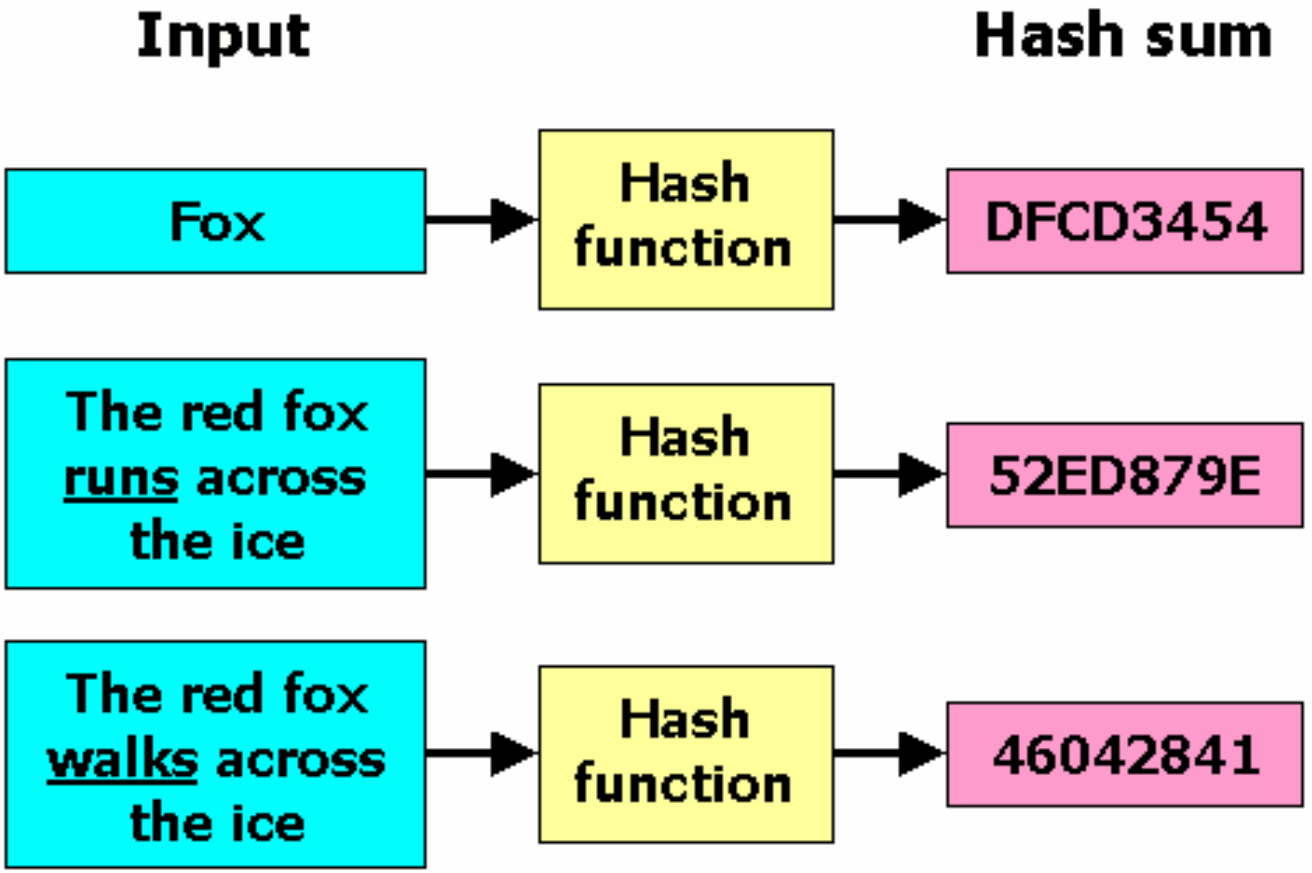
❑Hiệu năng

- Rất thấp so với mật mã đối xứng
- Thích hợp để trao đổi khóa, ký số

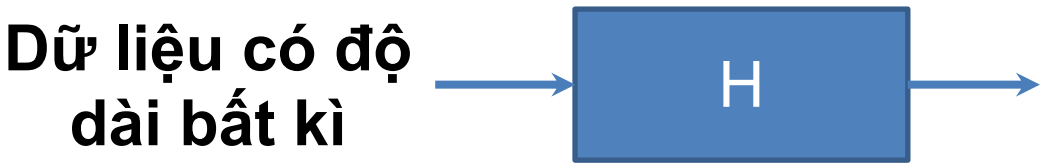
Sử dụng kết hợp mật mã đối xứng và mật mã khóa công khai



Hàm băm



MD4
MD5
SHA1
SHA224
SHA256
SHA512



Hàm băm

- Nén → quan hệ giữa thông điệp và bản tóm lược không phải là tương ứng 1:1
- Kháng tiền ảnh: từ H(x) không thể tìm được x
- Kháng tiền ảnh thứ hai: cho trước x, không thể tìm được x' sao cho H(x) = H(x')
- Kháng va chạm: không thể tìm được cặp (x, y) sao cho H(x) = H(y)

Trong ứng dụng thực tế, có thể coi quan hệ x : H(x) là một tương ứng 1:1. Có thể dùng H(x) để đại diện cho x

