

CƠ SỞ AN TOÀN THÔNG TIN

Bài 6. Đảm bảo an toàn thông tin bằng mật mã

1

Tổng quan về mật mã

2

Đảm bảo tính bí mật

3

Đảm bảo tính toàn vẹn

4

Đảm bảo tính xác thực

5

Xác thực thực thể

1

Tổng quan về mật mã

2

Đảm bảo tính bí mật

3

Đảm bảo tính toàn vẹn

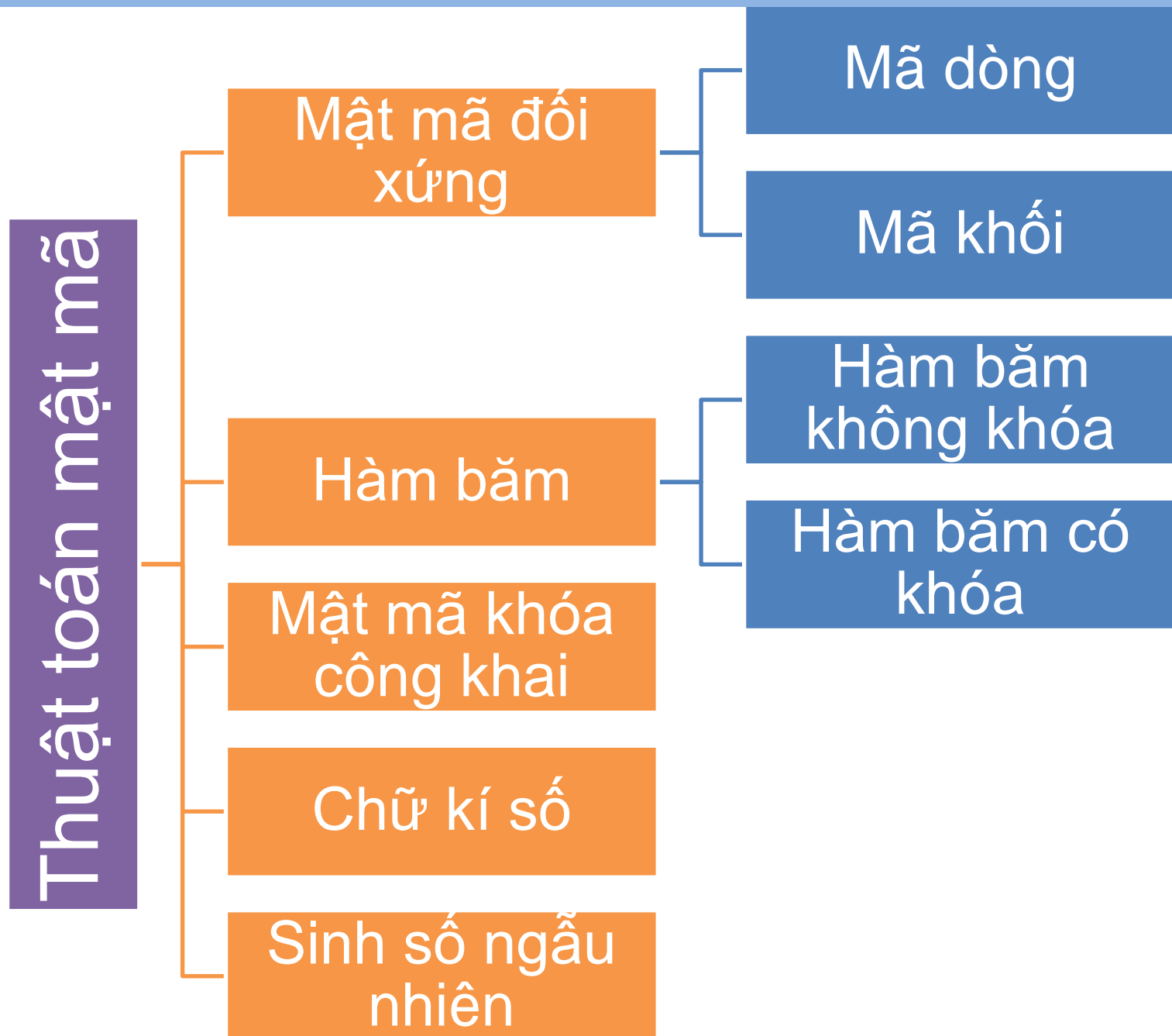
4

Đảm bảo tính xác thực

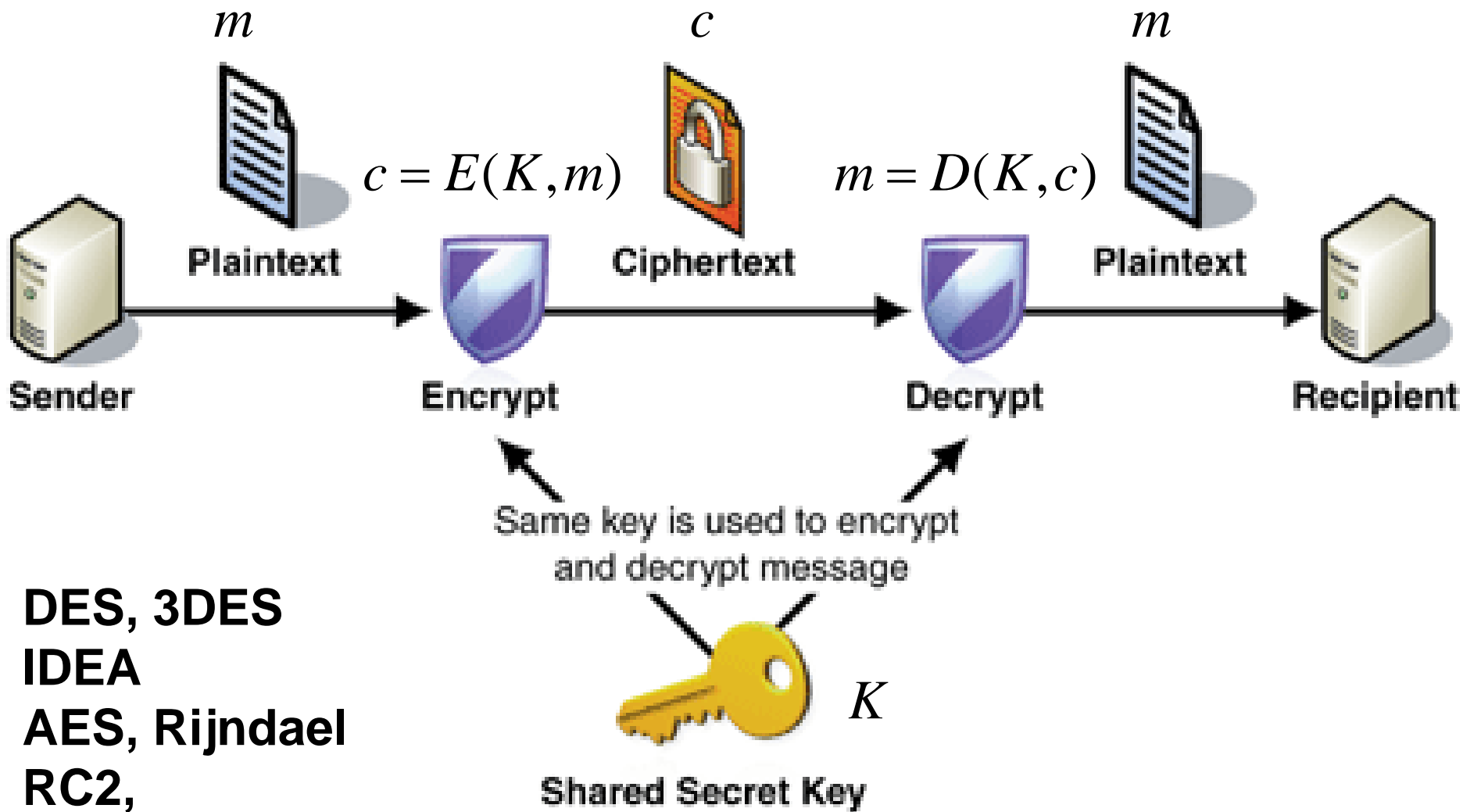
5

Xác thực thực thể

Phân loại



Mật mã đối xứng



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

Tính chất của mật mã đối xứng

- ➡ Khóa mã hóa và khóa giải mã là như nhau, được chia sẻ và giữ bí mật bởi hai bên
- ➡ Số lượng khóa trong hệ thống n người dùng là $n(n-1)/2$
- ➡ Nói chung, chưa chứng minh được độ an toàn về mặt lý thuyết → An toàn thực tế
- ➡ Các phép toán thường đơn giản nên cho tốc độ cao

Tính chất của mật mã đối xứng

AES

AES là viết tắt của Advanced Encryption Standard

AES cho phép độ dài dữ liệu (kích thước văn bản thuần túy) là 128, 192 và 256 bit.

AES chia bản rõ thành các khối 16 byte (128-bit) và xử lý mỗi khối như một mảng Trạng thái 4×4 và hỗ trợ ba độ dài khóa khác nhau, 128, 192 và 256 bit.

Số vòng là 10, dành cho trường hợp khóa mã hóa dài 128 bit. (Như đã đề cập trước đó, số vòng là 12 khi khóa là 192 bit và 14 khi khóa là 256.)

AES được thiết kế bởi Vincent Rijmen và Joan Daemen.

AES nhanh hơn.

AES có một khóa bí mật lớn do đó tương đối an toàn hơn.

Subbyte, Shiftrows, Trộn cột, Addroundkey.

10 vòng đối với mật số 128 bit
12 vòng đối với bí danh 192 bit,
14 vòng đối với bí danh 256 bit

DES

DES là viết tắt của Data Encryption Standard.

Chuẩn mã hóa dữ liệu lấy bản rõ 64 bit làm đầu vào và tạo ra Bản mã 64 bit tức là nó mã hóa dữ liệu trong một khối có kích thước 64 bit trên mỗi khối.

Trong bản tin rõ ràng DES được chia thành từng khối 64 bit kích thước và được mã hóa bằng khóa 56 bit ở mức ban đầu.

Bản rõ bên trái và bản rõ bên phải trải qua 16 vòng quy trình mã hóa cùng với 16 khóa khác nhau cho mỗi vòng.

DES được thiết kế bởi IBM.

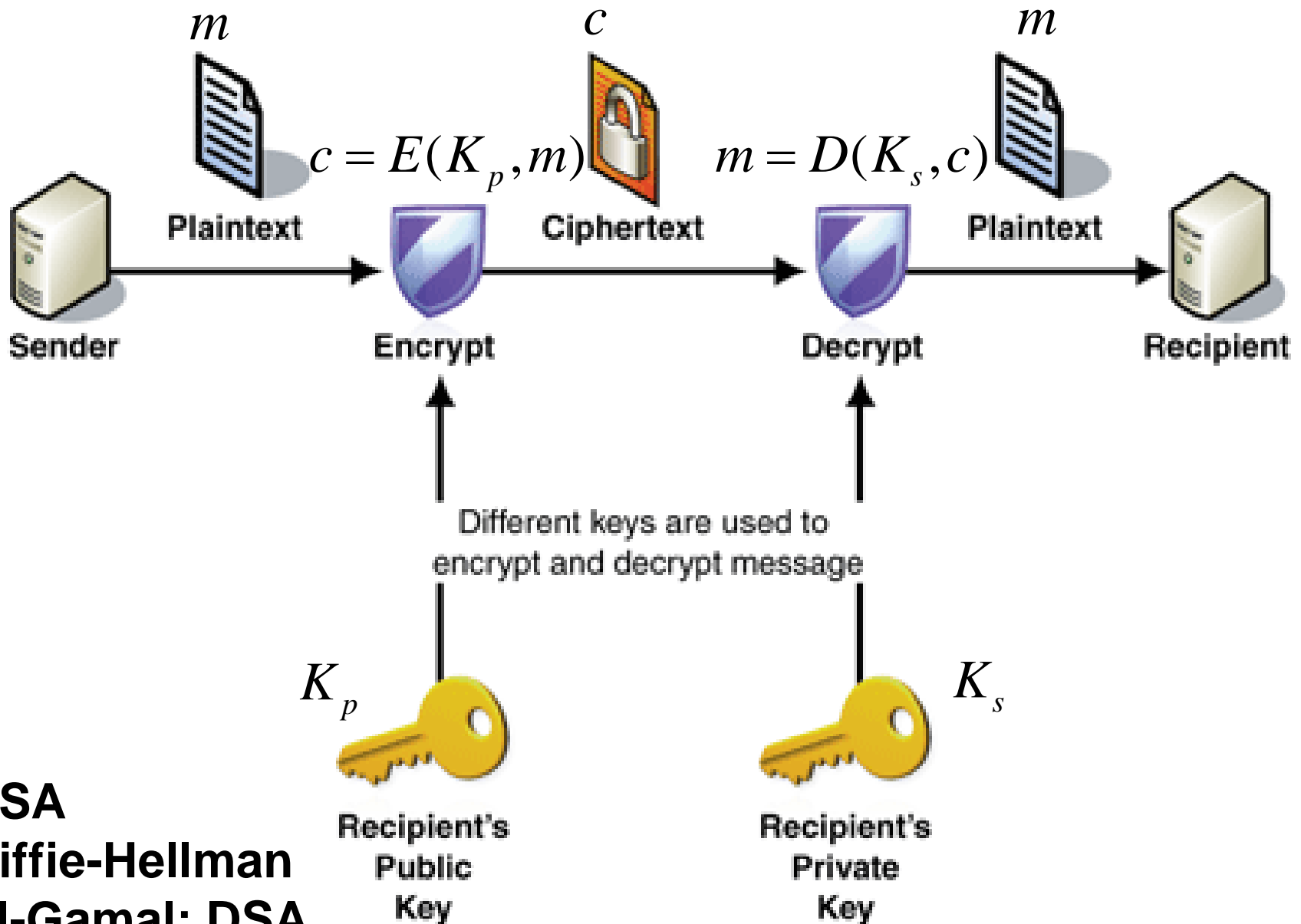
DES tương đối chậm hơn.

