# MỤC LỤC

### LỜI CẢM ƠN 3

### MỞ ĐẦU 4

### CHƢƠNG 1: CƠ SỞ TOÁN HỌC CỦA CHỮ KÝ SỐ 5

### SỐ HỌC MODUL 5

### Số nguyên tố 5

### Đồng dƣ 5

### 1.3 Trong tập hợp Zn và Z\*

n

### ................................................................................. 5

### Phần tử nghịch đảo trong Zn 6

### Nhóm nhân Z\*

n

### .............................................................................................. 6

* 1. [Thặng dƣ bậc hai theo modulo 7](#_TOC_250010)

1. [Hàm băm 8](#_TOC_250009)
   1. Giới thiệu 8
   2. [Định nghĩa 8](#_TOC_250008)

[2.3 Ứng dụng 9](#_TOC_250007)

* 1. Một số hàm Hash sử dụng trong chữ ký số 10
  2. Các hàm Hash mở rộng 11

1. Hệ mật mã 13

[3.1 Giới thiệu về hệ mật mã 13](#_TOC_250006)

* 1. Sơ đồ hệ thống mật mã 13
  2. Mật mã khóa đối xứng 13
  3. Mã khóa công khai 21

1. [Hệ mật mã Elgamma 24](#_TOC_250005)

[CHƢƠNG II. CHỮ KÝ SỐ 26](#_TOC_250004)

* 1. [Chữ ký số 26](#_TOC_250003)

[............................................................................ 26](#_TOC_250002)



* + 1. [Định nghĩa chữ ký số 26](#_TOC_250001)
    2. [Các ƣu điểm của chữ ký số 26](#_TOC_250000)

### 2.1.4 Tình trạng hiện tại - luật pháp và thực tế 27

### 2.1.5.Quy trình tạo ra và kiểm tra chữ ký điện tử 28

### Sơ đồ chữ ký 30

### Định nghĩa sơ đồ chữ ký 30

### Chữ ký số RSA 30

### Chữ ký Elgamal 32

### Chữ ký không chối bỏ 33

### CHƢƠNG 3: DỊCH VỤ CHỨNG THỰC CHỮ KÝ SỐ 38

### Tổ chức chứng thực là gì ? 38

### Giới thiệu về một số tổ chức chứng thực. 38

### Dịch vụ chứng thực chữ ký số 39

### Tình hình phát triển dịch vụ chứng thực chữ ký số trên thế giới và ở VIệt Nam.

### ................................................................................................................................ 40 3.4.1 Tình hình triển khai trên thế giới .............................................................. 40

### 3.4.2 Chữ ký số ở Việt Nam 42

### Hành lang pháp lý 44

### Ví Dụ: Chứng thực macro trong Word và Excel bằng chữ ký điện tử 46

### KẾT LUẬN 50

### TÀI LIỆU THAM KHẢO 51

# LỜI CẢM ƠN.

### Em xin chân thành cám ơn Ts. Lê Phê Đô – ngƣời luôn chỉ bảo, hƣớng dẫn, cung cấp những tài liệu quý báu trong quá trình học và hoàn thành đồ án này.

Em xin cám ơn các thầy cô giáo trong khoa công nghệ thông tin – trƣờng DHDL Hải Phòng và gia đình đã tạo điều kiện giúp đỡ về vật chất cũng nhƣ tinh thần để em có thể học tập tốt và hoàn thành đồ án này

Sinh viên

Hà Thị Hồng Gấm

# MỞ ĐẦU

Hàng ngày chúng ta vẫn hay dùng chữ ký để xác minh một vấn đề, hay để xác nhận quyền của mình đối với một vật thông qua những giấy tờ hoặc là một hợp đồng nào đó. Chẳng hạn nhƣ trên một bức thƣ nhận tiền từ ngân hàng, hay những hợp đồng ký kết mua bán, chuyển nhƣợng. Những chữ ký nhƣ vậy còn gọi là chữ ký viết tay, bởi nó đƣợc viết bởi chính tay ngƣời ký không thể sao chụp đƣợc. Thông thƣờng chữ ký viết tay trên các văn bản, trên các tài liệu hay trên các hợp đồng kinh tế ...v.v ... thì đƣợc dùng để xác nhận ngƣời ký nó.

Ngày nay khi sự phát triển của internet và công nghệ thông tin ngày càng cao. Đã cho phép chúng ta thực hiện những giao dịch điện tử thông qua internet,nhƣng tính linh hoạt của internet cũng tạo cơ hội cho “bên thứ ba” có thể thực hiện các hành động bất hợp pháp nhƣ: nghe trộm,giả mạo,mạo danh. Do vậy để đảm bảo an toàn trong các thƣơng mại điện tử và các giao dịch điện tử cần có các hình thức bảo mật có hiệu quả nhất công nghệ phổ biến hiện nay đƣợc sử dụng là chữ ký số.

Từ những vấn đề an toàn về giao dịch và tính tƣơng đồng và hợp lý của chữ ký bằng tay thì chữ ký điện tử ra đời co những nét đặc trƣng của chữ ký bằng tay. Nhƣng thông tin trên máy tính luôn đƣợc sao chép một cách dễ dàng việc thay đổi hoặc đánh cắp thông tin của một văn bản là rất đơn giản, cách sử dụng hình ảnh của chữ ký bằng tay không thể áp dụng vào đƣợc do vậy tạo ra một chữ ký số ngƣời ta phải áp dụng những công nghệ nhƣ mã hóa,chứng thực…

Đồ án này đề cập tới vấn đề chữ ký số và dịch vụ chứng thực chữ ký số. Đồ án gồm 3 chƣơng :

Chƣơng I: Cơ sở toán học của chữ ký số.

Trong chƣơng này đề cập tới các khái niệm toán học và cơ sở toán của chữ ký điện tử. Chƣơng II: Chữ ký số

Trong chƣơng này ta tìm hiểu chi tiết về chữ ký số và một vài phƣơng pháp ký Chƣơng III: Dịch vụ chứng thực chữ ký số.

Tìm hiểu về dịch vụ chứng thực chữ ký số và tình hình triển khai dịch vụ này trên thế giới và ở Việt Nam.

VÍ DỤ: Chứng thực macro trong Word và Excel

# CHƯƠNG 1: CƠ SỞ TOÁN HỌC CỦA CHỮ KÝ SỐ

## SỐ HỌC MODUL

* 1. **Số nguyên tố**

Định nghĩa:

Số nguyên tố là số nguyên dƣơng chỉ chia hết cho 1 và chính nó Tính chất:

 Giả sử p là số nguyên tố và p|a.b thì p|a hoặc p|b hoặc cả hai đều chia hết cho p.  Có vô số số nguyên tố.

## Đồng dư

Định nghĩa:

Nếu a và b là hai số nguyên, khi đó a đƣợc gọi là đồng dƣ với b theo modulo n, đƣợc viết a b(mod n) nếu (a - b)chia hết cho n, và n đƣợc gọi là modulus của đồng dƣ.

Ví dụ :

24 9 (mod 5) vì 24 – 9 = 3 \* 5.

-11 17 (mod 7) vì -11 – 17 = -4 \* 7.

Tính chất

 a b(mod n), nếu và chỉ nếu a và b đều trả số dƣ nhƣ nhau khi đem chia chúng cho n  a a(mod n) Tính phản xạ

 Nếu a b (mod n) thì b a (mod n) Tính đối xứng

 Nếu a b (mod n) và b c (mod n) thì a c (mod n) Tính bắc cầu  Nếu a a1 (mmod n) và b b1 (mod n) thì a + b a1 + b1 (mod n)  Nếu a a1 (mmod n) và b b1 (mod n) thì a \* b a1 \* b1 (mod n)

## 1.3 Trong tập hợp Zn và Z\*n

Ta kí hiệu{0, 1, 2, ……., n-1} Zn. Tập Zn có thể đƣợc coi là tập hợp tất cả lớp tƣơng đƣơng trên Zn theo modulo n. Trên tập Zn các phép toán cộng, trừ, nhân đƣợc thực hiện theo modulo n.

Ví dụ: Z25 ={0,1,2,...,24}. Trong Z25 : 13+16 =4 bởi vì :13+16=29 4(mod 25)

Tƣơng tự, 13\*16 = 8 trong Z25 Z\*n = { p Zn | UCLN(n,p) = 1 } Ví dụ: Z2 = { 0,1 }

Z\*n ={1 } vì UCLN(1,2)=1

## Phần tử nghịch đảo trong Zn



1

Cho a Zn. Nghịch đảo nhân của a theo modulo n là một số nguyên x Zn sao cho a\*x (mod n). Nếu tồn tại thì đó là giá trị duy nhất và a gọi là khả đảo, nghịch đảo của a ký hiệu là a-1.

Tính chất

Cho a, b Zn, a/b mod n = a.b-1 mod n đƣợc xác định khi và chỉ khi b là khả nghịch theo modulo n với a Zn, phần tử a là khả nghịch khi và chỉ khi gcd(a,n) =1.

Hệ quả

Cho d=gcd(a,n). Khi đó phƣơng trình đồng dƣ có dạng a.x b mod n sẽ có nghiệm x khi và chỉ khi b chia hết cho d.

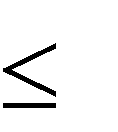
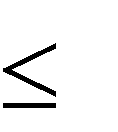
Thuật toán: Tính phần tử nghịch đảo trên Zn INPUT: a Zn

OUTPUT: a-1 mod n, nếu tồn tại.

Sử dụng thuật toán Euclide mở rộng, tìm x và y để ax+ny=d, trong đó gcd(a,n) Nếu d>1, thì a-1 mod n không tồn tại, ngƣợc lại kết quả x

## Nhóm nhân Z\*n

Định nghĩa:

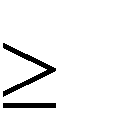
Nhóm nhân của Zn ký hiệu là Z\* ={ a Z | gcd(a,n)=1}. Đặc biệt, nếu n là số nguyên tố thì Z\* ={ a | 1 a n-1 }.

n

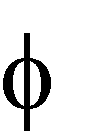
n n

Tập Z\* lập thành một nhóm con đối với phép nhân của Zn vì trong Z\* phép chia theo

n

modulo n bao giờ cũng thực hiện đƣợc. Tính chất 1

Cho n 2 là số nguyên

(i).Định lý Euler: Nếu a Z\* thì a (n) 1(mod n).

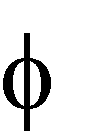


s

n

(ii).Nếu n là tích của các số nguyên tố phân biệt và nếu r

(mod (n)) thì at as (mod n) với

mọi số nguyên a. Nói cách khác, làm việc với các số theo modulo nguyên tố p thì số mũ có thể giảm theo modulo (n).

Tính chất 2

Cho số nguyên tố p



1

Định lý Fermat: Nếu gcd(a,p)=1 thì ap-1

(mod p)

Nếu r s (mod p-1) thì at as (mod p) với mọi số nguyên a. Nói cách khác, làm việc với các số theo modulo nguyên tố p thì số mũ có thể giảm theo modulo p-1.

Đặc biệt, ap a(mod p) với mọi số nguyên a.

## Thặng dư bậc hai theo modulo

Định nghĩa:

Cho a Z\* , a đƣợc gọi là thặng dƣ bậc hai theo modulo n, nếu tồn tại một x Z\* , sao cho x2 a mod n, và nếu không tồn tại x nhƣ vậy thì a đƣợc gọi là bất thặng dƣ bậc hai theo modulo n, Tập các thặng dƣ bậc hai ký hiệu là Qn và tập các bất thặng dƣ bậc hai ký hiệu là *Qn* .

n n

Tính chất:

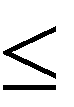
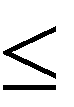
Cho p là nguyên tố lẻ và là phần tử sinh của Z\* , thì a Z\*

là thặng dƣ bậc hai modulo p

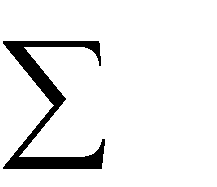
p p

khi và a =ai mod p.

Thuật toán: Tính luỹ thừa theo modulo n trong Zn

INPUT: a Zn, số nguyên 0 k n trong đó k biểu diễn dạng nhị phân. k= OUTPUT: ak mod n

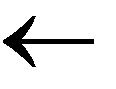
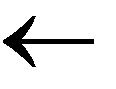
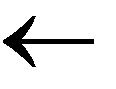
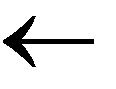
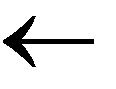
*t*



*k* 2*i*

*i*

*i* 0

1. Đặt b 1, nếu k=0 thì kết quả b
2. Đặt A  a.
3. Nếu k0=1, thì đặt b a.
4. Với mỗi I từ 1 đến t, thực hiện nhƣ sau:
   1. Đặt A A2 mod n.
   2. Nếu ki=1, thì b A.b mod n
5. Kết quả b

Ví dụ: Bảng dƣới đây mô tả các bƣớc thực hiện để tính luỹ thừa theo *modulo 1234*. của phép tính *5596 mod 1234 = 1013*.

