ĐẠI NAM
UNIVERSITY

Bài 9

CHỮ KÝ SỐ VÀ QUẢN LÝ KHÓA

Giảng viên: TS.
(namtq@dainam.edu.vn)

1. Khái niệm chữ ký số

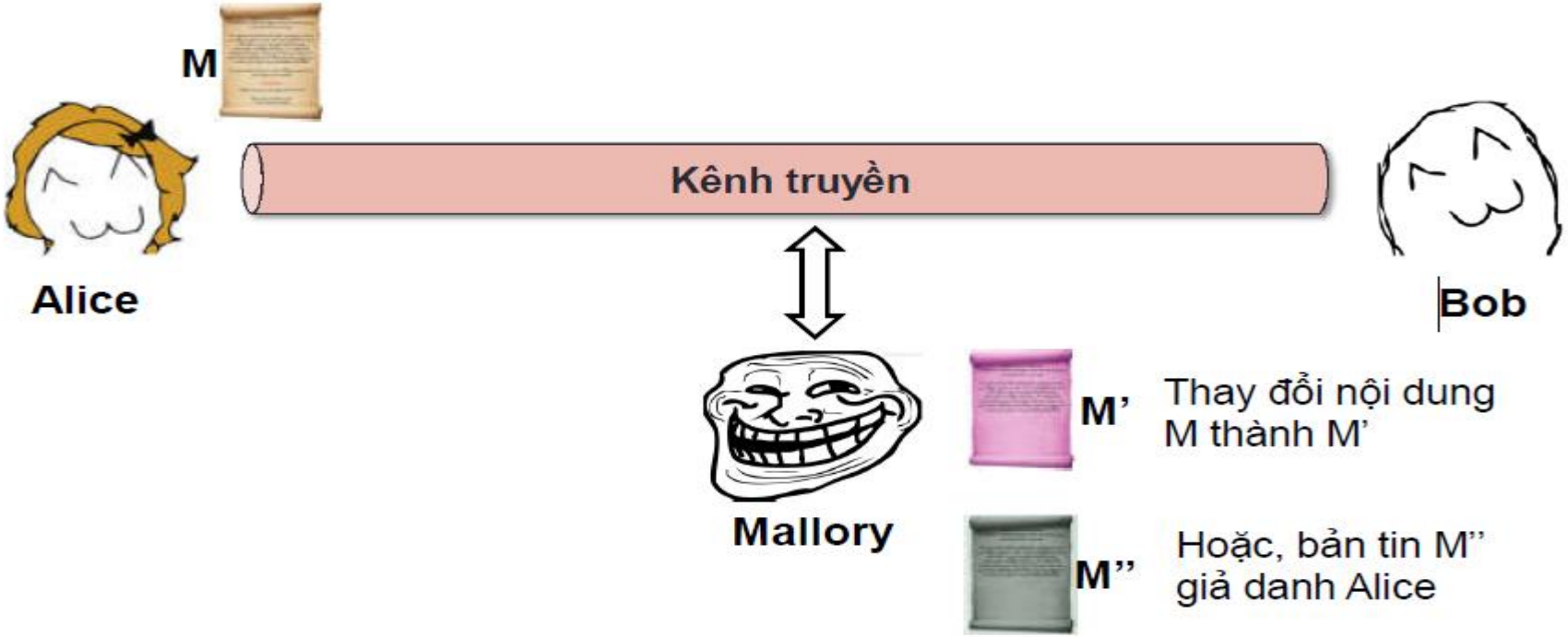
2. Chữ ký số RSA và Elgamal

3. Trao đổi khóa, thỏa thuận khóa

4. Luyện tập Lab 9

PHẦN I - CHỮ KÝ SỐ

ĐẶT VẤN ĐỀ


M
Kênh truyền
Alice
Bob
Mallory
M'
Thay đổi nội dung M thành M'
M''
Hoặc, bản tin M'' giả danh Alice

GIỚI THIỆU CHỮ KÝ SỐ

Khoản 6 Điều 3 Nghị định 130/2018 NĐ-CP : “Chữ ký số là một dạng chữ ký điện tử được tạo ra bằng sự biến đổi một thông điệp dữ liệu sử dụng hệ thống mật mã không đối xứng”

GIỚI THIỆU CHỮ KÝ SỐ

- Tính chống chối bỏ
- Tính toàn vẹn
- Tính xác thực
- Tính bảo mật

Đối tượng sử dụng chữ ký số

SỬ DỤNG AI, SEARCH….

- Dùng ChatGPT hoặc Google, DeepSeek,… hỏi: “Chữ ký số hoạt động như thế nào” ➔ Các em ghi vào vở tóm tắt và giải thích ?
- “Chữ ký số dùng thực tế ở đâu” ➔ Em giải thích vai trò ý nghĩa của chữ ký số trong thực tế ?
- Ưu điểm của chữ ký số là gì?
- Tại sao chữ ký số được dùng phổ biến trong thực tế?
- Chữ ký số khác chữ ký giấy mực ở đặc điểm nào?

GIỚI THIỆU CHỮ KÝ SỐ

Digital Signature (Chữ ký số)

- Độ an toàn cao, được sử dụng rộng rãi
- Được phát triển dựa trên lý thuyết về mật mã và thuật toán mã hóa bất đối xứng
- Thuật toán mã hóa dựa vào cặp khóa bí mật (Private Key) và công khai (Public Key)
- Được sử dụng thông qua một nhà cung cấp chính thức (CA – Certificate Authority)

Digital Signature (Chữ ký số)

- Chữ ký số giúp người nhận thông điệp có thể tin tưởng ở nội dung văn bản mình nhận được là của một người quen biết.
- Người gửi cũng không thể chối bỏ trách nhiệm là chính mình đã gửi bản thông điệp đó.
- Thông điệp đã được số hóa là một chuỗi các bit (vd: email, contracts…được gửi thông qua những giao thức mã hóa).

Digital Signature (Chữ ký số)

- Phương pháp chữ ký số chủ yếu bao gồm 3 giải thuật chính:

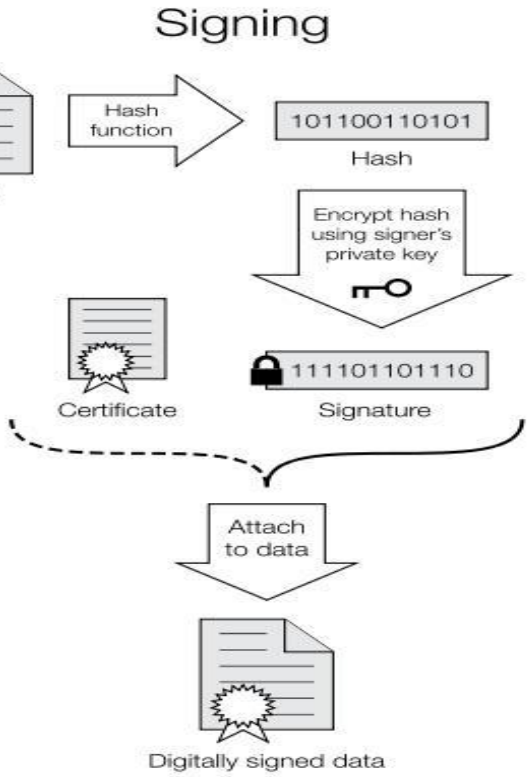
✓ Tạo 1 cặp Private Key và Public Key

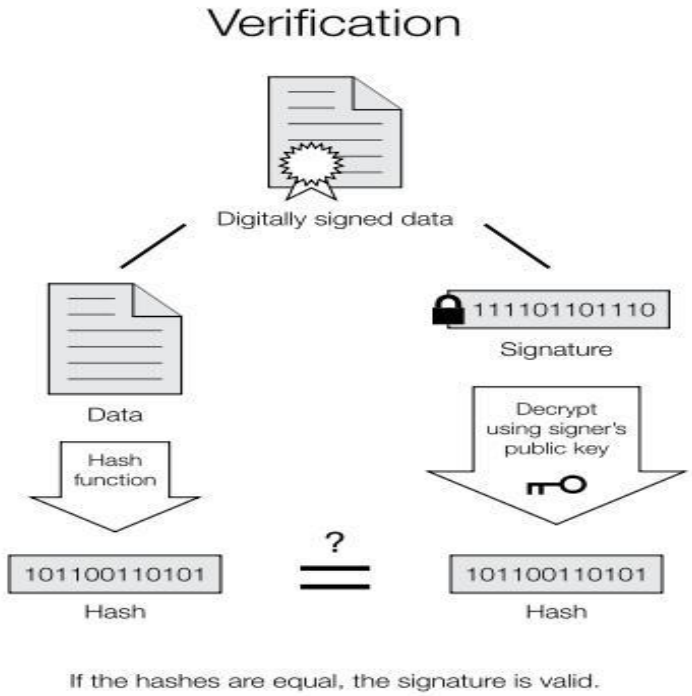
✓ Một giải thuật Signing

✓ Một giải thuật Verification (xác minh)

Digital Signature (Chữ ký số)

Sử dụng các giải thuật mã hóa như RSA, ELGAMAL, DSA…



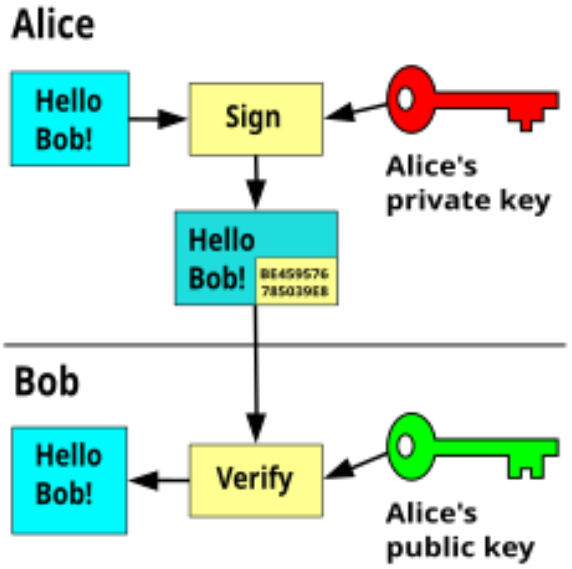


ENGLISH PRACTICE

- A digital signature is a mathematical scheme for verifying the authenticity of digital messages or documents. A valid digital signature on a message gives a recipient confidence that the message came from a sender known to the recipient.
- Digital signatures are a standard element of most cryptographic protocol suites, and are commonly used for software distribution, financial transactions, contract management software, and in other cases where it is important to detect forgery or tampering.

Chữ ký số và hàm băm

- Mỗi thông điệp đầu vào chỉ có thể tính ra được một văn bản đại diện, giá trị băm tương ứng duy nhất
- Hai thông điệp khác nhau chắc chắn có hai văn bản đại diện khác nhau.
- Khi đã có văn bản đại diện duy nhất cho bức thông điệp, áp dụng các sơ đồ chữ ký số ký trên văn bản đại diện đó.



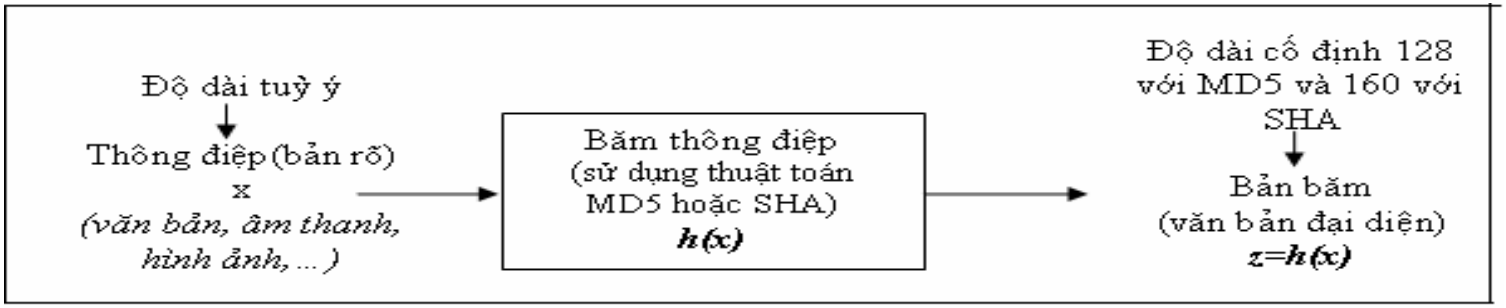
Giả sử A muốn gửi cho B thông điệp *x*. A thực hiện các bước sau:

(1) A băm thông điệp ***x***, thu được bản đại diện $z = h(x)$ – có kích thước cố định 128 bit hoặc 160 bit.

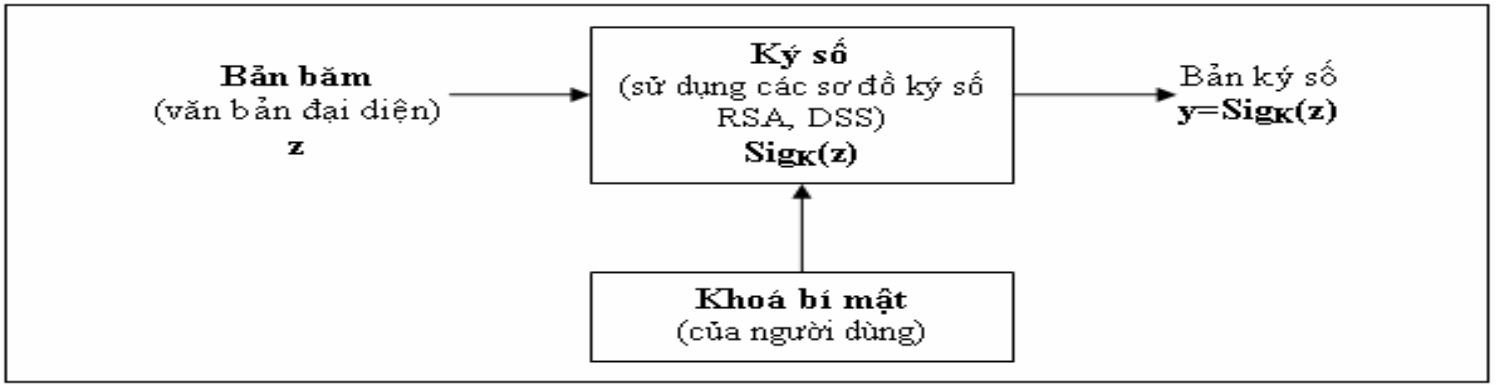
(2) A ký số trên bản đại diện z, bằng khóa bí mật của mình, thu được bản ký số y = sig(z).

(3) A gửi **(x, y)** cho B.

