TRƯỜNG ĐẠI HỌC BÁCH KHOA HÀ NỘI
HANOI UNIVERSITY OF SCIENCE AND TECHNOLOGY

AN NINH MẠNG

TS. Lê Xuân Thành
Bộ môn Kỹ thuật Máy tính, Viện CNTT&TT
thanh.lexuan@hust.edu.vn
0906755789

Chương 4
Căn bản về mật mã

Lê Xuân Thành
Bộ môn Kỹ thuật Máy tính, Viện CNTT&TT
lxthanh@gmail.com
0906755789

MỤC TIÊU

- **Cung cấp cho người học một cái nhìn tổng quan về mật mã và ứng dụng của mật mã trong an ninh mạng.**
- **Sau khi hoàn tất chương, sinh viên có những khả năng:**
  - **Trình bày được khái niệm về mật mã.**
  - **Phân biệt được các giải thuật dùng trong mật mã như giải thuật băm, đối xứng và bất đối xứng.**
  - **Trình bày được ứng dụng của mật mã trong an ninh mạng.**
  - **Hiểu được khái niệm cơ sở hạ tầng khóa công khai (PKI).**
  - **Trình bày được khái niệm chữ ký số, chứng chỉ số và việc quản lý chữ ký điện tử và chứng chỉ số.**

KHÁI NIỆM VỀ MẬT MÃ

- **Mật mã (cryptography)**

Mật mã là 1 nghệ thuật làm biến đổi dữ liệu gốc và sau đó sẽ khôi phục lại để sử dụng trong tương lai.

Đầu vào là dữ liệu gốc (plaintext)

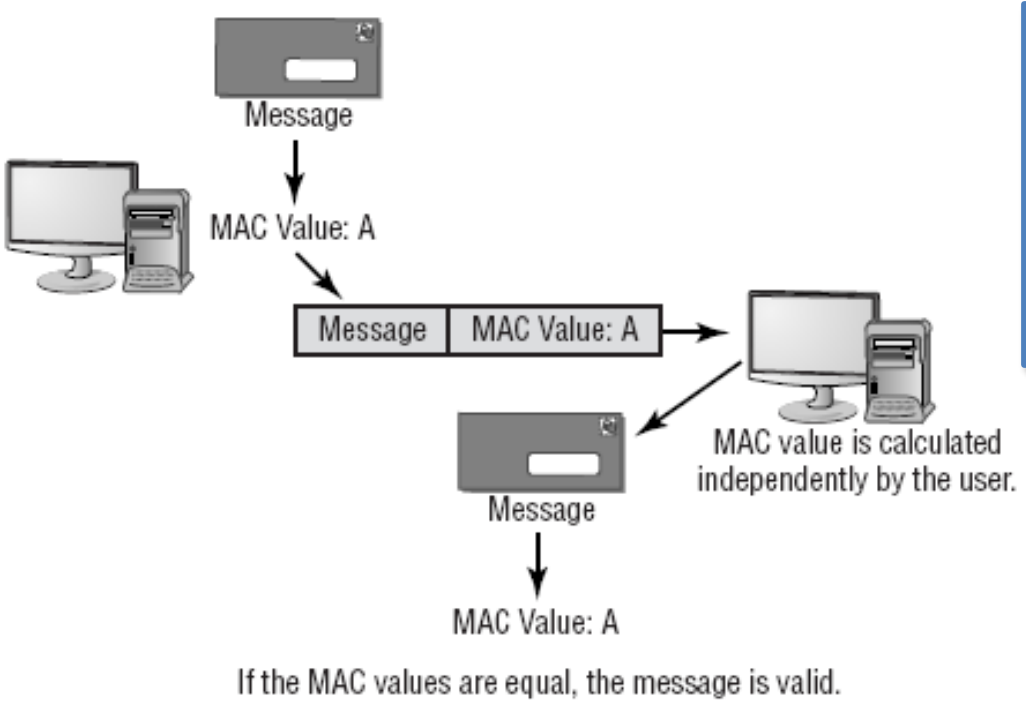
Đầu ra là dữ liệu đã mã hóa (ciphertext)

Khóa (dưới nhiều dạng khác nhau) luôn được yêu cầu

Mật mã sử dụng các giải thuật :
- Băm (hashing)
- Mã hóa đối xứng (symmetric)
- Mã hóa bất đối xứng (Asymmetric)

CÁC GIẢI THUẬT TRONG MẬT MÃ

- **Giải thuật băm (hashing)**



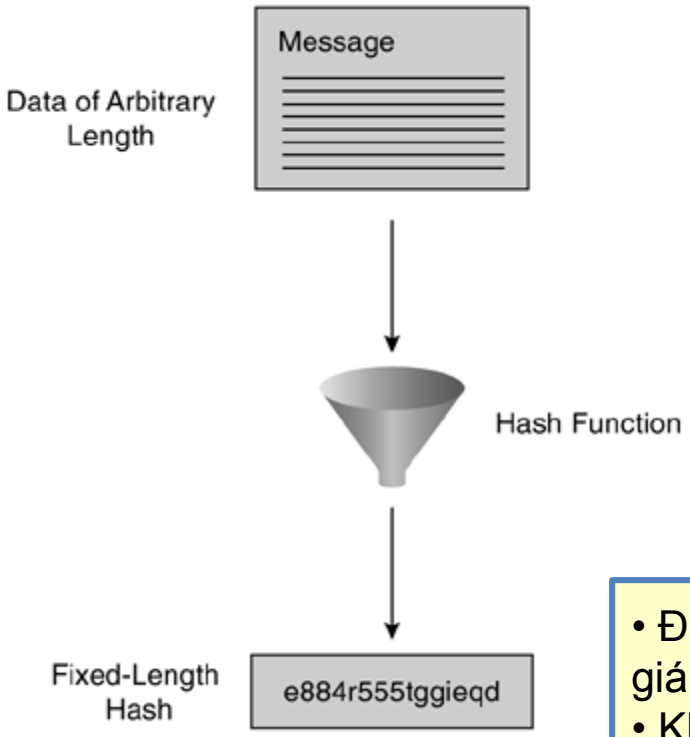
• Băm dùng để tạo ra "dấu vân tay" (MAC-message authentication code hay **message digest**) của dữ liệu.
• Giá trị này được gửi kèm với dữ liệu để nơi nhận **kiểm tra tính toàn vẹn dữ liệu**.

Các giải thuật băm:
• Message-Digest 5(MD5)
• Secure Hash Algorithm 1 (SHA-1)

Băm (hashing) công dụng **không** phải là mã hóa (encryption)

CÁC GIẢI THUẬT TRONG MẬT MÃ

- **Giải thuật băm MD5**



• Được phát minh bởi Ron Rivest của RSA Security.
• Mô tả trong RFC-1321

MD5 thường dùng để kiểm tra phần checksum của những phần mềm cho phép download từ Internet nhằm đảm bảo đó không phải là phần mềm giả mạo.

• Đầu ra của MD5 luôn là 1 digest có giá trị **128 bits** hay 32 ký tự Hex.
• Không thể "dịch ngược" lại được dữ liệu gốc từ digest của MD5.

CÁC GIẢI THUẬT TRONG MẬT MÃ

- **Giải thuật băm SHA-1**

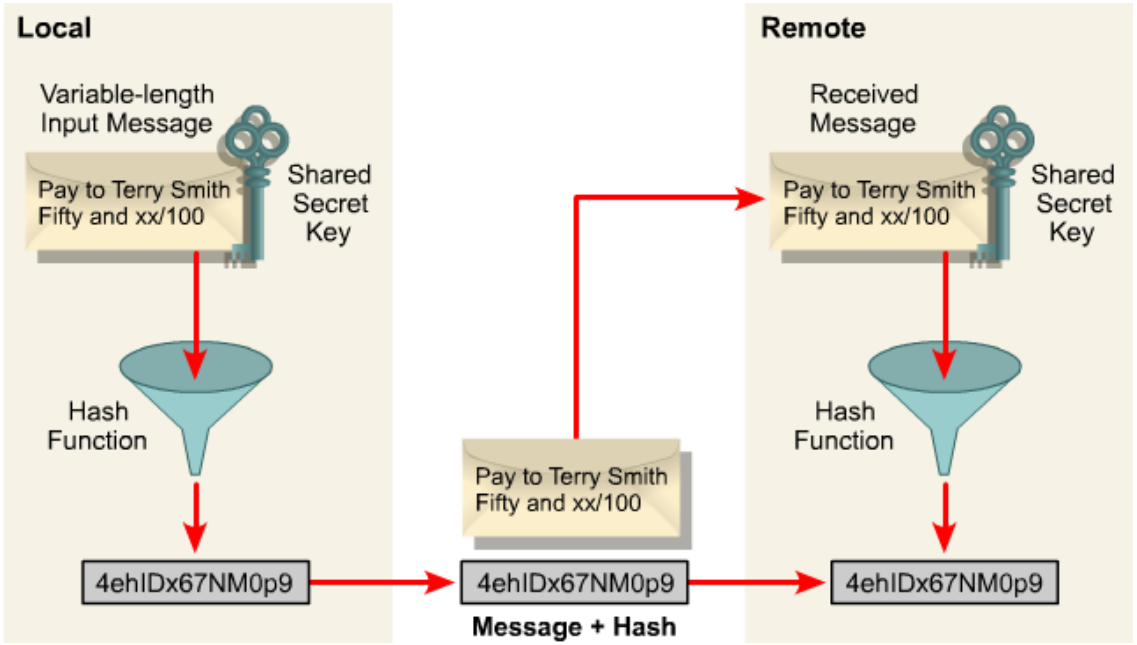
• Được tạo ra bởi chính phủ Mỹ (NIST và NSA).
• Mô tả trong RFC-3174
• Khắc phục điểm yếu trong MD5.

SHA-1 thông thường được sử dụng trong việc cài đặt IPSec.

• Đầu ra của SHA luôn là 1 digest có giá trị **160 bits**.
• Bảo mật hơn MD5

CÁC GIẢI THUẬT TRONG MẬT MÃ

- **Giải thuật băm HMAC**



Các giải thuật băm có điểm yếu khi gặp dạng tấn công "Kẻ đứng giữa" (Man-in-the-middle): giả mạo dữ liệu và cả digest gửi kèm.