Hàm băm

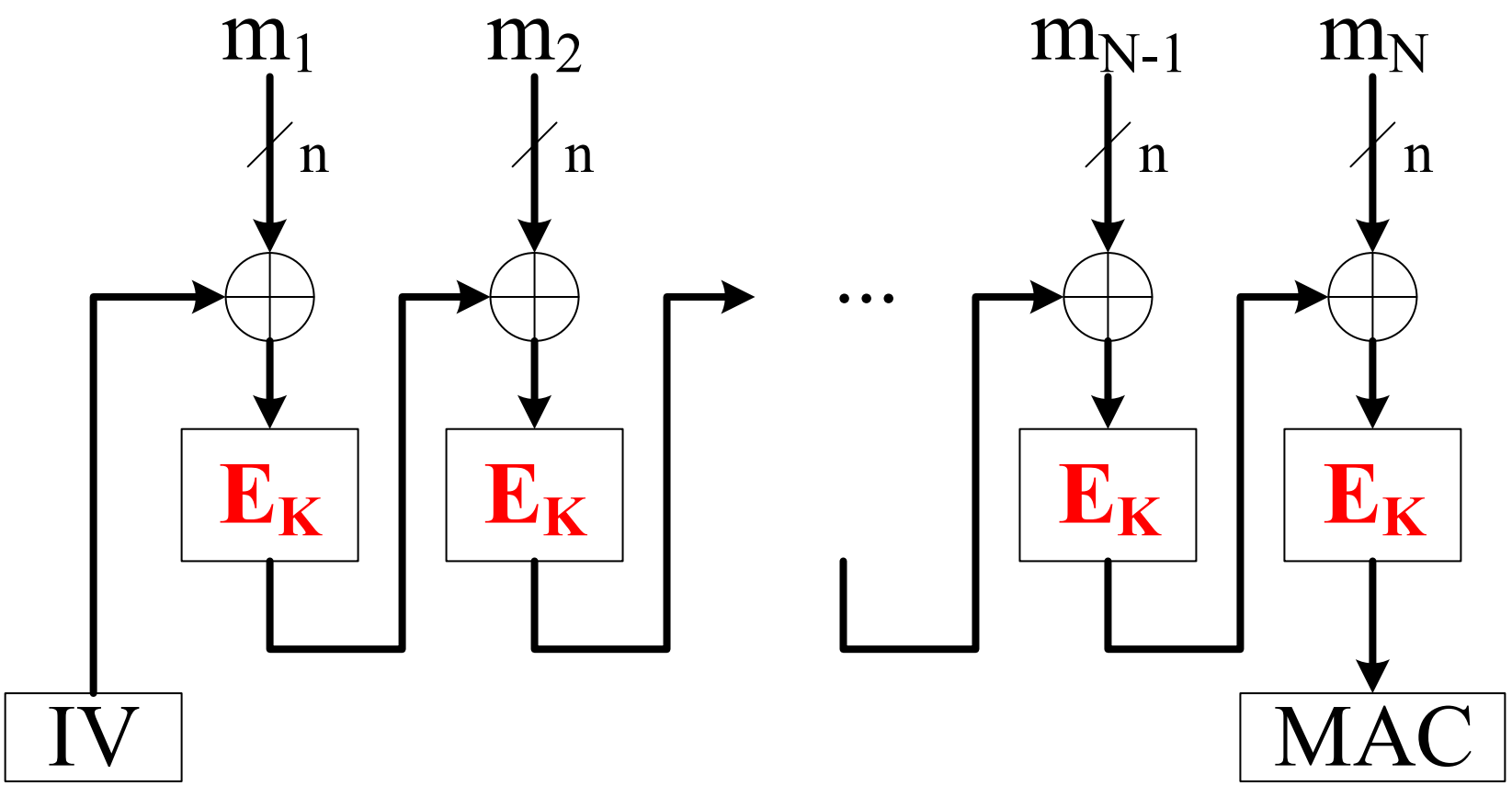
- **Ứng dụng của hàm băm trong giao thức an toàn mạng**
  - Tạo mã xác thực (lược đồ HMAC)
  - Xác thực thực thể (cơ chế thách đố - giải đố)
  - Dẫn xuất khóa

Mã xác thực thông điệp

- MAC = Message Authentication Code (không phải Medium Access Control!!!!)
- Được tạo bởi người gửi S
- Để người nhận R có thể kiểm tra được rằng thông điệp M được tạo ra bởi S.
- MAC phải chứa đựng yếu tố bí mật
  ➔ MAC(m, K)
- Kỹ thuật: HMAC, CBC-MAC

CBC-MAC

- Tạo MAC dựa trên chế độ CBC của mã khối bất kỳ



HMAC

- HMAC = Hash-based MAC
- Cách gọi khác: Keyed hash MAC
- Cách tính kém an toàn

  MAC = H(key || message)
- Cách tính an toàn

  MAC = H(key || H(key || message))
- Có thể sử dụng bất kỳ hàm băm nào

Kết hợp mã hóa và xác thực

- **Trường hợp riêng**: Cần đảm bảo đồng thời tính bí mật và tính xác thực cho M
- **Trường hợp tổng quát**: Thông điệp gồm 2 phần M=(M1, M2), trong đó cả hai phần đều cần được xác thực, còn tính bí mật chỉ cần áp dụng cho M1