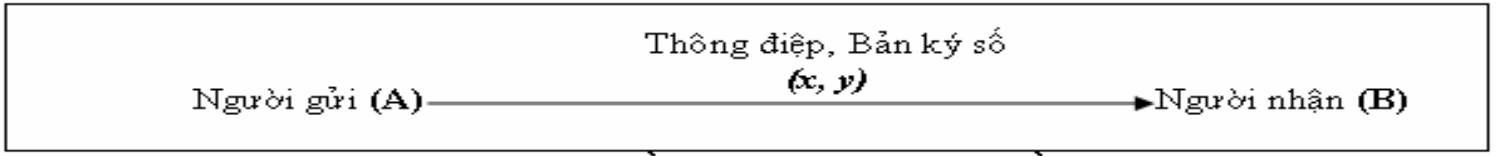
Chữ ký số và hàm băm



(1) *Băm thông điệp.*



(2) *Ký trên bản băm.*



(3) *Truyền dữ liệu thông tin cần gửi.*

Khi B nhận được (***x***, ***y***). B thực hiện các bước sau:

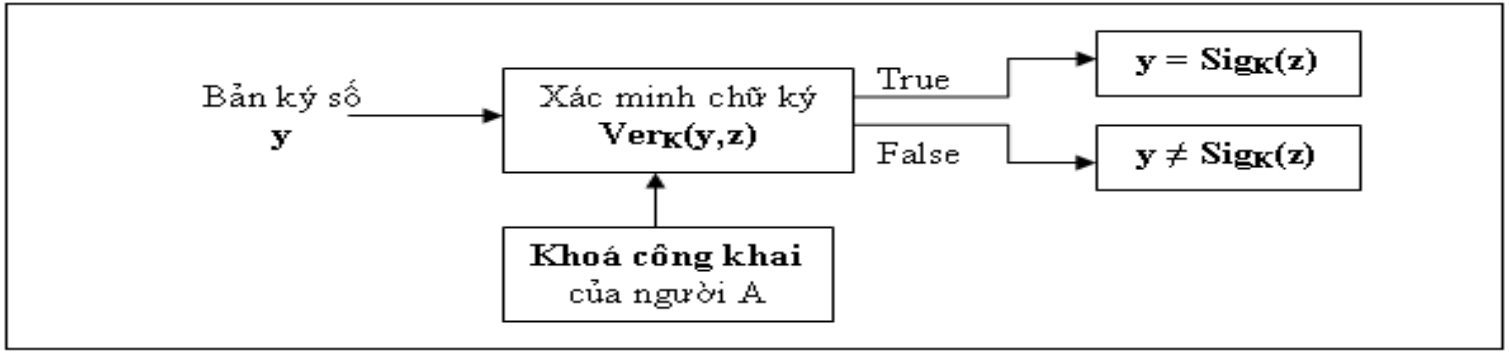
(4) B kiểm tra chữ ký số để xác minh xem thông điệp mà mình nhận được có phải được gửi từ A hay không bằng cách giải mã chữ ký số y, bằng khóa công khai của A, được z.

(5) B dùng một thuật toán băm – tương ứng với thuật toán băm mà A dùng – để băm thông điệp x đi kèm, nhận được h(x).

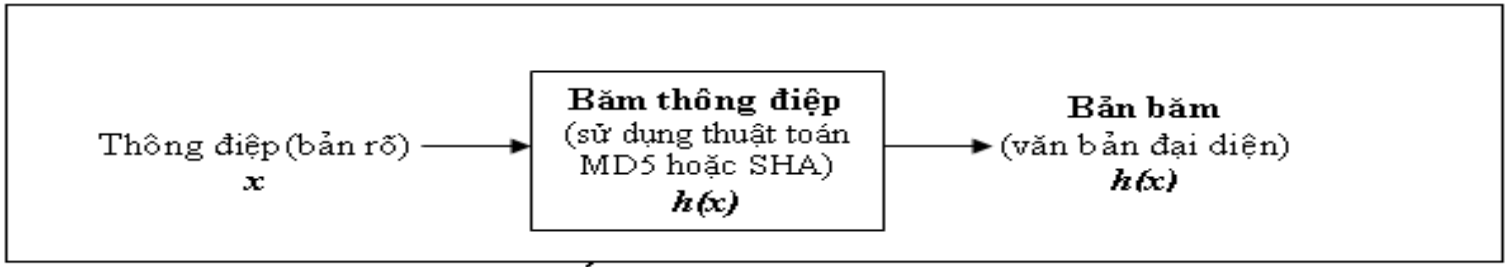
(6) B so sánh 2 giá trị băm z và h(x), nếu giống nhau thì chắc chắn rằng thông điệp x – mà A muốn gửi cho B – còn nguyên vẹn, bên cạnh đó cũng xác thực được người gửi thông tin là ai.

ĐẠI NAM UNIVERSITY

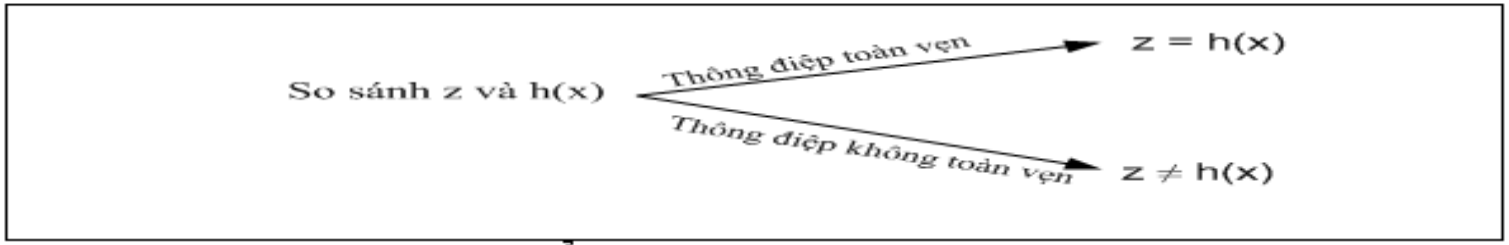
Chữ ký số và hàm băm



(4) *Xác minh chữ ký*



(5) *Tiến hành băm thông điệp x đi kèm*



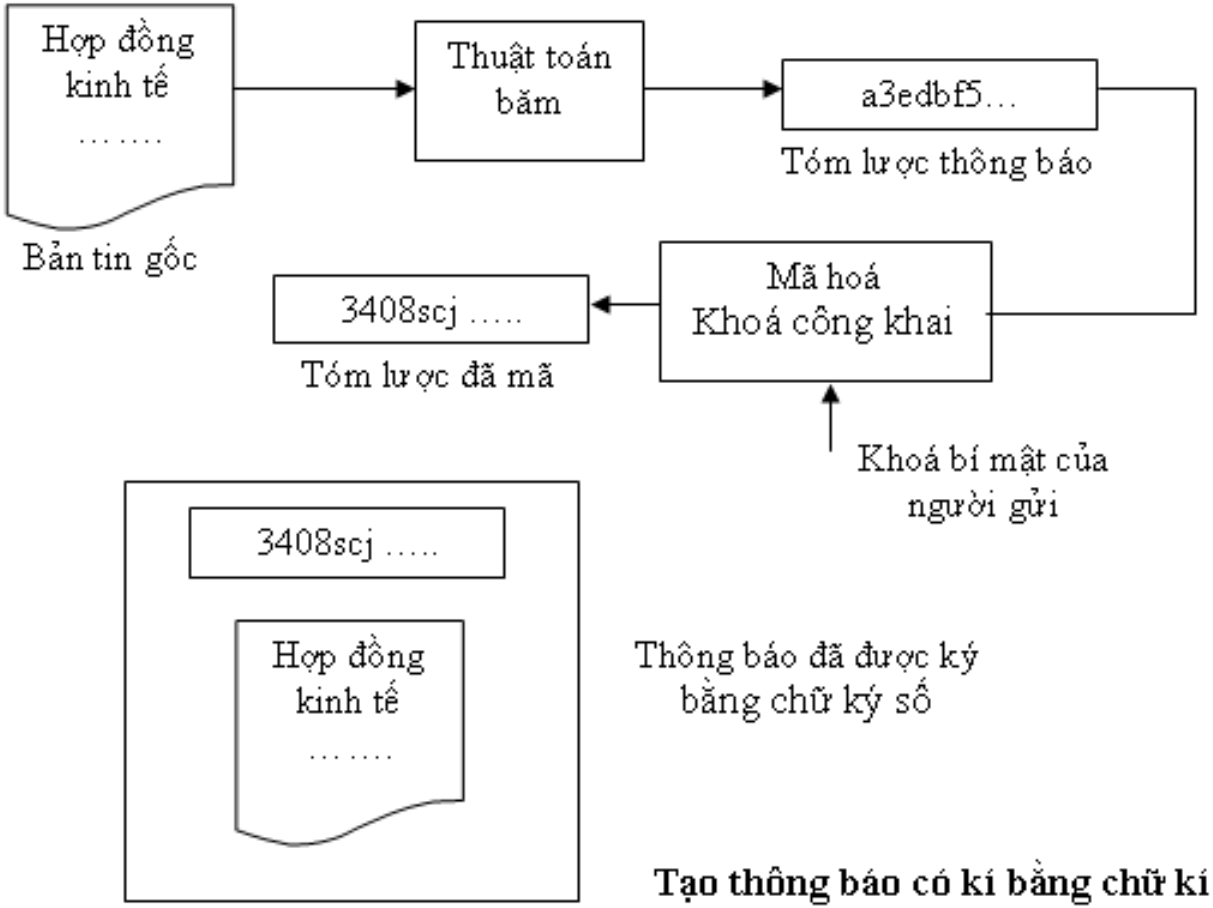
(6) *Kiểm tra tính toàn vẹn của thông điệp*