HMACs đưa vào thêm 1 khóa bí mật trước khi dùng giải thuật băm:
Data + key => Digest

- Cơ chế dùng thêm khóa bí mật gọi là "Message Authentication Codes" (MAC).
- Khóa bí mật chỉ được biết bởi người gửi và người nhận.
- Dùng HMAC với 2 giải thuật băm chính:
  - HMAC + MD5 = HMAC-MD5 sử dụng khóa 128 bits
  - HMAC + SHA-1 = HMAC-SHA-1 sử dụng khóa 160 bits

CÁC GIẢI THUẬT TRONG MẬT MÃ

- **Giải thuật mã hóa (encryption algorithms)**

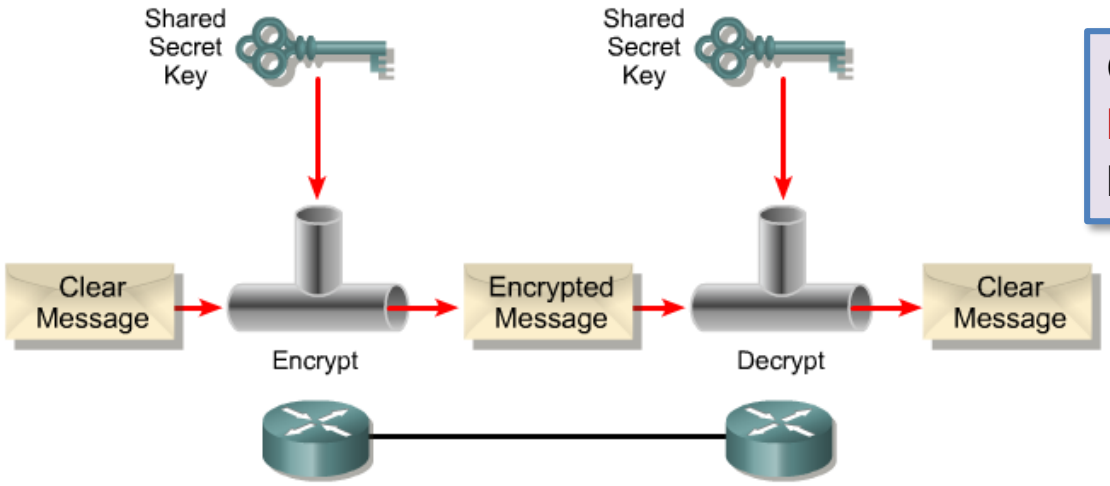
• Mã hóa là 1 hình thức của mật mã
• Mã hóa tạo ra sự bí mật (bảo mật) cho dữ liệu khi lưu trữ hay truyền đi trên mạng.

• Mã hóa sử dụng những giải thuật để biến đổi dữ liệu gốc (plaintext) sang dạng dữ liệu không thể hiểu được (ciphertext).
• Các giải thuật mã hóa dùng khóa (key) để mã hóa và giải mã.
• Khóa càng dài => bảo mật càng cao.

Có 2 dạng mã hóa:
• Đối xứng (*symmetric key encryption*): sử dụng chung 1 khóa cho mã hóa và giải mã.
• Bất đối xứng (A*symmetric key encryption*): sử dụng 2 khóa
  - 1 khóa cho mã hóa
  - 1 khóa cho giải mã

CÁC GIẢI THUẬT TRONG MẬT MÃ

- **Giải thuật mã hóa đối xứng (Symmetric)**



Còn gọi là "mã hóa với **khóa bí mật**" hay "mã hóa với khóa chia sẻ"

- Có thể bị các tấn công "vét cạn" để tìm ra khóa.
- Có tốc độ nhanh và cài đặt đơn giản hơn so với mã hóa bất đối xứng.
- SSL sử dụng mã hóa đối xứng.

Một số giải thuật mã hóa đối xứng:
- Data Encryption Standard (DES)
- Triple Data Encryption Standard (3DES)
- Advanced Encryption Standard (AES)
- International Data Encryption Algorithm (IDEA)
- Twofish
- Carlisle Adams/Stafford Tavares (CAST)

CÁC GIẢI THUẬT TRONG MẬT MÃ

- **Giải thuật mã hóa DES**

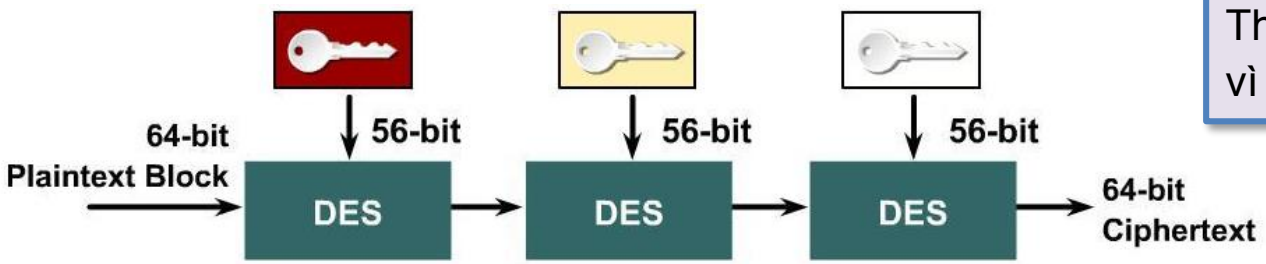
• Phát triển từ thuật toán Lucifer của Horst Feistel (IBM).
• Được chuẩn hóa năm 1976.

• Mã hóa từng khối dữ liệu 64 bits.
• Độ dài khóa 64 bits: **56 bits** cho khóa và 8 bits cho kiểm tra (parity).
• Dữ liệu được chia làm 2 (32 bits) xử lý qua 16 chu trình (mạng Feistel).
• Mỗi hàm Feistel thực thi sẽ sử dụng 1 khóa con 48 bits (tính ra từ khóa chính 56 bits).

•Giải thuật được sử dụng rộng rãi vì tốc độ mã hóa nhanh,
• Hiện nay, DES được xem là không đủ an toàn vì độ dài khóa ngắn (56bits) => chuyển qua dùng 3DES

CÁC GIẢI THUẬT TRONG MẬT MÃ

- **Giải thuật mã hóa 3DES**

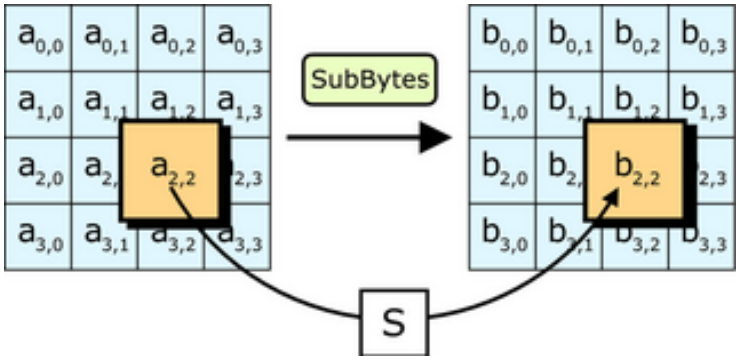


Thay thế dần cho DES vì an toàn hơn

- Dùng 3 lần liên tiếp thuật toán DES với **3 khóa khác nhau** K1, K2 và K3.
- Khóa sử dụng = 3 x 56 bits = **168 bits**
- Gần như không thể dò tìm được khóa bằng phương pháp vét cạn.
- Phiên bản khác là 2TDES có khóa là 112 bits vì sử dụng khóa K1=K3.
- Tốc độ thực thi chậm nên được thay thế dần bởi thuật toán AES.

CÁC GIẢI THUẬT TRONG MẬT MÃ

- **Giải thuật mã hóa AES**



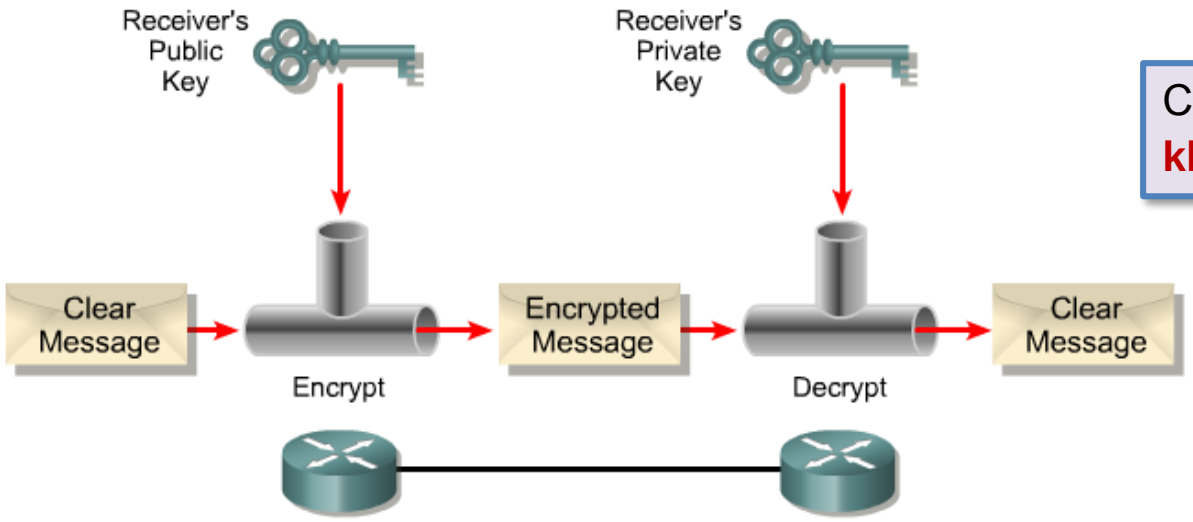
• Được phát triển bởi 2 nhà mật mã người Bỉ Joan Daemen và Vincent Rijmen, lấy tên là thuật toán Rijndael.
• Tạm dịch là "Tiêu chuẩn mã hóa tiên tiến"

• Sử dụng thuật toán thay thế hoán vị.
• Khối dữ liệu 128 bits.
• Khóa **128**, **192** hoặc **256** bits.
• Số chu trình thực hiện là 10, 12 hoặc 14 tùy theo độ dài khóa.

• Được sử dụng phổ biến vì dễ thực hiện, tốc độ cao và ít tốn bộ nhớ.
• Được Mỹ áp dụng làm tiêu chuẩn mã hóa vào tháng 5 năm 2002.

CÁC GIẢI THUẬT TRONG MẬT MÃ

- **Giải thuật mã hóa bất đối xứng (Asymmetric)**



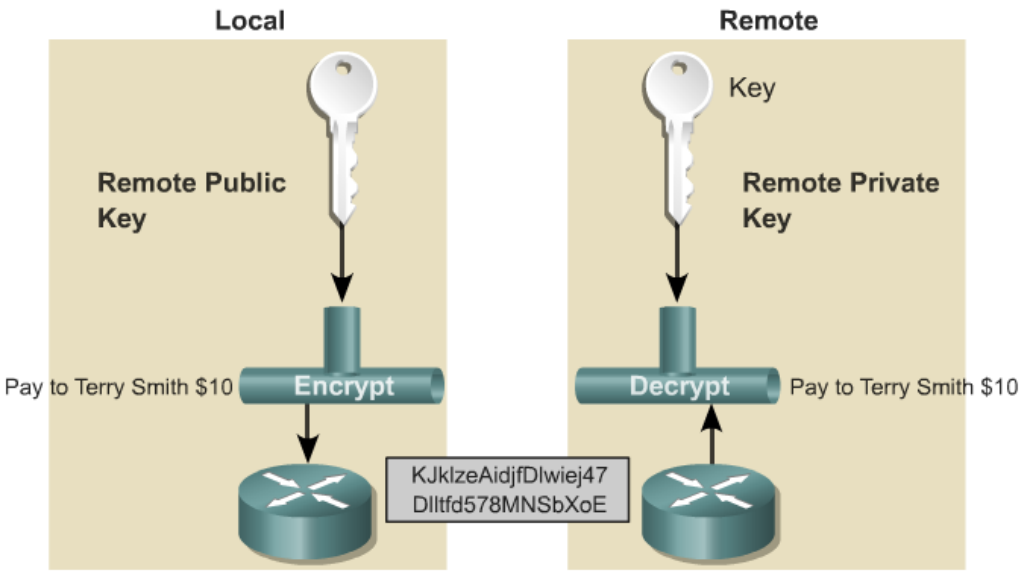
Còn gọi là "mã hóa với **khóa công khai**"

• Dùng khóa công khai để mã hóa và dùng khóa bí mật để giải mã lại.
• Khóa bí mật được lưu giữ cẩn thận, khóa công khai công bố cho mọi người.
• Giải thuật thực thi chậm.