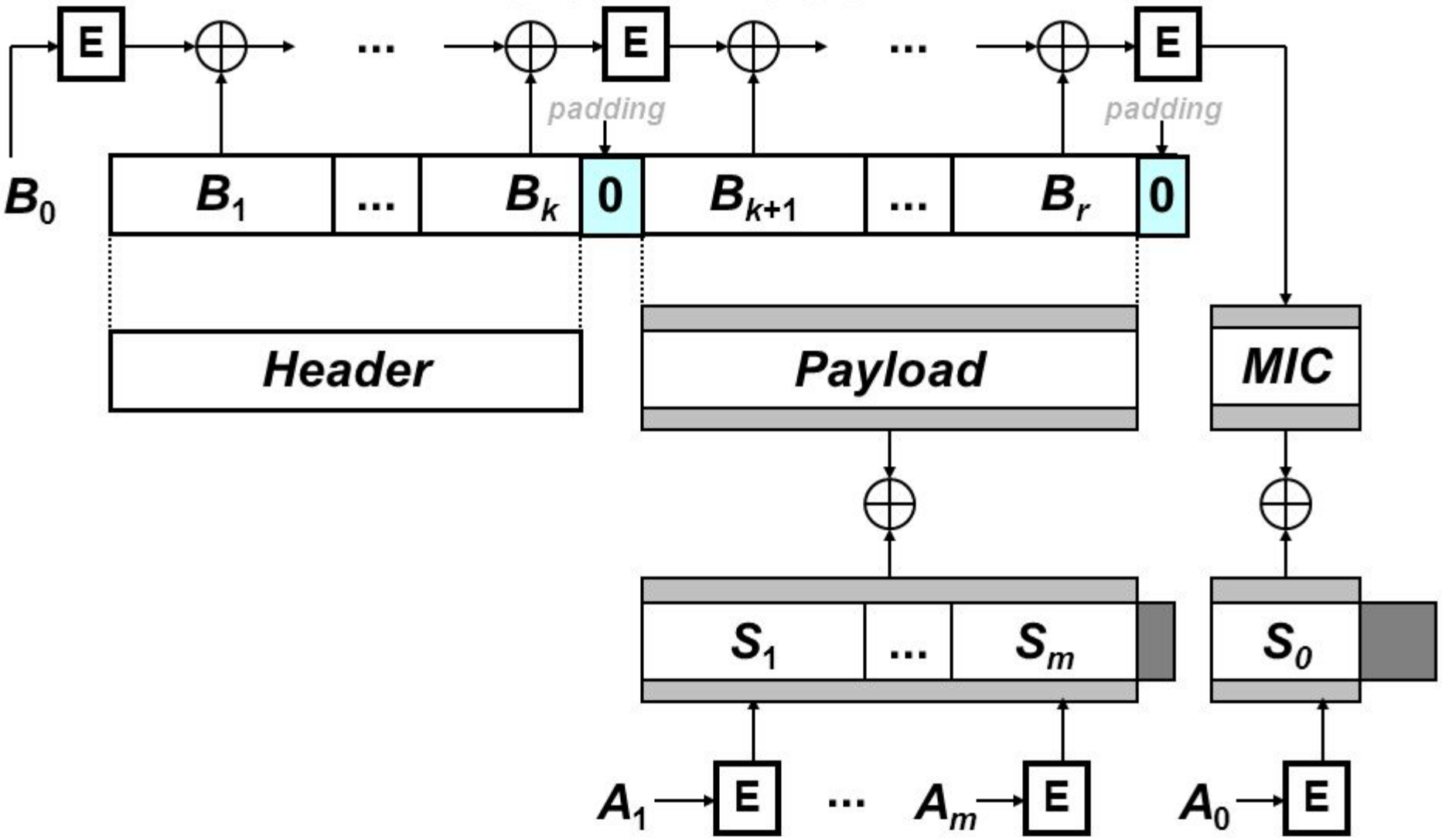
➔AEAD = Authenticated Encryption with Associated Data

Kết hợp mã hóa và xác thực

❑AEAD Modes

- CCM: Counter with CBC-MAC
- GCM: Galois Counter Mode
- EAX: Encrypt-then-Authenticate-then-translate
- OCB: Offset Codebook
- CWC: Carter-Wegman + CTR