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| i | | *0* | *1* | *2* | *3* | *4* | *5* | *6* | | *7* | *8* | *9* |
| k  i | | *0* | *0* | *1* | *0* | *1* | *0* | *1* | | *0* | *0* | *1* |
| A | | *5* | *25* | *625* | *681* | *1011* | *369* | *421* | | *779* | *947* | *925* |
| b | | *1* | *1* | *625* | *625* | *67* | *67* | *1059* | | *1059* | *1059* | *1013* |
|  | Phép toán | | | | | | | | Độ phức tạp | | | |

|  |  |  |
| --- | --- | --- |
| Phép cộng modulo | (a+b)mod n | O(ln n) |
| Phép trừ modulo | (a-b)mod n | O(ln n) |
| Phép nhân modulo | (a.b)mod n | O((ln n)2) |
| Phép lấy nghịch đảo | a-1 mod n | O((ln n)2) |
| Phép tính lũy thừa modulo | ak mod n, k<n | O((ln n)3) |

## Hàm băm

## Giới thiệu

Theo các sơ đồ chữ ký thì chữ ký của thông điệp cũng có độ dài bằng độ dài của thông điệp, đó là một điều bất tiện. Ta mong muốn nhƣ trong trƣờng hợp chữ ký viết tay, chữ ký có độ dài ngắn và hạn chế cho dù văn bản có độ dài bằng bao nhiêu. Vì chữ ký số đƣợc ký cho từng bit của thông điệp, nếu muốn chữ ký có độ dài hạn chế trên thông điệp có độ dài tùy ý thì ta phải tìm cách rút gọn độ dài thông điệp. Nhƣng bản thân thông điệp không thể rút ngắn đƣợc, nên chỉ còn cách là tìm cho mỗi thông điệp một thông điệp thu gọn có độ dài hạn chế và thay việc ký trên thông điệp, ta ký trên thông điệp thu gọn.

Để giải quyết vấn đề này ta sử dụng hàm băm, chấp nhận một thông điệp có độ dài tuỳ ý làm đầu vào. Hàm băm sẽ biến đổi thông điệp này thành một thông điệp rút gọn và sau đó sẽ dùng lƣợc đồ ký để ký lên thông điệp rút gọn đó.

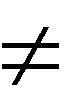
## Định nghĩa

Hàm Hash là hàm tính toán có hiệu quả khi ánh xạ các dòng nhị phân có độ dài tùy ý thành những dòng nhị phân có độ dài cố định nào đó.

* Hàm Hash yếu: hàm Hash gọi là yếu nếu cho một thông báo x thì về mặt tính toán không tìm ra đƣợc thông báo x’ khác x sao cho:

h(x’) = h(x)

* Hàm Hash mạnh: hàm Hash đƣợc gọi là mạnh nếu về mặt tính toán không tìm ra đƣợc hai thông báo x và x’ sao cho:

x1  x2 và h(x1) = h(x2)

Nói cách khác, tìm hai văn bản khác nhau có cùng một đại diện là cực kỳ khó

Hàm Hash phải là hàm một phía, nghĩa là cho x tính z = h(x) thì dễ, nhƣng ngƣợc lại, biết z tính x là công việc cực khó.

Hàm Hash yếu làm cho chữ ký trở lên tin cậy giống nhƣ việc ký trên toàn thông báo.

Hàm Hash mạnh có tác dụng chống lại kẻ giả mạo tạo ra hai bản thông báo có nội dung khác nhau, sau đó thu nhận chữ ký hợp pháp cho một bản thông báo dễ đƣợc xác nhận rồi lấy nó giả mạo làm chữ ký của thông báo thứ 2 hay nói cách khác tìm 2 văn bản khác nhau có cùng một đại diện là cực kỳ khó.

Một hàm băm tốt phải thỏa mãn các điều kiện sau:  Tính toán nhanh.

 Các khoá đƣợc phân bố đều trong bảng.  Ít xảy ra đụng độ.

 Xử lý đƣợc các loại khóa có kiểu dữ liệu khác nhau.

#### 2.3 Ứng dụng

Các hàm băm đƣợc ứng dụng trong nhiều lĩnh vực, chúng thƣờng đƣợc thiết kế phù hợp với từng ứng dụng. Ví dụ, các [hàm băm mật mã học](http://vi.wikipedia.org/wiki/H%C3%A0m_b%C4%83m_m%E1%BA%ADt_m%C3%A3_h%E1%BB%8Dc) giả thiết sự tồn tại của một đối phƣơng - ngƣời có thể cố tình tìm các dữ liệu vào với cùng một giá trị băm. Một hàm băm tốt là một phép biến đổi "một chiều", nghĩa là không có một phƣơng pháp thực tiễn để tính toán đƣợc dữ liệu vào nào đó tƣơng ứng với giá trị băm mong muốn, khi đó việc [giả mạo](http://vi.wikipedia.org/w/index.php?title=Gi%E1%BA%A3_m%E1%BA%A1o&action=edit&redlink=1) sẽ rất khó khăn. Một [hàm một chiều](http://vi.wikipedia.org/w/index.php?title=H%C3%A0m_m%E1%BB%99t_chi%E1%BB%81u&action=edit&redlink=1) mật mã học điển hình không có tính chất [hàm đơn ánh](http://vi.wikipedia.org/wiki/%C3%81nh_x%E1%BA%A1) và tạo nên một hàm băm hiệu quả; một [hàm trapdoor](http://vi.wikipedia.org/w/index.php?title=H%C3%A0m_trapdoor&action=edit&redlink=1) mật mã học điển hình là hàm đơn ánh và tạo nên một hàm ngẫu nhiên hiệu quả.

[Bảng băm](http://vi.wikipedia.org/w/index.php?title=B%E1%BA%A3ng_b%C4%83m&action=edit&redlink=1), một ứng dụng quan trọng của các hàm băm, cho phép tra cứu nhanh một bản ghi dữ liệu nếu cho trƣớc khóa của bản ghi đó (Lƣu ý: các khóa này thƣờng không bí mật nhƣ trong [mật mã học](http://vi.wikipedia.org/wiki/M%E1%BA%ADt_m%C3%A3_h%E1%BB%8Dc), nhƣng cả hai đều đƣợc dùng để "mở khóa" hoặc để truy nhập thông tin.) Ví dụ, các khóa trong một từ điển điện tử Anh-Anh có thể là các từ tiếng Anh, các bản ghi tƣơng ứng với chúng chứa các định nghĩa. Trong trƣờng hợp này, hàm băm phải ánh xạ các xâu chữ cái tới các chỉ mục của [mảng](http://vi.wikipedia.org/w/index.php?title=M%E1%BA%A3ng_%28c%E1%BA%A5u_tr%C3%BAc_d%E1%BB%AF_li%E1%BB%87u%29&action=edit&redlink=1) nội bộ của bảng băm.

Các hàm băm dành cho việc phát hiện và sửa lỗi tập trung phân biệt các trƣờng hợp mà dữ liệu đã bị làm nhiễu bởi các quá trình ngẫu nhiên. Khi các hàm băm đƣợc dùng cho các [giá trị tổng kiểm](http://vi.wikipedia.org/wiki/Gi%C3%A1_tr%E1%BB%8B_t%E1%BB%95ng_ki%E1%BB%83m), giá trị băm tƣơng đối nhỏ có thể đƣợc dùng để kiểm chứng rằng một file dữ liệu có kích thƣớc tùy ý chƣa bị sửa đổi. Hàm băm đƣợc dùng để phát hiện lỗi truyền dữ liệu. Tại nơi gửi, hàm băm đƣợc tính cho dữ liệu đƣợc gửi, giá trị băm này đƣợc gửi cùng dữ liệu. Tại đầu nhận, hàm băm lại đƣợc tính lần nữa, nếu các giá trị băm không trùng nhau

thì lỗi đã xảy ra ở đâu đó trong quá trình truyền. Việc này đƣợc gọi là [kiểm tra dƣ](http://vi.wikipedia.org/w/index.php?title=Ki%E1%BB%83m_tra_d%C6%B0&action=edit&redlink=1) (redundancy check).

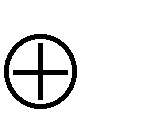
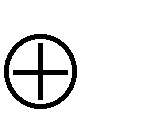
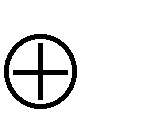
Các hàm băm còn đƣợc ứng dụng trong việc nhận dạng âm thanh, chẳng hạn nhƣ xác định xem một file [MP3](http://vi.wikipedia.org/wiki/MP3) có khớp với một file trong danh sách một loại các file khác hay không.

[Thuật toán tìm kiếm xâu Rabin-Karp](http://vi.wikipedia.org/w/index.php?title=Thu%E1%BA%ADt_to%C3%A1n_t%C3%ACm_ki%E1%BA%BFm_x%C3%A2u_Rabin-Karp&action=edit&redlink=1) là một [thuật toán tìm kiếm xâu kí tự](http://vi.wikipedia.org/w/index.php?title=Thu%E1%BA%ADt_to%C3%A1n_t%C3%ACm_ki%E1%BA%BFm_x%C3%A2u_k%C3%AD_t%E1%BB%B1&action=edit&redlink=1) tƣơng đối nhanh, với thời gian chạy trung bình [O(n)](http://vi.wikipedia.org/w/index.php?title=K%C3%AD_hi%E1%BB%87u_O_l%E1%BB%9Bn&action=edit&redlink=1). Thuật toán này dựa trên việc sử dụng băm để so sánh xâu.

## Một số hàm Hash sử dụng trong chữ ký số

##### *Các hàm Hash đơn giản:*

Tất cả các hàm Hash đều đƣợc thực hiện theo quy tắc chung là: Đầu vào đƣợc biểu diễn dƣới dạng một dãy các khối n bit, các khối n bit này đƣợc xử lý theo cùng một kiểu và lặp đi lặp lại để cuối cùng cho đầu ra có số bit cố định.

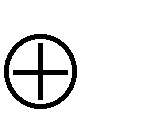
Hàm Hash đơn giản nhất là thực hiện phép toán XOR từng bit một của mỗi khối. Nó đƣợc biểu diễn nhƣ sau:

Ci = b1i b2i … bmi Trong đó :

Ci : là bit thứ i của mã Hash, i = 1, *n*

m : là số các khối đầu vào

bji : là bit thứ i trong khối thứ j là phép cộng modulo 2



:

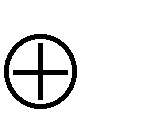
Sơ đồ hàm Hash sử dụng phép XOR.

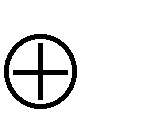
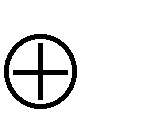
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Khối 1: | b11 | b12 | … | b1n |
| Khối 2: | b21 | b22 | … | b2n |
| … | … | … | … | … |
| Khối m: | bm1 | bm2 | … | bmn |
| Mã Hash: | C1 | C2 | … | Cn |

Ci là bit kiểm tra tính chẵn lẻ cho vị trí thứ i khi ta chia tệp dữ liệu thành từng khối, mỗi khối con vị trí. Nó có tác dụng nhƣ sự kiểm tra tổng thể tính toàn vẹn của dữ liệu.

Khi mã hóa một thông báo dài thì ta sử dụng mode CBC (The Cipher Block Chaining), thực hiện nhƣ sau:

Giả sử thông báo X đƣợc chia thành các khối 64 bit liên tiếp X= X1X2 … Xn

Khi đó mã Hash C sẽ là: C = XNH = X1 X2 … Xn



Sau đó mã hóa toàn bộ thông báo nối với mã Hash theo mode CBC sản sinh ra bản mã.

Y1Y2 …YN+1

##### *Kỹ thuật khối xích :*

Ngƣời ta đầu tiên đề xuất kỹ thuật mật mã xích chuỗi nhƣng không có khóa bí mật là Rabin.

Kỹ thuật này đƣợc thực hiện nhƣ sau :

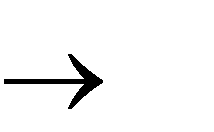
Chia thông báo M thành các khối có cỡ cố định là M1, M2, …, MN, sử dụng hệ mã thuận tiện nhƣ DES để tính mã Hash nhƣ sau :

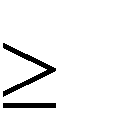
H0 = giá trị ban đầu

Hi = EMi(Hi-1), i = 1, *N*

G = HN

## Các hàm Hash mở rộng:

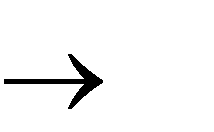
Ở trên, ta đề cập đến hàm Hash có nhiều đầu vào hữu hạn. Tiếp theo ta sẽ đề cập tới loại hàm Hash mạnh với đầu vào vô hạn thu đƣợc do mở rộng một hàm Hash mạnh có đầu vào độ dài hữu hạn. Hàm này sẽ cho phép ký các thông báo có độ dài tùy ý.



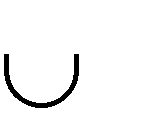
t

Giả sử h: (Z2 )m (Z2 )t là một hàm Hash mạnh, trong đó m hàm Hash mạnh :

+ 1 ta sẽ xây dựng một

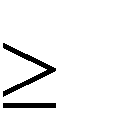
h\*: X (Z2 )t, trong đó



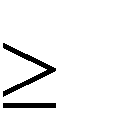
*X* = (Z2 )i

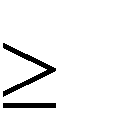
*i m*

* Xét trƣờng hợp m + 2

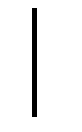
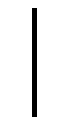
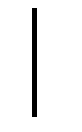
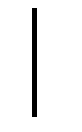
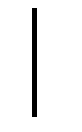
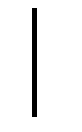


t

Giả sử x X, vậy thì tồn tại n để x (Z2 )n, n m.

Ký hiệu : |x| là độ dài của x tính theo bit. Khi đó, |x| = n. Ký hiệu : x || y là dãy bit thu đƣợc do nối x với y.

Giả sử |x| = n m. Ta có thể biểu diễn x nhƣ sau: x = x1 x2 … xk



Trong đó

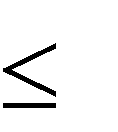
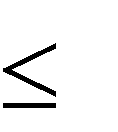
*x*1 =

*x*2 = … =

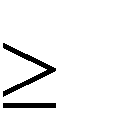
*xk* 1

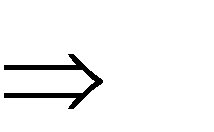
= m – t – 1 và

*xk* = m – t – 1 – d,

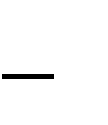
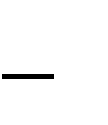
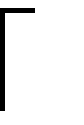
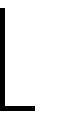
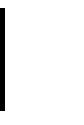
0 d m – t – 2



*xk*



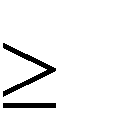
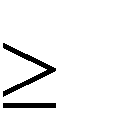
Khi đó: k =



*n*

*m t* 1

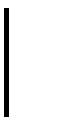
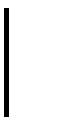
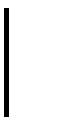
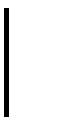
1 và m – t – 1 1, k 2.