Một số giải thuật mã hóa bất đối xứng:
• RSA (Rivest Shamir Adleman)
• DSA (Digital Signature Algorithm)
• DH (Diffie-Hellman)
• ECC (Error Correcting Code)
• El Gamal

CÁC GIẢI THUẬT TRONG MẬT MÃ

- **Giải thuật mã hóa RSA**



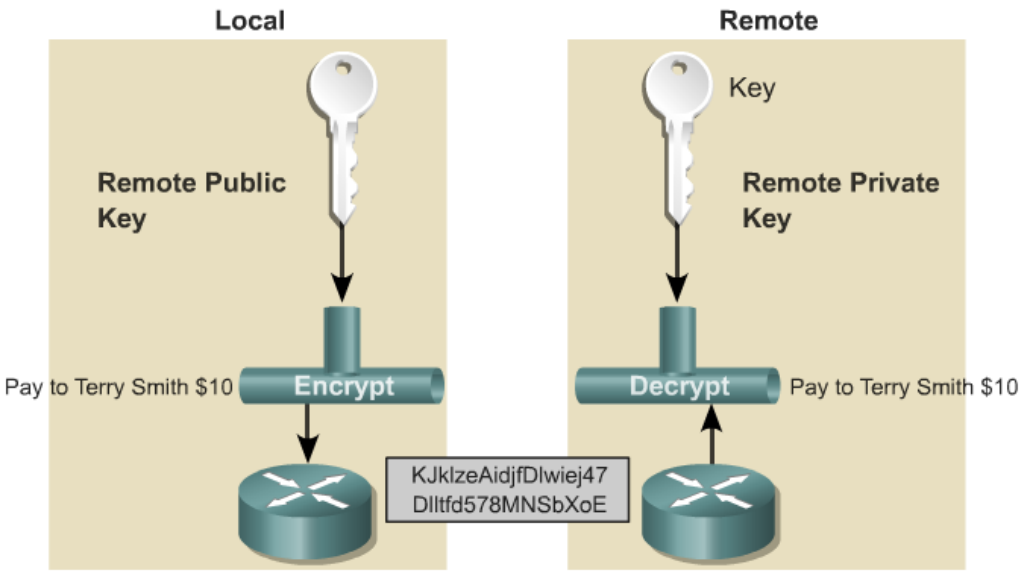
• Được phát minh vào năm 1977 bởi Rivest, Shamir và Adleman tại MIT.
• Mã hóa dữ liệu: dùng khóa chung (public key) để mã hóa, khóa riêng (private key) để giải mã.
• Tạo chữ ký số: khóa riêng để mã hóa, khóa chung để giải mã.

• Khóa có độ dài từ 1024-2048 bits.
• Giải thuật rất phức tạp, sử dụng nhiều công thức toán học.
• Gần như không có một phương pháp nào tìm ngược lại được khóa riêng từ dữ liệu được mã hóa và khóa chung.

• RSA được sử dụng trong IPSec.
• Tốc độ thực thi chậm hơn DES và các giải thuật mã hóa đối xứng khác.

CÁC GIẢI THUẬT TRONG MẬT MÃ

- **Giải thuật mã hóa DSA**



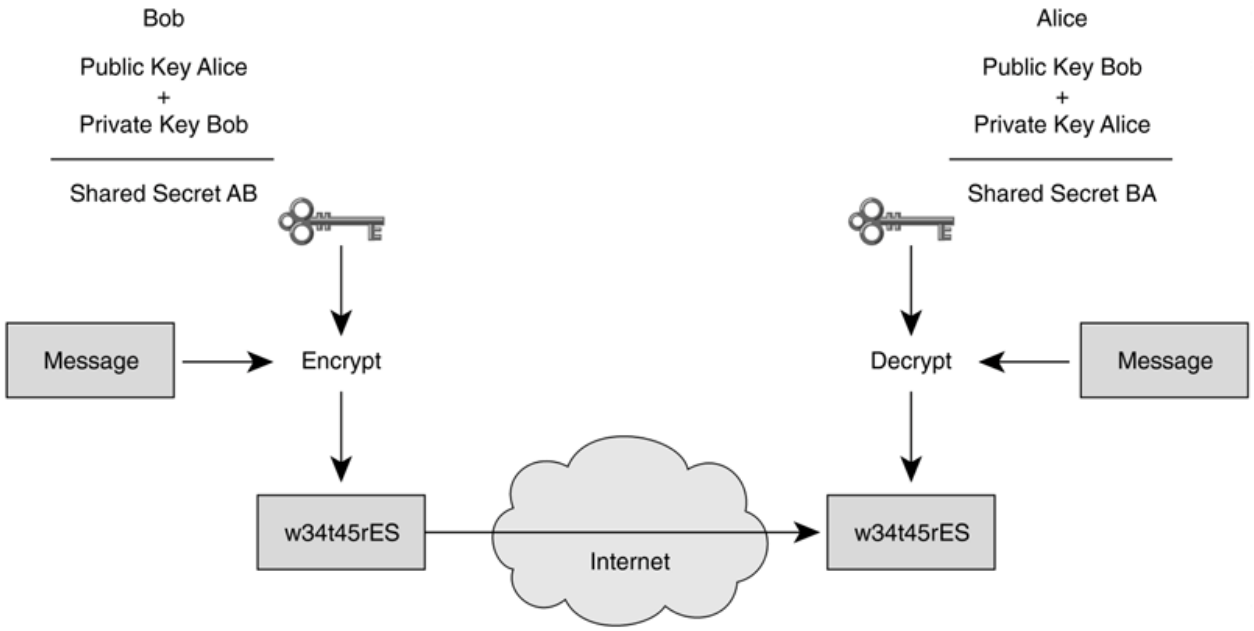
• Được tạo ra bởi NIST vào năm 1994.
• Là chuẩn của chính phủ Mỹ trong việc tạo ra chữ ký điện tử.

•Tốc độ tương đương như RSA khi tạo ra chữ ký số.
• Chậm hơn 10-40 lần khi kiểm tra chữ ký số.

• Sử dụng SHA-1 cho giải thuật băm
• Khóa có độ dài từ 512 – 1024 bits
• Hiện nay, được khuyến cáo nên dùng 2048 bits cho khóa.

CÁC GIẢI THUẬT TRONG MẬT MÃ

- **Giải thuật mã hóa DH (Diffie-Hellman)**

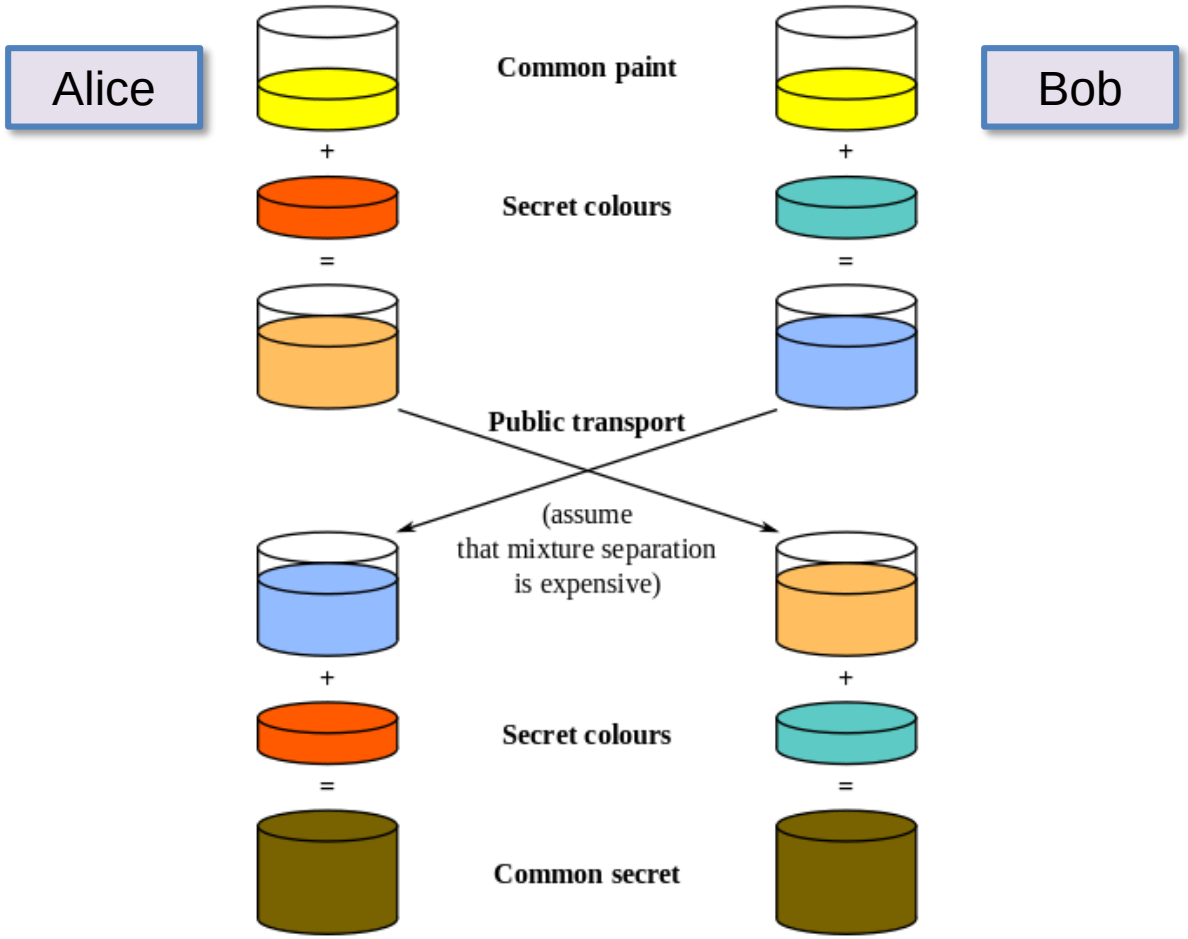


- Được tạo ra năm 1976 bởi Whitfield Diffie và Martin Hellman.
- DH có điểm yếu với dạng tấn công kẻ đứng giữa.
- DH dùng cung cấp cơ chế bảo mật, nhưng **không cung cấp dịch vụ chứng thực**.

Giải thuật DH dùng để tạo ra "Khóa bí mật chia sẻ" (sử dụng cho mã hóa đối xứng) giữa 2 host trên đường truyền không an toàn.