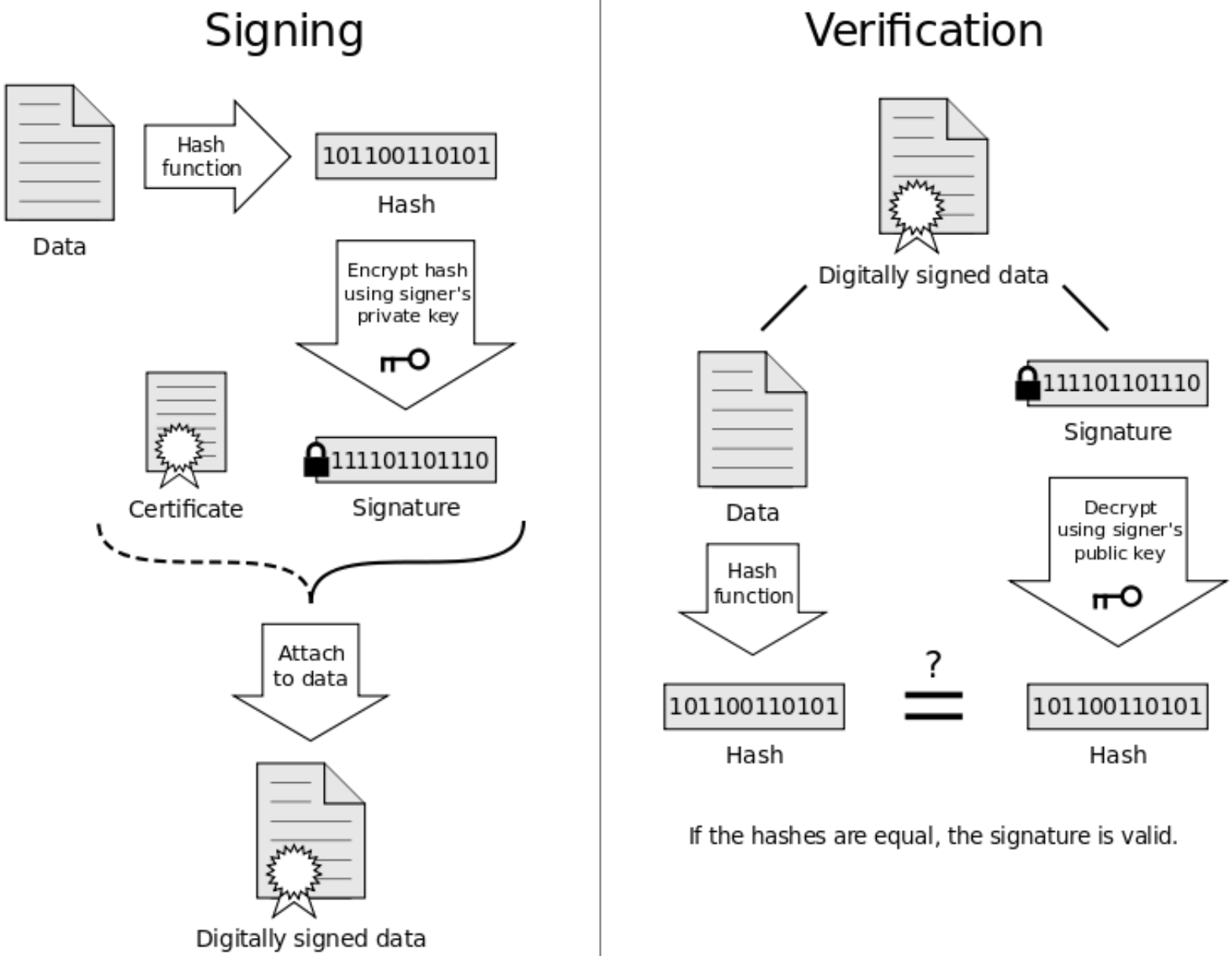
Kết hợp mã hóa và xác thực. Ví dụ: CCM



Chữ ký số

- Có thể coi là một dạng MAC
- Sử dụng mật mã khóa công khai
  - Ký: s = Enc(KS, msg)
  - Gửi đi: s, msg
  - Kiểm tra: msg == Dec(KP, s)?
- Thường thì thông điệp "msg" có kích thước lớn → thay bằng giá trị băm

Chữ ký số


Signing
Data
Hash function
101100110101
Hash
Encrypt hash using signer's private key
Certificate
111101101110
Signature
Attach to data
Digitally signed data
Verification
Digitally signed data
Data
111101101110
Signature
Decrypt using signer's public key
Hash function
?
101100110101
Hash
101100110101
Hash
If the hashes are equal, the signature is valid.