Chữ ký số và hàm băm

- Hàm băm trợ giúp cho các sơ đồ ký số nhằm giảm dung lượng của dữ liệu cần thiết để truyền qua mạng
- Lúc này chỉ còn bao gồm dung lượng của bức thông điệp gốc và 256 bit (sử dụng MD) hay 320 bit (sử dụng SHA) của bức ký số được ký trên bản đại diện của thông điệp gốc, tương đương với việc giảm thời gian truyền tin qua mạng.
- Hàm băm thường kết hợp với chữ ký số để tạo ra một loại chữ ký điện tử vừa an toàn hơn (không thể cắt/dán) vừa có thể dùng để kiểm tra tính toàn vẹn của thông điệp.

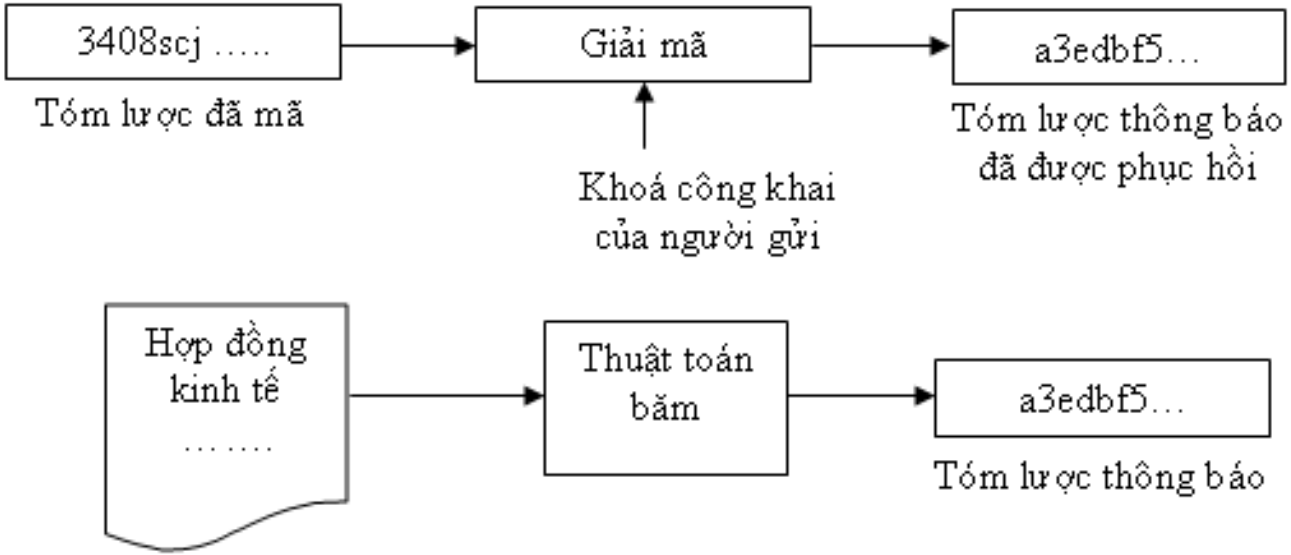
A digital signature can only sign a relatively small amount of information, which is why the digest is signed instead of the original message. Because of this limitation, the digest must be a faithful representation of the complete message. A cryptographically-secure hash is require to resist collision attacks, second preimage attacks, and preimage attacks, all of which can invalidate the guarantees that people expect from a digital signature. In other words, if one signature is valid for two distinct messages, the signature is useless. A cryptographically-secure hash prevents this. Also note that digital signatures are not simply encrypted digests. This is a simplified explanation which is common, but technically incorrect. This describes signatures for RSA.

Ký số RSA



Tạo thông báo có kí bằng chữ kí

Ký số RSA



Các bước kiểm tra một thông báo đã kí

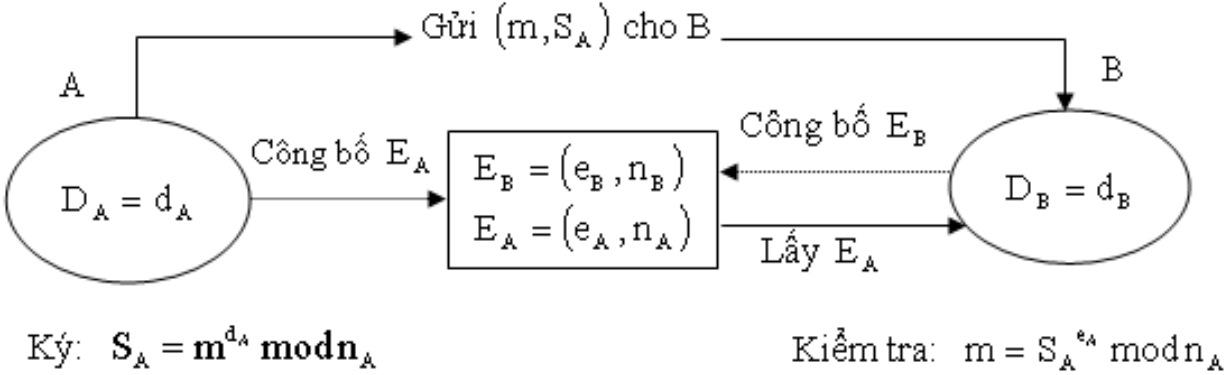
Chữ ký số RSA

- Xác định n = p.q với p, q là các số nguyên tố lớn có kích thước tương đương
- Với K = {(n, e, d): d $\in Z_p^*$, e*d $\equiv$ 1 mod (n)}
- Ta có D = (n, d) là khóa bí mật, E = (n, e) là khóa công khai, m là bản tin cần kí
  - ✓ Tạo chữ kí: $S = sig_D(m) = m^d \bmod n$
  - ✓ Kiểm tra chữ kí: $ver_E(m, S) = TRUE \Leftrightarrow m \equiv S^e \bmod n$

Trường hợp bản tin m không cần bí mật:

A ký bản tin m và gửi cho B.

B kiểm tra chữ ký của A



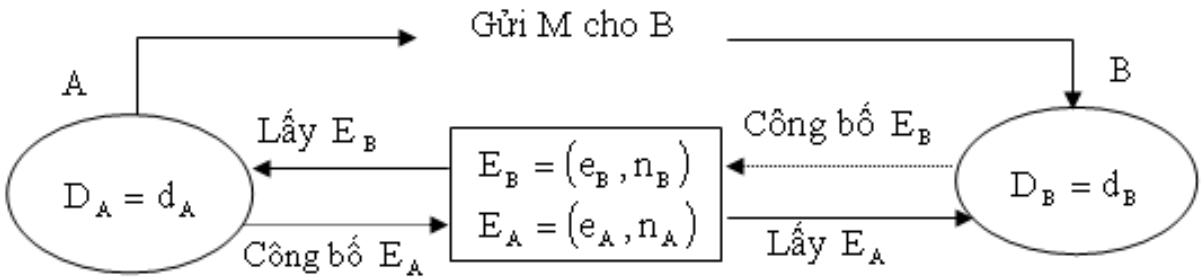
Sơ đồ chữ kí số RSA (không bí mật bản tin)

Chữ ký số RSA

Trường hợp bản tin m cần giữ bí mật:

A ký bản tin rõ m để được chữ ký S_A.