+ 1

Thuật toán xây dựng h thành h\* đƣợc mô tả nhƣ sau :

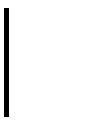
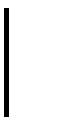
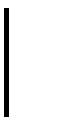
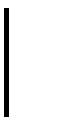
1. Cho i = 1 tới k-1 gán yi = xi ;
2. yk = xk || 0d (0d là dãy có d số 0. Khi đó yk dài m-t-1)
3. yk+1 là biểu diễn nhị phân của d (|yk+1| = m-t-1)

4. g1 = h( 0t+1 y1) ( *g* = t, 0t+1 y1 dài m)

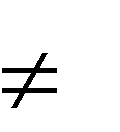
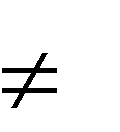


1

1. Cho i=1 tới k thực hiện gi+1 = h( gi 1 yi+1 )



* 1. h\*(x) = gk+1

Ký hiệu y(x) = y1 || y2 ||… || yk+1 Ta thấy rằng y(x) y(x’) nếu x x’

* Xét trƣờng hợp m=t+1

Cũng nhƣ trên, ta giả sử |x| = n >m Ta xác định f nhƣ sau:

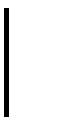
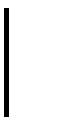
f(0) = 0;

f(1) = 01;

Thuật toán xây dựng h\* khi m=t+1 nhƣ sau :

1. Cho y= y1,y2, …, yk =11 || f(x1) || f(x2) … f(xn) (x1 là một bit)

2. g1 = h( 0t y1) ( *y*

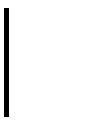
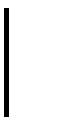


1

= m – t )

1. Cho i=1 tới k -1 thực hiện

gi+1 = h( gi yi+1 ) ( *yi*



1. h\*(x) = gk\*s

= m – t - 1)

Ngoài ra còn có một số hàm Hash khác nhƣ hàm Hash MD4 và hàm Hash MD5.

## Hệ mật mã

* 1. **Giới thiệu về hệ mật mã**

Mật mã đã đƣợc sử dụng từ rất sớm, khi con ngƣời biết trao đổi thông tin cho nhau và trải qua bao nhiêu năm nó đã đƣợc phát triển từ những hình thức sơ khai cho đến hiện đại và tinh vi. Mật mã đƣợc sử dụng trong rất nhiều lĩnh vực của con ngƣời và các quốc gia, đặc biệt trong các lĩnh vực quân sự, chính trị, ngoại giao và thƣơng mại. Mục đích của mật mã là tạo ra khả năng trao đổi thông tin trên một kênh thông tin chung cho những đối tƣợng cùng tham gia trao đổi thông tin và không muốn một đối tƣợng thứ ba khác biết đƣợc những thông tin mà họ trao đổi.

Khi một đối tƣợng A muốn gửi một thông điệp cho những ngƣời nhận, A sẽ phải mã hóa thông điệp và gửi đi, những ngƣời nhận đƣợc thông điệp mã hóa muốn biết đƣợc nội dung thì phải giải mã thông điệp mã hóa. Các đối tƣợng trao đổi thông tin cho nhau phải thỏa thuận với nhau về cách thức mã hóa và giải mã, quan trọng hơn là khóa mật mã đã sử dụng trong quá trình mã hóa và giải mã, nó phải tuyệt đối đƣợc giữ bí mật. Một đối tƣợng thứ ba mặc dù có biết đƣợc nhƣng sẽ không biết đƣợc nội dung thông điệp đã mã hóa.

Có hai phƣơng pháp mã hóa dữ liệu là Mã hóa khóa đối xứng và Mã hóa khóa công khai.

## Sơ đồ hệ thống mật mã

Là một bộ năm (P, C, K, E, D) trong đó:

+ P là một tập hữu hạn các bản rõ.

+ C là một tập hữu hạn các bản mã.

+ K là một tập hữu hạn các khoá.

+ Với mỗi k є K, có một hàm lập mã ek є E ek: P → C

và một hàm giải mã dk є D

dk: C → P sao cho dk(ek(x)) = x với mọi x є P

## Mật mã khóa đối xứng

Phƣơng pháp mã hóa đối xứng (symmetric cryptography) còn đƣợc gọi là mã hóa khóa bí mật (secret key cryptography). Với phƣơng pháp này, ngƣời gửi và ngƣời nhận sẽ dùng chung một khóa để mã hóa và giải mã thông điệp. Trƣớc khi mã hóa thông điệp gửi

đi, hai bên gửi và nhận phải có khóa chung và phải thống nhất thuật toán dùng để mã hóa và giải mã. Có nhiều thuật toán ứng dụng cho mã hóa khóa bí mật DES - Data Encrytion Standard, 3DES - triple-strength DES, RC2 - Rons Cipher 2 và RC4, v.v... và sơ khai nhất là các hệ mật mã cổ điển.

Nhƣợc điểm chính của phƣơng pháp này là khóa đƣợc truyền trên kênh an toàn nên chi phí tốn kém và không kip thời. Ƣu điểm là tốc độ mã hóa và giải mã rất nhanh.

#### Một số hệ mật mã cổ điển

* + 1. **Mã dịch chuyển:**

**Định nghĩa:** Mã dịch chuyển: (P, C, K, E, D)

P = C = K = Z với k є K, định nghĩa e (x) = (x + k) mod 26 d (y) = (y – k) mod 26

26 k k

(x, y є Z )

26

*Ví dụ*: Dùng khoá k = 9 để mã hoá dòng thƣ: “toinaydichoi” dòng thƣ đó tƣơng ứng với dòng số

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| t | o | i | n | a | y | d | i | c | h | o | i |
| 19 | 14 | 8 | 12 | 0 | 24 | 3 | 8 | 2 | 7 | 14 | 8 |

qua phép mã hoá e sẽ đƣợc:

9

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 2 | 23 | 17 | 22 | 9 | 7 | 12 | 17 | 11 | 16 | 23 | 17 |
| c | x | r | w | j | h | m | r | l | q | x | r |

bản mã sẽ là:

“qnwcxrcqdkjh”

Nhận đƣợc bản mã đó, dùng d9 để nhận đƣợc bản rõ.

Cách đây 2000 năm mã dịch chuyển đã đƣợc Julius Ceasar sử dụng, với khoá k=3 mã địch chuyển đƣợc gọi là mã Ceasar.

Tập khoá phụ thuộc vào Zm với m là số khoá có thể.

Trong tiếng Anh tập khoá chỉ có 26 khoá có thể, việc thám mã có thể đƣợc thực hiện bằng cách duyệt tuần tự 26 khoá đó, vì vậy độ an toàn của mã dịch chuyển rất thấp.

#### Mã thay thế:

**Định nghĩa** Mã thay thế: (P, C, K, E, D)

P = C = Z , K = S (Z ) Với mỗi π є K, tức là một hoán vị trên Z , ta xác định

26 26 26

e (x) = π (x)

π

-1

dπ(y) = π (y)

-1

với x, y є Z , π

26

là nghịch đảo của л

*Ví dụ:* π đƣợc cho bởi (ở đây ta viết chữ cái thay cho các con số thuộc Z ):

26





bản rõ:

“toinaydichoi”

sẽ đƣợc mã hoá thành bản mã (với khoá π):

“mfzsxdazygfz”

-1

Dễ xác định đƣợc π , và do đó từ bản mã ta tìm đƣợc bản rõ.

Mã thay thế có tập hợp khoá khá lớn - bằng số các hoán vị trên bảng chữ cái, tức số các

26

hoán vị trên Z

, hay là 26! > 4.10

26

. Việc duyệt toàn bộ các hoán vị để thám mã là rất khó,

ngay cả đối với máy tính. Tuy nhiên, bằng phƣơng pháp thống kê, ta có thể dễ dàng thám đƣợc các bản mã loại này, và do đó mã thay thế cũng không thể đƣợc xem là an toàn.

#### Mã Anffine:

**Định nghĩa** Mã Anffine: (P, C, K, E, D)

P = C = Z , K = { (a, b) є Z x Z : (a, 26) = 1 }

26 26 26

với mỗi k = (a, b) є K ta định nghĩa: e (x) = ax + b mod 26

k

-1

d (y) = a

k

(y – b) mod 26

trong đó x, y є Z

26

*Ví dụ:* Lấy k = (5, 6). Bản rõ:

“toinaydichoi”

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | t | o | i | n | a | y | d | i | c | h | o | i |
| x | 19 | 14 | 8 | 13 | 0 | 14 | 3 | 8 | 2 | 7 | 14 | 8 |

y=5x + 6 mod 26

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| y | 23 | 24 | 20 | 19 | 6 | 24 | 21 | 20 | 16 | 15 | 24 | 20 |
|  | x | y | u | t | g | y | v | u | q | p | y | u |

Bản mã:

“xyutgyvuqpyu”

Thuật toán giải mã trong trƣờng hợp này có dạng: dk(y) = 21(y − 6) mod 26

Với mã Apphin, số các khoá có thể có bằng (số các số ≤ 26 và nguyên tố với 26) × 26, tức

là 12 × 26 = 312. Việc thử tất cả các khoá để thám mã trong trƣờng hợp này tuy khá mất thì giờ nếu tính bằng tay, nhƣng không khó khăn gì nếu dùng máy tính. Do vậy, mã Apphin cũng không phải là mã an toàn.

#### Mã Vigenère:

**Định nghĩa** Mã Vigenere: (P, C, K, E, D) Cho m là số nguyên dƣơng.

P = C = K = Z m

26

với mỗi khoá k = (k , k ,…,k ) є K có:

1 2 m

e (x , x ,…, x ) = (x + k , x + k ,…, x + k )

k 1 2 m 1 1 2 2 m m

d (y , y ,…, y ) = (y – k , y – k ,…, y – k )

k 1 2 m 1 1 2 2 m m

các phép cộng phép trừ đều lấy theo modulo 26

*Ví dụ:* Giả sử m = 6 và khoá k là từ CIPHER - tức k=(2, 8, 15, 7, 4, 17). Bản rõ:

“toinaydichoi”

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | t | o | i | n | a | y | d | i | c | h | o | i |
| x | 19 | 14 | 8 | 13 | 0 | 24 | 3 | 8 | 2 | 7 | 14 | 8 |
| k | 2 | 8 | 15 | 7 | 4 | 17 | 2 | 8 | 15 | 7 | 4 | 17 |
| y | 21 | 22 | 23 | 20 | 4 | 15 | 5 | 16 | 17 | 14 | 18 | 25 |
|  | v | w | x | u | e | p | f | q | r | o | s | z |

Bản mã

“vwxuepfqrosz”

Từ bản mã đó, dùng phép giải mã dk tƣơng ứng, ta lại thu đƣợc bản rõ. Chú ý: Mã Vigenere với m = 1 sẽ trở thành mã Dịch chuyển.

Tập hợp các khoá trong mã Vigenere mới m ≥ 1 có tất cả là 26m khoá có thể có. Với m

= 6, số khoá đó là 308.915.776, duyệt toàn bộ chừng ấy khoá để thám mã bằng tính tay thì khó, nhƣng với máy tính thì vẫn là điều dễ dàng.

#### Mã Hill:

**Định nghĩa** Mã Hill: (P, C, K, E, D) Cho m là số nguyên dƣơng.

P = C = *Z m*

*26*

K = { k є *Z mxm* : (det(k), 26) = 1 } với mỗi k є K định nghĩa:

*26*

e (x , x ,…, x ) = (x , x ,…, x ).k

k 1 2 m 1 2 m

d (y , y ,…, y

) = (y , y ,…,y

-1

).k

k 1 2 m 1 2 m

*Ví dụ:* Lấy m = 2, và k =

Với bộ 2 ký tự (x , x ), ta có mã là (y , y ) = (x , x ). k đƣợc tính bởi

1 2 1 2 1 2

y = 11.x

1 1

+ 3.x

2

y = 8.x

2 1

+ 7.x

2

Giả sử ta có bản rõ: “**tudo**”, tách thành từng bộ 2 ký tự, và viết dƣới dạng số ta đƣợc

19 20 | 03 14 , lập bản mã theo quy tắc trên, ta đƣợc bản mã dƣới dạng số là: 09 06 | 23 18, và dƣới dạng chữ là “**fgxs**”.

Chú ý:

Để đơn giản cho việc tính toán, thông thƣờng chọn ma trận vuông 2×2. Khi đó có thể tính ma trận nghịch đảo theo cách sau :

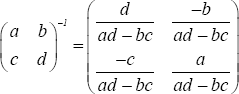
Giả sử ta có



Ta có ma trận nghịch đảo



Và đƣợc tính nhƣ sau



Một chú ý là để phép chia luôn thực hiện đƣợc trên tập Z thì nhất thiết định thức của k

26

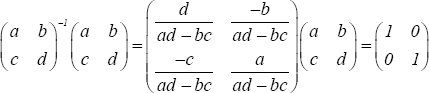
: det(k) = (ad – bc) phải có phần tử nghịch đảo trên Z , nghĩa là (ad – bc) phải là một trong

26

các giá trị : 1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, hoặc 25. Đây cũng là điều kiện để ma trận k tồn tại ma trận nghịch đảo.

