# CHỮ KÝ SỐ

### Sơ lược về chữ ký số:

Chữ ký là khái niệm chắc hẳn ai cũng biết. Trong đời sống, chúng ta thường xuyên phải sử dụng chữ ký để xác nhận những văn bản, tài liệu. Trong các doanh nghiệp hay nhà nước thì có thể dùng thêm con dấu. Tuy được sử dụng rộng rãi nhưng chữ ký vẫn có một số mặt hạn chế:

* + Mất nhiều thời gian nếu sử dụng cho hang loạt những văn bản, tài liệu cùng một lúc.
	+ Việc xác minh chữ ký khó khăn và tốn nhiều thời gian.
	+ Có thể dễ bị làm giả.

Chữ ký thông thường có rất nhiều mặt hạn chế, mức độ bảo mật không không cao. Vì vậy cần có phương pháp để khắc phục những mặt hạn chế nêu trên, giúp nâng cao tính bảo mật và an toàn. Chữ ký điện số ra đời trong thời buổi công nghệ thông tin đang phát triển chóng mặt. Người ta có thể sử dụng chữ ký điện số để ký vào các văn bản, tài liệu giúp việc xác minh nhanh chóng hơn và đặc biệt là tính xác thực cao hơn, an toàn hơn vì rất khó làm giả.

Chữ ký điện số có các ưu điểm vượt trội so với chữ ký thông thường:

* + Bảo mật: chữ ký điện số có khả năng bảo mật cao, chìa khóa được bảo mật với tất cả mọi người trừ những người được phép biết.
	+ Toàn vẹn thông tin: Cả hai bên tham gia vào quá trình thông tin đều có thể tin tưởng 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.
	+ 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 như một chứng cứ để bên thứ ba giải quyết

### Nội dung

### Quá trình ký và nhận thông điệp

* + Quá trình ký (bên gửi)
		- Tính toán chuỗi đại diện (message digest/ hash value) của thông điệp sử dụng một giải thuật băm (Hashing algorithm)
		- Chuỗi đại diện được ký sử dụng khóa riêng (Priavte key) của người gửi và 1 giải thuật tạo chữ ký (Signature/ Encryption algorithm). Kết quả chữ ký số (Digital signature) của thông điệp hay còn gọi là chuỗi đại diện được mã hóa (Encryted message digest)
		- Thông điệp ban đầu (message) được ghép với chữ ký số( Digital signature) tạo thành thông điệp đã được ký (Signed message)
		- Thông điệp đã được ký (Signed message) được gửi cho người nhận

 Quá trình kiểm tra chữ ký (bên nhận)

* + - Tách chữ ký số và thông điệp gốc khỏi thông điệp đã ký để xử lý riêng;
		- Tính toán chuỗi đại diện MD1 (message digest) của thông điệp gốc sử dụng giải thuật băm (là giải thuật sử dụng trong quá trình ký)
		- Sử dụng khóa công khai (Public key) của người gửi để giải mã chữ ký số -> chuỗi đại diện thông điệp MD2
		- So sánh MD1 và MD2:
* Nếu MD1 =MD2 -> chữ ký kiểm tra thành công. Thông điệp đảm bảo tính toàn vẹn và thực sự xuất phát từ người gửi (do khóa công khai được chứng thực).
* Nếu MD1 <>MD2 -> chữ ký không hợp lệ. Thông điệp có thể đã bị sửa đổi hoặc không thực sự xuất phát từ người gửi.

### Giải thuật Euclide mở rộng

Giải thuật Eclid mở rộng kết hợp quá trình tìm UCLN(a,b) trong thuật toán Eclid với việc tìm một cặp số x, y thoả mãn phương trình Đi-ô-phăng. Giả sử cho

hai số tự nhiên a, b, ngoài ra a>b>0. Đặt r0 = a, r1 = b, chia r0 cho r1 được số dư r2 và

thương là q1. Nếu r2 = 0 thì dừng, ngược lại chia r1 cho r2 được số dư các ri giảm nên sau hữu hạn bước ta thu được rm + 2 = 0

**r0 = q1 \* r1 + r2 , 0 < r2 < r1 ; r1 = q2\* r2 + r3 , 0 < r3 < r2 ;**

**…….**

**rm-1 = qm \* rm + rm+1 , 0 < rm+1 < rm ;**

r3,.... Vì dãy

**rm = qm+1 \* rm+1**

trong đó số dư cuối cùng khác 0 là **rm+1 = d**. Bài toán đặt ra là tìm x, y sao cho

**a \*x + b \* y = rm+1 ( =d** )

Để làm điều này ta tìm x, y theo công thức truy hồi, nghĩa là sẽ tìm xi và yi sao cho:

**a \*xi + b \* yi = ri**

Khi đó từ

suy ra

**ri = qi+1 \* ri+1 + ri+2**

**ri - qi+1 \* ri+1 = ri+2**

**(a \* xi +b \* yi) - qi+1 \* (a \* xi+1 + b \* yi+1) = ri+2 a \* (xi - qi+1 \* xi+1) + b \* (yi - qi+1 \* yi+1) = ri+2**

Từ đó có thể chọn

**xi+2 = xi - qi+1 \* xi+1 yi+2 = yi - qi+1 \* yi+1**

Ví dụ minh họa: đầu vào là 240 và 46

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **index i** | **qi-1** | **ri** | **xi** | **yi** |
| 0 |  | 240 | 1 | 0 |
| 1 |  | 46 | 0 | 1 |
| 2 | 240 / 46 = 5 | 240 – 5 \* 46 = 10 | 1 – 5 \* 0 = 1 | 0 – 5 \* 1 = -5 |
| 3 | 46 / 10 = 4 | 46 – 4 \* 10 = 6 | 0 – 4 \*1 = -4 | 1 – 4 \* -5 = 21 |
| 4 | 10 / 6 = 1 | 10 – 1 \* 6 =4 | 1 – 1 \* -4 = -5 | -5 – 1 \* 21 = -26 |
| 5 | 6 / 4 = 1 | 6 – 1 \* 4 = 2 | -4 – 1 \* 5 = -9 | 21 – 1 \* -26 = 47 |
| 6 | 4 / 2 = 2 | 4 – 2 \* 2 = 0 | 5 – 2 \* -9 = 23 | -26 – 2 \* 47 = -120 |

Theo bảng tính ta có 2 số x, y cần tìm lần lượt là -9 và 47

-9 \* 240 + 47 \* 46 = 2