Sau đó A dùng khoá mã công khai E_B của B để lập bản mã M = E_B(m, S_A) rồi gửi đến B



A tính:

i. $S_A = m^{d_A} \bmod n_A$

ii. $X = m \| S_a$

iii. $M = X^{e_B} \bmod n_B$

B tính:

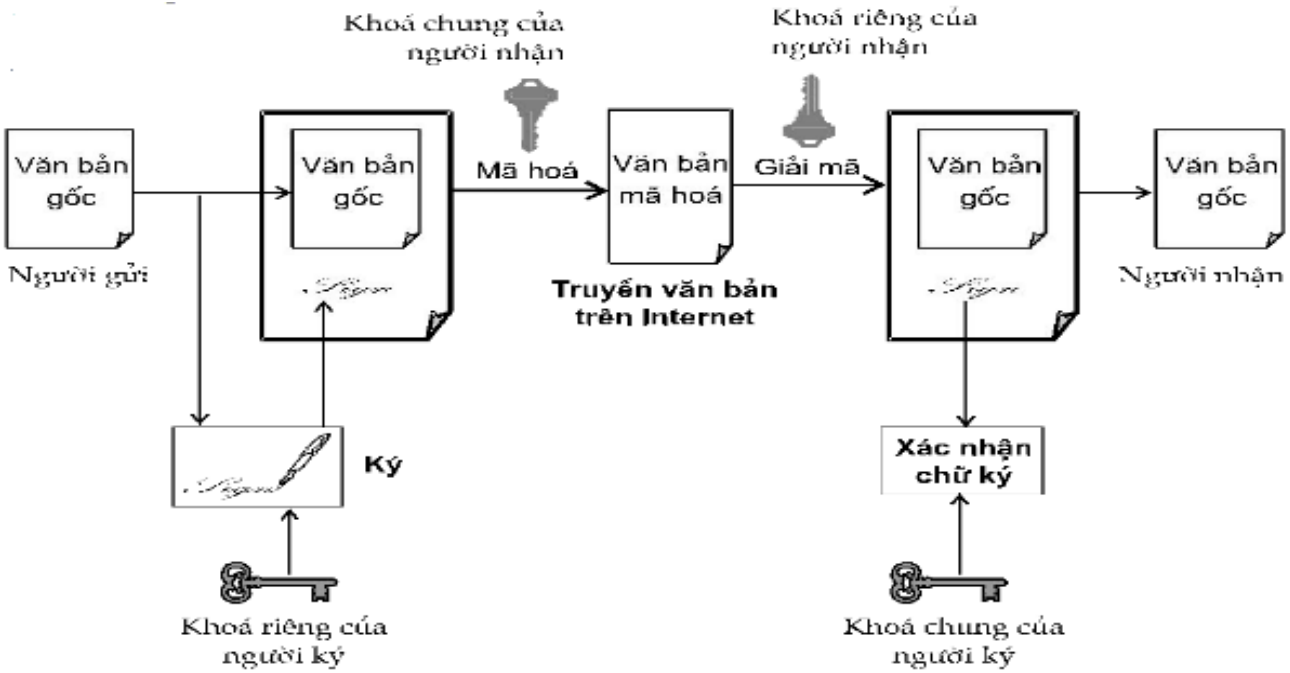
i. $X = M^{d_B} \bmod n_B$

ii. $X = m \| S_a$

iii. Kiểm tra: $m = S_A^{e_A} \bmod n_A$

Sơ đồ chữ kí số RSA (có bí mật bản tin)

SƠ ĐỒ CHỮ KÝ SỐ



Video giải thích ký số Elgamal: https://www.youtube.com/watch?v=OeFEywEa0iY

Chữ ký số Elgamal

Bước 1: Tạo cặp khóa (bí mật, công khai):

Bước đầu tiên trong quy trình chữ ký số Elgamal là tạo khóa. Bước này liên quan đến việc tạo ra một cặp khóa công khai. Khóa riêng được giữ bí mật bởi người ký, trong khi khóa chung được cung cấp cho bất kỳ ai muốn xác minh chữ ký. Quá trình tạo khóa bao gồm các bước sau:

1.1. Chọn số nguyên tố: Chọn hai số nguyên tố lớn, p và q, sao cho q chia hết (p-1). Những số nguyên tố này nên được giữ bí mật.

Chữ ký số Elgamal

1.2. Tính toán tạo khóa: Chọn một số căn nguyên thủy g của p (còn gọi là phần tử sinh p).

1.3. Tính khóa riêng: Chọn một số nguyên ngẫu nhiên x, sao cho $1 \leq x \leq q-1$. Số nguyên này sẽ là khóa riêng.

1.4. Tính khóa công khai: Tính khóa công khai y, sử dụng công thức $y = g^x \bmod p$.

Khi đó, khóa công khai là (p, g, y) và khóa riêng là x

Bước 2: Tạo chữ ký

2.1. Băm tin nhắn: Tính toán giá trị băm của tin nhắn sẽ được ký bằng cách sử dụng hàm băm mật mã như MD5 hay SHA-256, SHA-512. Giá trị băm này đảm bảo tính toàn vẹn của tin nhắn.

2.2. Tạo số ngẫu nhiên: Chọn một số ngẫu nhiên, k, sao cho $1 \leq k \leq q-1$.

2.3. Tính r: Tính $r = g^k \bmod p$.

2.4. Tính s: Tính s = (H(m) - x*r) * k^{-1} mod (p-1), trong đó H(m) là giá trị băm của thông báo và k^{-1} biểu thị nghịch đảo modulo .

2.5. Tạo chữ ký: Chữ ký điện tử là cặp (r, s).

Bước 3: Xác minh chữ ký

3.1. Băm tin nhắn: Tính toán giá trị băm của tin nhắn đã nhận bằng cách sử dụng cùng một hàm băm mật mã được sử dụng bởi người ký.

Chữ ký số Elgamal

3.2. Tính u1 và u2: Tính $u1 = H(m) * s^{-1} \bmod (p-1)$ và:

$u2 = r * s^{-1} \bmod (p-1)$, trong đó s^{-1} biểu thị nghịch đảo modulo của s.

3.3. Tính v: Tính $v = (g^{u1} * y^{u2} \bmod p) \bmod q$.

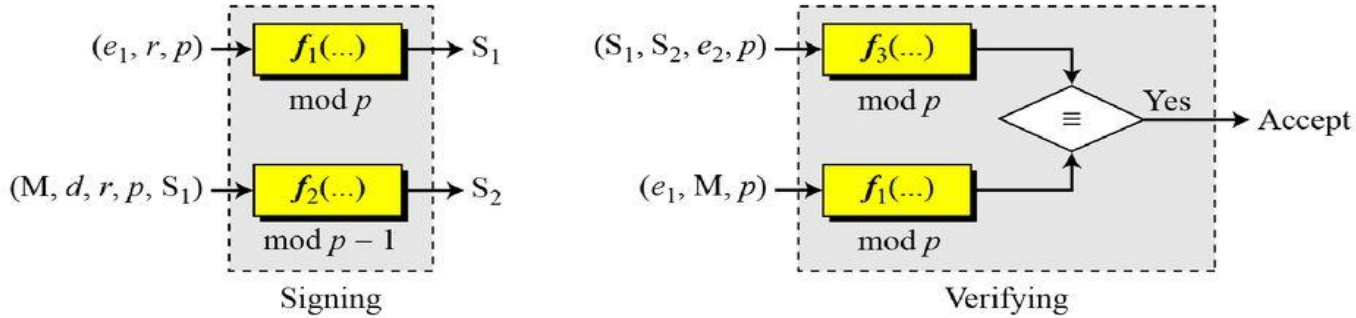
3.4. Xác minh chữ ký: Nếu v bằng r, thì chữ ký hợp lệ; nếu không, chữ ký là không hợp lệ.