-1

Khi đó: k .k = I là ma trận đơn vị (đƣờng chéo chính bằng 1)



Định thức của

Là 11\*7 – 8\*3 = 1 ≡ 1 mod 26 Khi đó

#### Mã hoán vị:

**Định nghĩa** Mã hoán vị: (P, C, K, E, D) Cho m là số nguyên dƣơng.

P = C = Z26 , K = Sm

với mỗi k = π є S , ta có

m



-1

trong đó π là hoán vị nghịch đảo của π

*Ví dụ:* Giả sử m = 6, và khoá k đƣợc cho bởi phép hoán vị π

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 1 | 2 | 3 | 4 | 5 | 6 |
| 3 | 5 | 1 | 6 | 4 | 2 |

-1

Khi đó phép hoán vị nghịch đảo π là:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 1 | 2 | 3 | 4 | 5 | 6 |
| 3 | 6 | 1 | 5 | 2 | 4 |

Bản rõ:

“toinaydichoi”

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | t | o | i | n | a | y | d | i | c | h | o | i |
| vt | 1 | 2 | 3 | 4 | 5 | 6 | 1 | 2 | 3 | 4 | 5 | 6 |
| π | 1->3 | 2->5 | 3->1 | 4->6 | 5->4 | 6->2 | 1->3 | 2->5 | 3->1 | 4->6 | 5->4 | 6->2 |
| vt | 3 | 5 | 1 | 6 | 4 | 2 | 3 | 5 | 1 | 6 | 4 | 2 |
|  | i | a | t | y | n | o | c | o | d | i | h | i |

Bản mã:

“iatynocodihi”

Dùng hoán vị nghịch đảo, từ bản mật mã ta lại thu đƣợc bản rõ. Chú ý:

Mã hoán vị là một trƣờng hợp riêng của mã Hill. Thực vậy, cho phép hoán vị π của {1,

2,…, m}, ta có thể xác định ma trận K =(k ), với

π ij



Thì dễ thấy rằng mã Hill với khoá K trùng với mã hoán vị với khoá π.

π

Với m cho trƣớc, số các khoá có thể có của mã hoán vị là m! Dễ nhận thấy với m = 26 ta có số khóa 26! (mã Thay thế).

## Mã khóa công khai:

Phƣơng pháp mã hóa khóa công khai (*public key cryptography*) còn đƣợc gọi là mã hóa bất đối xứng (*asymmetric cryptography*) đã giải quyết đƣợc vấn đề của phƣơng pháp mã hóa khóa bí mật (*đối xứng*) là sử dụng hai khóa: khóa bí mật (*private key*) và (*public key*). Khóa bí mật đƣợc giữ kín, trong khi đó đƣợc gửi công khai bởi vì tính chất khó tính đƣợc khóa bí mật từ khóa công khai. Khóa công khai và khóa bí mật có vai trò trái ngƣợc nhau, một khóa dùng để mã hóa và khóa kia sẽ dùng để giải mã.

Hiện nay các hệ mật mã khóa công khai đều dựa trên hai bài toán “khó” là bài toán logarith rời rạc trên trƣờng hữu hạn và bài toán tìm ƣớc số nguyên tố.

Phƣơng pháp cho phép trao đổi khóa một cách dễ dàng và tiện lợi. Nhƣng tốc độ mã hóa khá chậm hơn rất nhiều so với phƣơng pháp mã hóa khóa đối xứng rất nhiều, Tuy nhiên, hệ mật mã khóa công khai có một ƣu điểm nổi bật là cho phép tạo chữ ký điện tử.

* + - Một số hệ mật mã khóa công khai

#### 3.4.1 Hệ mật mã RSA

Trong mật mã học, RSA là một thuật toán mật mã hóa khóa công khai. Đây là thuật toán đầu tiên phù hợp với việc tạo ra chữ ký điện tử đồng thời với việc mã hóa. Nó đánh dấu một sự tiến bộ vƣợt bậc của lĩnh vực mật mã học trong việc sử dụng khóa công cộng. RSA đang đƣợc sử dụng phổ biến trong thƣơng mại điện tử và đƣợc cho là đảm bảo an toàn với điều kiện độ dài khóa đủ lớn.Thuật toán đƣợc Ron Rivest, Adi Shamir và Len Adleman mô tả lần đầu tiên vào năm 1977 tại Học viện Công nghệ Massachusetts (MIT). Tên của thuật toán lấy từ 3 chữ cái đầu của tên 3 tác giả.Trƣớc đó, vào năm 1973, Clifford Cocks, một nhà toán học ngƣời Anh làm việc tại GCHQ, đã mô tả một thuật toán tƣơng tự. Với

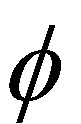
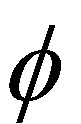
khả năng tính toán tại thời điểm đó thì thuật toán này không khả thi và chƣa bao giờ đƣợc thực nghiệm. Tuy nhiên, phát minh này chỉ đƣợc công bố vào năm 1997 vì đƣợc xếp vào loại tuyệt mật.Thuật toán RSA đƣợc MIT đăng ký bằng sáng chế tại Hoa Kỳ vào năm 1983 (Số đăng ký 4.405.829). Bằng sáng chế này hết hạn vào ngày 21 tháng 9 năm 2000. Tuy nhiên, do thuật toán đã đƣợc công bố trƣớc khi có đăng ký bảo hộ nên sự bảo hộ hầu nhƣ không có giá trị bên ngoài Hoa Kỳ. Ngoài ra, nếu nhƣ công trình của Clifford Cocks đã đƣợc công bố trƣớc đó thì bằng sáng chế RSA đã không thể đƣợc đăng ký.

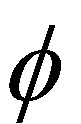
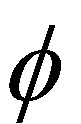
Hệ mật mã khóa công khai RSA đƣợc đƣa ra năm 1977, là công trình nghiên cứu của ba đồng tác giả Ronald Linn Revest, Adi Shamir, Leonard Aldeman. Hệ mật mã đƣợc xây dựng dựa trên tính khó giải của bài toán phân tích thừa số nguyên tố hay còn gọi là bài toán RSA

Định nghĩa: Bài toán RSA

Cho một số nguyên dƣơng n là tích của hai số nguyên tố lẻ p và q. Một số nguyên dƣơng b sao cho gcd(b, (p-1) \*(q-1)) =1 và một số nguyên c. Bài toán đặt ra là phải tìm số nguyên x sao cho xb c(mod n)

Thuật toán: Sinh khóa cho mã khóa công khai RSA Sinh hai số nguyên tố lớn p và q có giá trị xấp xỉ nhau.

Tính n=p\*q, và (n) = (p-1) (q-1), sao cho gcd(b, (n)) =1 Chọn một số ngẫu nhiên b, 1 < b < φ(n), sao cho gcd(b, φ(n)) = 1

Sử dụng thuật toán Euclide để tính số a, 1<a<(n), sao cho a\*b 1(mod (n))

Khóa công khai là (n, b). Khóa bí mật là a Thuật toán: Mã hóa RSA

(i). Lập mã :

1. Lấy khóa công khai (n, b) theo thuật toán trên
2. Chọn một bản rõ x, trong khoảng [1, n-1]
3. Tính : y = xb mod n
4. Nhận đƣợc bản mã y (ii). Giải mã :

Sử dụng khóa bí mật a để giải mã : x = ya mod n Ví dụ

Sau đây là một ví dụ với những số cụ thể. Ở đây chúng ta sử dụng những số nhỏ để tiện tính toán còn trong thực tế phải dùng các số có giá trị đủ lớn.

Lấy:

p=61: Số nguyên tố thứ nhất ( giữ bí mật sau hoặc huỷ sau khi tạo khoá) q=53: Số nguyên tố thứ hai ( giữ bí mật sau hoặc huỷ sau khi tạo khoá) n=pq=3233: Môđun ( công bố công khai)

b=17: Số mũ công khai

a=2753: Số mũ bí mật

Khóa công khai là cặp (b, *n*). Khóa bí mật là a. Hàm mã hóa là: y = *xb* mod *n* = y17 mod 3233

với *x* là văn bản rõ. Hàm giải mã là: x = ya mod *n* = y2753 mod 3233

với y là văn bản mã.

Để mã hóa văn bản có giá trị 123, ta thực hiện phép tính: y= 12317 mod 3233 = 855

Để giải mã văn bản có giá trị 855, ta thực hiện phép tính: x = 8552753 mod 3233 = 123

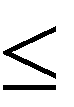
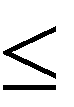
Cả hai phép tính trên đều có thể đƣợc thực hiện hiệu quả nhờ giải thuật bình phƣơng và nhân.

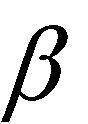
Hệ mã khóa công khai RSA đƣơc gọi là an toàn nếu ta chọn số nguyên tố p, q đủ lớn để việc phân tích phần khóa công khai n thành tích 2 thừa số nguyên tố là khó có thể thực hiện trong thời gian thực.

Tuy nhiên việc sinh một số nguyên tố đƣợc coi là lớn lại là việc rất khó, vấn đề này thƣờng đƣợc giải quyết bằng cách sinh ra các số lớn (khoảng 100 chữ số) sau đó tìm cách kiểm tra tính nguyên tố của nó.

Một vấn đề đặt ra là phải kiểm tra bao nhiêu số nguyên tố ngẫu nhiên (với kích thƣớc xác định) cho tới khi tìm đƣợc một số nguyên tố. Một kết quả nổi tiếng trong lý thuyết số (Định lý số nguyên tố) phát biểu rằng: “Số các số nguyên tố không lớn hơn N xấp xỉ bằngN/lnN”. Vậy nếu P là một số nguyên tố ngẫu nhiên thì sắc xuất để P là số nguyên tố là 1/lnP. Nói chung vấn đề cố lõi của hệ mã RSA đó là việc chọn đƣợc số nguyên tố p, q đủ lớn để đảm bảo an toàn cho bản mã. Nhƣ đã biết nếu kẻ thám mã mà biết đƣợc số nguyên tố q, p thì dễ dàng tính đƣợc khóa bí mật (a) từ khóa công khai (b, n) do đó bản mã sẽ bị lộ.

## Hệ mật mã Elgamma

Hệ mật mã khóa công khai ElGamal đƣợc đƣa ra năm 1978. Hệ mật mã này đƣợc xây dựng dựa trên tính khó giải của Bài toán logarit rời rạc phần tử sinh α của tập Z\*. Bài toán đặt ra: tìm một số nguyên x, 0 x  p-2, sao cho x mod p



Thuật toán: Sinh khóa cho mã hóa công khai Elgamal

1. Sinh ngẫu nhiên một số nguyên tố lớn p và α là phần tử sinh của Z\*p
2. Chọn ngẫu nhiên một số nguyên a, 1 ≤ a ≤ p−2, tính αa mod p
3. Khóa công khai la (p, α, αa). Khóa bí mật (a)

Thuật toán Mã hóa ElGamal (i). Lập mã:

* 1. Lấy khóa công khai (p, α, αa) theo thuật toán trên
  2. Chọn một bản mã x, trong khoảng [0, p−1]
  3. Chọn ngẫu nhiên một số nguyên k, 1 ≤ k ≤ p−2
  4. Tính γ = αk mod p và δ = x.(αa)k mod p
  5. Nhận đƣợc bản mã là (γ, δ) (ii). Giải mã:

1. Sử dụng khóa bí mật (a) và tính γp-1-a mod p
2. Lấy bản rõ: x = γp-1-a .δ mod p

Thuật toán ElGamal lấy đƣợc bản rõ vì: (γ-a).δ ≡ (α-ak).x.(αak) ≡ x (mod p). Ví dụ:

Sinh khóa: Đối tƣợng A chọn một số nguyên p = 2357 và một phần tử sinh α = 2 của tập Z\*2357. A chọn một khóa bí mật a = 1751

Và tính: αa mod p = 21751mod 2357 = 1185. Khóa công khai của A (p=2357; α=2; αa=1185).

Lập mã: Mã hóa bản rõ x = 2035, B chọn một số nguyên k = 1520 và tính: γ = 21520 mod 2357 = 1430.

và

δ = 2035.11851520 mod 2357 = 697.

B gửi γ = 1430 và δ = 697 cho A. Giải mã: Để giải mã A tính:

γp−1−a = 1430605 mod 2357 = 872.

và lấy lại đƣợc bản rõ khi tính x = 872.697 mod 2357 = 2035.

## Chữ ký số.

**CHƯƠNG II. CHỮ KÝ SỐ**

* + 1. **Giới thiệu về chữ số**

Trong 

.





?





, 



.

## Định nghĩa chữ ký số

Chữ ký số (digital signature) là đoạn dữ liệu ngắn đính kèm với văn bản gốc để chứng thực tác giả (ngƣời ký văn bản) của văn bản và giúp ngƣời nhận kiểm tra tính toàn vẹn của nội dung văn bản gốc.

## Các ưu điểm của chữ ký số

Việc sử dụng chữ ký số mang lại một số lợi điểm sau:

#### Khả năng nhận thực:

Các hệ thống mật mã hóa khóa công khai cho phép mật mã hóa văn bản với khóa bí mật mà chỉ có ngƣời chủ của khóa biết. Để sử dụng chữ ký số thì văn bản không cần phải đƣợc mã hóa mà chỉ cần mã hóa hàm băm của văn bản đó (thƣờng có độ dài cố định và ngắn hơn văn bản). Khi cần kiểm tra, bên nhận giải mã (với khóa công khai) để lấy lại hàm băm và kiểm tra với hàm băm của văn bản nhận đƣợc. Nếu 2 giá trị này khớp nhau thì bên nhận có thể tin tƣởng rằng văn bản xuất phát từ ngƣời sở hữu khóa bí mật. Tất nhiên là chúng ta không thể đảm bảo 100% là văn bản không bị giả mạo vì hệ thống vẫn có thể bị phá vỡ.

Vấn đề nhận thực đặc biệt quan trọng đối với các giao dịch tài chính. Chẳng hạn một chi nhánh ngân hàng gửi một gói tin về trung tâm dƣới dạng *(a,b)*, trong đó *a* là số tài khoản và *b* là số tiền chuyển vào tài khoản đó. Một kẻ lừa đảo có thể gửi một số tiền nào đó để lấy nội dung gói tin và truyền lại gói tin thu đƣợc nhiều lần để thu lợi (tấn công truyền lại gói tin).