CÁC GIẢI THUẬT TRONG MẬT MÃ

- **Giải thuật mã hóa DH (Diffie-Hellman)**



ỨNG DỤNG CỦA MẬT MÃ

- **Ứng dụng của mật mã trong an ninh mạng**

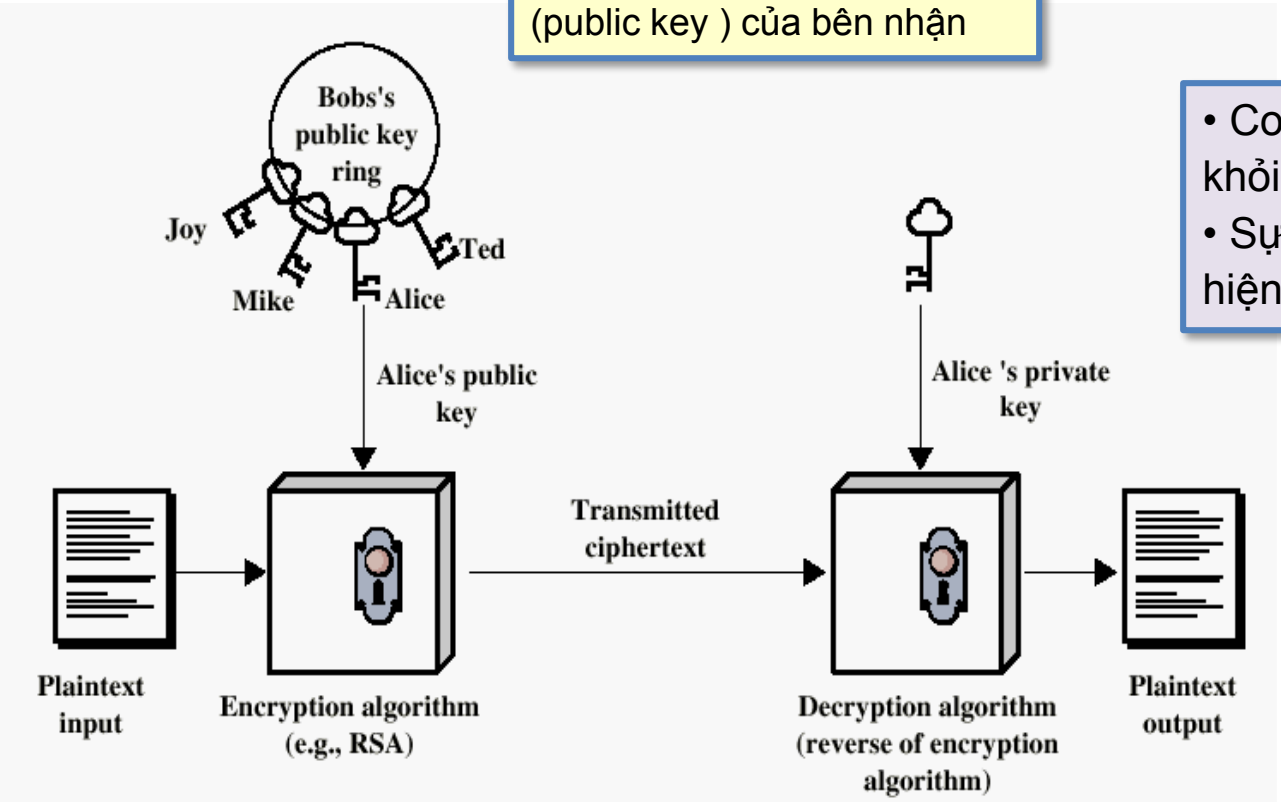
Mật mã có thể được sử dụng trong nhiều dịch vụ an ninh cung cấp các khả năng như:

- Tính bảo mật (confidentiality)
- Tính toàn vẹn (integrity)
- Chứng thực (authentication)
- Tính không thể phủ nhận (nonrepudiation)

ỨNG DỤNG CỦA MẬT MÃ

- **Trong dịch vụ bảo mật**

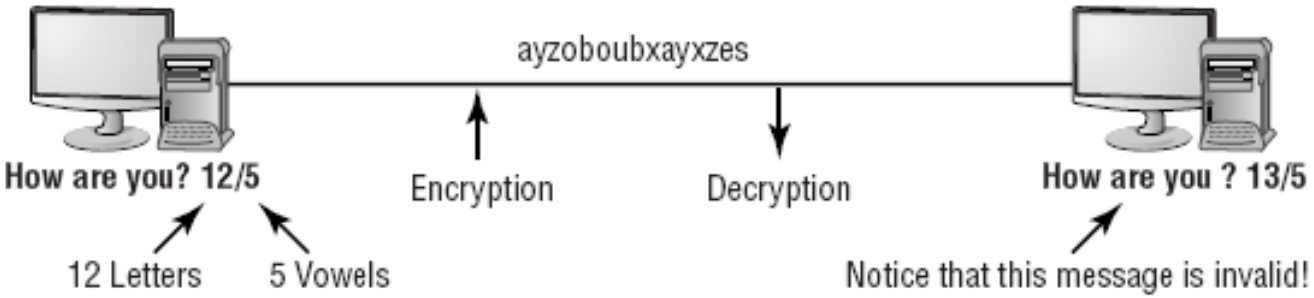
Mã hóa dùng khóa công khai (public key) của bên nhận



- Cơ chế để bảo vệ dữ liệu khỏi sự truy cập trái phép.
- Sự bảo mật được thực hiện thông qua mã hóa.

ỨNG DỤNG CỦA MẬT MÃ

- **Trong dịch vụ toàn vẹn**

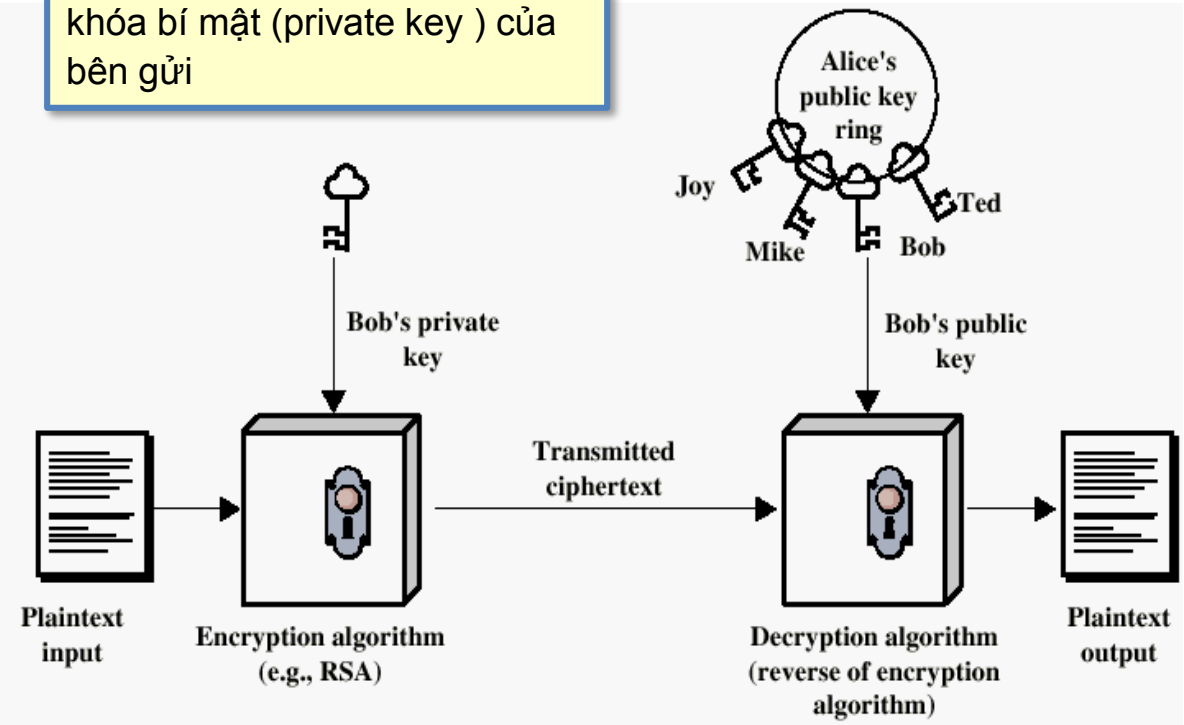


• Cơ chế để có thể kiểm tra được dữ liệu có bị biến đổi hay không.
• Sự dụng giải thuật băm MD5 hay SHA-1.

ỨNG DỤNG CỦA MẬT MÃ

- **Trong dịch vụ chứng thực tại các điểm cuối**

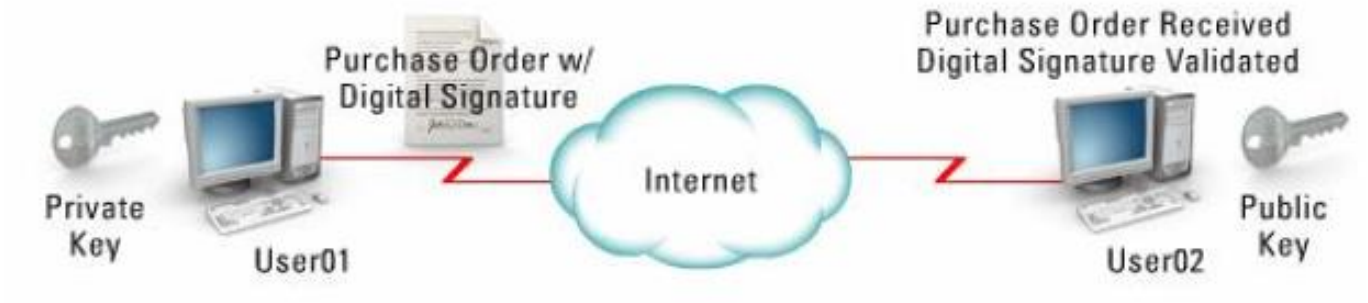
Chứng thực sẽ mã hóa dùng khóa bí mật (private key) của bên gửi



• Chứng thực được thực hiện thông qua việc chấp nhận khóa của thuật toán DH.
• Có 3 cách để chứng thực:
  + Sử dụng khóa bí mật chia sẻ
  + Sử dụng chữ ký số
  + Sử dụng số ngẫu nhiên được mã hóa

ỨNG DỤNG CỦA MẬT MÃ

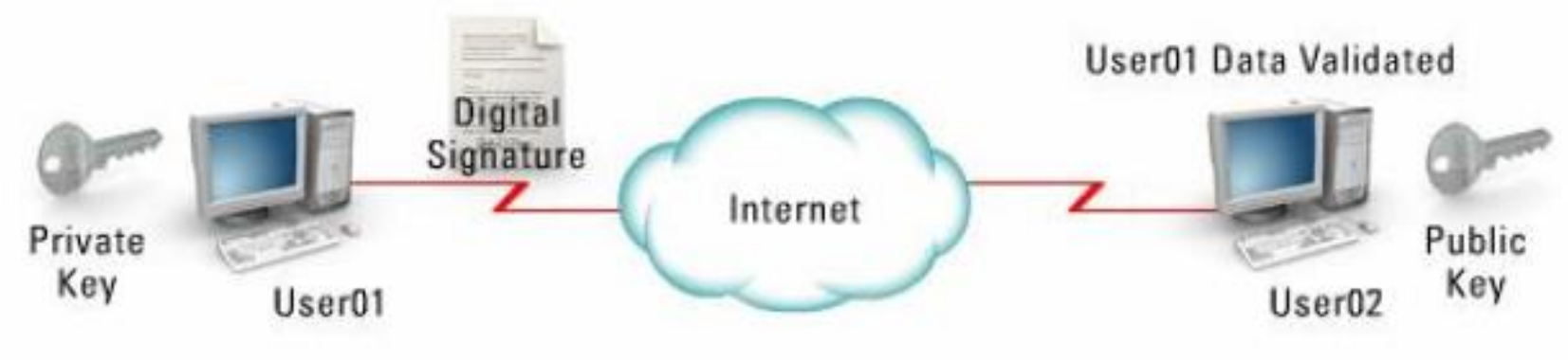
- **Trong dịch vụ không thể phủ nhận (nonrepudiation)**



• Chứng tỏ rằng một thực thể đã làm 1 việc gì và đã được "ký nhận" vào tài liệu. Sau này, thực thể đó không thể chối bỏ được việc làm đó.
• Tính không thể phủ nhận được thực hiện qua chữ ký số.
• Chữ ký số là duy nhất, xác nhận đúng là cá nhân hay thực thể đó.