ElGamal Digital Signature Scheme

- Ý tưởng tổng quát của chữ ký ElGamal

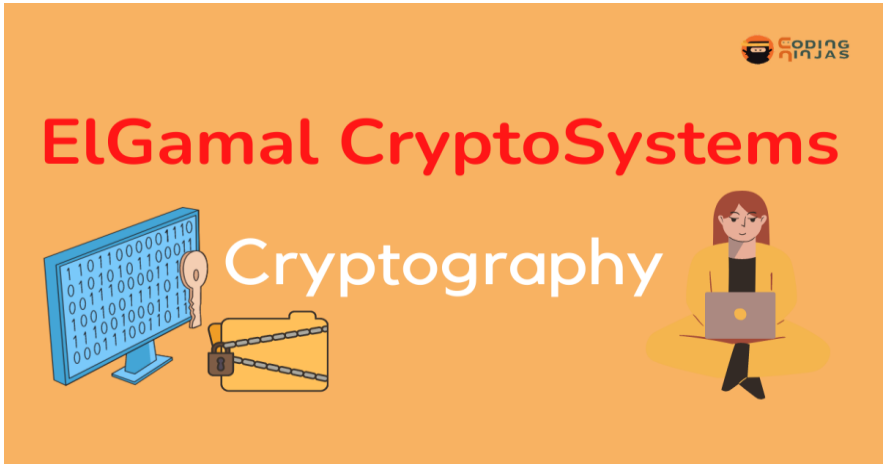
S_1, S_2: Signatures
M: Message
(e_1, e_2, p): Alice's public key

d: Alice's private key
r: Random secret



Chữ ký số Elgamal

- Dùng ChatGPT hay Google hỏi và chúng ta cùng thảo luận: “Mô tả cách thức hoạt động của chữ ký số ElGamal và ví dụ?”



Đặc điểm chữ ký số

1. Đảm bảo tính xác thực

- Chứng minh tính hợp pháp của người gửi
- Chứng minh tính toàn vẹn của dữ liệu

2. Chữ ký số là hàm của các tham số

- Thông báo giao dịch (văn bản gốc)
- Thông tin bí mật của người gửi (Khóa riêng của sender)
- Thông tin công khai trên mạng (Khóa công khai)
- Mã xác thực : Đảm bảo tính toàn vẹn của thông điệp

Đặc điểm chữ ký số

Khóa bí mật	**Tính bí mật của Khóa bí mật**	Chỉ có người chủ mới biết
Khóa công khai	**Tính sẵn sàng truy cập của khóa công khai**	Có thể truy cập thông qua phương tiện thông dụng vào bất cứ thời điểm: Chứa trong một thư mục công cộng Đảm bảo tính chính xác và không giả mạo
Chứng thư số	**Công bố khóa công khai**	Được cấp phát bởi tổ chức có thẩm quyền
Độ dài khóa	**Tương ứng tính an toàn của khóa**	Khóa có thể có độ dài (thông dụng là) 512, 1024, 2048, 4096 Khóa càng dài mã càng chậm
Tính pháp lý	**Với công nghệ đảm bảo sẽ tương đương chữ ký tay**	Được cấp phát theo quy trình an toàn với các thông số kỹ thuật đảm bảo Được lưu trữ an toàn
Tính khả dụng	**Ngày càng dễ sử dụng**	Được lưu trong các thiết bị cá nhân như USB-token, smart card Ngày càng nhiều ứng dụng hỗ trợ

PHẦN I – QUẢN LÝ KHÓA

Khái niệm quản lý khóa

- Một người cần trao đổi thông điệp bảo mật với N người, thì người đó cần N khóa khác nhau. Vậy N người giao tiếp với N người khác thì cần tổng số là N*(N-1) khóa
- Số lượng khóa không chỉ là vấn đề, mà phân phối khóa là một vấn đề khác.
- Độ tin cậy của một hệ thống mật mã phụ thuộc vào công nghệ phân phối khóa (key distribution technique).

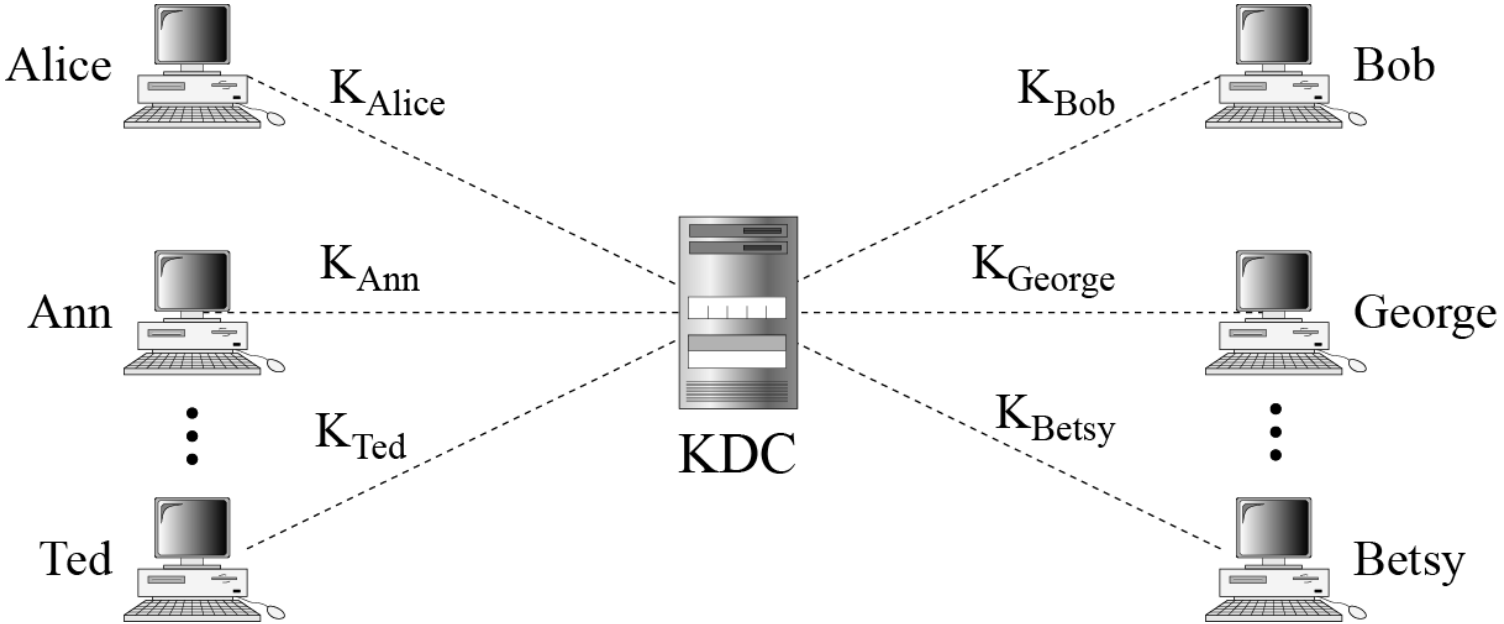
➔ Public Key Infrastructure (PKI)

Khái niệm quản lý khóa

- Phương pháp chuyển giao khóa đến hai thực thể muốn trao đổi dữ liệu, và không cho phép phía thứ ba biết được khóa.
- Khoá có thể được lựa chọn bởi A và vận chuyển vật lý đến B.
- Khoá có thể được lựa chọn bởi phía thứ 3 và vận chuyển vật lý đến cả hai phía A và B.