#### Tính toàn vẹn

Cả hai bên tham gia vào quá trình thông tin đều có thể tin tƣởng là văn bản không bị sửa đổi trong khi truyền vì nếu văn bản bị thay đổi thì hàm băm cũng sẽ thay đổi và lập tức bị phát hiện. Quá trình mã hóa sẽ ẩn nội dung của gói tin đối với bên thứ 3 nhƣng không ngăn cản đƣợc việc thay đổi nội dung của nó. Một ví dụ cho trƣờng hợp này là tấn công đồng hình (homomorphism attack): tiếp tục ví dụ nhƣ ở trên, một kẻ lừa đảo gửi 1.000.000 đồng vào tài khoản của a, chặn gói tin *(a,b)* mà chi nhánh gửi về trung tâm rồi gửi gói tin *(a,b3)* thay thế để lập tức trở thành triệu phú!

#### Tính không thể phủ nhận

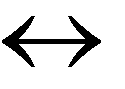
Trong giao dịch, một bên có thể từ chối nhận một văn bản nào đó là do mình gửi. Để ngăn ngừa khả năng này, bên nhận có thể yêu cầu bên gửi phải gửi kèm chữ ký số với văn bản. Khi có tranh chấp, bên nhận sẽ dùng chữ ký này nhƣ một chứng cứ để bên thứ ba giải quyết. Tuy nhiên, khóa bí mật vẫn có thể bị lộ và tính không thể phủ nhận cũng không thể đạt đƣợc hoàn toàn.

#### 2.1.4 Tình trạng hiện tại - luật pháp và thực tế

Tất cả các mô hình chữ ký số cần phải đạt đƣợc một số yêu cầu để có thể đƣợc chấp nhận trong thực tế:

 Chất lƣợng của thuật toán: một số thuật toán không đảm bảo an toàn;  Chất lƣợng của phần mềm/phần cứng thực hiện thuật toán;

 Khóa bí mật phải đƣợc giữ an toàn;

 Quá trình phân phối khóa công cộng phải đảm bảo mối liên hệ giữa khóa và thực thể sở hữu khóa là chính xác. Việc này thƣờng đƣợc thực hiện bởi hạ tầng khóa công cộng (PKI) và mối liên hệ khóa ngƣời sở hữu đƣợc chứng thực bởi những ngƣời điều hành PKI. Đối với hệ thống PKI *mở*, nơi mà tất cả mọi ngƣời đều có thể yêu cầu sự chứng thực trên thì khả năng sai sót là rất thấp. Tuy nhiên các PKI thƣơng mại cũng đã gặp phải nhiều vấn đề có thể dẫn đến những văn bản bị ký sai.

 Những ngƣời sử dụng (và phần mềm) phải thực hiện các quá trình đúng thủ tục (giao thức).

Chỉ khi tất cả các điều kiện trên đƣợc thỏa mãn thì chữ ký số mới là bằng chứng xác định ngƣời chủ (hoặc ngƣời có thẩm quyền) của văn bản.

Một số cơ quan lập pháp, dƣới sự tác động của các doanh nghiệp hy vọng thu lợi từ PKI hoặc với mong muốn là ngƣời đi tiên phong trong lĩnh vực mới, đã ban hành các điều luật cho phép, xác nhận hay khuyến khích việc sử dụng chữ ký số. Nơi đầu tiên thực hiện việc này là bang Utah (Hoa kỳ). Tiếp theo sau là các bang Massachusetts và California. Các nƣớc khác cũng thông qua những đạo luật và quy định và cả Liên hợp quốc cũng có những dự án đƣa ra những bộ luật mẫu trong vấn đề này. Tuy nhiên, các quy định này lại thay đổi theo từng nƣớc tùy theo điều kiện về trình độ khoa học (mật mã học). Chính sự khác nhau này làm bối rối những ngƣời sử dụng tiềm năng, gây khó khăn cho việc kết nối giữa các quốc gia và do đó làm

chậm lại tiến trình phổ biến chữ ký số.

## 2.1.5.Quy trình tạo ra và kiểm tra chữ ký điện tử:

#### Quy trình tạo

 Dùng giải thuật băm để thay đổi thông điệp cần truyền đi,kết quả ta đƣợc một message diget,dùng giải thuật md5 ta đƣợc digest có chiều dài 128 bit,dùng giải thuật sha ta có chiều dài 160bit.

 Sử dụng khóa private key của ngƣời để mã hóa message digest thu đƣợc ở bƣớc 1,thông thƣờng ở bƣớb này ta dùng giải thuật RSA,kết quả thu đƣợc

#### Các bước kiểm tra

 Dùng public key của ngƣời gửi (khóa này đƣợc thông báo đến mọi ngƣời) để giải mã chữ ký số của message.

 Dùng giải thuật md5 hoặc sha băm message đính kèm.

 So sánh kết quả thu đƣợc ở các bƣớc trên.Nếu trgùng nhau,ta kết luận message này không bị thay đổi trong quá trình truyền và message này là của ngƣời gửi

**Quy trình tạo chữ ký số**

Thông điệp dữ liệu



Hàm băm

Khóa bí mật

Bản tóm lƣợc

Mã hóa

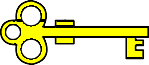
Chữ ký số

Gắn với thông điệp dữ liệu

Thông điệp dữ liệu

đƣợc ký số

**Quy trình kiểm tra chữ ký số**



Tách

Thông điệp dữ liệu

đƣợc ký số

Giải mã

Chữ ký số

Thông điệp dữ liệu

Hàm băm

Giải mã đƣợc ?

Bản tóm lƣợc

Bản tóm lƣợc

Không đúng ngƣời gửi

Giống nhau ?

Nội dung thông điệp bị thay đổi

Nội dung thông điệp

tòan vẹn

## Sơ đồ chữ ký

* + 1. **Định nghĩa sơ đồ chữ ký**

Một sơ đồ chữ ký số là bộ 5 (P, A, K, S, V) thoả mãn các điều kiện sau :

 P: là tập hữu hạn các bức điện có thể.  A: là tập hữu hạn các chữ ký có thể.

 K: không gian khoá¸ là tập hữu hạn các khoá có thể.

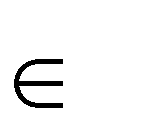
 Với mỗi *K* K tồn tại một thuật toán ký Sigk S và một thuật toán xác minh Verk V.

Mỗi Sigk: P->A và Verk: P xA -> {TRUE, FALSE} là những hàm sao cho mỗi bức điện x thuộc P và mỗi bức điện y A thoả mãn phƣơng trình sau đây :

Ver(x,y) =

TRUE nếu y= Sig(x)

FALSE nếu y # Sig(x)

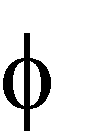
Với mỗi *K* K hàm Sig*K* và Ver*K* là các hàm thời gian đa thức. Ver*K* sẽ là hàm công khai còn Sig*K* là hàm bí mật. Ta gọi Alice là ngƣời gửi còn Bob là ngƣời nhận. Không thể dễ dàng tính toán để giả mạo chữ ký của Bob trên bức điện x. Nghĩa là với x cho trƣớc, chỉ có Bob mới có thể tính đƣợc chữ ký y để Ver(x,y) =True. Một sơ đồ chữ kí không thể an toàn vô điều kiện vì một ngƣời tò mò nào đó có thể kiểm tra tất cả các chữ số y có thể trên bức điện x nhờ dùng thuật toán Ver công khai cho đến khi anh ta có thể tìm thấy một chữ ký đúng. Vì thế, nếu có đủ thời gian anh ta luôn luôn có thể giả mạo chữ ký của Bob. Nhƣ vậy, giống nhƣ trƣờng hợp hệ thống mã hoá công khai, mục đích của chúng ta là tìm các sơ đồ chữ ký số an toàn về mặt tính toán.

## Chữ ký số RSA.

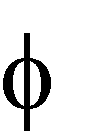
Lƣợc đồ chữ ký RSA đƣợc định nghĩa nhƣ sau:

 ***Tạo khóa***:

Sơ đồ chữ ký cho bởi bộ năm (P,A,K,S,V)

Cho n=p.q; với mỗi p,q là các số nguyên tố lớn khác nhau (n) = (p - 1)(q - 1).

Cho P = A = Zn và định nghĩa:

K là tập các khóa, K=(K’,K’’); với K’=a; K’’=(n,b) a,b Zn\*, thỏa mãn ab 1mod (n).

Các giá trị n,b là công khai, các giá trị p,q,a là các giá trị bí mật.

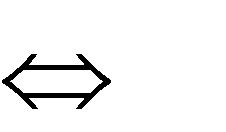
##### *Tạo chữ ký:*

Với mỗi K=(n.p,q,a,b) xác định:

SigK’(x)= xa mod n

##### *Kiểm tra chữ ký:*

VerK’’(x,y)= true x yb mod n; x, y Zn.



Giả sử A muốn gửi thông báo x, A sẽ tính chữ ký y bằng cách : y=sigK’(x)= xa mod n (a là tham số bí mật của A)

A gửi cặp (x,y) cho B. Nhận đƣợc thông báo x, chữ ký số y, B bắt đầu tiến hành kiểm tra đẳng thức

x= yb mod(n) (b là khóa công khai A)

Nếu đúng, B công nhận y là chữ ký trên x của A. Ngƣợc lại, B sẽ coi x không phải của A gửi cho mình (chữ ký không tin cậy).

Ngƣời ta có thể giả mạo chữ ký của A nhƣ sau: chọn y sau đó tính

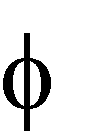
x= verK’’(y), khi đó y= sigK’(x). Một cách khắc phục khó khăn này là việc yêu cầu x phải có nghĩa. Do đó chữ ký giả mạo thành công với xác suất rất nhỏ. Ta có thể kết hợp chữ ký với mã hóa làm cho độ an toàn tăng thêm.

Giả sử trên mạng truyền tin công cộng, ta có hai hệ mật mã khóa công khai δ1 và hệ xác nhận chữ ký δ2. Giả sử B có bộ khóa mật mã K=(K’,K’’) với K’=(n,e) và K’’=d trong hệ δ1, và A có bộ khóa chữ ký Ks=(Ks’,Ks’’) với Ks’= a và Ks’’=(n,b) trong hệ δ2. A có thể gửi đến B một thông báo vừa bảo mật vừa có chữ ký xác nhận nhƣ sau: A tính chữ ký của mình là: y= sigA(x), và sau đó mã hóa cả x và y bằng cách sử dụng mật mã công khai eB của B, khi đó A nhận đƣợc z= eB(x,y), bản mã z sẽ đƣợc gửi tới B. khi nhận đƣợc z việc trƣớc tiên B phải

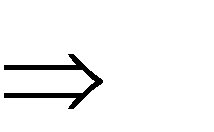
giải mã bằng hàm dB để nhận đƣợc (x,y). Sau đó B sử dụng hàm kiểm tra công khai của A để kiểm tra xem verA(x,y)= true? Tức là kiểm tra xem chữ ký đó có đúng là của A?.

*Ví dụ*:

A dùng lƣợc đồ chữ ký số RSA với n=247,(p=13,q=19);

(n) = 12.18 = 216. Khóa công khai của A là b=7.

= 7-1mod216 = 31.



a

A công khai (n,b) = (247,7)

A ký trên thông báo x=100 với chữ ký:

y = xa modn = 10031 mod247 = 74.

A gửi cặp (x,y) = (100,74) cho B, B kiểm tra bằng cách sử dụng khóa công khai của A nhƣ sau:

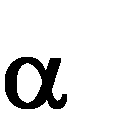
x = yb modn = 747 mod247 = 100 = x. B chấp nhận y=74 là chữ ký tin cậy.

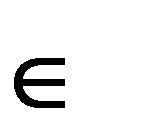
## Chữ ký Elgamal.

Lƣợc đồ chữ ký ElGamal đƣợc giới thiệu năm 1985 và đƣợc Viện tiêu chuẩn và Công nghệ quốc gia Mỹ sửa đổi thành chuẩn chữ ký số. Lƣợc đồ chữ ký ElGammal không tất định cũng giống nhƣ hệ mã hóa ElGamal. Điều này có nghĩa là có nhiều chữ ký hợp lệ cho một thông báo bất kỳ. Thuật toán kiểm tra phải có khả năng khả năng chấp nhận bất kỳ chữ ký hợp lệ nào khi xác minh.

Lƣợc đồ chữ ký ElGamal đƣợc định nghĩa nhƣ sau:

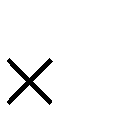
##### *Tạo khóa:*

Cho p là số nguyên tố sao cho bài toán logarit rời rạc trong Zp là khó và giả sử 

* là phần tử nguyên thủy

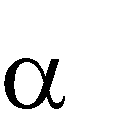
**Z**

*p*

Cho P = Z \* , A = Z \* Zp-1 và định nghĩa

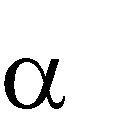
*p p*

* + K = {(p, a,



, ):

= a modp }.

Các giá trị p, , là công khai, a là bí mật.



##### *Tạo chữ ký*

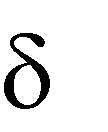
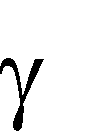
Với K = (p, a, và với số ngẫu nhiên k Z\* ,

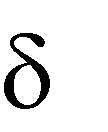


, )

*p* 1

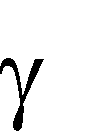
định nghĩa sigk( , ), trong đó:



o = modp và = (x - a k -1mod(p - 1).