Vấn đề giả mạo khóa công khai

Hi Bob, I'm Alice.
I wanna send you a secret
Send me your public key

KP_{Malice}

$Enc(KP_{Malice}, Secret)$

I've got the secret. It's OK

Hi Bob, I'm Alice.
I wanna send you a secret
Send me your public key

KP_{Bob}

$Enc(KP_{Bob}, Secret)$

I've got the secret. It's OK

Chứng thực khóa công khai

CHỨNG THƯ
KHÓA CÔNG KHAI

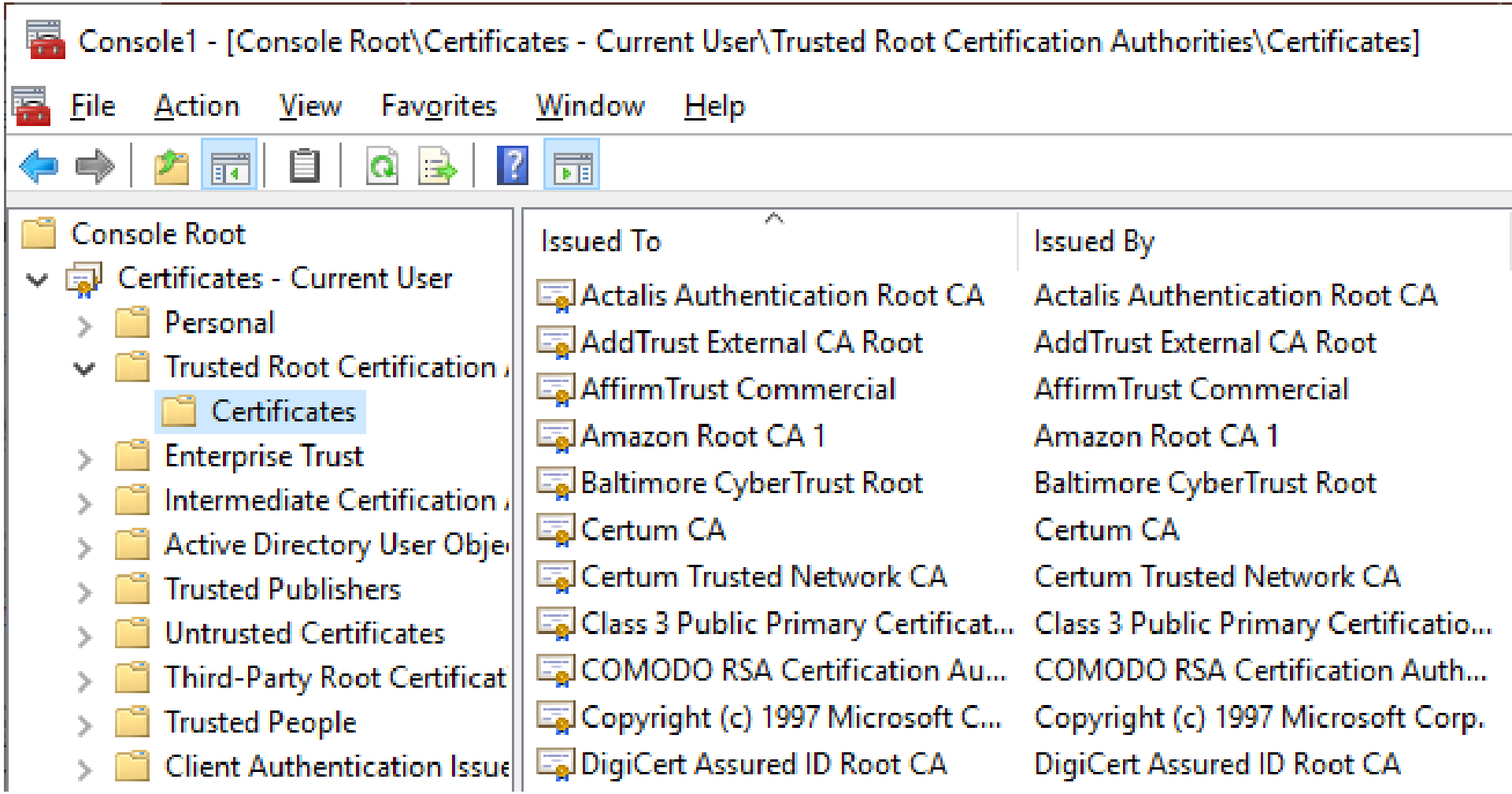
Tôi là: Trent

Chứng thực cho: Bob

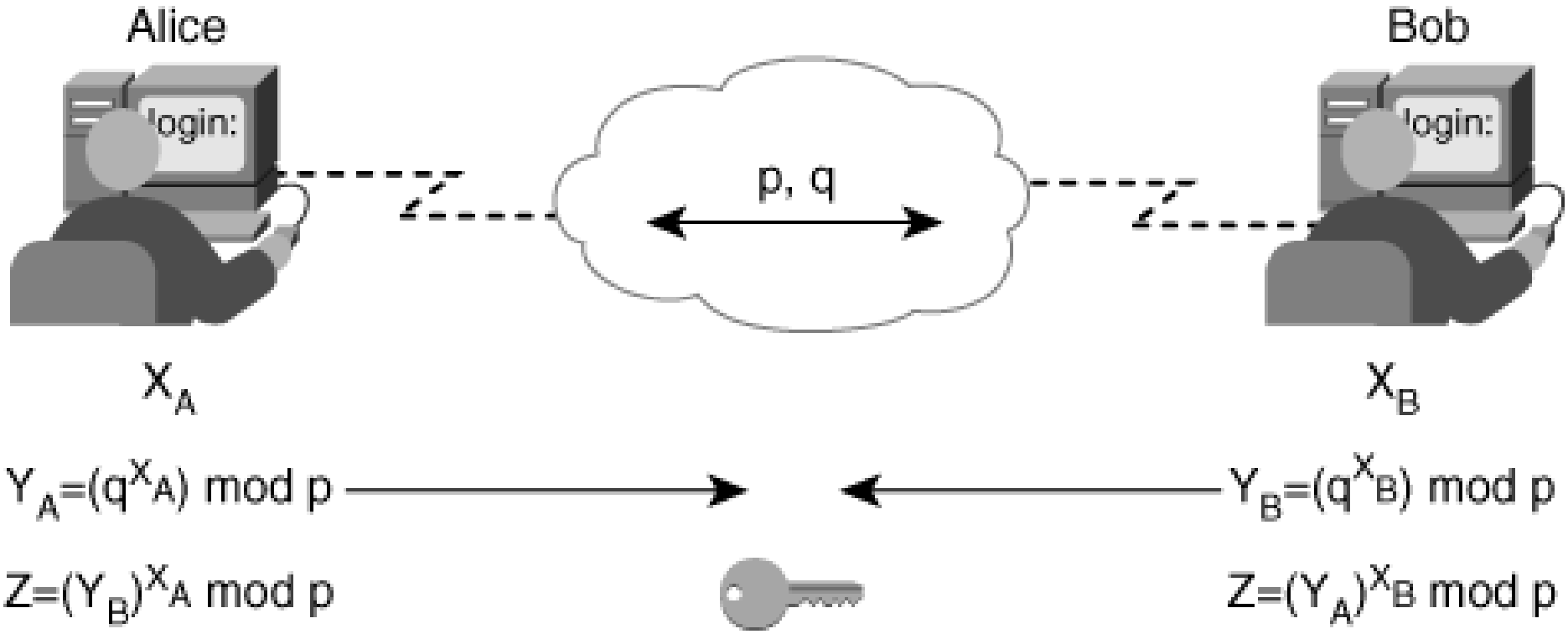
Có khóa công khai là: KP_{Bob}

Ký tên
(Trent)

Chưng thư khóa công khai



Trao đổi khóa Diffie-Hellman



By exchanging numbers (p,q) in the clear, two entities can determine a new unique number (z) known only to them.

Dẫn xuất khóa

- **Nguồn khóa thường gặp:**
  - Mật khẩu
  - Khóa trao đổi, ví dụ, bằng Diffie-Hellman
- **Yêu cầu đối với khóa được sử dụng:**
  - Độ dài xác định theo hệ mật
  - Có tính chất của dãy ngẫu nhiên
  - Có thể phải thay đổi khóa khi mã hóa nhiều thông điệp

➔ **Cần phải thực hiện dẫn xuất khóa!**

Dẫn xuất khóa

- Dẫn xuất khóa (Key Derivation) là việc tạo ra khóa để sử dụng từ một giá trị bí mật cho trước.
- Kỹ thuật thường dùng:
  - Băm (một hoặc nhiều lần) bí mật ban đầu
  - Lấy một lượng bít cần thiết từ kết quả băm để làm khóa
  - Nếu cần nhiều khóa thì khóa sau được dẫn xuất từ khóa trước