ỨNG DỤNG CỦA MẬT MÃ

- **Chữ ký số (Digital signature)**



Chữ ký số là thông tin đi kèm theo dữ liệu (văn bản, hình ảnh, video...) nhằm mục đích xác định người chủ của dữ liệu đó.

Chữ ký số là 1 tập con của chữ ký điện tử (electronic signature).

Chữ ký số hoạt động bằng cách sử dụng giải thuật băm và 1 trong 2 dạng:
- Mã hóa đối xứng
- Mã hóa bất đối xứng.

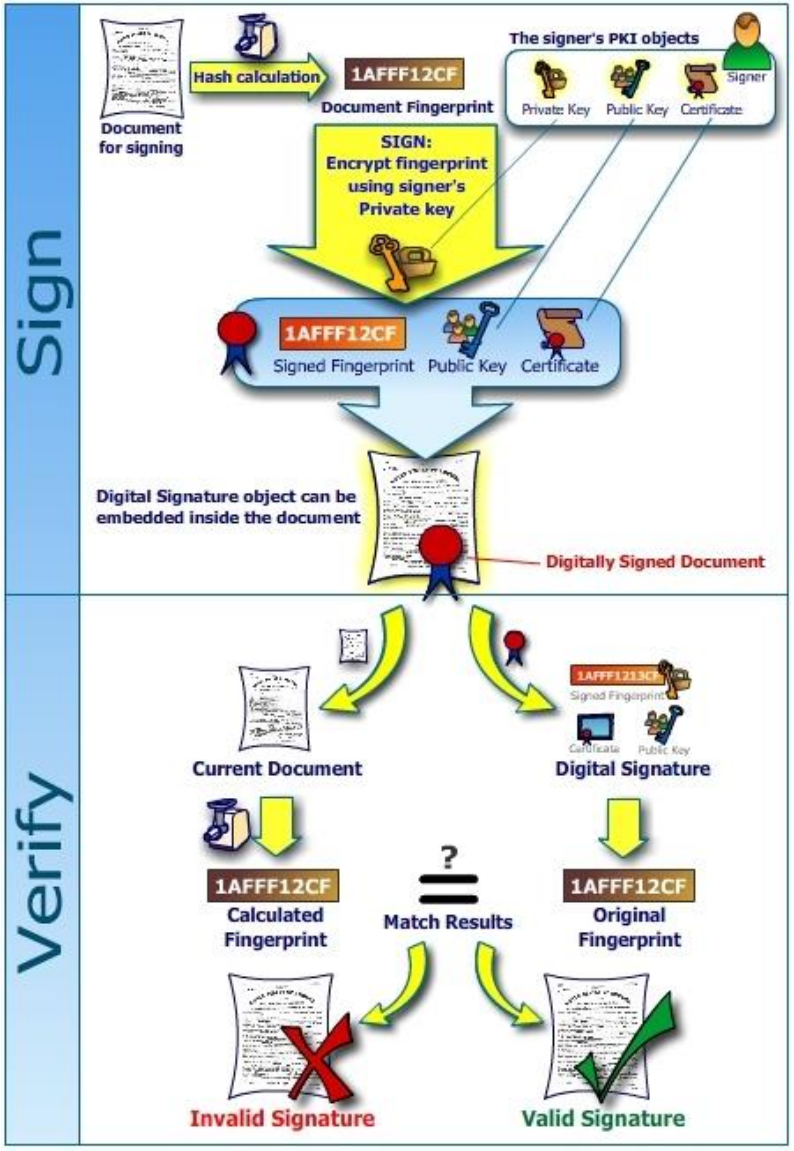
ỨNG DỤNG CỦA MẬT MÃ

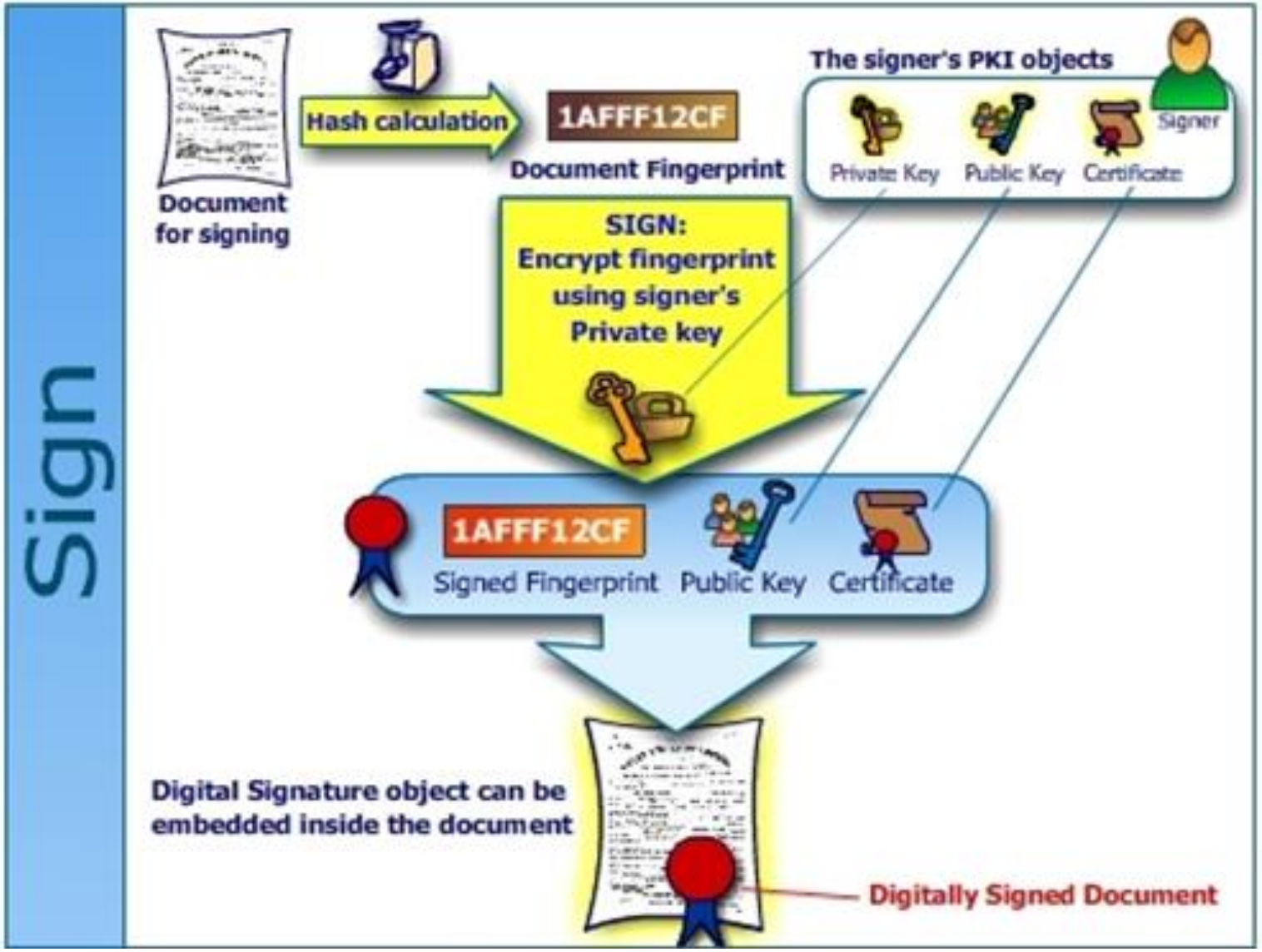
- **Chữ ký số**

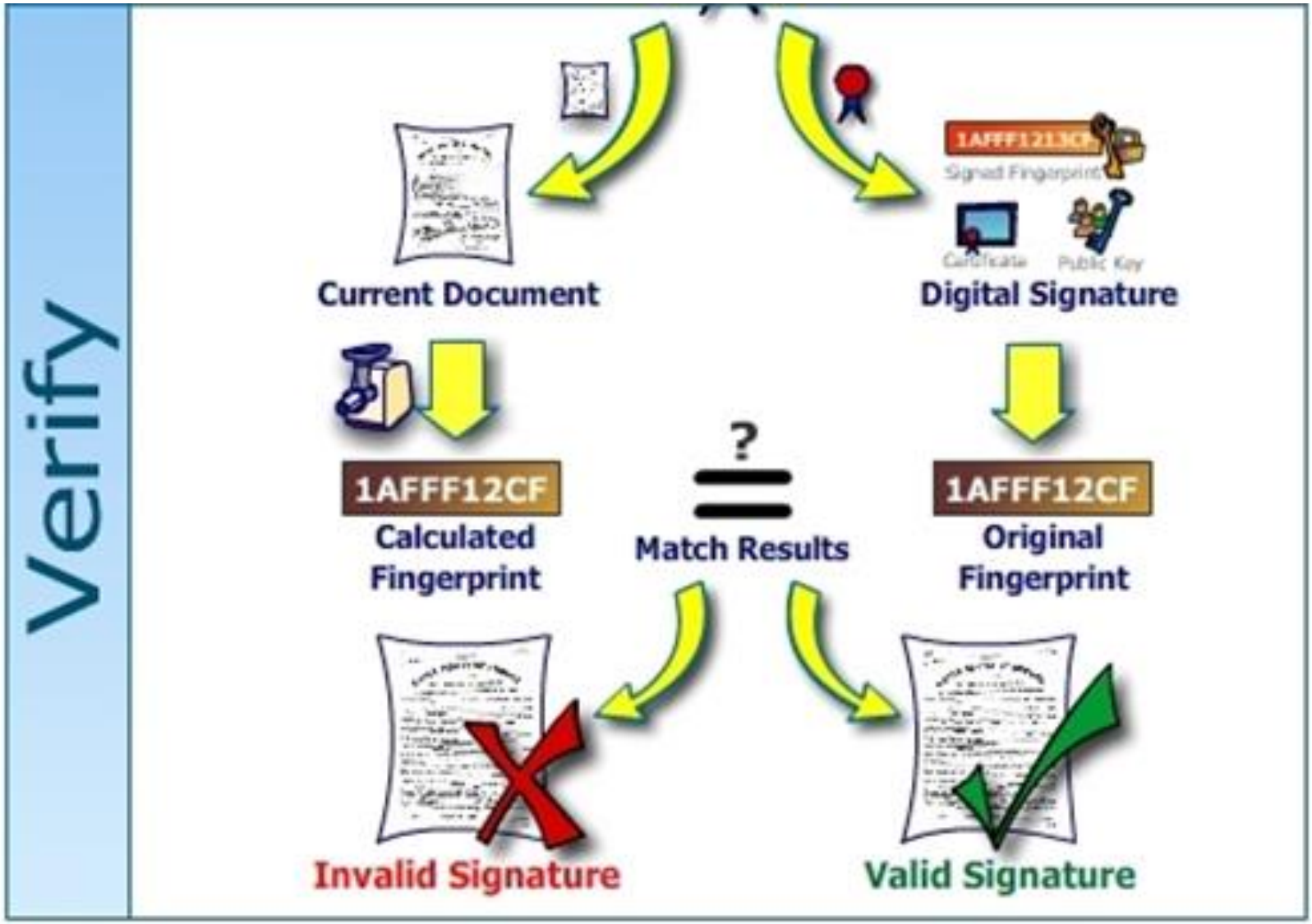
Quá trình sử dụng chữ ký số bao gồm 2 quá trình: tạo chữ ký và kiểm tra chữ ký