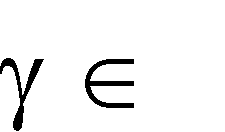


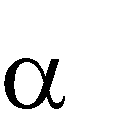
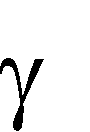
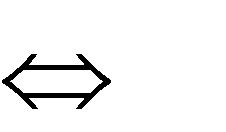
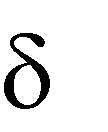
k



)

##### *Kiểm tra chữ ký số*

Với x, Z \* và Zp-1 , ta định nghĩa :

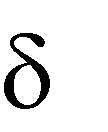
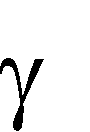


.

x

*p*

Ver (x,



, )

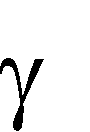
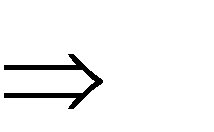
= True

modp.

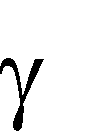
*Chứng minh*:

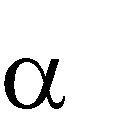
Nếu chữ ký đƣợc thiết lập đúng thì hàm kiểm tra sẽ thành công vì:

modp

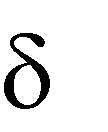


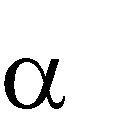
a. r.

modp ( vì a + r x mod(p - 1)).



x



A tính chữ ký bằng cách dùng cả giá trị bí mật a( là một phần của khóa ) lẫn số ngẫu nhiên bí mật k ( dùng để ký trên x). Việc kiểm tra có thể thực hiện duy nhất bằng thông tin công khai.

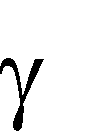
*Ví dụ*: Giả sử p=467, = 2, a = 127



a

Khi đó: =

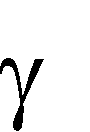
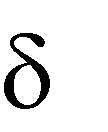
modp = 2127mod467 = 132

Giả sử A có thông báo x=100 và A chọn ngẫu nhiên k=213 vì (213,466)=1 và 213-1 mod466 = 431, A ký trên x nhƣ sau:



k

= modp = 2213mod467 = 29

Và = (x - a )k-1 mod(p -1) = (100 – 127. 29).431 mod466 = 51.

Chữ ký của A trên x= 100 là (29,51).

Bất kỳ ngƣời nào đó cũng có thể kiểm tra chữ ký bằng cách: 13229 . 2951 189 mod 467

2100 189 mod 467

Do đó, chữ ký là tin cậy.

## Chữ ký không chối bỏ.

Chữ ký không chối bỏ đƣợc công bố bởi Chaum và Van Antverpen vào năm 1989. Nó có một nét riêng mới lạ và thú vị. Quan trọng nhất trong số đó là chữ ký không thể kiểm tra khi không có sự cộng tác của ngƣời ký, A(giả sử ngƣời ký là A).

Sự bảo vệ này của A đề phòng khả năng chữ ký trong tài liệu của anh ta bị sao chép và phân bố bởi thiết bị điện tử mà không có sự đồng ý của anh ta.

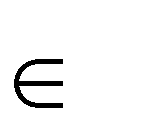
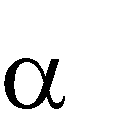
Ví dụ: A có một phần mềm và chữ ký kèm theo đƣợc tạo ra nhờ thuật toán của chữ ký số thông thƣờng. Nhƣ vậy, sẽ không tránh khỏi trƣờng hợp phần mềm đó bị sao chép mà B không biết. Ngƣời mua sẽ kiểm tra chữ ký kèm theo nhờ thuật toán kiểm tra công khai Ver và công nhận chữ ký đó là đúng. Vì nhƣ chúng ta đã biết bản sao của chữ ký số đồng nhất với bản gốc. Đƣơng nhiên nhƣ vậy A sẽ bị mất bản quyền. Để tránh điều bất tiện đó A đã dùng chữ ký không chối bỏ. Sự kiểm tra sẽ thành công khi thực hiện giao thức hỏi - đáp.

Lƣợc đồ chữ ký chống chối bỏ gồm 3 phần: thuật toán ký, giao thức kiểm tra, giao thức chối bỏ.

#### Thuật toán ký:

\* Tạo khóa:

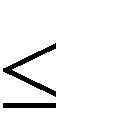
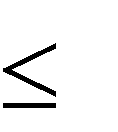
Cho p,q là các số nguyên tố lẻ sao cho p=2q+1 và bài toán rời rạc trên Zp là khó. Lấy



0

Zp\* là một phần tử bậc q( Nếu

là phần tử nguyên thủy của Zp thì

= 0(p -1)/q modp) lấy 1 a q-1 và xác định: =



a

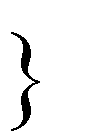
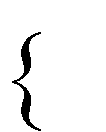
modp.

Lấy G là phân nhóm nhân của Z\*

p

bậc q (G bao gồm các thặng dƣ bậc hai theo modun p).

Lấy P=A=G, xác định:

K = (p, , a, = modp



):



a

Các giá trị p, , là công khai, a là bí mật.



\* Tạo chữ ký:

Với K= (p, , a, và x G, xác định chữ ký y trên thông báo x:



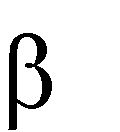
)

y = sigk(x) = xa modp

#### Giao thức kiểm tra :

Với x, y G, sự kiểm tra đƣợc tiến hành theo giao thức sau :

* + - 1. A chọn e1,e2 ngẫu nhiên, e1, e2 Zp\*.
      2. A tính c = y *e*1

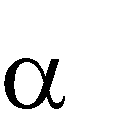


*e*2

* + - 1. B tính d= c *a* 1 mod *q*

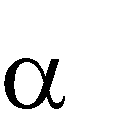
modp gửi nó cho B. modp và gửi nó cho A.

* + - 1. A chấp nhận chữ đúng khi và chỉ khi :

d x *e*1 *e*2 modp. (\*)

\* Vai trò của p, q trong lƣợc đồ:

Lƣợc đồ nằm trong Zp; tuy nhiên chúng ta cần tính toán trong phân nhóm nhân G của Zp\* của bậc nguyên tố lẻ. Đặc biệt, chúng ta cần tính phần tử nghịch đảo theo modun |G|, điều này lý giải tại sao |G| nên là nguyên tố lẻ. Nó thuận tiện lấy p=2q+1 với q là số nguyên tố lẻ. Trong trƣờng hợp này, phân nhóm G tồn tại.

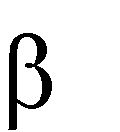
*Ví dụ*: giả sử ta lấy p = 467, từ 2 là căn nguyên thủy => 22 = 4 là thặng dƣ bậc hai theo modun 267 và 4 là phần tử sinh của G, lấy = 4. Giả sử a=101, ta có:

= amodp = 4101 mod467 = 449 A sẽ ký thông báo x=119 với chữ ký:

y = xa modp = 119101 mod467 = 129

Giả sử B muốn kiểm tra chữ ký y, B chọn ngẫu nhiên e1 = 38,e2 = 397.

Ta có: c = y *e*1



*e*2

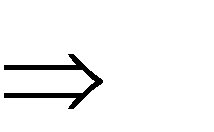
modp = 12938 449397 mod467 = 13

B gửi c=13 cho A và A tính d theo:

d = c *a* 1 mod *q*

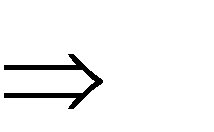
modp

= 13101 1 mod233 mod467 (q = (p - 1)/2 = (467 –1 )/2 = 233)



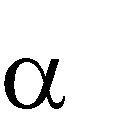
d

= 9

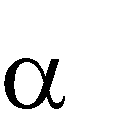


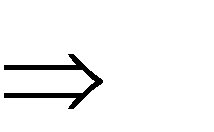
d

B muốn kiểm tra chữ ký y theo bƣớc 4. Có:

x *e*1

*e*2 modp = 11938 4397 mod467 = 9

d x *e*1 *e*2 modp



=> B chấp nhận chữ ký là đúng

***Giao thức chối bỏ***

Một vấn đề đặt ra, nếu sự cộng tác của chủ thể ký là cần thiết trong việc kiểm tra chữ ký thì điều gì đã ngăn cản anh ta trong việc từ chối chữ ký do anh ta tạo ra. Tất nhiên, anh ta có thể cho rằng chữ ký đúng đó là giả mạo và từ chối kiểm tra nó hoặc anh ta thực hiện một giao thức mà theo đó chữ ký sẽ không đƣợc kiểm tra. Vì vậy, một lƣợc đồ chữ ký chống chối bỏ đƣợc kết hợp chặt chẽ với một giao thức chối bỏ và nhờ điều đó chủ thể ký có thể chứng minh đƣợc chữ ký đó là giả mạo. (Nếu anh ta từ chối thực hiện 1 phần trong

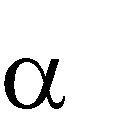
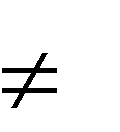
giao thức chối bỏ, điều đó đồng nghĩa với dấu hiệu chứng minh chữ ký đó là của anh ta và anh ta đang cố gắng từ chối chữ ký của mình).

Giao thức chối bỏ gồm hai tiến trình của giao thức kiểm tra và có các bƣớc sau:

1. B chọn e1, e2 ngẫu nhiên, e1, e2 Zq\*.
2. B tính c = y *e*1



*e*2

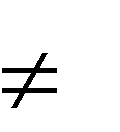
1. A tính d = c *a* 1 mod *q*
2. B kiểm tra d x *e*1

modp và gửi nó cho A modp và gửi nó cho B *e*2 modp.

1. B chọn f1,f2 ngẫu nhiên, f1, f2 Zq\*.
2. B tính C = y *f*1

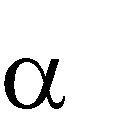


*f*2

1. A tính D = c *a* 1 mod *q*
2. B kiểm tra D x *f*1

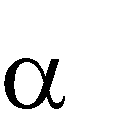
modp và gửi nó cho A modp và gửi nó cho B

modp

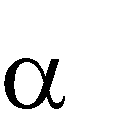


*f*2

1. B kết luận rằng y là chữ ký giả mạo khi và chỉ khi



(d *e*2 ) *f*1

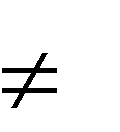


(D *f*2 ) *e*1

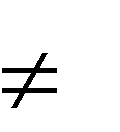
modp

*Ví dụ*: Lấy p=467, = 4, a = 101, = 449. Ký trên thông báo x=286 với chữ ký y= 83 (là giả mạo). A muốn thuyết phục B rằng chữ ký đó là không đúng. Vậy phải thực hiện nhƣ sau:

Chọn ngẫu nhiên e1 = 45, e2 = 237. B tính c=305 và A trả lời với d= 109. B tính 28645. 4237mod467 = 149.

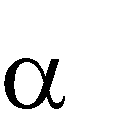
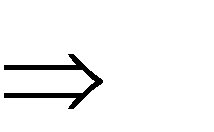
Vì 149 109 nên ta phải thực hiện giao thức chối bỏ

B chọn tiếp f1 = 125, f2 = 9, ngẫu nhiên, B tính C=270 và A trả lời với D=68. B tính: 286125.49mod467 = 25.

Vì 25 68 nên B thực hiện tiếp bƣớc cuối cùng của giao thức là thực hiện kiểm tra tính chính xác.

Ta có: 109.4-237)125 188 mod467

và (68.4-9)45 188 mod467 ; (d

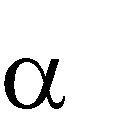


*e*2 ) *f*1

(D *f*2 ) *e*1

modp

 Vậy B tin chắc rằng đó là chữ ký không đúng Bây giờ vấn đề đặt ra là:



- A có thuyết phục đƣợc B rằng chữ ký không đúng đó là giả mạo

- A không thể làm cho B bị thuyết phục rằng chữ kí đó đúng là giả mạo ngoại trừ xác suất rất nhỏ.

# CHƯƠNG 3: DỊCH VỤ CHỨNG THỰC CHỮ KÝ SỐ

## Tổ chức chứng thực là gì ?.

Tổ chức chứng thực điện tử(CA) là một bên thứ 3 đƣợc cả hai bên gửi và nhận tin cậy đứng ra chứng nhận public key là đảm bảo.

Chức năng của của tổ chức chứng thực điện tử là chứng thực nhận dạng ngƣời ký thông qua hình thức cấp chứng chỉ số chứa khóa công khai của ngƣời ký, và duy trì cơ sở dữ liệu về chứng chỉ số.

Khi chứng chỉ số đƣợc CA cung cấp thì nó đƣợc tin tƣởng trong khi sử dụng

Hiện nay trên thế giới có nhiều tổ chức chứng thực điện tử tin cậy nhƣ VeriSign, Entrust, CyberTrust...

Còn ở Việt Nam có một vài tổ chức chứng thực điện tử nhƣ VASC, DES...

## Giới thiệu về một số tổ chức chứng thực.

#### Tổ chức Entrust -một trong những hãng đi đầu về phát triển PKI

Entrust là một tổ chức chứng thực điện tử tin cậy trên thế giới đƣợc các công ty thuộc lĩnh vực thƣơng mại điện tử trên thế giới tin cậy.

Misof cũng là nhà phân phối sản phẩm về hệ thống cấp phát chứng chỉ của Entrust tại Việt Nam.

Giải pháp của Entrust không những đáp ứng đầy đủ các yêu cầu về hệ thống CA mà còn cung cấp thêm nhiều ứng dụng của chứng chỉ số, tích hợp chúng trong các ứng dụng khác nhƣ email, mã hóa file thƣ mục....

Các sản phẩm của Entrust cho việc nhận dạng và quản lý truy cập tuân theo chuẩn X509 V3, ngoài ra còn tuân theo các chuẩn quốc tế về mã hóa nhƣ PKCS, RFC.

#### Tổ chức chứng thực điện tử tại Việt Nam\_VASC

Công ty VASC đã đƣợc xây dựng thành công hệ thống quản lý và cung cấp chứng chỉ số của mình từ tháng 4/2002 và từ tháng 8/2002 đã chính thức phục vụ khách hàng.