Dẫn xuất khóa. Ví dụ: PBKDF1

$$T_1 = Hash(P \| S)$$

$$T_2 = Hash(T_1)$$

$$\ldots$$

$$T_c = Hash(T_{c-1})$$

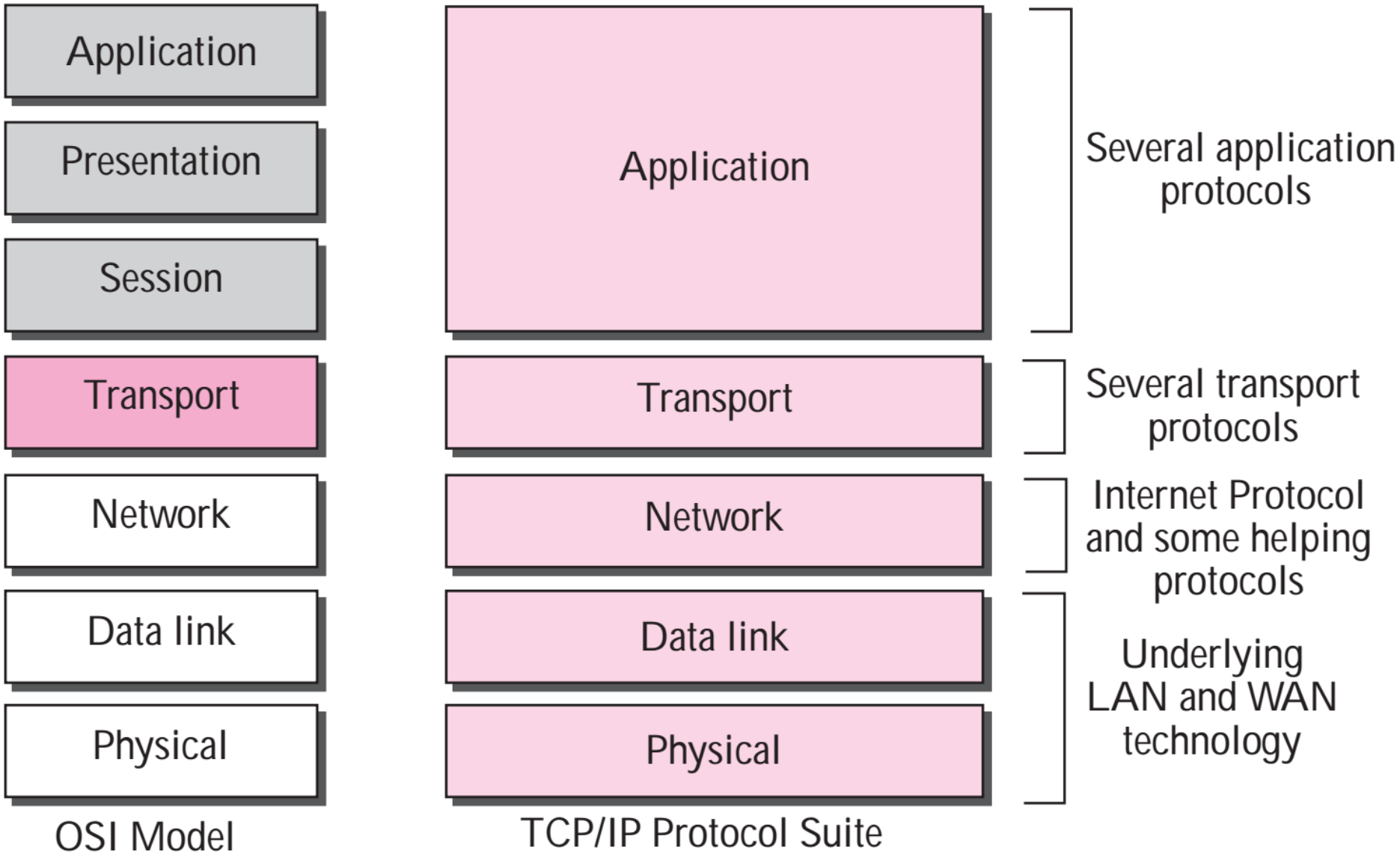
$$DK = T_c[0..dkLen - 1]$$

1 Giới thiệu học phần

2 Cơ sở mật mã cho an toàn mạng

3 Tổng quan về giao thức an toàn mạng

Chồng giao thức TCP/IP



Khái niệm

- **An toàn mạng máy tính** là việc ngăn chặn và giám sát các truy cập trái phép, sự lạm dụng, sửa đổi hoặc làm gián đoạn hoạt động của mạng máy tính và các tài nguyên mạng.

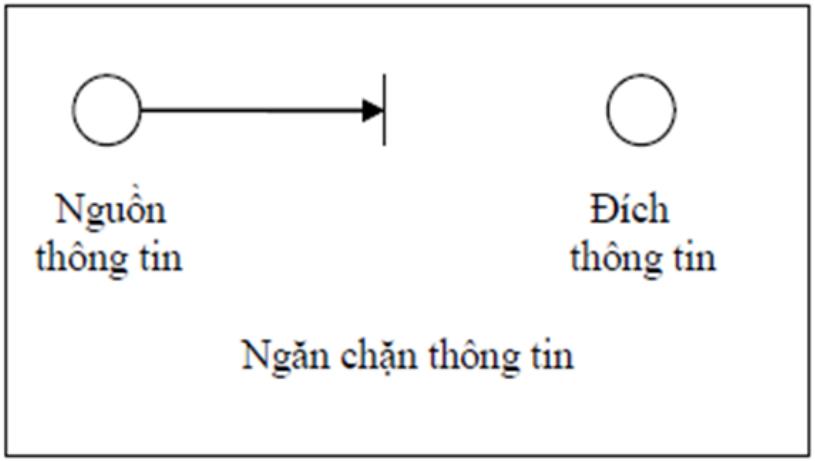
- An toàn mạng máy tính được đảm bảo bằng một tập hợp các chính sách và giải pháp kỹ thuật.
- An toàn mạng máy tính đòi hỏi phải cấp quyền và giám sát việc truy cập các tài nguyên mạng.