1. Người gửi tạo tài liệu
2. Băm tài liệu => tạo ra Digest
3. Sử dụng khóa bí mật để mã hóa số digest đó.
4. Gắn số Digest được mã hóa (chữ ký số) vào tài liệu
5. Gửi qua người nhận

1. Người nhận tách tài liệu và chữ ký số ra
2. Sử dụng khóa công khai để giải mã chữ ký số thành số Digest1.
3. Băm tài liệu => tạo ra số Digest2
4. So sánh 2 số Digest1 và Digest2:
   + Nếu trùng: xác nhận đúng người gửi
   + Nếu sai: không phải




Sign
Document for signing
Hash calculation
1AFFF12CF
Document Fingerprint
The signer's PKI objects
Signer
Private Key
Public Key
Certificate
SIGN:
Encrypt fingerprint using signer's Private key
1AFFF12CF
Signed Fingerprint
Public Key
Certificate
Digital Signature object can be embedded inside the document
Digitally Signed Document


Verify
Current Document
Digital Signature
1AFFF12CF
Calculated Fingerprint
?
Match Results
1AFFF12CF
Original Fingerprint
Invalid Signature
Valid Signature

ỨNG DỤNG CỦA MẬT MÃ

- **Chữ ký số**

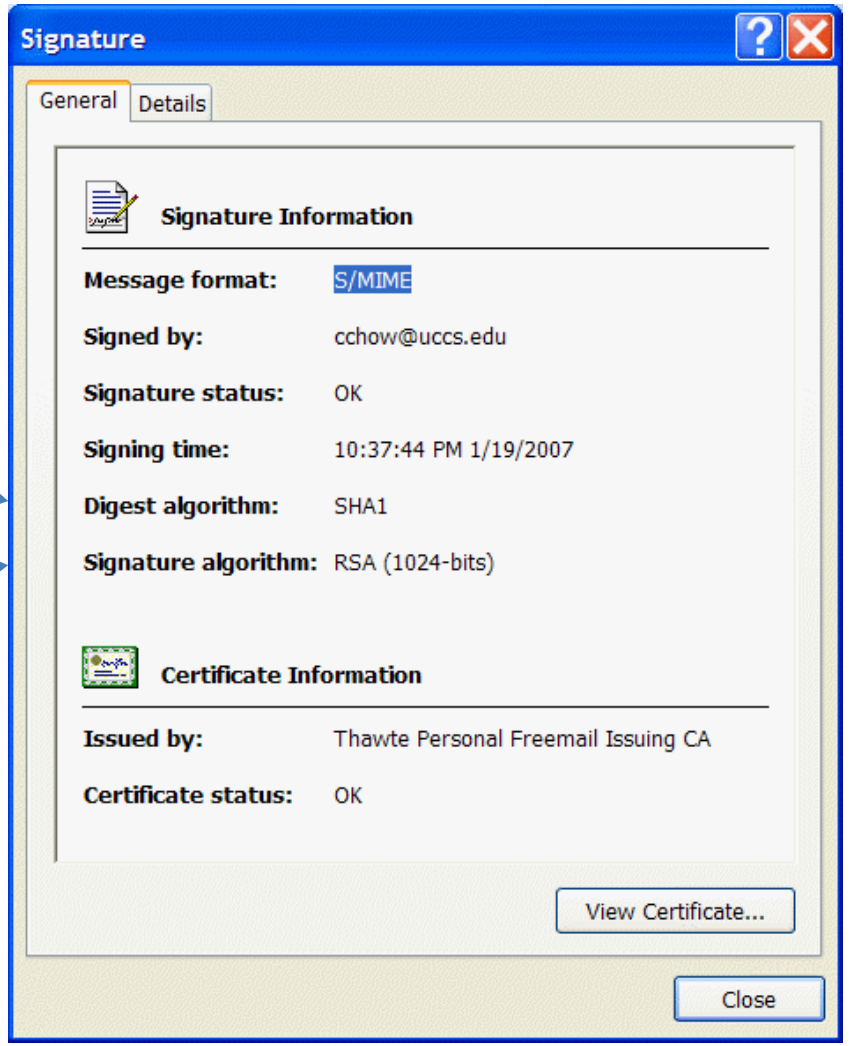
Thông tin của 1 chữ ký số

Người ký

Giải thuật băm

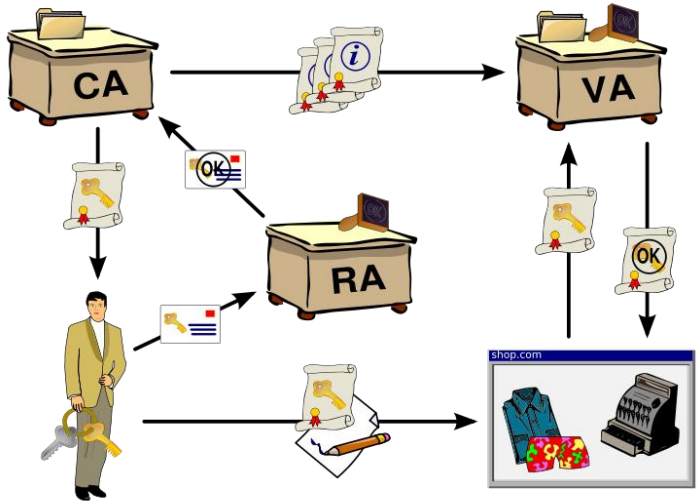
Giải thuật mã hóa chữ ký số

Thông tin của 1 chứng chỉ số đi kèm



HẠ TẦNG KHÓA CÔNG KHAI (PKI)

- **Khái niệm**



Là cơ chế để cho một bên thứ 3 (thường là nhà cung cấp chứng chỉ số - CA) cung cấp và chứng thực định danh các bên tham gia vào quá trình trao đổi thông tin.

Từng bên tham gia sẽ cung cấp cặp khóa công khai và khóa bí mật:

• Mã hóa: mã hóa bằng khóa công khai, giải mã bằng khóa bí mật.

• Chữ ký điện tử: mã hóa bằng khóa bí mật, giải mã bằng khóa công khai.

Ứng dụng của PKI:

• Open PGP: mã hóa email và chứng thực người gửi email.

• Mã hóa và xác thực văn bản.

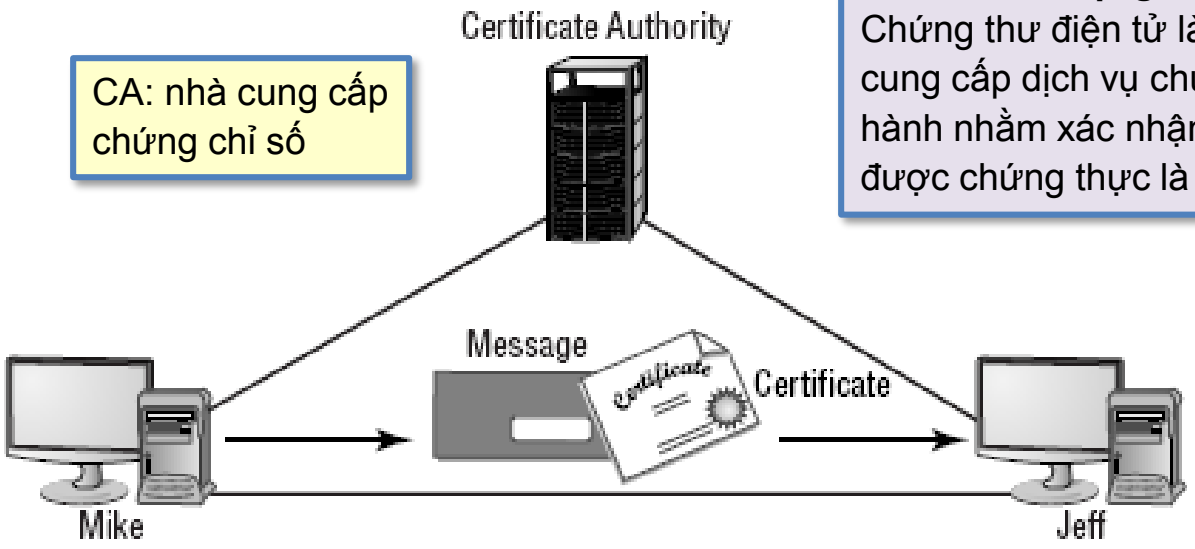
• Chứng thực người dùng ứng dụng: đăng nhập bằng smartcard, trong SSL.

• Trong các giao thức truyền thông an toàn.

HẠ TẦNG KHÓA CÔNG KHAI (PKI)

- **Chứng chỉ số (Digital certificate)**

CA: nhà cung cấp chứng chỉ số

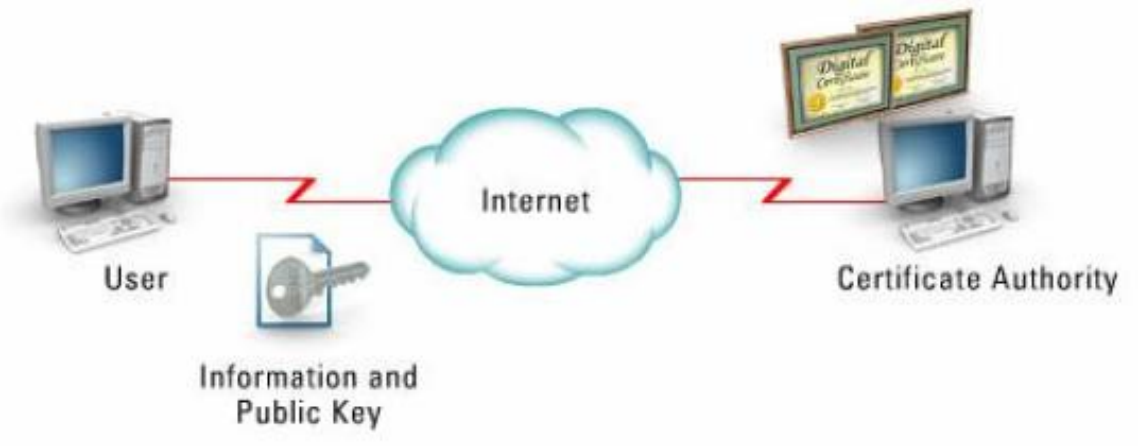


Điều 4 của luật giao dịch điện tử Việt Nam: Chứng thư điện tử là thông điệp dữ liệu do tổ chức cung cấp dịch vụ chứng thực chữ ký điện tử phát hành nhằm xác nhận cơ quan, tổ chức, cá nhân được chứng thực là người ký chữ ký điện tử