Chứng chỉ số VASC CA đƣợc dùng trong các giao dịch trên môi trƣờng mạng hoặc Internet để :

 Chứng thực các đối tƣợng sử dụng.  Đảm bảo an toàn và bảo mật thông tin

Cung cấp bằng chứng pháp lý nếu xảy ra tranh chấp

VASC-CA hiện nay cung cấp với cac giải pháp :

 Chứng chỉ số cá nhân VASC-CA : Giúp mã hóa thông tin, bảo mật e-mail, sử dụng chữ ký điện tử cá nhân, chứng thực với một web server thông qua giao thức bảo mật SSL.

 Chứng chỉ số SSL Server VASC-CA: Giúp bảo mật hoạt động trao đổi thông tin trên website, xác thực ngƣời dùng bằng SSL, xác minh tính chính thống, chống giả mạo, cho phép thanh toán bằng thẻ tín dụng, ngăn chặn hacker dò mật khẩu.

 Chứng chỉ số nhà phát triển phần mềm VASC-CA: Cho phép nhà phát triển phần mềm ký vào các chƣơng trình applet, script, Java software, ActiveX control, EXE, CAB và DLL, đảm bảo tính hợp pháp của sản phẩm, cho phép ngƣời sử dụng nhận diện đƣợc nhà cung cấp, phát hiện đƣợc sự thay đổi của chƣơng trình (do hỏng, bị hacker hay virus phá hoại).

Tƣơng tự nhƣ vậy, số lƣợng đơn vị cung cấp giải pháp ứng dụng có dùng CKS ở Việt Nam hiện nay cũng chƣa nhiều. Các công ty nhƣ Giải Pháp Thẻ Minh Thông (www.tomica.vn), MI-SOFT(www.misoft.com.vn)... là những công ty cung cấp tích hợp giải pháp chữ ký số HSM (Hardware Security Module) vào thẻ thông minh và USB Token vào các ứng dụng và giao dịch cần bảo mật nhƣ: Internet Banking, Money Tranfer, VPN hay e-Signing.

## Dịch vụ chứng thực chữ ký số.

Cung cấp bởi Tổ chức cung cấp dịch vụ chứng thực Chữ ký số (Certification Authority

- CA) - Ngƣời thứ ba đáng tin cậy bao gồm:  kiểm tra, xác minh một chủ thể

 cấp cặp khóa

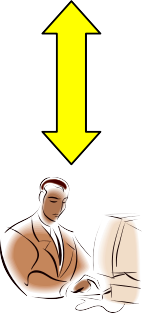
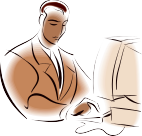
 cấp chứng thƣ số (chứng minh thƣ ++)  bao gồm cả khóa công khai

 duy trì trực tuyến CSDL Chứng thƣ số  khác

#### Bản chất dịch vụ

 Tƣơng tự nhƣ cấp chứng minh thƣ nhân dân hay các giấy tờ tùy thân khác Áp dụng cho môi trƣờng mạng

#### Cung cấp và sử dụng dịch vụ



**Certification Authority (CA)**

yêu cầu

Đ

Đ

cơ sở dữ liệu chứng thực số

cấp

chứng thựcsố/khóa

Xác minh

Thông điệp dữ liệu ký số

ơn vị cấp chứng thực (IA)

ơn vị đăng ký (RA)

Thuê bao

## Tình hình phát triển dịch vụ chứng thực chữ ký số trên thế giới và ở VIệt Nam.

* + 1. **Tình hình triển khai trên thế giới**

Đây là dịch vụ mới, xuất hiện vào khoảng cuối 1990s. Hiện đã đƣợc triển khai ở Mỹ, EU, Nhật, Hàn Quốc, Trung Quốc

VD:Hàn Quốc: 9 triệu thuê bao (20% dân số) Đƣợc ứng dụng trong các lĩnh vực:

* + - * Internet banking (chuyển tiền qua mạng)
      * hành chính công (khai sinh, khai tử, nộp thuế, cấp các loại giấy tờ và chứng chỉ, ...)
      * mua bán, đấu thầu qua mạng
      * Y tế, giáo dục, .....

Đây là một vài ví dụ về việc triển khai dịch vụ chứng thực chữ ký số trên thế giới :

#### “Hệ thống nộp hồ sơ xin phép xây dựng “ – Singapore

Việc xây dựng các công trình phải có ý kiến của rất nhiều cơ quan có thẩm quyền (>10). Phê duyệt nhiều loại hồ sơ (đề án, dự án, …).Việc nộp hồ sơ mất rất nhiều thời gian, công sức (nhiều cửa). Chính vì vậy nên họ đã đƣa ra một giải pháp kỹ thuật là:

Hệ thống CORENET e-Submission, tích hợp nhiều ứng dụng phê duyệt

 Hồ sơ nộp có chữ ký số

* + - * + Phê chuẩn dùng chữ ký số

Sử dụng bắt buộc từ năm 2002 và đã mang lại hiệu quả đáng kể :  Tiện lợi, tiết kiệm thời gian, công sức

 Cải cách hành chính

* + - * + “One stop”
        + Có thể kiểm tra trạng thái phê chuẩn online

#### “Phê chuẩn của cha mẹ “ - Hàn Quốc

Vấn đề:

* + - * + Tranh cãi giữa cha mẹ và doanh nghiệp nội dung về việc chơi online game và tải nội dung thông tin di động của trẻ em

 Sở cứ pháp lý:

* + - * + Đạo luật khai thác và bảo vệ thông tin

các doanh nghiệp chỉ đƣợc cung cấp dịch vụ cho trẻ em khi có sự phê chuẩn của bố mẹ

MIC:

* Các doanh nghiệp không tuân thủ sẽ bị phạt
* 4/2006: 13 cổng thông tin và online game website đã bị phạt 68,000 USD

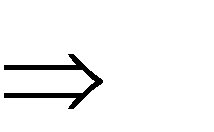
 Giải pháp kỹ thuật

* + Thông báo có chữ ký số của cha mẹ  Hiệu quả
  + Giảm đáng kể đơn từ và tranh cãi
  + Bảo vệ trẻ em khỏi việc sử dụng các nội dung và game không phù hợp

#### “Mạng chăm sóc sức khỏe và thuốc” – Nhật Bản

Vấn đề

* + chữa bệnh lâu dài, chữa bệnh từ xa

Cần cơ sở dữ liệu về quá trình điều trị, lịch sử bệnh tật, tình trạng sức khỏe ,

* + Thông tin nhạy cảm, mang tính riêng tƣ
  + Chỉ truy nhập đƣợc bởi những ngƣời có trách nhiệm và thẩm quyền, cần xác thực đúng ngƣời (bác sĩ ?)

 Đối tƣợng phục vụ

* + bệnh viện, trung tâm sức khỏe, bác sĩ, hộ lý, dƣợc sĩ, bệnh nhân
  + dịch vụ: cấp hồ sơ, kê đơn thuốc, trả tiền chữa bệnh, trả tiền thuốc, ....

 Thời gian: 1995-2004 Hiệu quả

* + Hơn 80,000 ngƣời
  + Giảm chi phí khám, chữa bệnh, điều trị
  + Nâng cao hiệu quả chữa bệnh và điều trị

## Chữ ký số ở Việt Nam

Khái niệm “chứng thực số” và “chữ ký số” còn tƣơng đối mới đối với ngƣời sử dụng tại VN. Để hiểu đƣợc vai trò của nó trong giao dịch điện tử, ngƣời dùng đòi hỏi phải có một kiến thức nhất định về CNTT (mã hóa bất đối xứng, public key, private key…). Vì vậy một phần khách hàng vẫn chƣa hƣởng ứng dịch vụ này vì “không tin” vào chứng thực số và chữ ký số. Hiện nay đã có một số đơn vị cung cấp dịch vụ phục vụ nhu cầu giao dịch nội bộ (ngân hàng công thƣơng) và một số các đơn vị đã cung cấp thử nghiệm cho công cộng: VASC

Sau thời gian dài chuẩn bị soạn thảo, lấy ý kiến các chuyên gia và ngƣời dân, Nghị định 26 về chữ ký số và dịch vụ chứng thực chữ ký số đã đƣợc Thủ tƣớng Chính phủ ban hành ngày 15/2/2007, công nhận chữ ký số và chứng thực số có giá trị pháp lý trong giao dịch điện tử, bƣớc đầu thúc đẩy sự phát triển của thƣơng mại điện tử tại Việt Nam

Ngày 31/12/2008, Bộ TT-TT ban hành 6 loại tiêu chuẩn trong giao dịch điện tử đƣợc quy định buộc phải áp dụng chữ ký số và chứng thực số, bao gồm: Chuẩn bảo mật cho HSM, Chuẩn mã hóa, Chuẩn tạo yêu cầu và trao đổi chứng thƣ số, Chuẩn về chính sách và quy chế chứng thực chữ ký số, Chuẩn về lƣu trữ và truy xuất chứng thƣ số và Chuẩn về kiểm tra trạng thái chứng thƣ số.

Theo Bộ TT-TT, danh mục các tiêu chuẩn này sẽ còn đƣợc định kỳ xem xét cập nhật, sửa đổi, bổ sung phù hợp với điều kiện thực tế của Việt Nam.

Các tổ chức cung cấp dịch vụ chứng thực chữ ký số quốc gia, tổ chức cung cấp dịch vụ chứng thực chữ ký số công cộng, tổ chức cung cấp dịch vụ chứng thực chữ ký số chuyên

dùng đƣợc Bộ Thông tin và Truyền thông cấp giấy chứng nhận đủ điều kiện đảm bảo an toàn cho chữ ký số, tổ chức cung cấp dịch vụ chứng thực chữ ký số nƣớc ngoài đƣợc Chính phủ Việt Nam công nhận sẽ dựa trên danh mục ban hành này để áp dụng chứng thực.

#### Ứng dụng “Chữ ký số” tại Việt Nam

Khả năng ứng dụng của CKS khá lớn, do có tác dụng tƣơng tự nhƣ chữ ký tay, nhƣng dùng cho môi trƣờng điện tử. Thƣờng CKS đƣợc sử dụng trong giao dịch cần an toàn qua mạng Internet, nhƣ giao dịch thƣơng mại điện tử, tài chính, ngân hàng. Thứ 2 là dùng để ký lên eMail, văn bản tài liệu Soft-Copy, phần mềm... module phần mềm và việc chuyển chúng thông qua Internet hay mạng công cộng. Tuy nhiên, sử dụng hay không sử dụng CKS vẫn còn tùy vào sự lựa chọn của ngƣời dùng.

Hiện nay nhiều ngân hàng Việt Nam đã ứng dụng CKS trong các hệ thống nhƣ Internet Banking, Home Banking hay hệ thống bảo mật nội bộ. Ngoài ra các website của các ngân hàng, công ty cần bảo mật giao dịch trên đƣờng truyền, mạng riêng ảo VPN đã áp dụng CKS. Có thể nói, càng ngày càng nhiều sự hiện diện của CKS trong các hệ thống, ứng dụng CNTT bảo mật của DN, tổ chức ở Việt Nam.

#### Chữ ký số đem lại lợi ích gì?

Ứng dụng CKS giúp giải quyết tốt hơn các giải pháp xác thực và bảo mật. CKS giải quyết vấn đề toàn vẹn dữ liệu và là bằng chứng chống chối bỏ trách nhiệm trên nội dung đã ký, giúp cho các tổ chức, cá nhân yên tâm với các giao dịch điện tử của mình trong môi trƣờng Internet.

Đối với lĩnh vực trao đổi thông tin, với sự phổ biến hiện nay của e-mail nhờ tính nhanh chóng linh hoạt, việc sử dụng CKS sẽ giúp cho việc trao đổi văn bản nội dung trở nên dễ dàng và đảm bảo. Ví dụ: Hệ thống quản lý văn bản, hợp đồng số sẽ đƣợc lƣu trữ, tìm kiếm bằng hệ thống máy tính. Các giao dịch, trao đổi văn bản giữa cá nhân - tổ chức nhà nƣớc (C2G), DN - Nhà Nƣớc(B-G), DN-DN(B2B) hay giữa các tổ chức cơ quan nhà nƣớc với nhau sẽ nhanh chóng và đảm bảo tính pháp lý, tiết kiệm rất nhiều thời gian, chi phí giấy tờ và vận chuyển, đi lại.

Đặc biệt, tăng cƣờng ứng dụng CKS sẽ thúc đẩy việc ứng dụng thƣơng mại điện tử, chính phủ điện tử, hành chính điện tử và kinh doanh điện tử, đồng thời cũng bảo vệ bản quyền các tài sản số hóa.

Sở TTTT TP.HCM là đơn vị đi tiên phong trong việc triển khai ứng dụng chữ ký số trong hoạt động giao dịch điện tử phục vụ công tác quản lý nhà nƣớc tại địa phƣơng. Hiện sở cũng đã có trung tâm Chứng Thực Chuyên Dùng, đƣợc bộ TTTT và Ban Cơ Yếu chính phủ (đơn vị chứng thực điện tử chuyên dùng chính phủ (G-CA), cung cấp và quản lý chứng chỉ điện tử phục vụ các cơ quan trong hệ thống chính trị thực hiện các yêu cầu xác thực thông tin và bảo mật thông tin thuộc phạm vi bí mật nhà nƣớc trên các hệ thống tác nghiệp, điều hành điện tử) đồng ý. Với trung tâm này sở TTTT đã và đang triển khai chứng thực CKS miễn phí cho khối quản lý đô thị nhƣ: Sở Tài Nguyên Môi Trƣờng, sở Kiến Trúc, sở Tài Chính, trung tâm Tài Nguyên Môi Trƣờng và Đăng Ký Nhà Đất…Trong năm 2009, sở TTTT TP.HCM sẽ tiếp tục nâng cấp trung tâm này và mở rộng chứng thực cho các sở, ngành khác. Đầu tháng 3/2009, sở TTTT đã có buổi làm việc với 2 cơ quan thuế và hải quan TP.HCM về việc chứng thực chữ ký số cho 2 đơn vị này để tiến tới thực hiện cơ chế “một cửa” và kê khai thuế qua mạng

Ngoài trung tâm Chứng Thực Chuyên Dùng, sở TTTT TP.HCM hiện đang chờ UBND TP.HCM phê duyệt cho phép thành lập trung tâm Chứng Thực Công Cộng. Với trung tâm này, sở TTTT sẽ chứng thực cho mọi đối tƣợng: DN, ngƣời dân, tổ chức...Trung tâm sẽ phục vụ theo loại hình dịch vụ”.