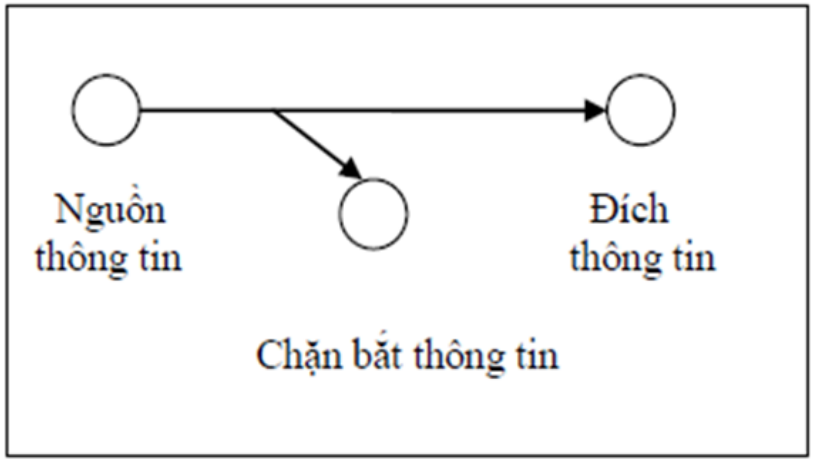
https://en.wikipedia.org/wiki/Network_security

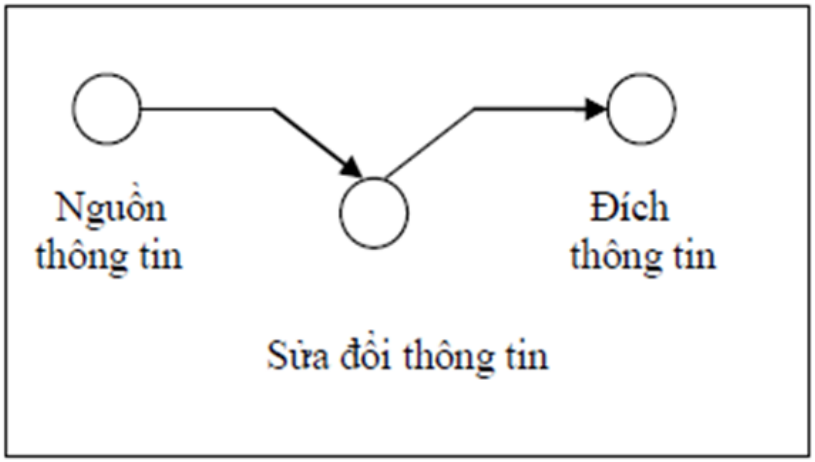
Khái niệm

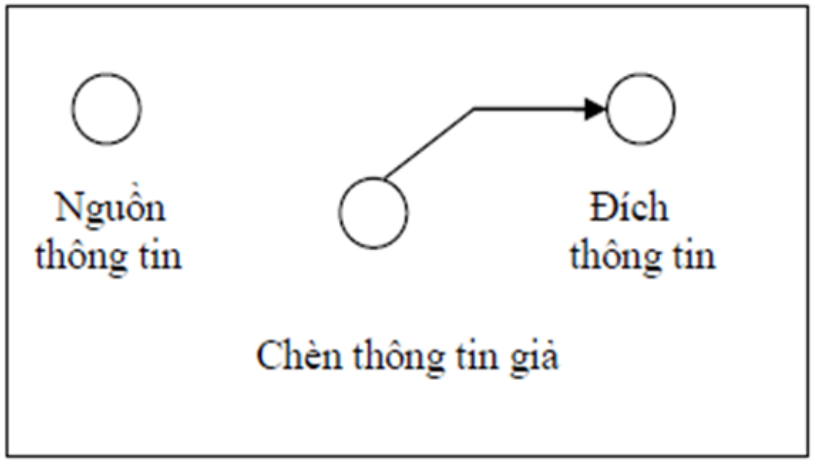
- **Tấn công**: Là hành động có chủ ý nhằm phá vỡ tính an toàn của thông tin, hệ thống thông tin được bảo vệ.

Phân loại tấn công mạng
Tiêu chí: cách thức tác động lên thông tin









Khái niệm

- **Dịch vụ an toàn**: Là dịch vụ nâng cao an toàn của các hệ thống. Mỗi dịch vụ an toàn sử dụng một hay nhiều kỹ thuật đảm bảo an toàn.
- **Kỹ thuật đảm bảo an toàn**: Là kỹ thuật được thiết kế để phát hiện, ngăn ngừa hoặc loại bỏ tấn công.