Jeff có thể kiểm tra thông điệp với chứng chỉ số kèm theo từ Mike là hợp lệ nếu Jeff tin tưởng nhà cung cấp chứng chỉ số

HẠ TẦNG KHÓA CÔNG KHAI (PKI)

- **Nhà cung cấp chứng chỉ số (CA)**



Certificate Authority:
- Là đối tác thứ 3 được tin cậy
- Cung cấp và ký xác nhận các chứng chỉ số

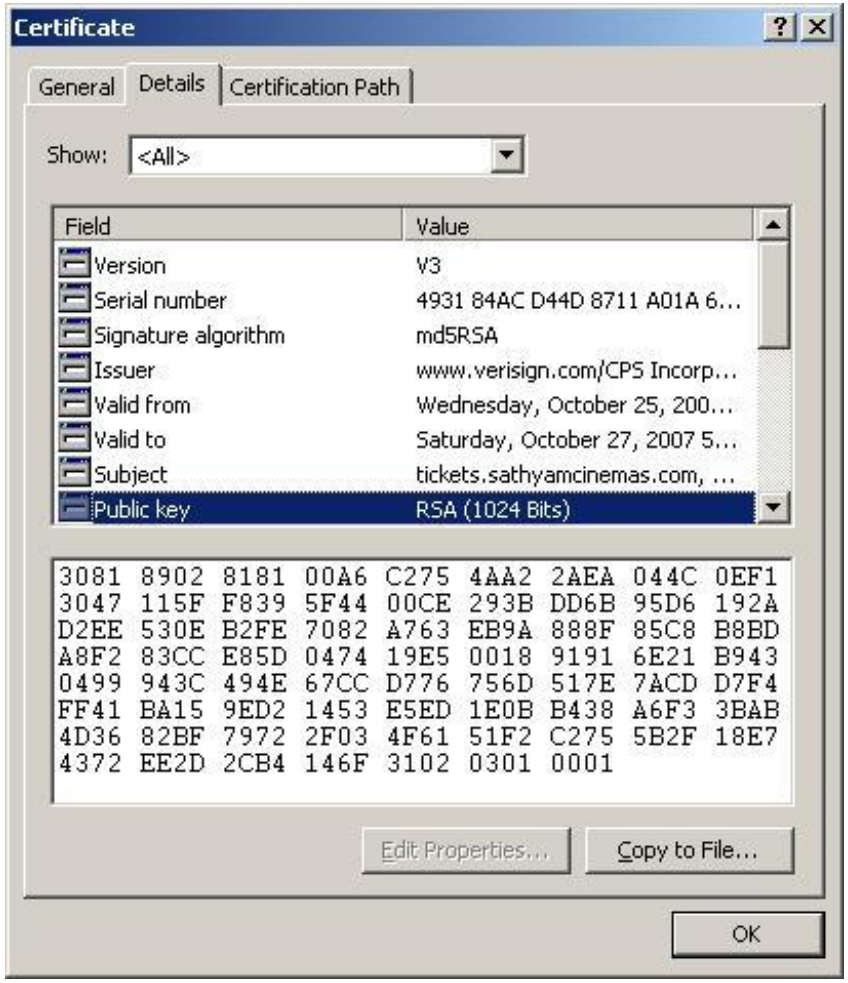
- Người dùng điền 1 form với các thông tin: tên, tổ chức, khóa công khai, giải thuật dùng để tạo khóa công khai, …
- Mã hóa form đó và gửi cho nhà cung cấp chứng chỉ số

→ "Chuẩn mật mã khóa công khai" (PKCS#10)

- CA nhận form, xác nhận thông tin người dùng, tạo ra chứng chỉ số và gửi chứng chỉ số trở lại cho người dùng.
- Chứng chỉ số được tạo ra theo chuẩn **X.509** version 3.

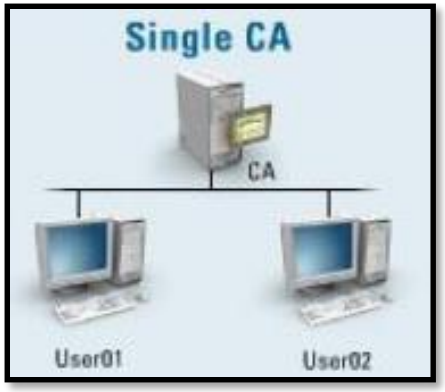
HẠ TẦNG KHÓA CÔNG KHAI (PKI)

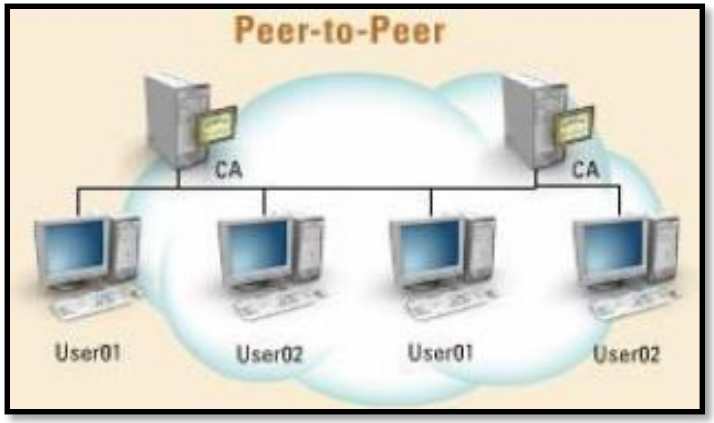
- **Chứng chỉ số (Digital certificate)**

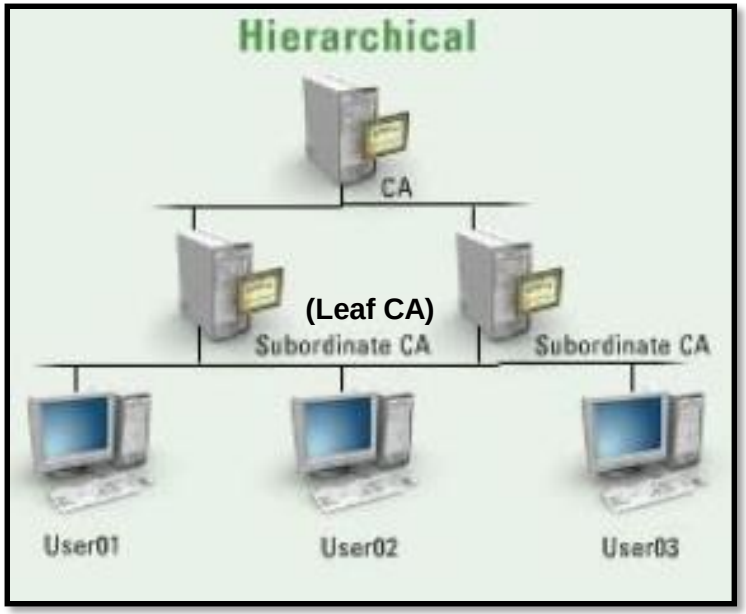


HẠ TẦNG KHÓA CÔNG KHAI (PKI)

- **Các mô hình tín nhiệm (trust models)**



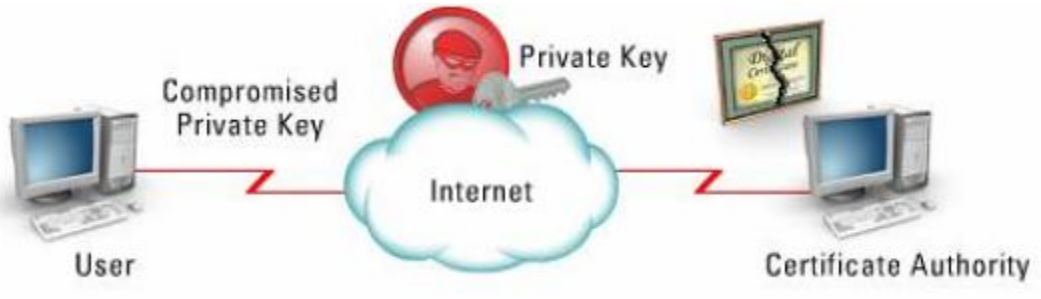




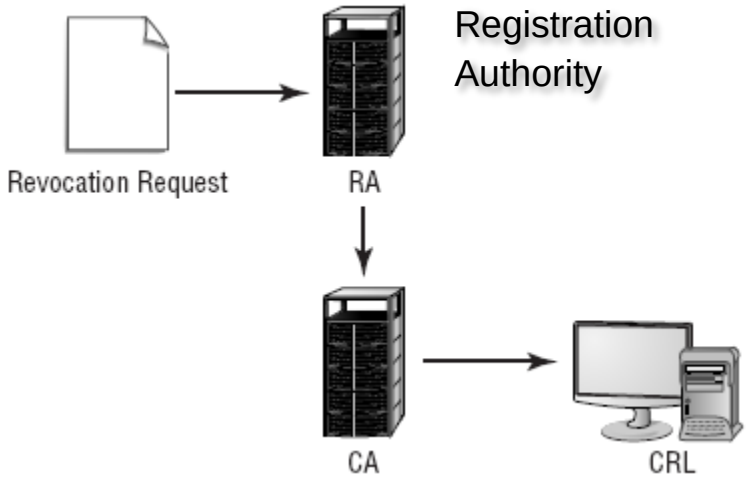
Mô hình phân cấp được sử dụng nhiều nhất

HẠ TẦNG KHÓA CÔNG KHAI (PKI)

- **Sự hủy bỏ (Revocation)**



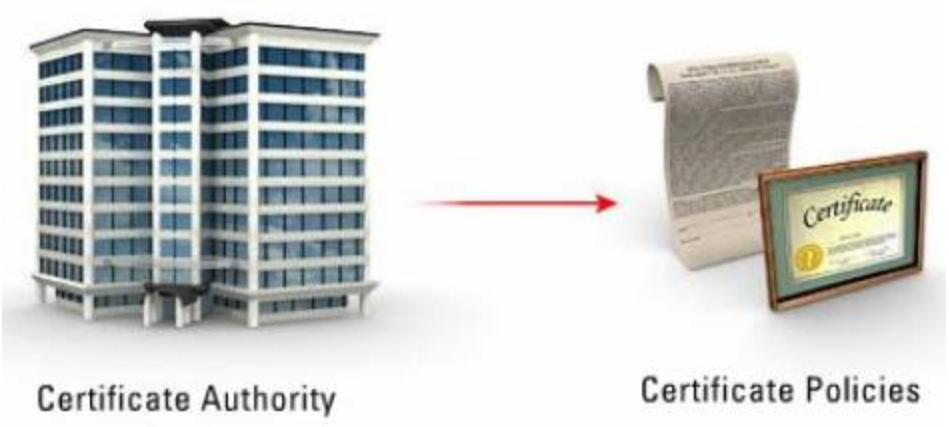
Chứng chỉ số (trước khi hết hạn) có thể bị hủy bỏ khi khóa bí mật bị lộ hay thông tin của người chủ chứng chỉ số có thay đổi.



- Mỗi chứng chỉ số đều có 1 số serial number.
- Hủy bỏ chứng chỉ số là đưa số serial number đó vào 1 danh sách CRL (Certificate Revocation List)
- Khi chứng thực, host sẽ kiểm tra danh sách CRL, nếu chứng chỉ số có serial number trong danh sách thì ngắt nối kết.