DES có một khóa nhỏ hơn kém an toàn hơn.

Hoán vị mở rộng, Xor, S-box, P-box, Xor và Swap.

16 vòng

Mật mã khóa công khai



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

Tính chất của mật mã khóa công khai

- ➡ Khóa mã hóa và khóa giải mã là khác nhau.
- ➡ Mỗi bên có khóa bí mật của riêng mình và khóa công khai tương ứng (K_s , K_p)
- ➡ Từ khóa công khai không thể tìm ra khóa bí mật
- ➡ Dữ liệu được mã hóa bằng khóa công khai, giải mã bằng khóa bí mật
- ➡ Mọi người đều có thể mã hóa nhưng chỉ một người có thể giải mã, chính người mã hóa cũng không thể giải mã
- ➡ Thường tính toán trên số lớn nên cho tốc độ thực thi thấp

So sánh mật mã đối xứng và mật mã khóa công khai

Mật mã đối xứng



Các bên CẦN thỏa thuận trước khóa bí mật cần dùng; số lượng nhỏ



→ có thể xử lý lượng LỚN dữ liệu

Mật mã khóa công khai

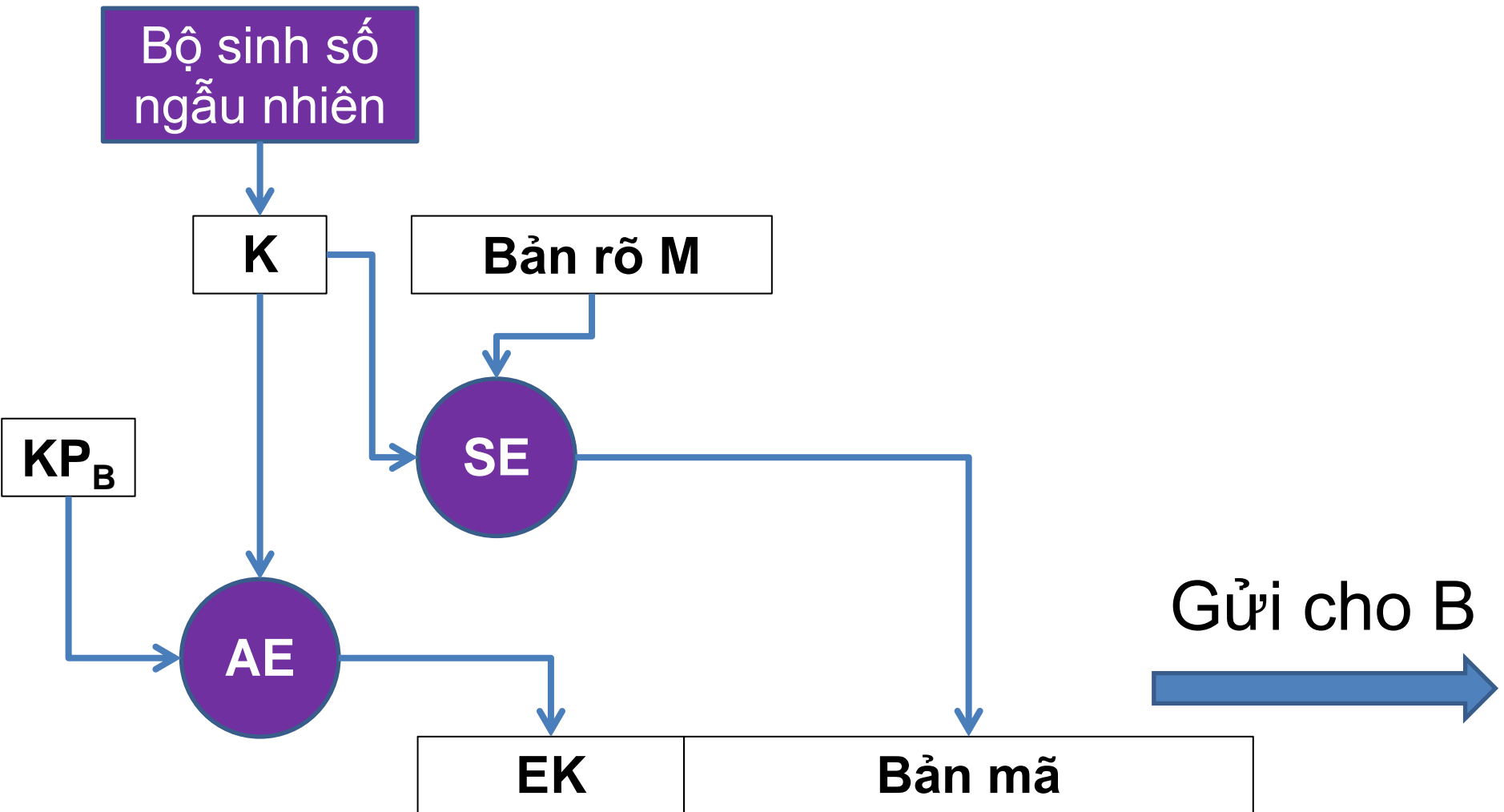


Các bên KHÔNG CẦN thỏa thuận trước về khóa; số lượng nhỏ

nh toán nên → chỉ phù hợp với lượng NHỎ dữ liệu

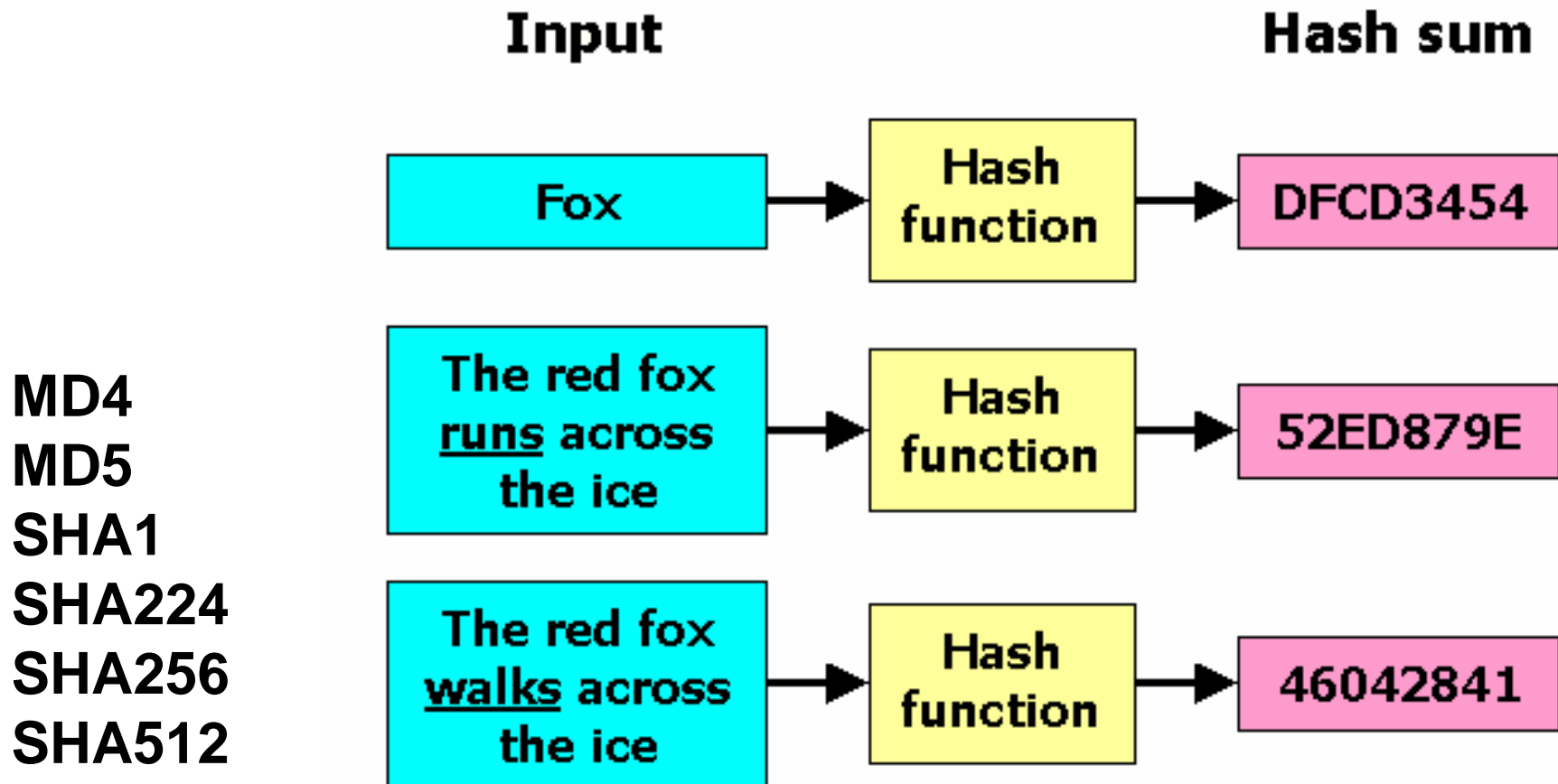
Sử dụng mật mã đối xứng hay mật mã khóa công khai?