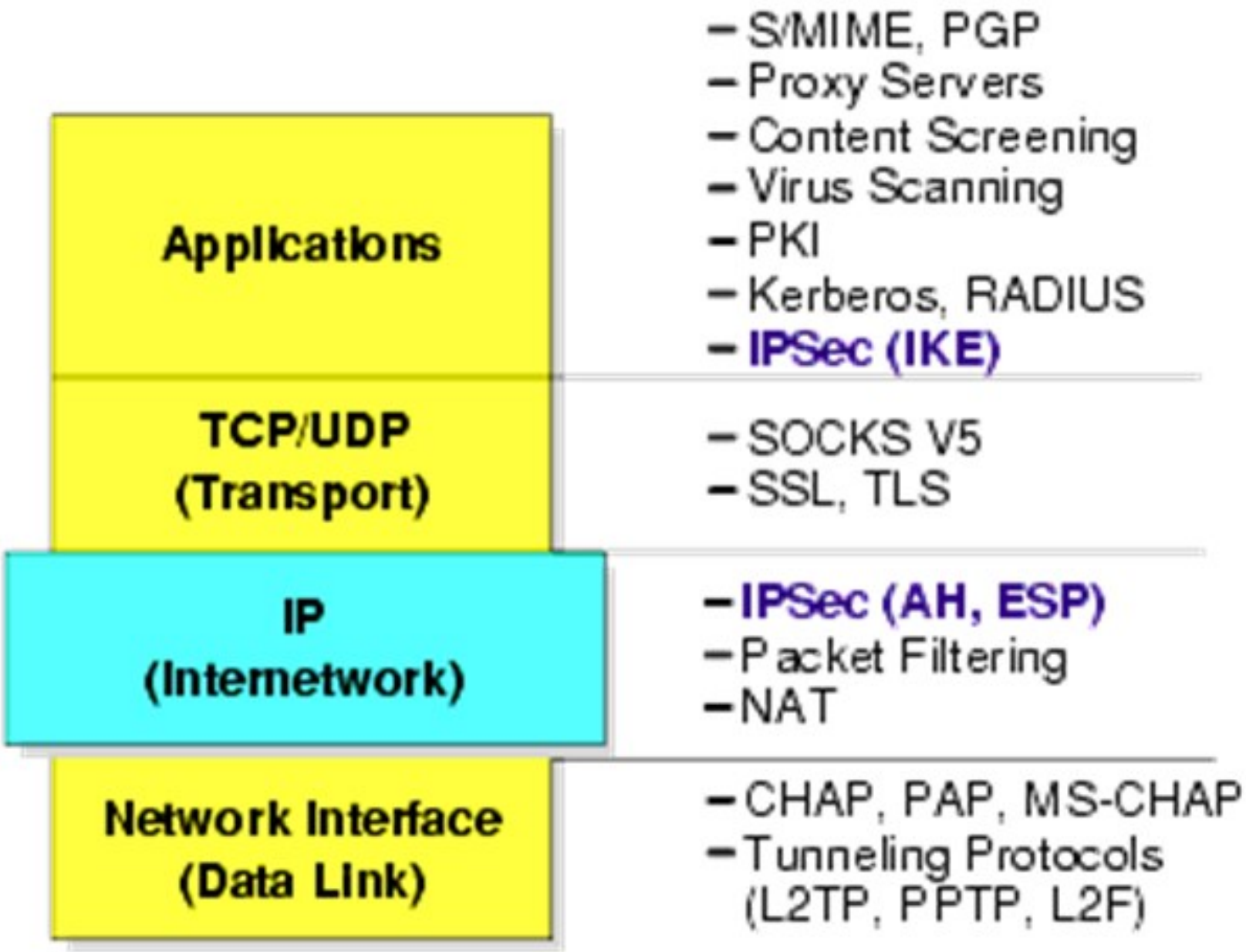
Dịch vụ an toàn vs. Kỹ thuật an toàn

Dịch vụ an toàn	Bí mật
	Xác thực
	Toàn vẹn
	Sẵn sàng
	Chống chối bỏ
Kỹ thuật an toàn	Ngăn cản vật lý
	Định danh
	Cấp quyền
	Xác thực
	Mã hóa
	Ký số

Giao thức an toàn mạng

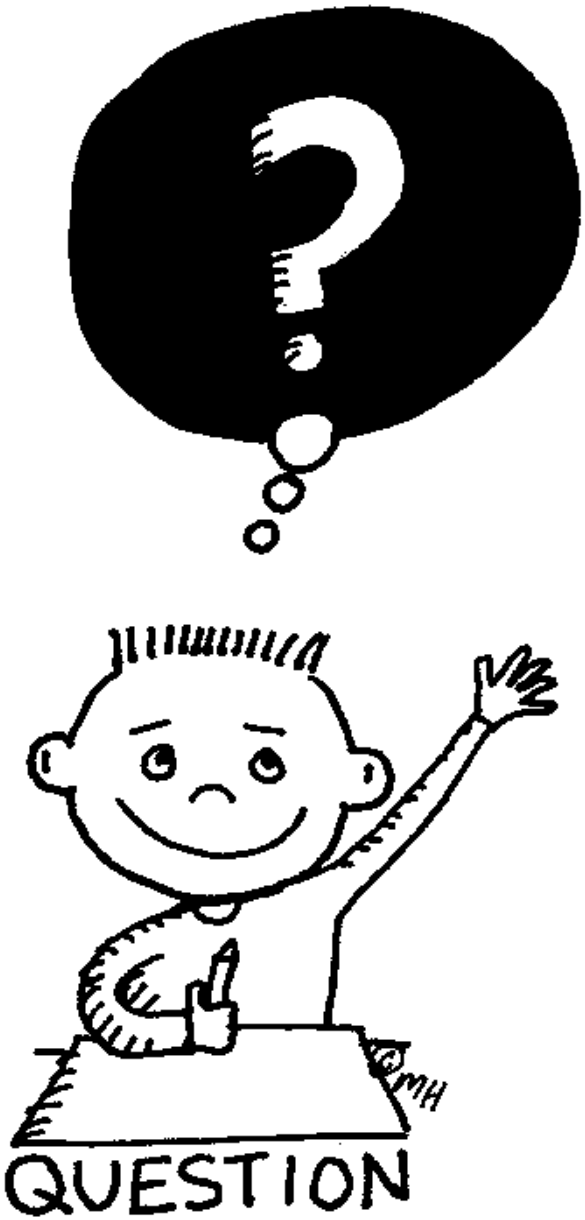
- **Giao thức mạng** là tập hợp các quy tắc và quy ước điều khiển việc trao đổi thông tin giữa các hệ thống máy tính.
- **Giao thức an toàn mạng** là một giao thức mật mã được sử dụng để bảo vệ dữ liệu trên máy tính và dữ liệu truyền thông.

Giao thức an toàn mạng



Giao thức sẽ xem xét trong học phần

- Giao thức xác thực: PAP/CHAP, Kerberos, EAP
- Các giao thức an toàn ở tầng Application và Transport: S/MIME, SSH, SSL/TLS
- Giao thức an toàn ở Network: IPsec
- Giao thức an toàn ở tầng Datalink: WEP, WPA, WPA2


QUESTION

TỰ TÌM HIỂU
Các chế độ của mã khối (Wikipedia, NIST)