HẠ TẦNG KHÓA CÔNG KHAI (PKI)

- **Chính sách cho chứng chỉ số (certificate policy)**



CA phải định nghĩa tốt các chính sách và cơ chế an ninh để đảm bảo dịch vụ mà họ cung cấp phải thật sự tin cậy.

Chính sách cho chứng chỉ số được định nghĩa trong X.509 và mô tả trong RFC-3647

Chính sách cho chứng chỉ số là tập các **quy định chung** về việc chứng chỉ số được sử dụng, quản lý và triển khai trong tổ chức như thế nào.

- Phải rõ ràng, súc tích.
- Giới hạn trong 2 trang
- Có xác nhận của lãnh đạo cấp cao.
- Viết theo dạng gạch đầu dòng.

HẠ TẦNG KHÓA CÔNG KHAI (PKI)

- **Chỉ dẫn thực tế cho chứng chỉ số (certificate pratice statements – CPS)**

CPS thường do bộ phận điều hành (có liên quan đến IT) soạn thảo và duy trì.
Có tính kỹ thuật hơn so với chính sách về chứng chỉ số.

CPS mô tả chi tiết việc thực hiện chính sách về chứng chỉ (CP) trong **ngữ cảnh của kiến trúc hệ thống và quy trình hoạt động của tổ chức**.

- CP trình bày về việc gì (what)
- CPS trình bày về cách thực hiện như thế nào (how)

QUẢN LÝ KHÓA VÀ CHỨNG CHỈ SỐ

- **Khái niệm**

• Khóa là 1 thành phần bên trong chứng chỉ số.
• Chứng chỉ số thực thi vai trò vận chuyển khóa.

• Khóa số phải được bảo quản như khóa của 1 căn nhà.
• Tương tự như mật khẩu và mã, khóa được tạo ra, phân phối, thay đổi phải tuân theo các cơ chế bảo mật.
• Khóa phải được quản lý an toàn suốt dòng đời của nó.

Có 2 phương pháp thông dụng để lưu trữ và phân phối khóa là:
• Trung tâm phân phối khóa (Key Distribution Center – KDC)
• Giải thuật trao đổi khóa (Key Exchange Algorithm – KEA)

QUẢN LÝ KHÓA VÀ CHỨNG CHỈ SỐ

- **Tập trung hay không tập trung**

• Tạo, quản lý và phân phối khóa tập trung.
• Doanh nghiệp lớn sử dụng mô hình này.

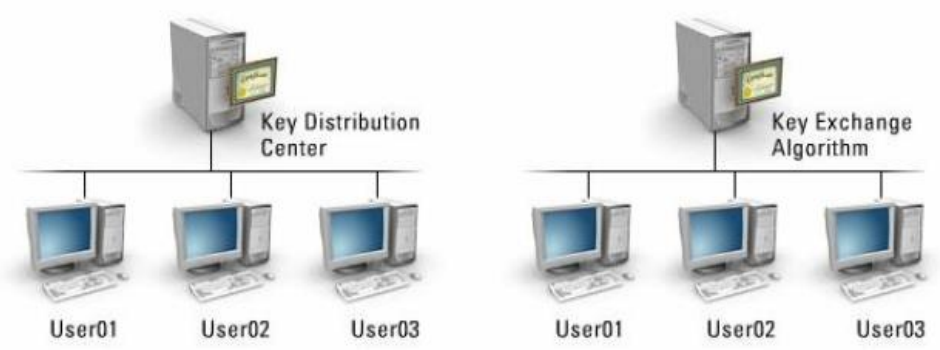
• Tạo, quản lý và phân phối khóa không tập trung.
• Verisign sử dụng mô hình này.

Ưu điểm:
•Dễ quản lý, tạo mới và phục hồi khóa.
• Các khóa được tạo ra trong môi trường an toàn.
Nhược điểm:
• Nếu CA có vấn đề sẽ ảnh hưởng đến hoạt động của toàn thể các người dùng.
• Số lượng người dùng gia tăng và chiều dài khóa tăng => xử lý nhiều hơn => ảnh hưởng đến hiệu năng của toàn hệ thống.
• Hình thành mục tiêu chính cho hacker tấn công.

Ưu điểm:
• Người dùng tự tạo và quản lý khóa bí mật.
• Khóa được user tạo ra nhanh hơn và chỉ cần gửi cho RA (Registration Authority). RA sẽ chuyển lên cho CA tạo ra chứng chỉ số.
Nhược điểm:
• Gặp khó khăn khi khóa bị thất lạc hay muốn khôi phục lại khóa.
• Có thể sẽ mất dữ liệu đã mã hóa khi khóa bị hỏng hay bị mất.

QUẢN LÝ KHÓA VÀ CHỨNG CHỈ SỐ

- **Lưu trữ và phân phối khóa**

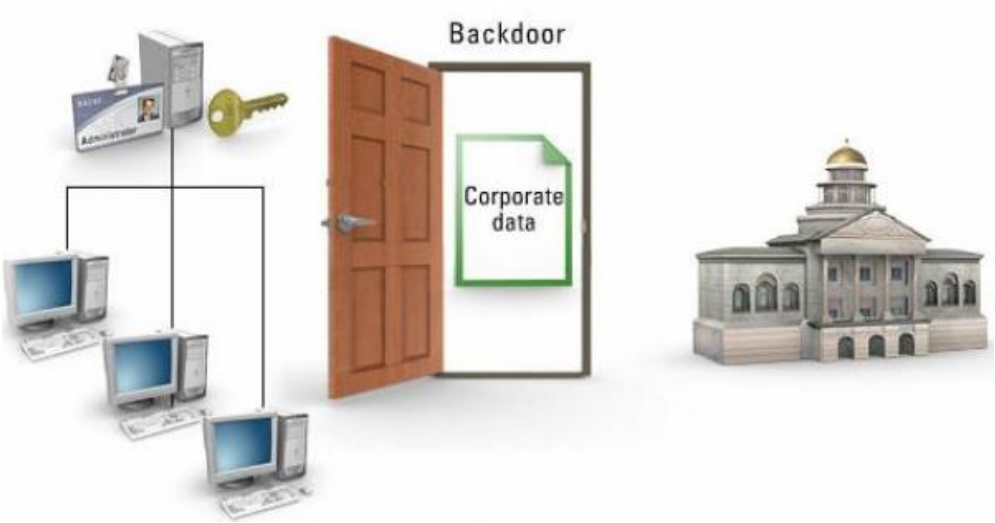


• Khóa được lưu trữ, quản lý và phân phối bởi trung tâm phân phối khóa (KDC) thông qua giải thuật trao đổi khóa (KEA).
• Một khi cần xác nhận khóa, Client sẽ gửi 1 yêu cầu đến KDC.
• Nếu chứng thực không thành công, Client sẽ bị loại bỏ.

Có 2 cách lưu trữ khóa:
• Bằng phần mềm:
  + Mềm dẽo
  + Kém an toàn
• Bằng phần cứng: card, flash disk
  + Không mềm dẽo
  + An toàn và tin cậy cao hơn

QUẢN LÝ KHÓA VÀ CHỨNG CHỈ SỐ

- **Lưu giữ (Escrow)**

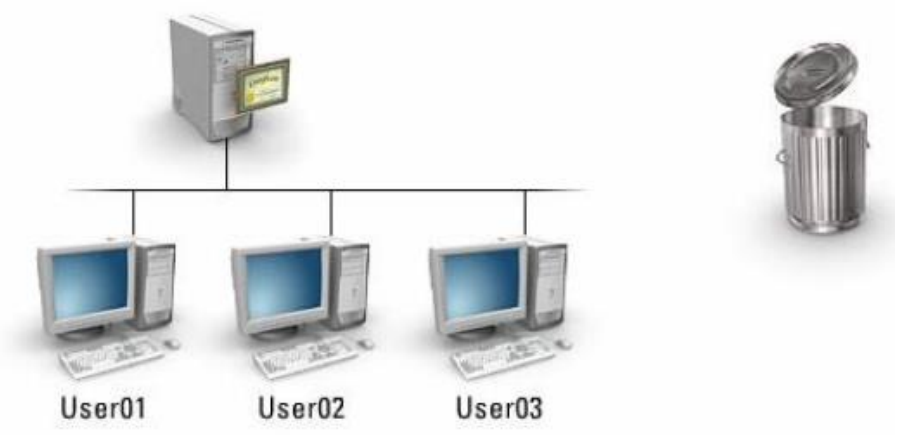


Escrow là nơi lưu trữ các bản sao của khóa bí mật trong hệ thống quản lý khóa tập trung.

- Người dùng nếu bị mất hay làm hỏng khóa, có thể phục hồi lại khóa bí mật này từ Escrow.
- Người dùng có thể lưu nhiều bản sao tại nhiều công ty Escrow.
- Tuy nhiên, người quản trị trong công ty hay hacker có thể tấn công vào nơi lưu trữ Escrow đó để lấy được khóa của người dùng.

QUẢN LÝ KHÓA VÀ CHỨNG CHỈ SỐ

- **Hết hạn, hủy bỏ và tạm dừng**



• Khóa và chứng chỉ số (giống như thẻ tín dụng) đều có hạn sử dụng .
• Khi **hết hạn sử dụng**, khóa và chứng chỉ sẽ bị hủy bỏ.

• Khi phát hiện khóa bị lộ hay mất, người dùng có thể yêu cầu **hủy bỏ** chứng chỉ số.
• CA sẽ đưa số serial number của chứng chỉ đó vào danh sách đen.
• Danh sách đen đó gọi là CRL và CA phải công bố danh sách đó.

• Khi muốn tạm thời ngưng sử dụng khóa hay chứng chỉ, người dùng có thể yêu cầu **tạm dừng**.
• Khóa và chứng chỉ khi tạm dừng có thể được khôi phục lại sau này.

QUẢN LÝ KHÓA VÀ CHỨNG CHỈ SỐ

- **Gia hạn**

• Trước khi khóa hay chứng chỉ số hết hạn, người dùng có thể gửi yêu cầu được gia hạn (làm mới) lại khóa và chứng chỉ.
• Việc sử dụng khóa cũ sẽ vi phạm chính sách về bảo mật => sẽ là rủi ro => cẩn thận và cân nhắc khi gia hạn.

QUẢN LÝ KHÓA VÀ CHỨNG CHỈ SỐ

- **Tiêu hủy (destruction)**

Khi các khóa và chứng chỉ không còn sử dụng nữa thì các thông tin về khóa và chứng chỉ phải được gở bỏ trong phần mềm hoặc phần cứng lưu trữ thông tin này phải bị tiêu hủy để tránh kẻ xấu lợi dụng.

QUẢN LÝ KHÓA VÀ CHỨNG CHỈ SỐ

- **Sử dụng khóa**

Khóa được sử dụng rộng rãi trong:

- VPN như IPSec.
- Các giao thức SSL và TSL
- SSL trong HTTP : HTTPS
- HTTP bảo mật: Secure HTTP (SHTTP)
- Truy cập từ xa an toàn: SSH
- Bảo mật Email: PGP, S/MIME

Chiến lược sử dụng khóa:

- Phải xác định khóa được sử dụng như thế nào?
- Sử dụng khóa đối xứng hay bất đối xứng ?
- Sử dụng 1 khóa hay cần thêm nhiều khóa khác?
- Ngoài khóa, có cần thêm các mức bảo mật khác?

HẾT BÀI