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



SE (Symmetry)
AE (Asymmetrical)

Hàm băm



Dữ liệu có độ dài bất kì



Bản tóm lược có độ dài định trước

Tính chất của hàm băm

- ➡ Nén \rightarrow 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

Chữ kí viết tay

- Đặc trưng cho người kí, mỗi người có một chữ kí đặc trưng, không thể được tạo ra bởi người khác
- Chữ kí gắn liền với một văn bản, không thể di chuyển sang văn bản khác
- Mọi người đều có khả năng kiểm tra chữ kí của một người bất kì

Chữ kí số

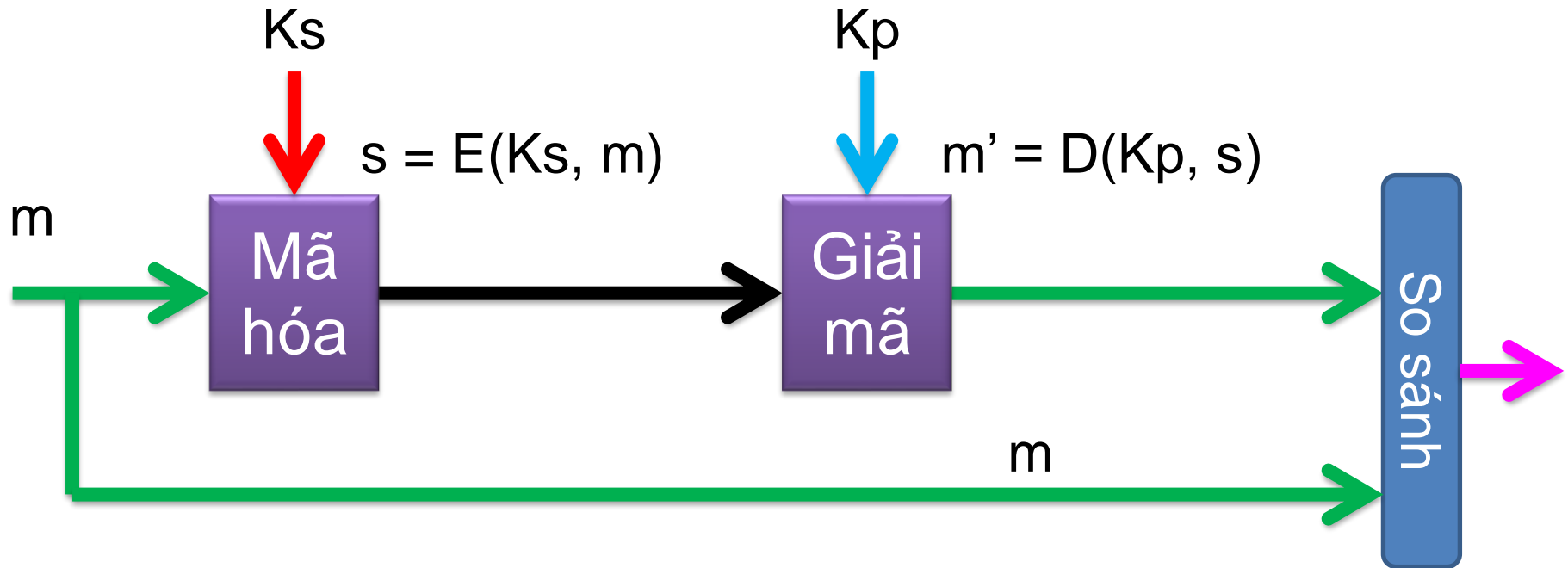
- Là thông điệp dữ liệu (dãy bit)
- Có các tính chất của chữ kí viết tay

Chữ kí số

- Đặc trưng cho người kí → phụ thuộc vào yếu tố bí mật của riêng người kí
- Không thể chuyển chữ kí sang văn bản khác → chữ kí phụ thuộc vào chính văn bản
- Người bất kì có thể kiểm tra → có một đại lượng công khai tương ứng với yếu tố bí mật

→ ứng dụng mật mã khóa công khai

Chữ kí số

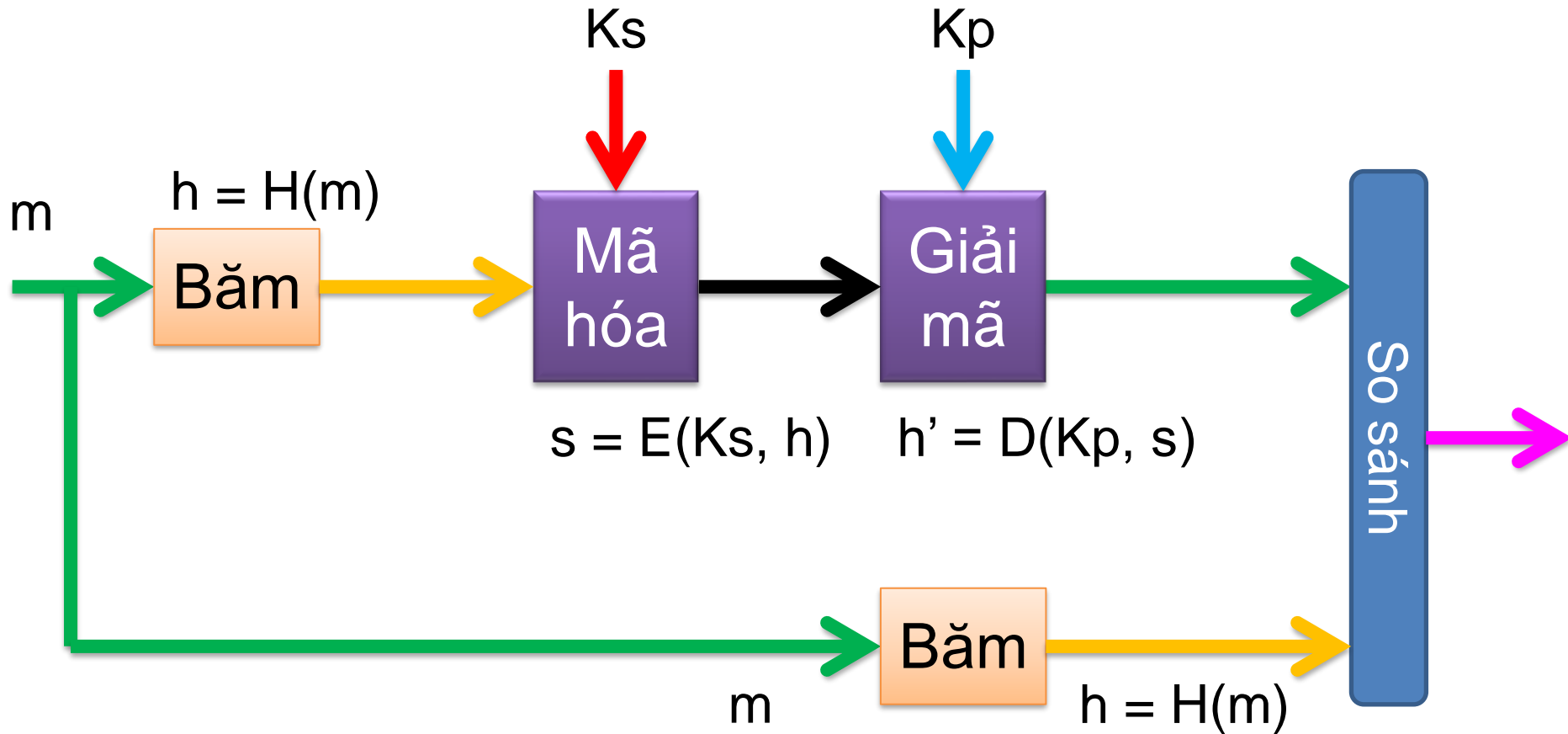


Lưu lượng tăng gấp đôi

Kích thước của m thường vượt quá khả năng tính toán hiện nay

→ Lấy đại diện của m

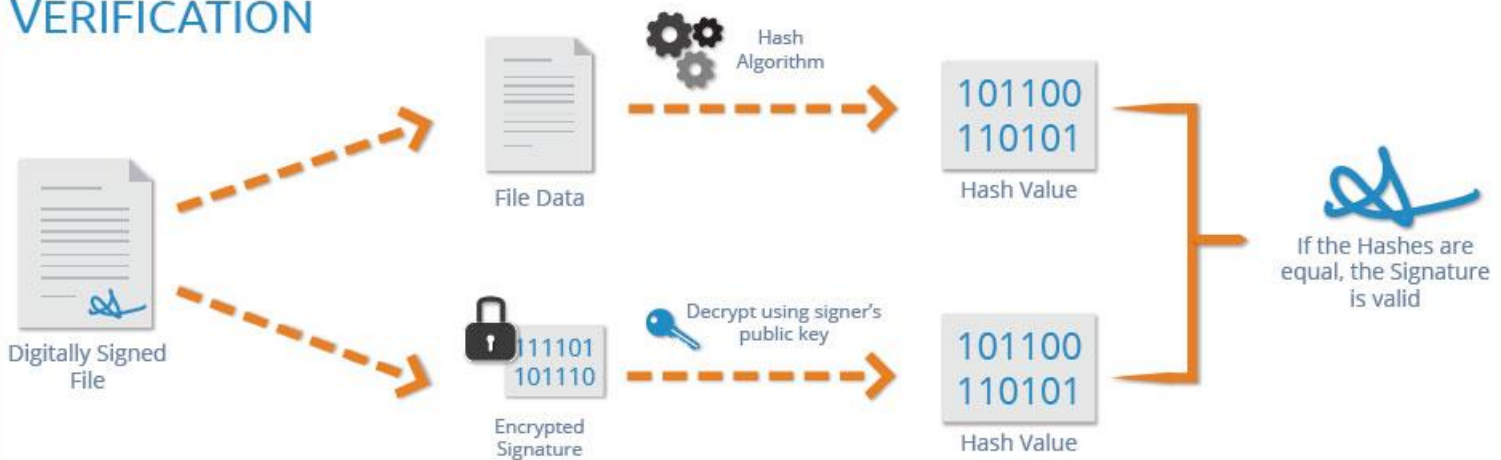
Chữ kí số



SIGNING



VERIFICATION



Ứng dụng của mật mã

Đảm bảo
tính bí
mật

Đảm bảo
tính toàn
vẹn

Đảm bảo
tính xác
thực

Đảm bảo
tính
chống
chối bỏ

1

Tổng quan về mật mã

2

Đảm bảo tính bí mật

3

Đảm bảo tính toàn vẹn

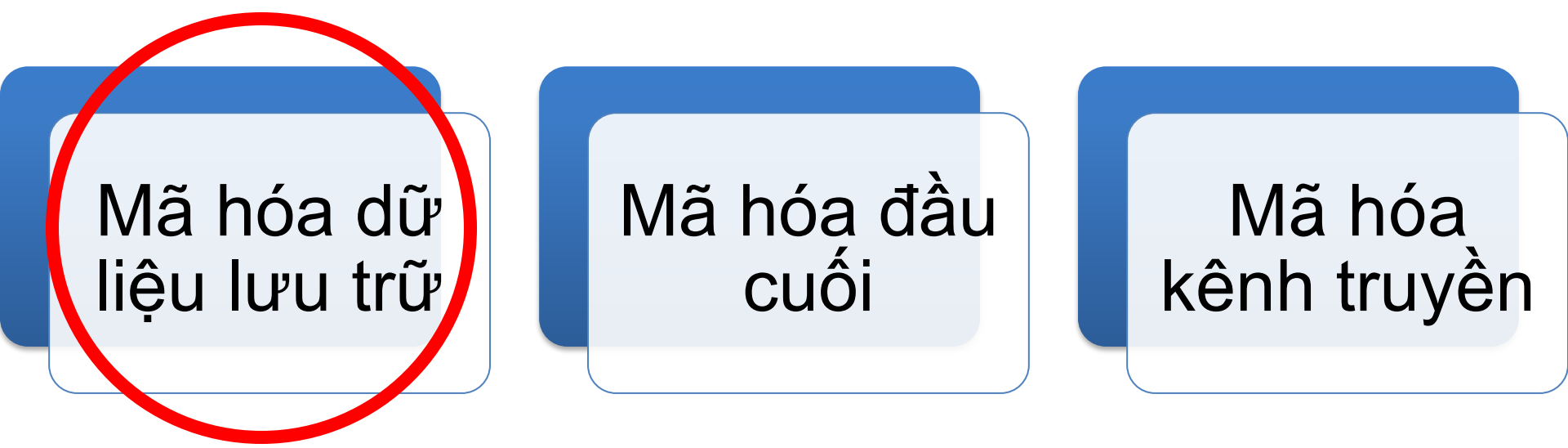
4

Đảm bảo tính xác thực

5

Xác thực thực thể

Các dạng đảm bảo tính bí mật



Mã hóa dữ liệu lưu trữ

Mã hóa đầu cuối

Mã hóa kênh truyền

❑ Mã hóa dữ liệu lưu trữ

- Dữ liệu chủ yếu tồn tại ở dạng mã hóa
- Dữ liệu chỉ được giải mã khi cần sử dụng
- Sau khi dùng xong, dữ liệu được mã hóa trở lại

❑ Ví dụ:

- Encryption File System
- Mã hóa ổ đĩa, ổ đĩa ảo
- Mã hóa email, điện mật
- Các ứng dụng mật mã khác: Office, PDF,...