Key-Distribution Center: KDC

Để giảm số lượng khóa, mỗi người sẽ thiết lập một khóa bí mật chia sẻ với KDC



Trao đổi khóa Diffie-Hellman

- Trao đổi khoá Diffie Hellman là sơ đồ khoá công khai đầu tiên được đề xuất bởi Diffie và Hellman năm 1976 cùng với khái niệm khoá công khai.
- Sau này được biết đến bởi James Ellis (Anh), người đã đưa ra mô hình tương tự năm 1970.
- Đây là phương pháp thực tế trao đổi công khai các khoá mật.
- Sơ đồ được sử dụng trong nhiều sản phẩm thương mại.

Trao đổi khóa Diffie-Hellman

- Dùng để thiết lập khoá chung.
- Chỉ có hai đối tác biết đến.
- Giá trị khoá phụ thuộc vào các đối tác (và các thông tin về khoá công khai và khoá riêng của họ).
- Dựa trên phép toán lũy thừa trong trường hữu hạn (modulo theo số nguyên tố hoặc đa thức) là bài toán dễ.
- Độ an toàn dựa trên độ khó của bài toán tính logarit rời rạc (giống bài toán phân tích ra thừa số) là bài toán khó.

Trao đổi khóa Diffie-Hellman

- Giao thức trao đổi khoá giữa A và B: A và B thống nhất chọn chung một số nguyên tố q và một phần tử sinh α.

Global Public Elements	
q	prime number
α	$\alpha < q$ *and* α a primitive root of q

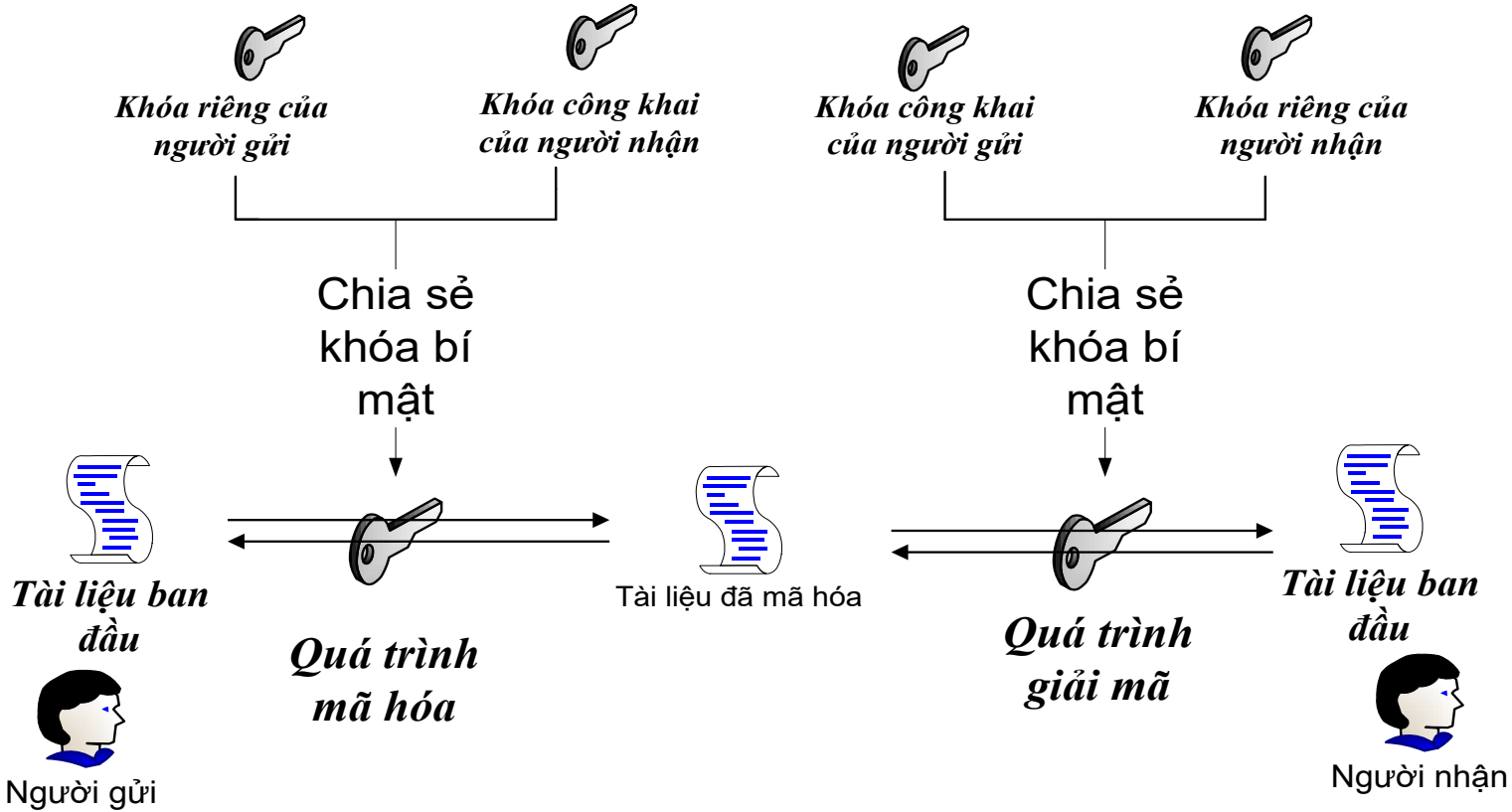
Trao đổi khóa Diffie-Hellman

- Tạo cặp khóa:

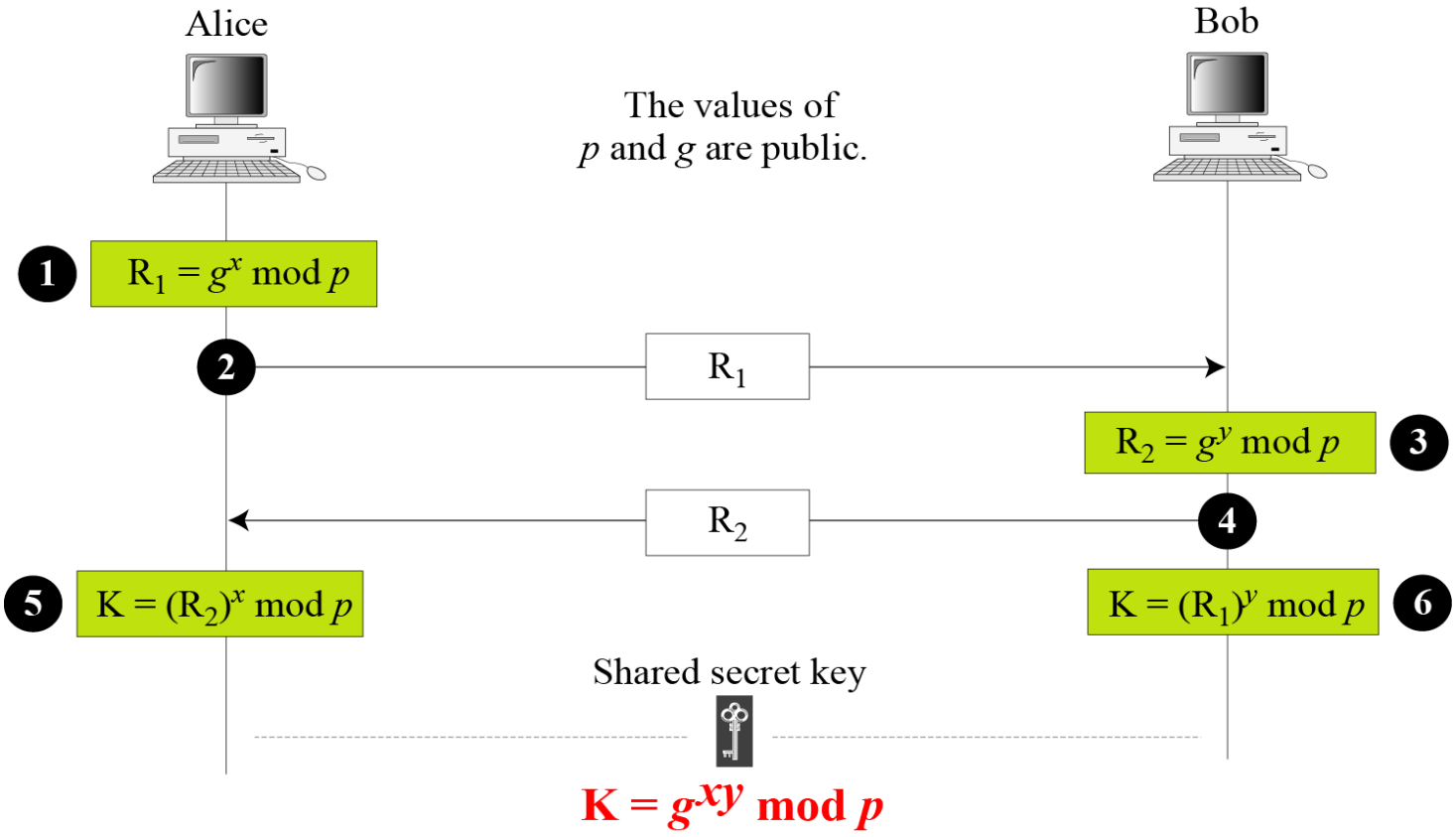
User A Key Generation	
Select private X_A	$X_A < q$
Calculate public Y_A	$Y_A = \alpha^{X_A} \bmod q$