## Hành lang pháp lý.

Ngày 23/2, Chính phủ đã ban hành Nghị định 27/2007/NĐ-CP về giao dịch điện tử trong hoạt động tài chính.

Trƣớc đó, ngày 15/2/2007, Chính phủ đã ban hành Nghị định 26/2007/NĐ-CP quy định chi tiết thi hành Luật Giao dịch điện tử về chữ ký số và dịch vụ chứng thực chữ ký số. Theo đó, trong trƣờng hợp pháp luật quy định văn bản cần có chữ ký thì yêu cầu đối với một thông điệp dữ liệu đƣợc xem là đáp ứng nếu thông điệp dữ liệu đó đƣợc ký bằng chữ ký số.

Sau khi nghị định của Thủ tƣớng đƣợc ban hành, Bộ TT-TT và các bộ, ngành liên quan cũng đã ra nhiều văn bản liên quan hƣớng dẫn thực hiện chữ ký số và dịch vụ chứng thực chữ ký số.

Ngày 31/12/2008, Bộ TT-TT ban hành 6 loại tiêu chuẩn trong giao dịch điện tử đƣợc quy định buộc phải áp dụng chữ ký số và chứng thực số, bao gồm: Chuẩn bảo mật cho HSM, Chuẩn mã hóa, Chuẩn tạo yêu cầu và trao đổi chứng thƣ số, Chuẩn về chính sách và

quy chế chứng thực chữ ký số, Chuẩn về lƣu trữ và truy xuất chứng thƣ số và chuẩn về kiểm tra trạng thái chứng thƣ số.

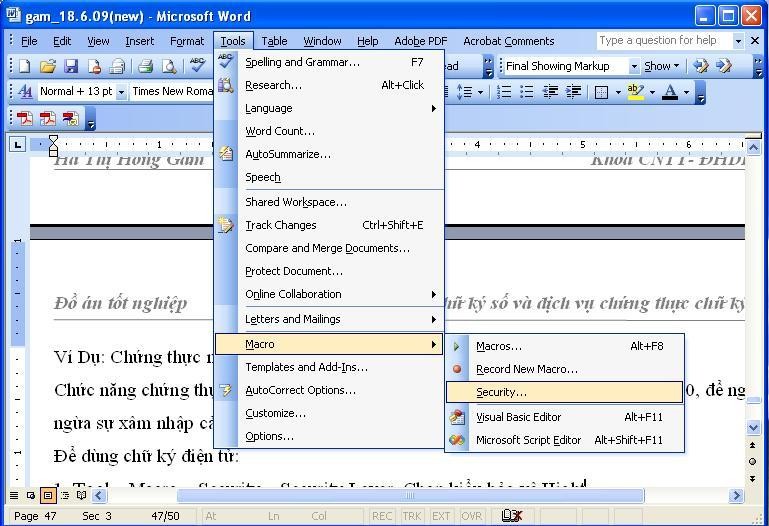
Theo Bộ TT-TT, danh mục các tiêu chuẩn này sẽ còn đƣợc định kỳ xem xét cập nhật, sửa đổi, bổ sung phù hợp với điều kiện thực tế của Việt Nam.Các tổ chức cung cấp dịch vụ chứng thực chữ ký số quốc gia, tổ chức cung cấp dịch vụ chứng thực chữ ký số công cộng, tổ chức cung cấp dịch vụ chứng thực chữ ký số chuyên dùng đƣợc Bộ Thông tin và Truyền thông cấp giấy chứng nhận đủ điều kiện đảm bảo an toàn cho chữ ký số, tổ chức cung cấp dịch vụ chứng thực chữ ký số nƣớc ngoài đƣợc Chính phủ Việt Nam công nhận sẽ dựa trên danh mục ban hành này để áp dụng chứng thực.

# Ví Dụ: Chứng thực macro trong Word và Excel bằng chữ ký điện tử

Chức năng chứng thực bằng chữ ký điện tử bắt đầu đƣợc bổ sung từ bộ Office 2000, để ngăn ngừa sự xâm nhập cảu virut macro.

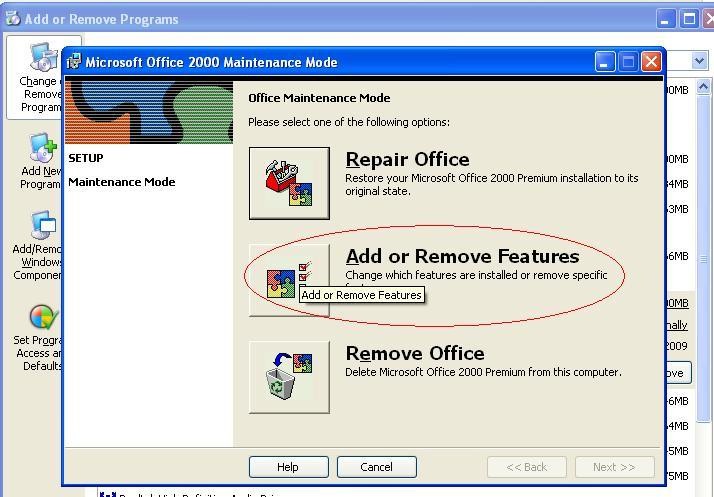
Để dùng chữ ký điện tử:

1. Tool – Macro – Security – Security Lever. Chọn kiểu bảo vệ Hight

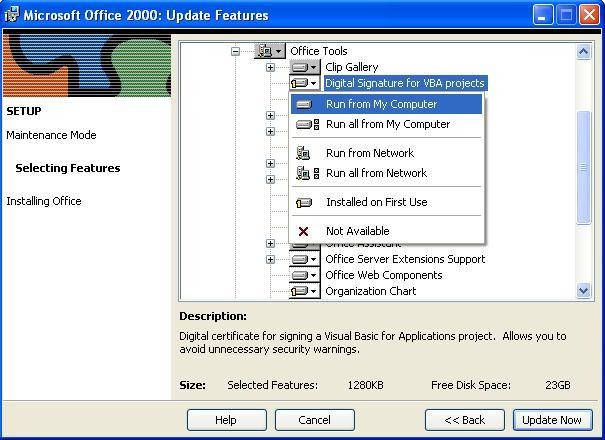


1. Nếu chƣa có chƣơng trình tạo chữ ký điện tử của VBA thì bạn cần cài đặt bổ sung :

Control Panel – Add/Remove Progams – Microsoft Office 2000 Premium – nhấn Add/Remove – Add or Remove Features



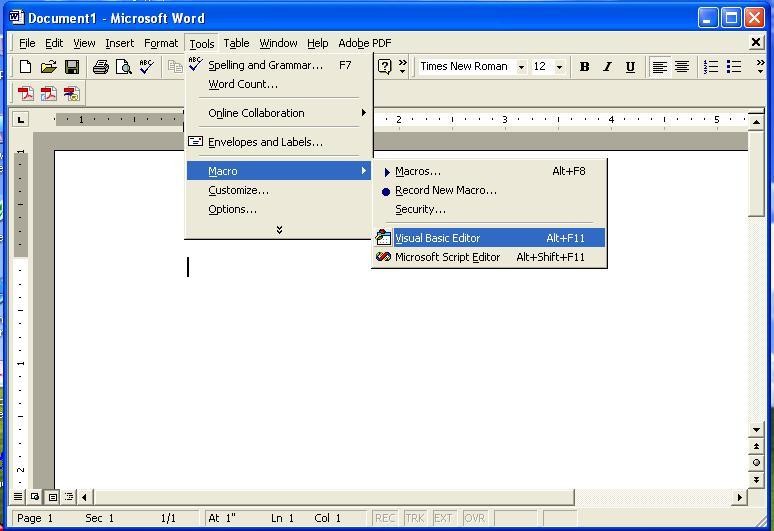
Bấm dấu cộng bên cạnh Office Tool, nhấn vào Digital Signature for VBA project và chọn Run from My Computer, xong bấm Update now. File Selfcert.exe đã đƣợc bổ xung vào tại đƣờng dẫn C:ProgamFile/Microsoft Office/ Office



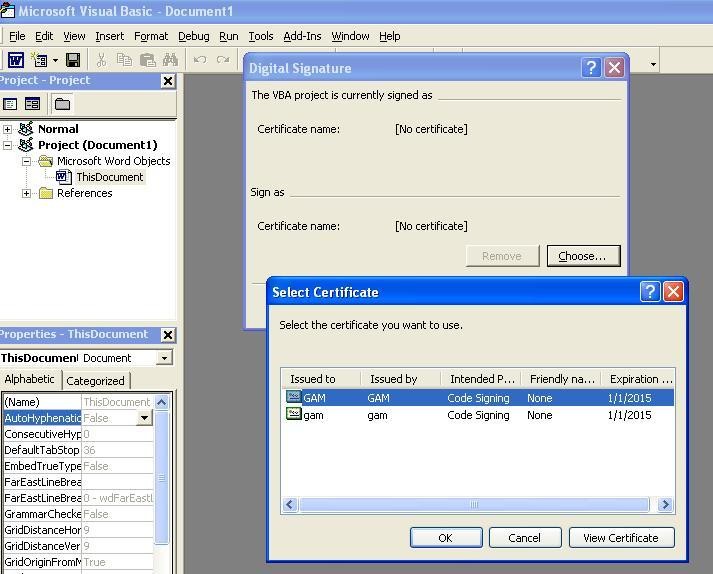
1. Để tạo chữ ký, chạy file Selfcert.exe, gõ tên vào hộp Your name – OK



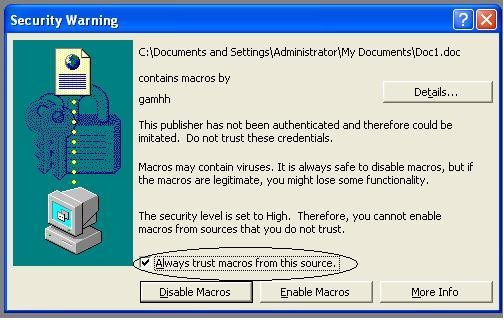
Sau đó chọn macro cần bảo vệ trong cửa sổ Visual Basic Editor,



Tool – Digital Signature – nhấn Choose rồi chọn chữ ký điện tử vừa mới đƣợc tạo trong danh sách Select Certificate.



1. Lần đầu tiên mở tập tin có chứa macro, hộp thoại Security Warning xuất hiện, yêu cầu bạn xác định đúng là macro và chữ ký của mình không, nếu đúng bạn đánh dấu vào hộp kiểm Always trust macro from this source. Macro của bạn bây giờ đã đƣợc chứng thực bằng chữ ký điện tử nên chƣơng trình sẽ không hỏi mỗi khi bạn chạy macro.



Nhƣng khi chạy một macro do bạn tạo ra mà chƣa đƣợc chứng thực hoặc có một virut macro khởi chạy thì chƣơng trình lập tức cảnh báo, khi đó bạn nhấn OK để vô hiệu hóa nó.



# KẾT LUẬN

### Việc nghiên cứu và tìm hiểu về chữ ký số và dịch vụ chứng thực chữ ký số để đáp ứng nhu cầu xác thực thông tin và ngƣời dùng hiện này là rất cần thiết đặc biệt là trong các giao dịch điện tử. Đồ án đã đạt đƣợc những kết quả chính sau:

Nghiên cứu và tìm hiểu trong tài liệu để hệ thống lại các vấn đề:

* Các khái niệm về toán học đƣợc sử dụng trong mật mã học.
* Các kiến thức chữ ký số.
* Tìm hiểu về dịch vụ chứng thực chữ ký số.

Ví dụ : Chứng thực macro trong Word và Excel bằng chữ ký điện tử.

Mặc dù có nhiều cố gắng, nhƣng trong đồ án vẫn có một số vấn đề chƣa thật sự hoàn thiện,chƣa thực hiện đƣợc mô phỏng chƣơng trình cấp chứng chỉ số để ký.

Xin các thầy cô giáo góp ý đề em có thể tiếp tục nghiên cứu đề tài này đƣợc tốt hơn.

**TÀI LIỆU THAM KHẢO**

* 1. Lý thuyết mật mã và an toàn thông tin\_ Phan Đình Diệu(NXB ĐHQG)
  2. An toàn tính toán\_Charles P.pheeger(Học Viện Kỹ Thuật Mật Mã)
  3. Báo cáo: Vai trò của chữ ký điện tử trong TMĐT\_Lê Thị Ngọc Mơ
  4. [http://vi.wikipedia.org/wiki/chữ\_ký\_số.](http://vi.wikipedia.org/wiki/ch?_ký_s%3F)
  5. [http://vi.wikipedia.org/wiki/Hàm\_băm](http://vi.wikipedia.org/wiki/Hàm_b?m).
  6. [http://www.3c.com.vn/Story/vn/hotrokhachhang/thuongmaidientu/ekienthuccob](http://www.3c.com.vn/Story/vn/hotrokhachhang/thuongmaidientu/ekienthuccoban/2009/5/54063.html)  [an](http://www.3c.com.vn/Story/vn/hotrokhachhang/thuongmaidientu/ekienthuccoban/2009/5/54063.html)
  7. [http://www.ddth.com](http://www.ddth.com/archive/index.php/t-225681.html)