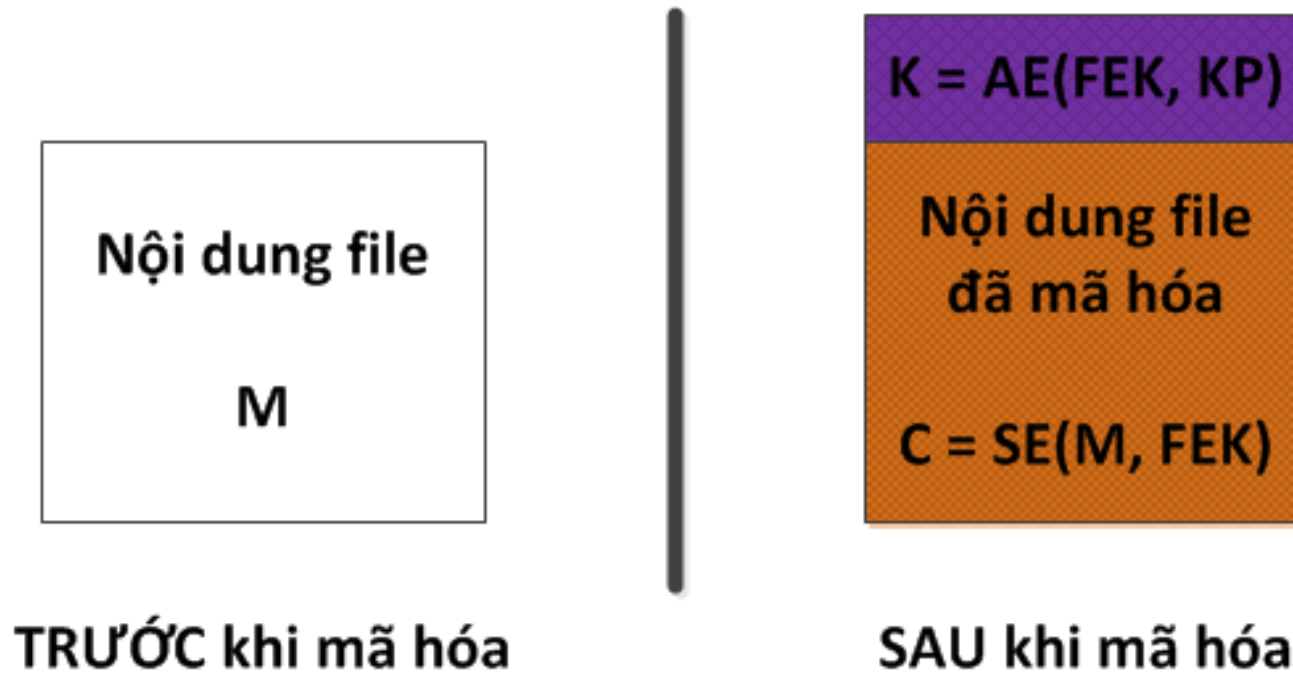
Mã hóa dữ liệu lưu trữ

- Hệ quản trị tập tin mật mã EFS
- Mã hóa ổ đĩa
- Mã hóa dữ liệu khi đồng bộ qua đám mây

- ❑ Các hệ quản trị tập tin mà Windows hỗ trợ
 - FAT, FAT32
 - NTFS
 - exFAT
- ❑ Chỉ có NTFS hỗ trợ mã hóa, trong đó chức năng mã hóa được thực hiện bởi thành phần EFS (Encryption File System)
- ❑ EFS xuất hiện trong NTFS 3.0 trở về sau với chức năng mã hóa dữ liệu một cách trong suốt, giúp bảo mật dữ liệu ngay cả khi tin tặc chiếm được (tiếp cận vật lý) thiết bị lưu trữ.

- ❑ EFS thực hiện mã hóa bằng việc sử dụng mật mã khóa công khai (RSA, ECC) kết hợp mật mã đối xứng (DES-X, AES).
- ❑ Thuật toán thuộc Suite-B (ECC và AES) được bắt đầu hỗ trợ từ Windows 7.
- ❑ File được mã hóa bằng mật mã đối xứng, sử dụng khóa ngẫu nhiên
- ❑ Khóa mã hóa file được mã hóa bằng khóa công khai của người dùng

EFS - Encryption File System



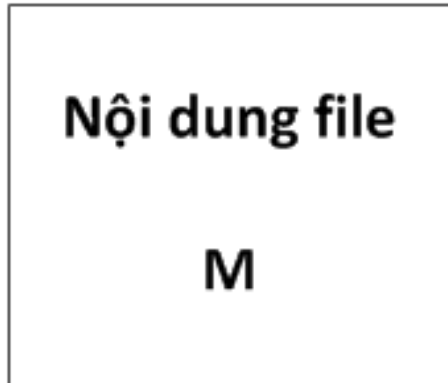
AE: Thuật toán bất đối xứng (Asymmetric Encryption)

SE: Thuật toán đối xứng (Symmetric Encryption)

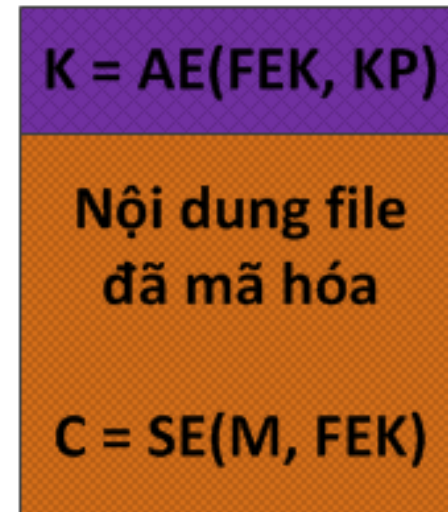
FEK: Khóa mã hóa file (File Encryption Key)

KP: Khóa công khai của người dùng (User's Public Key)

EFS - Encryption File System



TRƯỚC khi mã hóa



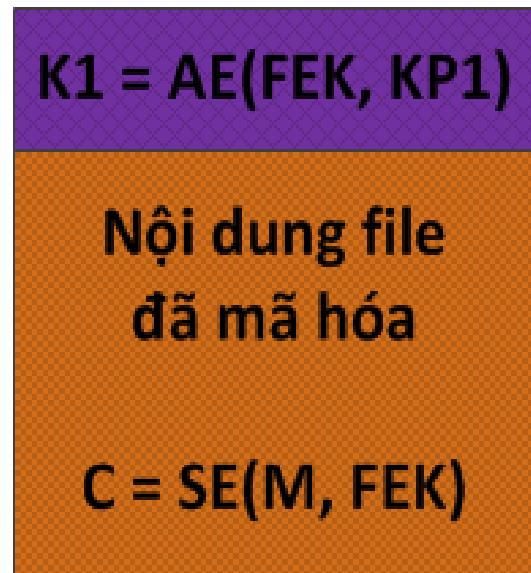
SAU khi mã hóa

Giải mã:

- $FEK = AD(K, KS)$
- $M = SD(C, FEK)$

EFS - Encryption File System

❑ Trường hợp file được chia sẻ với người khác



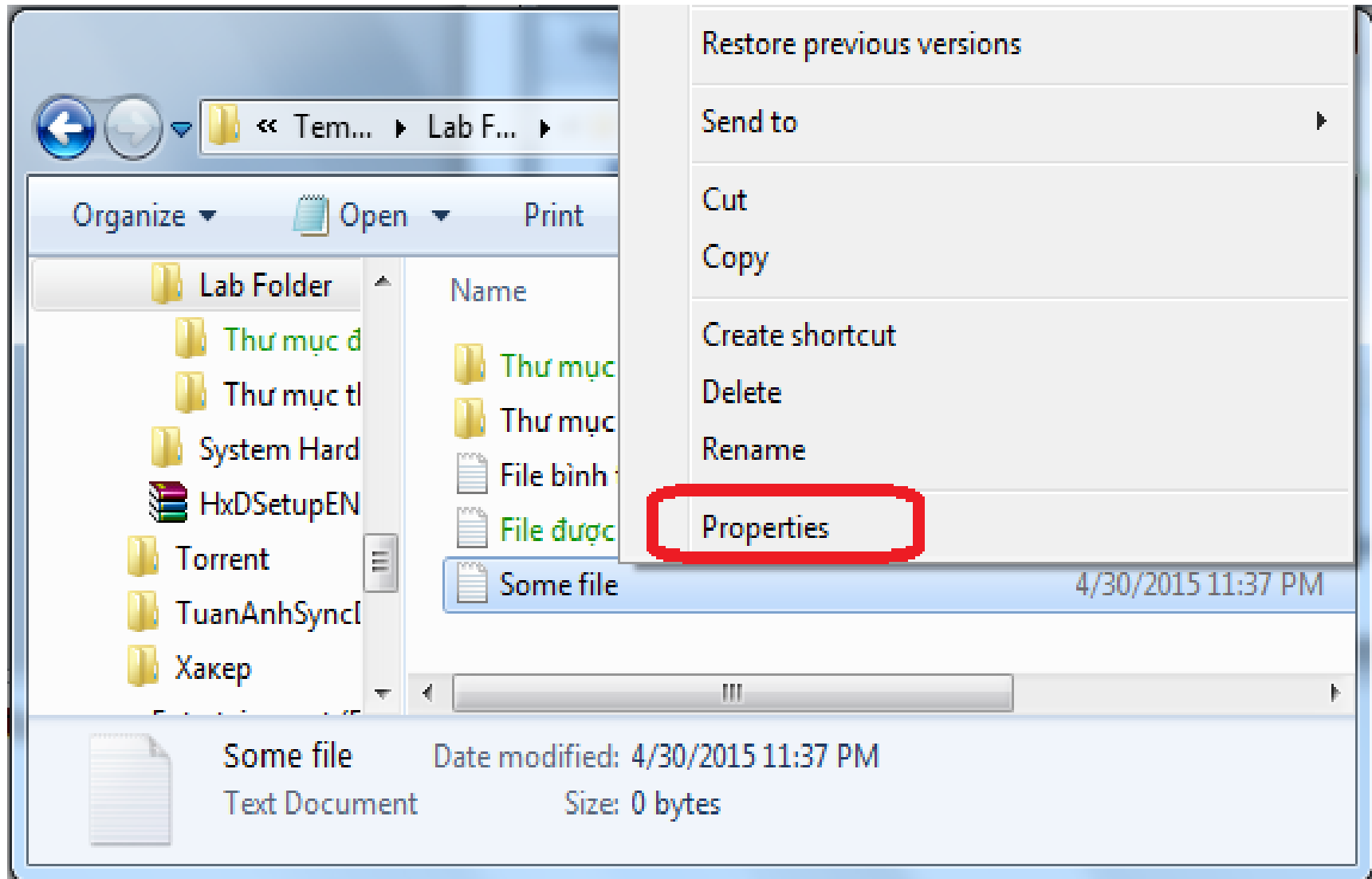
TRƯỚC khi chia sẻ



SAU khi chia sẻ

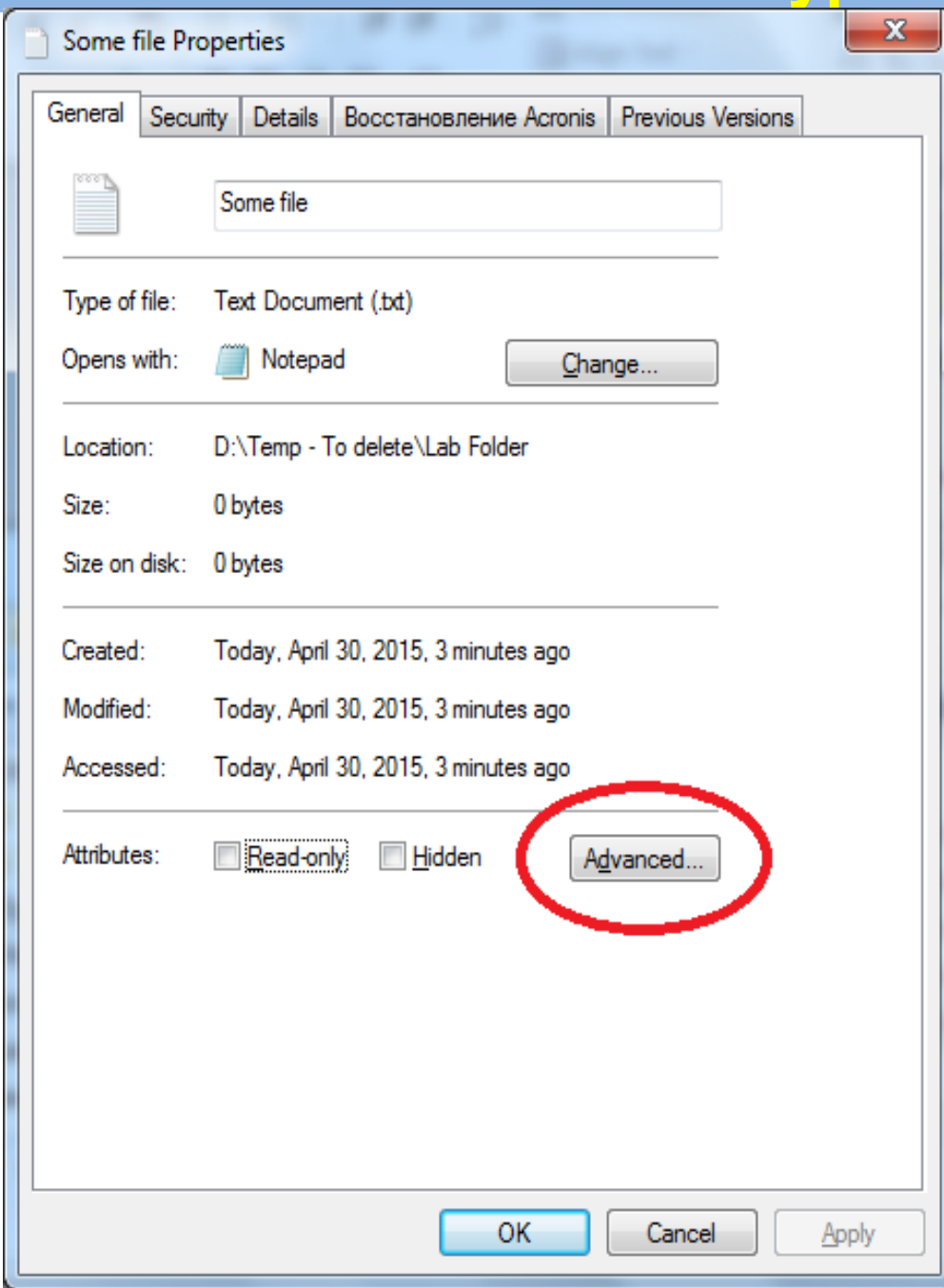
EFS - Encryption File System

❑ Để mã hóa file/thư mục, nhấn chuột phải và chọn mục «Properties»



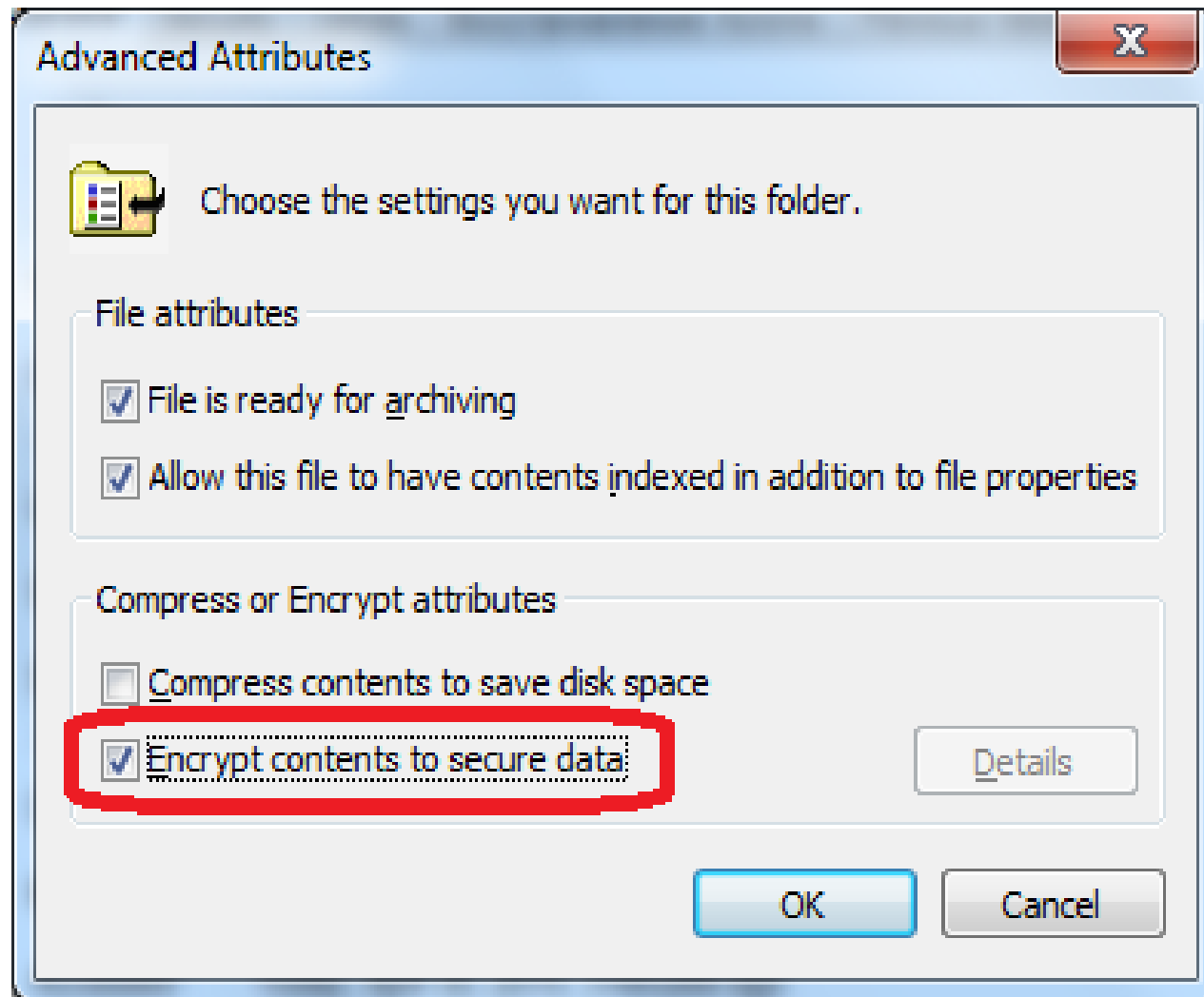
EFS - Encryption File System

□ Tiếp đó, chọn nút «Advanced» (tính năng nâng cao)



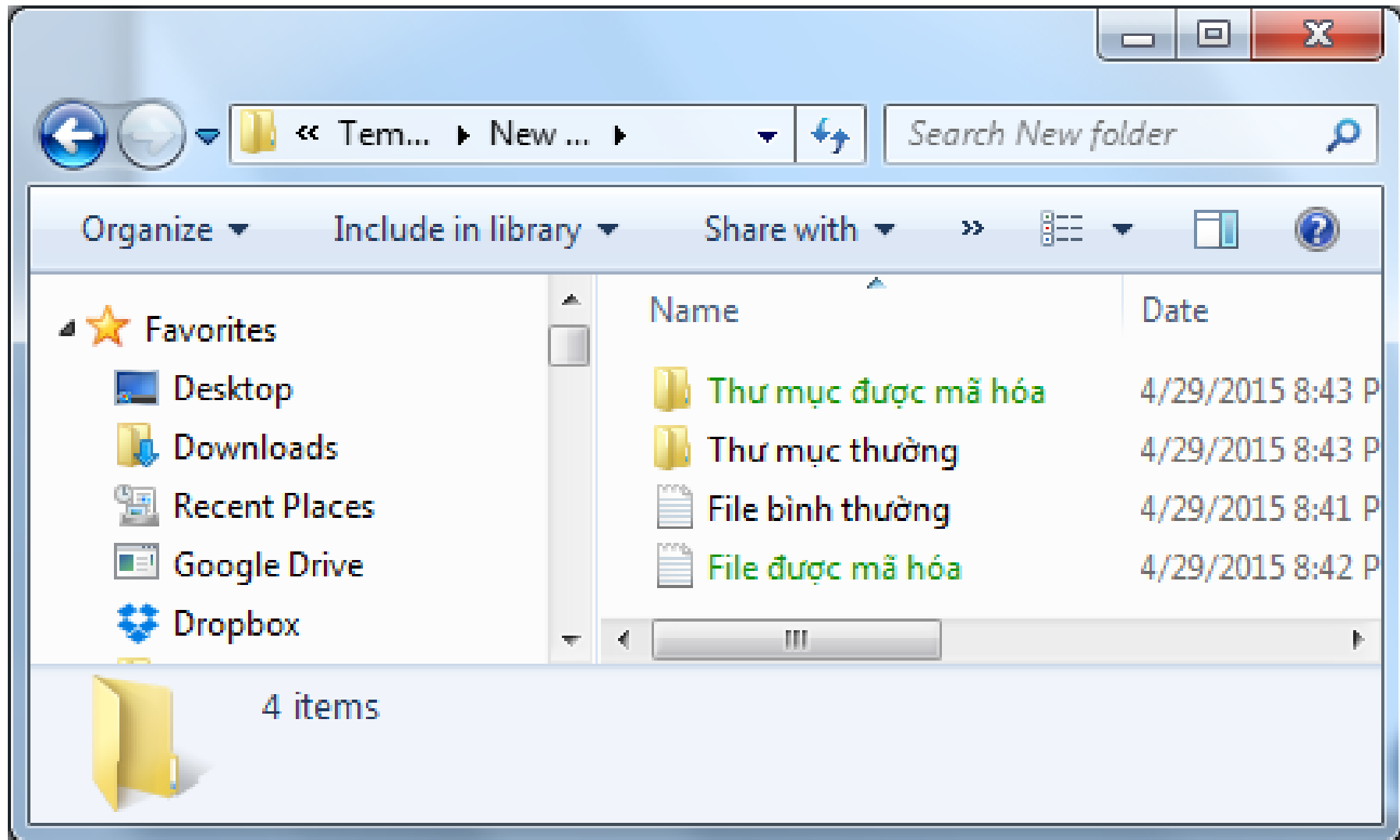
EFS - Encryption File System

- ❑ Đánh dấu chọn mục «Encrypt contents to secure data».



EFS - Encryption File System

❑ File/thư mục được mã hóa sẽ có màu xanh



Mã hóa dữ liệu lưu trữ

- Hệ quản trị tập tin mật mã EFS
- **Mã hóa ổ đĩa**
- Mã hóa dữ liệu khi đồng bộ qua đám mây

- ❑ Sản phẩm mã hóa dữ liệu của bên thứ ba thường ở dạng chương trình mã hóa ổ đĩa
 - Mã hóa ổ đĩa ảo
 - Đĩa ảo tồn tại dưới dạng một file duy nhất
 - Đĩa ảo tồn tại dưới dạng một thư mục
 - Mã hóa ổ đĩa vật lý
- ❑ Có những phần mềm mã hóa file dữ liệu nhưng không thuận tiện trong sử dụng

Mã hóa ổ đĩa

- ❑ Có những sản phẩm chuyên dụng, thực hiện mã hóa ổ đĩa bằng phần cứng
 - Hard Disk Drive (HDD) FDE (usually referred to as SED)
 - Enclosed hard disk drive FDE
 - Bridge and Chipset (BC) FDE