User B Key Generation	
Select private X_B	$X_B < q$
Calculate public Y_B	$Y_B = \alpha^{X_B} \bmod q$

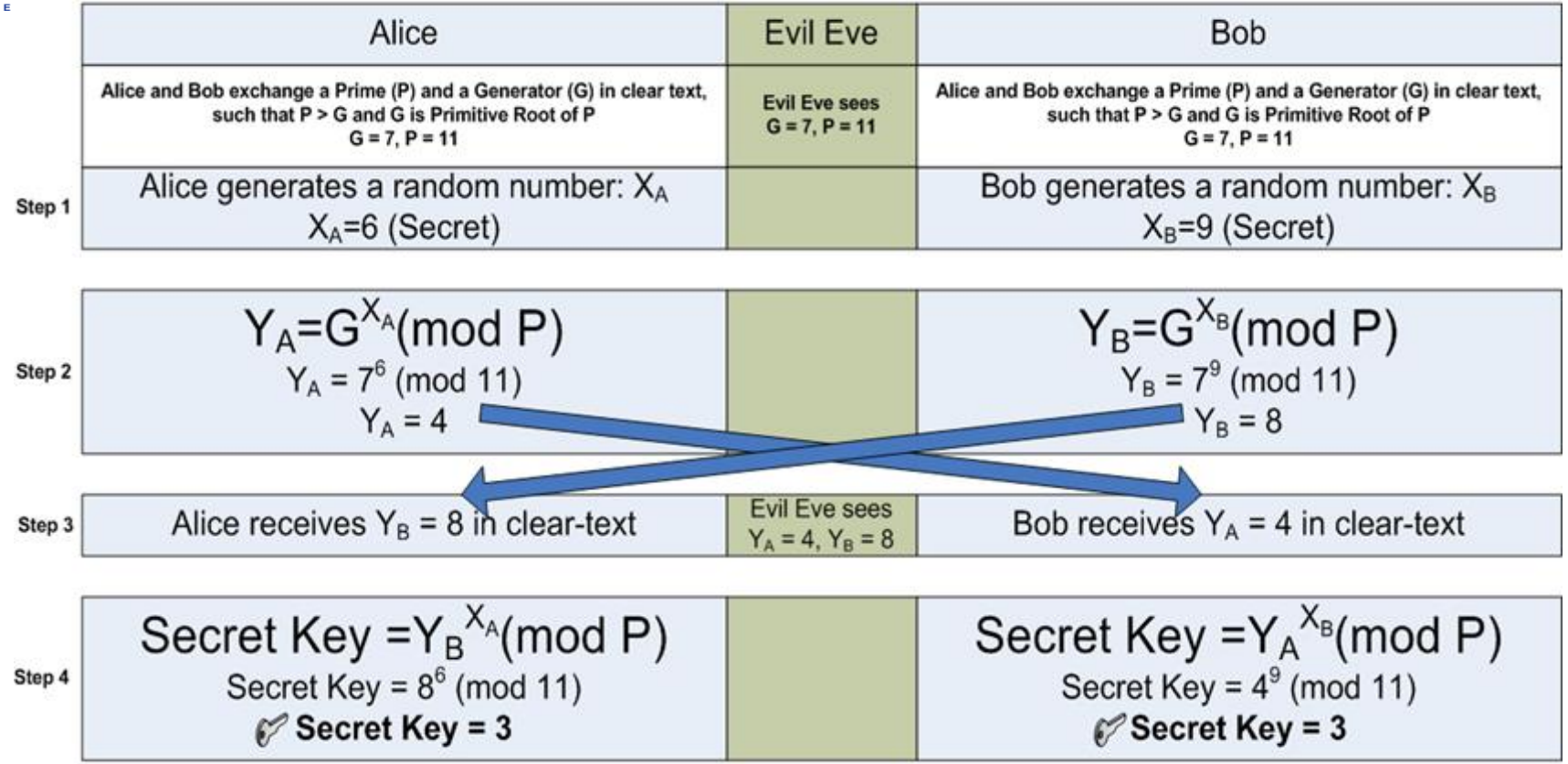
Trao đổi khóa Diffie-Hellman



Trao đổi khóa Diffie-Hellman



Trao đổi khóa Diffie-Hellman



Diffie–Hellman (DH) key exchange is a mathematical method of securely generating a symmetric cryptographic key over a public channel and was one of the first public-key protocols as conceived by Ralph Merkle and named after Whitfield Diffie and Martin Hellman. DH is one of the earliest practical examples of public key exchange implemented within the field of cryptography. Published in 1976 by Diffie and Hellman, this is the earliest publicly known work that proposed the idea of a private key and a corresponding public key.

Traditionally, secure encrypted communication between two parties required that they first exchange keys by some secure physical means, such as paper key lists transported by a trusted courier. The Diffie–Hellman key exchange method allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure channel. This key can then be used to encrypt subsequent communications using a symmetric-key cipher.

Diffie–Hellman is used to secure a variety of Internet services. However, research published in October 2015 suggests that the parameters in use for many DH Internet applications at that time are not strong enough to prevent compromise by very well-funded attackers, such as the security services of some countries.

LAB LUYỆN TẬP

1. **Làm Lab9 trên LMS**

2. Tham khảo thêm source codes C++ tại links:

https://github.com/Mich-Teng/RSA-Digital-Signature

https://tunghuynh.net/security/296/c-digital-signature-simulation-program/

https://onecompiler.com/cpp/3wvehmbxr

https://github.com/mohammedismailb18/RSA-El-Gamal-ECC-Encryption-Decryption-and-Digital-Signatures

https://github.com/SahibYar/Diffie-Hellman-key-exchange

https://www.tpointtech.com/diffie-hellmam-algorithm-in-cpp

SUMMARY

- Khái niệm chữ ký số
- Chữ ký số RSA
- Chữ ký số Elgamal
- Trao đổi khóa Diffie-Hellman
- Luyện tập với code C++

ĐẠI NAM
UNIVERSITY