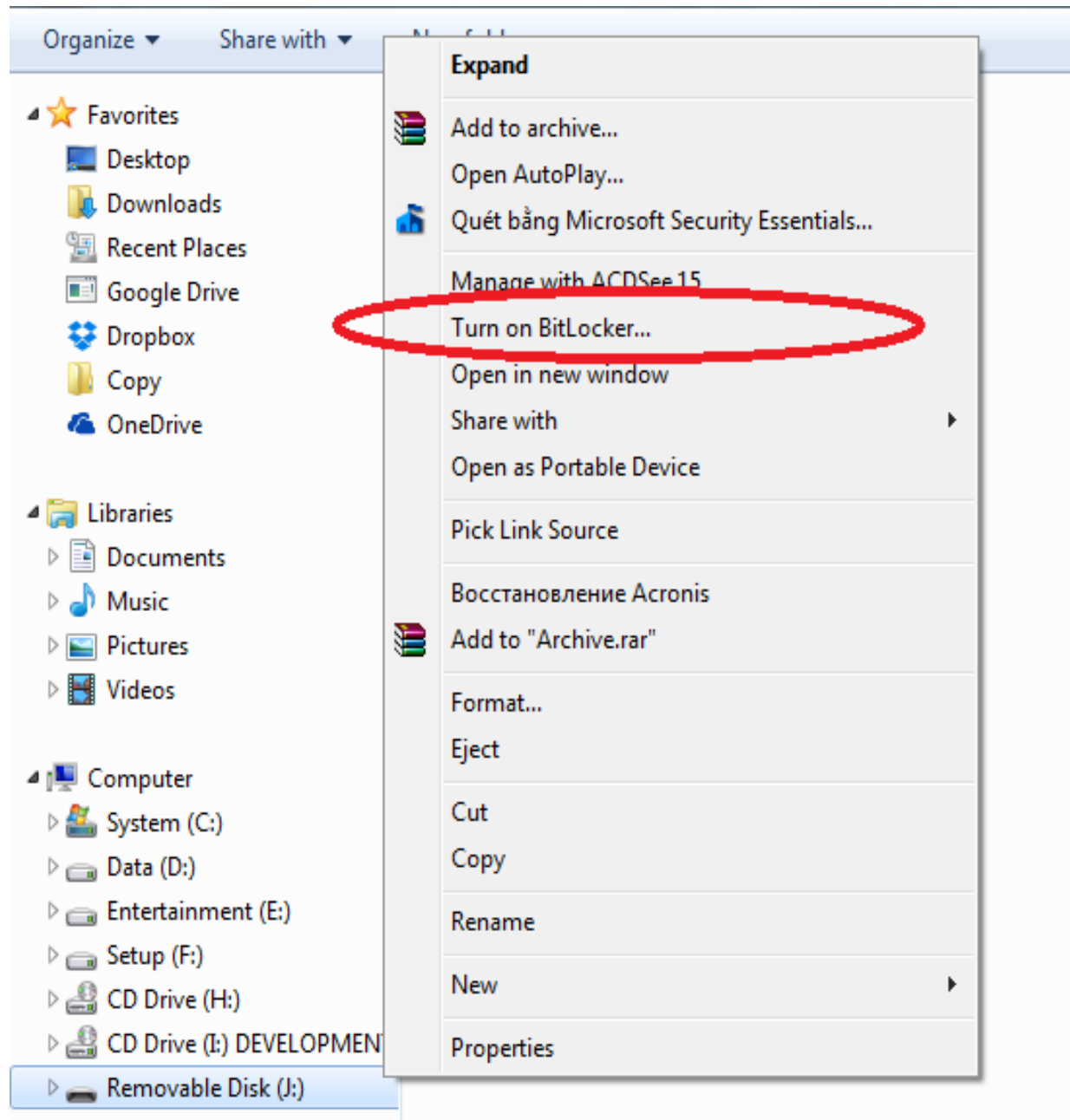
Mã hóa ổ đĩa

	Mã nguồn mở	Mã hóa đĩa ảo	Mã hóa đĩa vật lý	Tổ chức đĩa ảo
BitLocker			✓	
R-Crypto		✓		file
TrueCrypt	✓	✓	✓	file
FreeOTFE	✓	✓		file
Vera	✓	✓	✓	file
BoxCryptor		✓		Thư mục

Công cụ BitLocker của Windows

- ❑ BitLocker là phần mềm mã hóa ổ đĩa trong suốt (Windows Vista, Windows 7 trở về sau)
- ❑ Thuật toán: mặc định AES-128, có thể cấu hình để sử dụng AES-256
- ❑ Chức năng: bảo mật dữ liệu khi vật mang bị đánh cắp (khi đối phương có được mức tiếp cận vật lý)
- ❑ So sánh: EFS chỉ mã hóa file và thư mục
- ❑ Khóa bảo vệ: mật khẩu, smartcard

Công cụ BitLocker của Windows



Thông số kỹ thuật của VERA

❑ Thuật toán mật mã

- AES, Serpent, Twofish
- AES-Twofish, AES-Twofish-Serpent, Serpent-AES, Serpent-Twofish-AES and Twofish-Serpent

❑ Chế độ

❑ Dẫn xuất

- PBKDF2

- RIPEMD-160, SHA-256, SHA-512, Whirlpool

- Salt: 512 bit

- Bước lặp: $327,661 \div 655,331$ (tùy hàm băm)

VERA hỗ trợ nhiều thuật toán mã hóa hơn so với BitLocker

Mã hóa dữ liệu lưu trữ

- Hệ quản trị tập tin mật mã EFS
- Mã hóa ổ đĩa
- **Mã hóa dữ liệu khi đồng bộ qua đám mây**



BoxCryptor

- ☐ Định hướng mã hóa dữ liệu được đồng bộ qua đám mây
- ☐ Thuật toán mật mã: AES-256, RSA
- ☐ Mã hóa cả tên file (phiên bản thương mại)

Các dạng đảm bảo tính bí mật

Mã hóa dữ
liệu lưu trữ

Mã hóa đầu
cuối

Mã hóa
kênh truyền

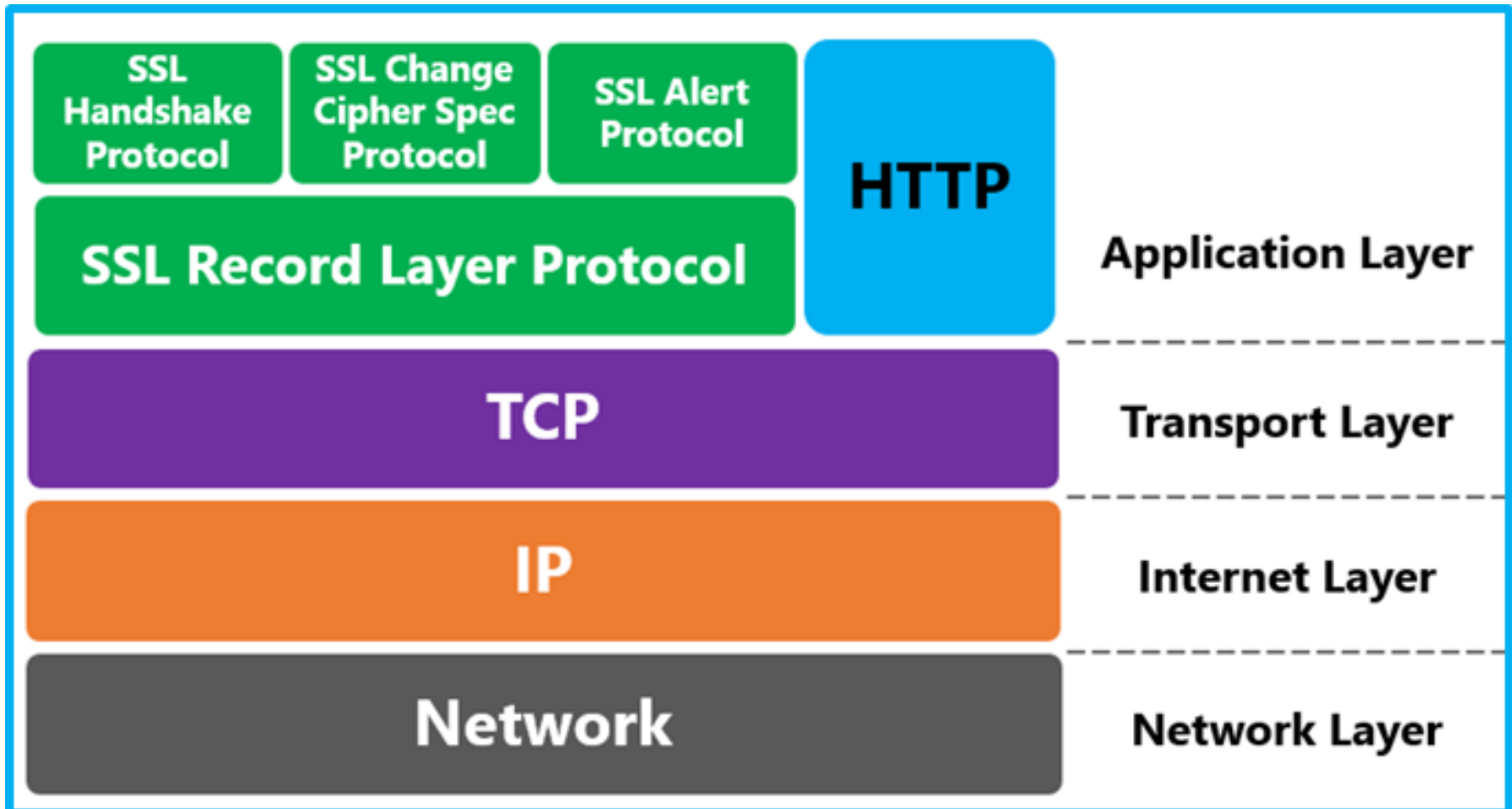
❑ Mã hóa đầu cuối

- Dữ liệu ở các điểm đầu cuối tồn tại ở dạng rõ
- Khi truyền đi, dữ liệu được mã hóa
- Ứng dụng truyền/nhận thực hiện mã hóa/giải mã một cách rõ ràng

❑ Ví dụ

- Mã thoại
- Các giao thức: HTTPS, SSH...

- HTTPS (HTTP over TLS)



- SSH (Secure Shell)

Application Layer	ssh-connection Session multiplexing, X11 and port forwarding, remote command execution, SOCKS proxy, etc.
	ssh-userauth User authentication using public key, password, host based, etc.
	ssh-transport Initial key exchange and server authentication, setup encryption
Transport Layer	TCP
Internet Layer	IP
Network Access Layer	Ethernet

Các dạng đảm bảo tính bí mật

Mã hóa dữ
liệu lưu trữ

Mã hóa đầu
cuối

Mã hóa
kênh truyền

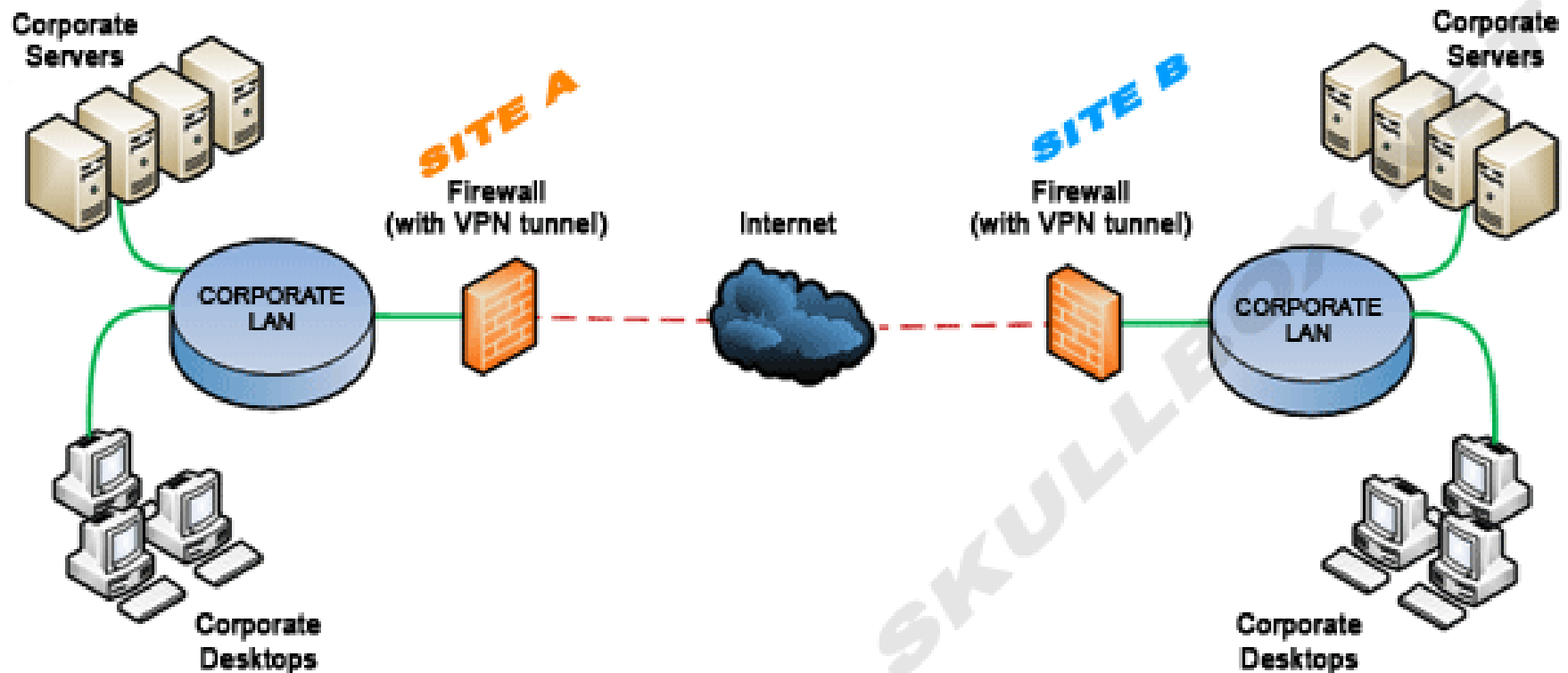
❑ Mã hóa kênh truyền

- Dữ liệu ở các điểm đầu cuối tồn tại ở dạng rõ
- Khi truyền đi, dữ liệu được mã hóa
- Dữ liệu được mã hóa ở tầng mạng hoặc bởi gateway; ứng dụng truyền/nhận không tự mình mã hóa

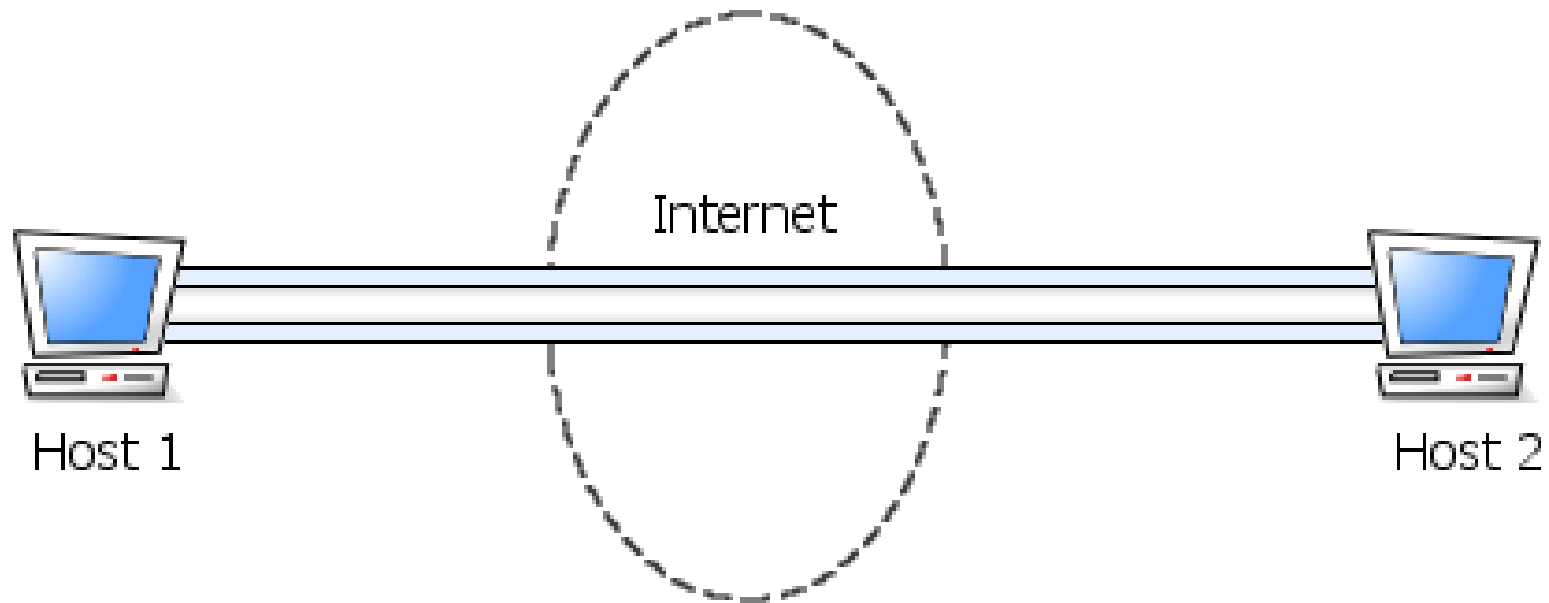
❑ Ví dụ

- Các giao thức VPN

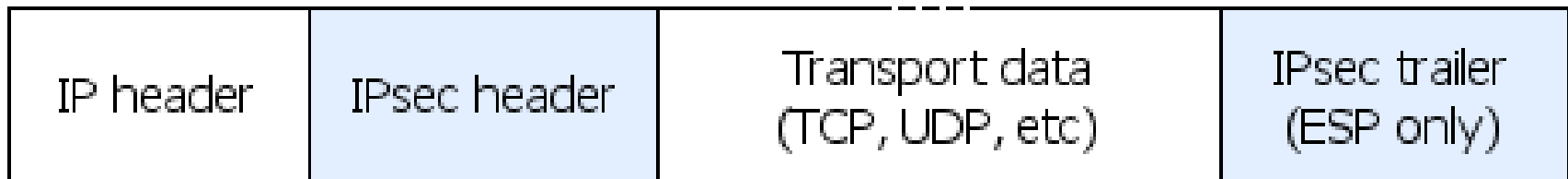
❑ Site-to-Site (Tunnel Mode) VPN



❑ Point-to-Point (Transport Mode) VPN

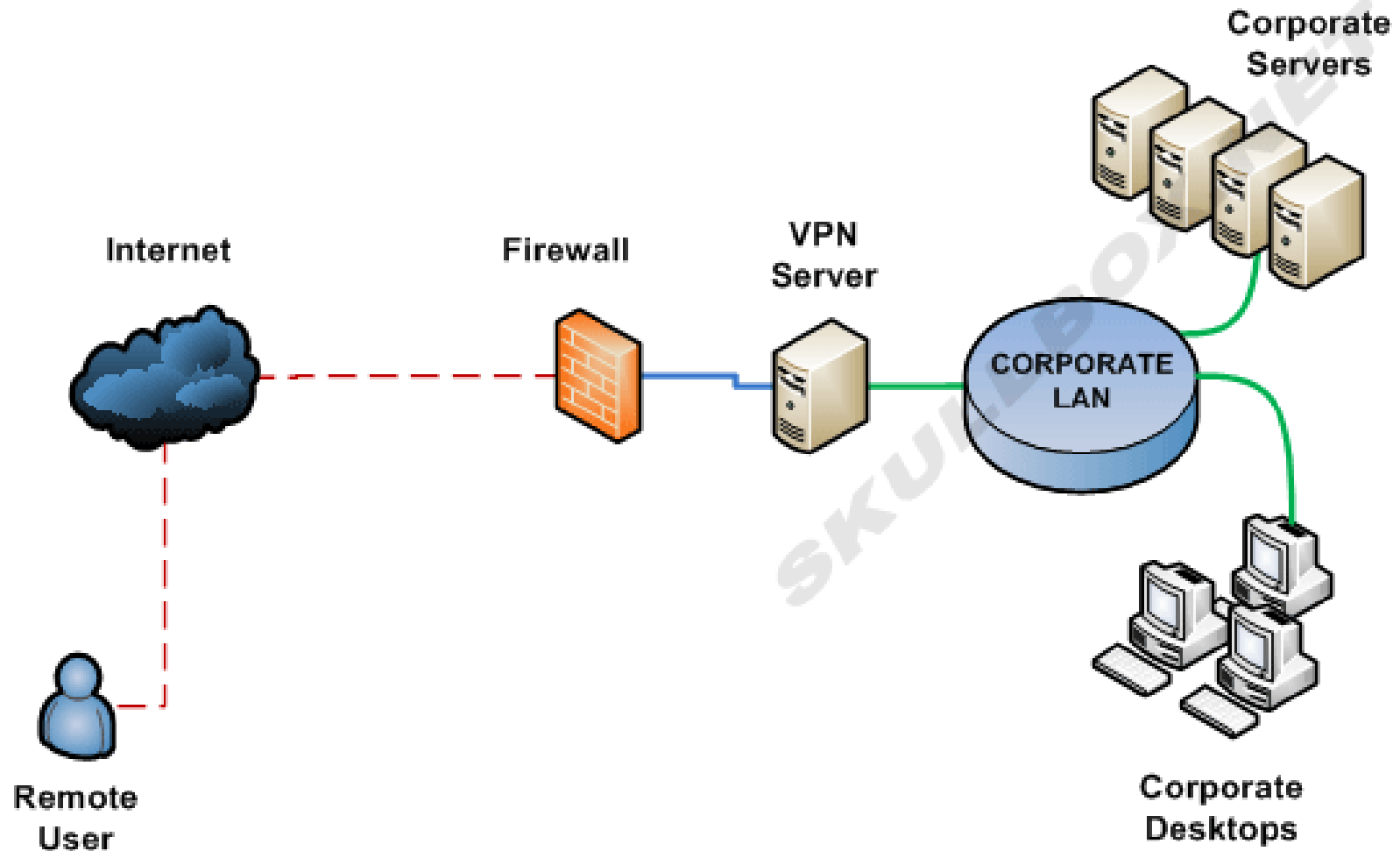


Transport-mode encapsulation:



← encrypted →
← authenticated →

❑ Point-to-Site (Remote Access) VPN



1

Tổng quan về mật mã

2

Đảm bảo tính bí mật

3

Đảm bảo tính toàn vẹn

4

Đảm bảo tính xác thực

5

Xác thực thực thể

Chỉ đảm bảo tính toàn vẹn

- Mã băm kiểm tra tính toàn vẹn (MDC – Manipulation Detection Code)
- Mã xác thực thông điệp (MAC – Message Authentication Code)
- Chữ ký số

Đảm bảo cả tính xác thực

Download Kali Linux Images

We generate fresh Kali Linux image files every few months, which we make available for download. This page provides the links to **download Kali Linux** in it's latest release. For a release history, check our [Kali Linux Releases](#) page.

Image Name	Direct	Torrent	Size	Version	SHA1Sum
Kali Linux 64 bit	ISO	Torrent	3.1G	2.0	aaeb89a78f155377282f81a785aa1b38ee5f8ba0
Kali Linux 32 bit	ISO	Torrent	3.2G	2.0	6e5e6390b9d2f6a54bc980f50d6312d9c77bf30b
Kali Linux 64 bit Light	ISO	Torrent	0.8G	2.0	fc54f0b4b48ded247e5549d9dd9ee5f1465f24ab
Kali Linux 32 bit Light	ISO	Torrent	0.9G	2.0	bd9f8ee52e4d31fc2de0a77ddc239ea2ac813572

❑ Hạn chế của mã kiểm tra toàn vẹn

- Thuật toán tạo MDC là công khai
- Đầu vào không có yếu tố bí mật
- Khi attacker thay đổi dữ liệu thì có thể thay đổi MDC cho phù hợp với dữ liệu mới

1

Tổng quan về mật mã

2

Đảm bảo tính bí mật

3

Đảm bảo tính toàn vẹn

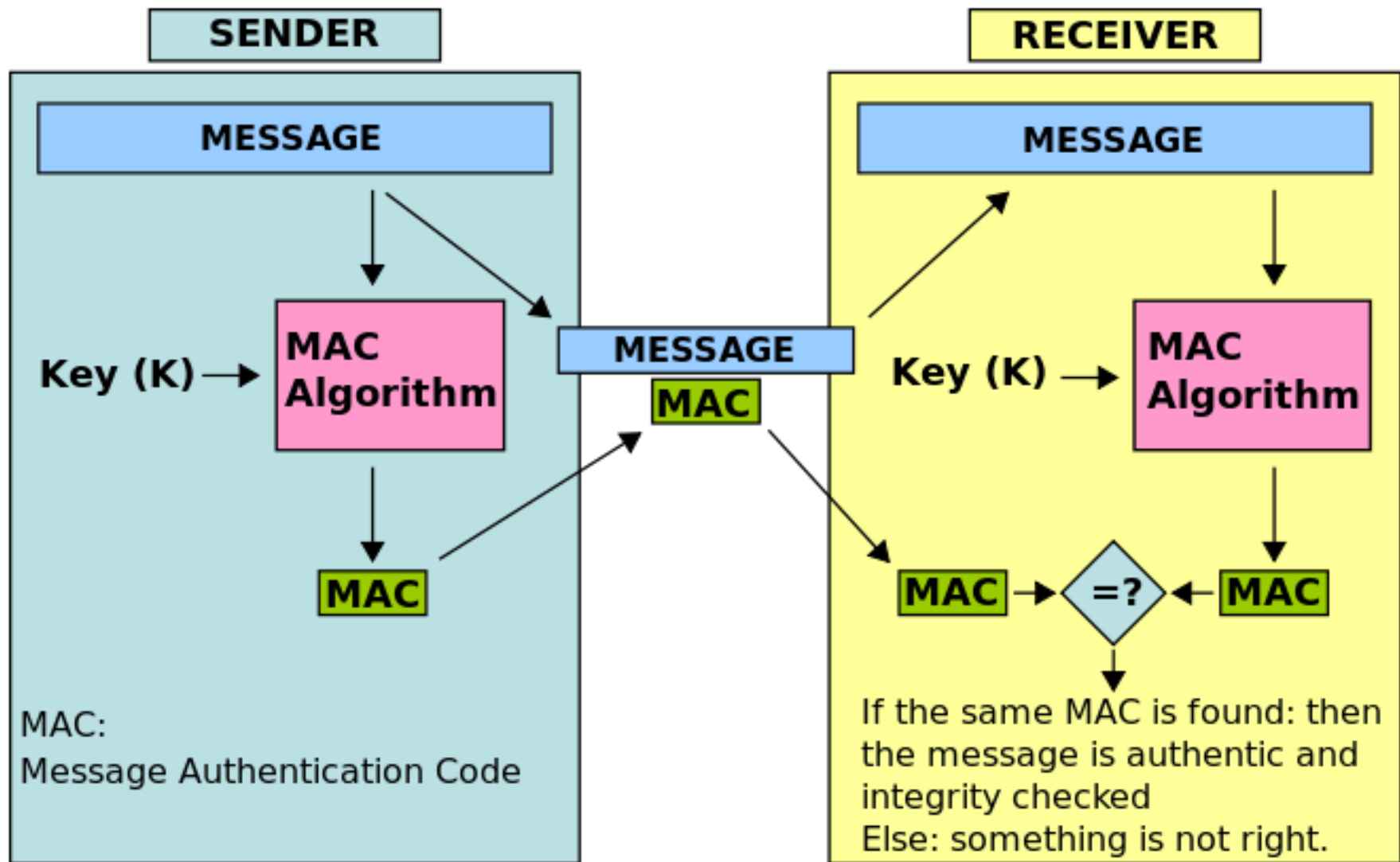
4

Đảm bảo tính xác thực

5

Xác thực thực thể

Đảm bảo tính xác thực



□ Chữ ký số

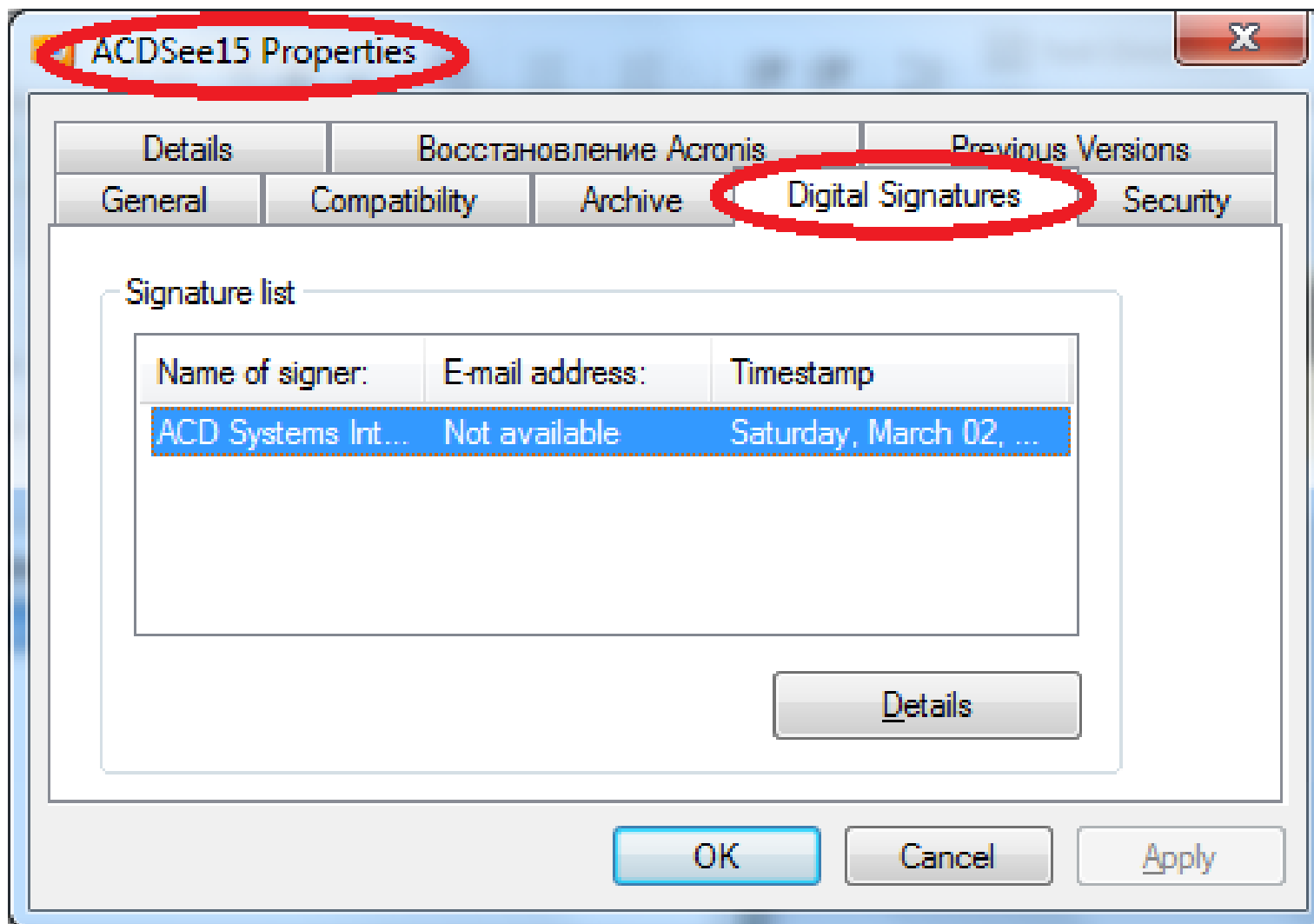
- Có yếu tố bí mật nên đảm bảo tính xác thực
- Yếu tố bí mật chỉ có 1 người biết nên có thể đảm bảo tính **chống chối bỏ**

Đảm bảo tính xác thực

❑ Mã hóa và ký thư điện tử (S/MIME, PGP/MIME)



❑ Ký phần mềm



1

Tổng quan về mật mã

2

Đảm bảo tính bí mật

3

Đảm bảo tính toàn vẹn

4

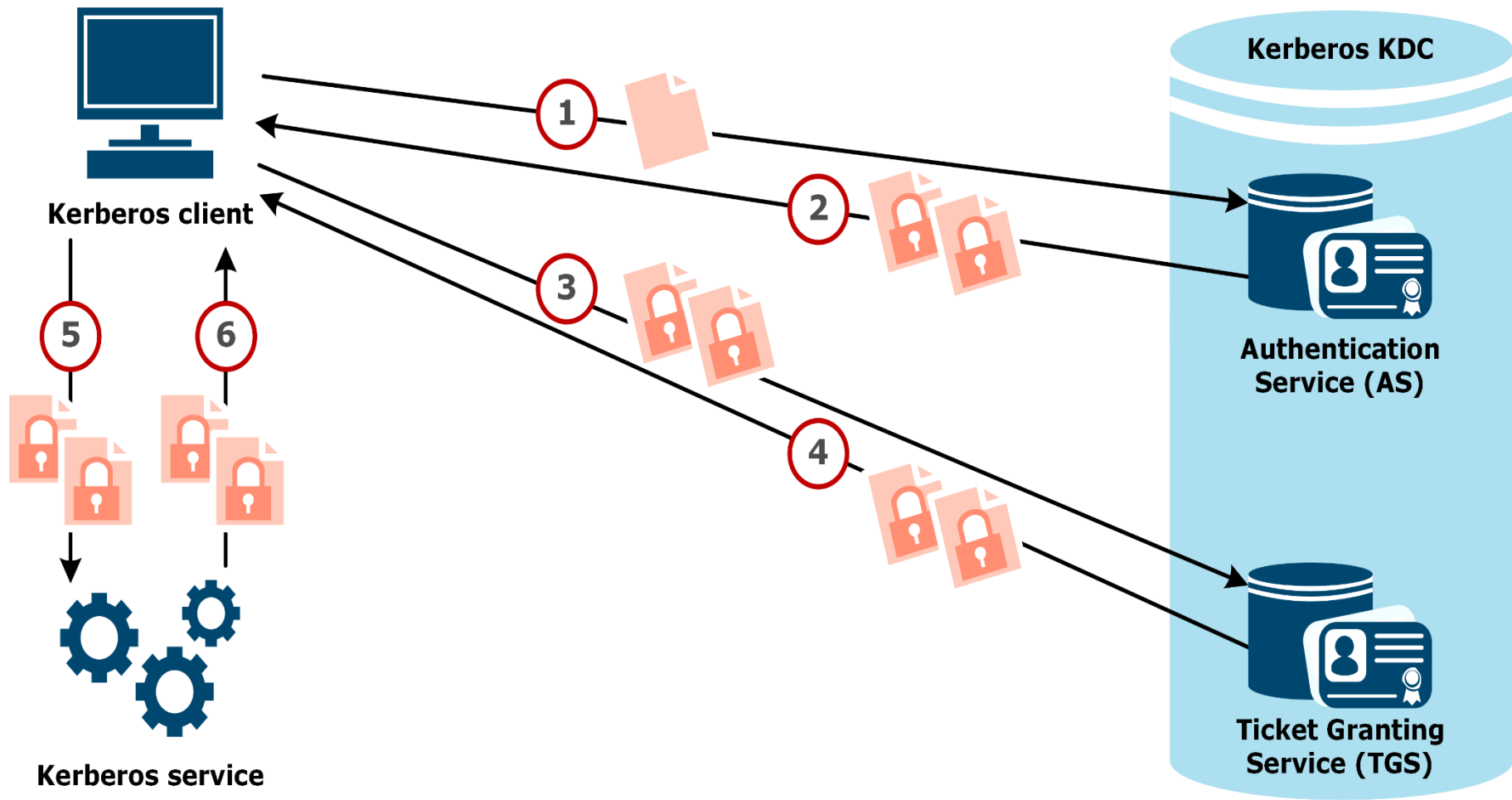
Đảm bảo tính xác thực

5

Xác thực thực thể

❑ Một số giao thức xác thực

- Kerberos
- Challenge-Handshake Authentication Protocol (CHAP)
- Remote Authentication Dial-In User Service (RADIUS)
- NT LAN Manager (NTLM)



RADIUS

- **Remote Authentication Dial-In User Service (RADIUS)** là một giao thức mạng, hoạt động trên cổng mặc định là UDP 1812 cung cấp quản lý xác thực tập trung (Authentication), phân quyền (Authorization) và tính cước (Accounting) (AAA) cho người dùng kết nối và sử dụng dịch vụ mạng. RADIUS được Livingston Enterprises, Inc. phát triển vào năm 1991 dưới dạng giao thức tính cước và xác thực truy cập, sau đó được đưa vào các tiêu chuẩn của Internet Engineering Task Force (IETF).[[]

- RADIUS rất phổ biến, được sử dụng rộng rãi, nó thường được các nhà cung cấp dịch vụ Internet (ISP) và doanh nghiệp sử dụng để quản lý truy cập Internet hoặc mạng nội bộ, mạng không dây và dịch vụ email tích hợp. Các mạng này có thể kết hợp modem, đường dây thuê bao kỹ thuật số (DSL), điểm truy cập, mạng riêng ảo (VPN), cổng mạng, máy chủ web, v.v.

