Đề tài: Tấn công lược đồ chữ ký số RSA

Vũ Thị Tâm - 20185403
Hoàng Phi Long - 20185375
Nguyễn Hải Đăng - 20185333
Nguyễn Quang Hiếu - 20185351
Phạm Huy Hoàng - 20185361

Hà Nội, tháng 5 năm 2021

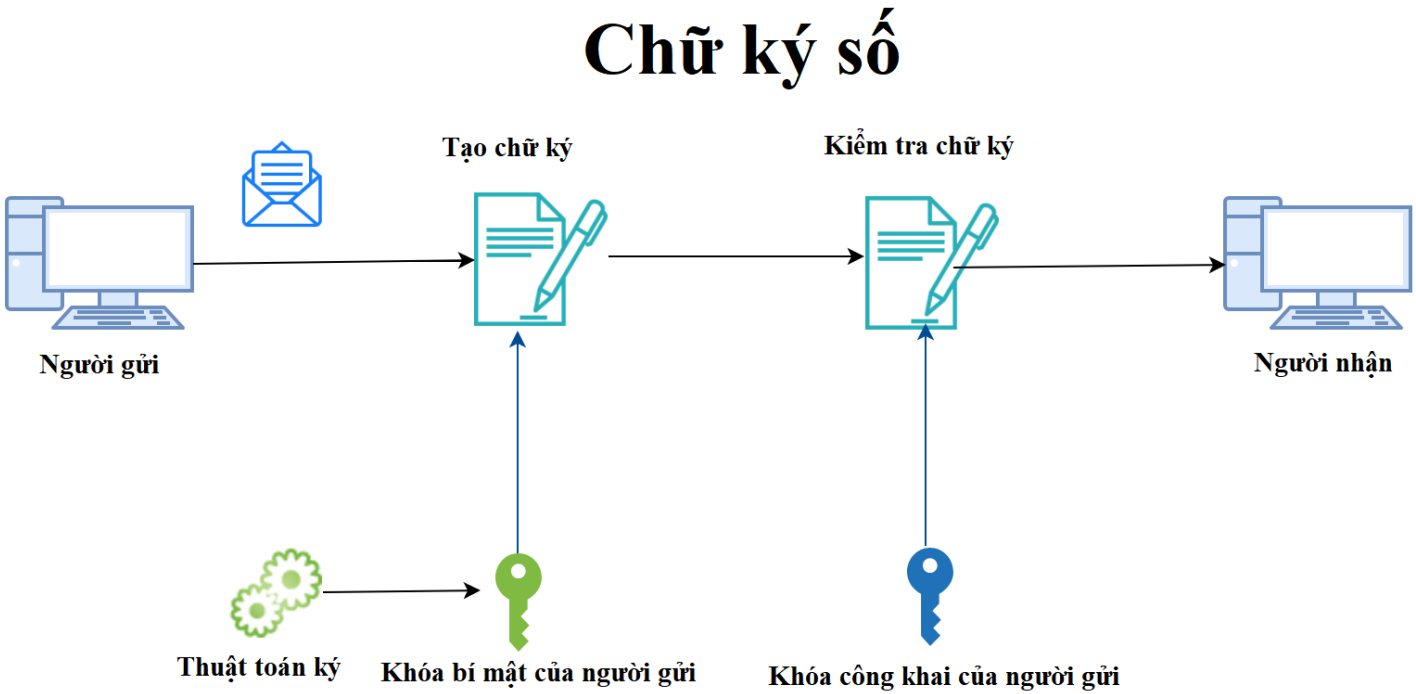
Nội dung

Nội dung

Đặt vấn đề

=> Tâm và Hiếu cần sử dụng chữ ký số để chứng thực tài liệu mình gửi

Khái niệm chữ ký số



- **Tài liệu số** hay tài liệu điện tử: Là một chuỗi các bit, xâu bit có thể rất dài.
- **Chữ ký số** là bản mã của xâu bit tài liệu với khóa lập mã. Như vậy **Ký số** trên **Tài liệu số** là ký trên từng bit tài liệu. Kẻ gian khó có thể giả mạo **chữ ký số** nếu không biết **khóa lập mã**.

Câu hỏi?

Ký số thực hiện trên từng bít tài liệu, nên độ dài của **chữ ký số** ít nhất cũng bằng độ dài tài liệu. Vậy nếu tài liệu của chúng ta có kích thước 100GB thì kích thước của chữ kí số cũng là 100GB?

Hàm băm

- Thay vì ký trên tài liệu dài, người ta thường dùng **hàm băm** thu nhỏ kích thước tài liệu gốc để tạo **đại diện** cho tài liệu, sau đó mới **Ký số** lên **đại diện** này.
- **Hàm băm** là hàm một chiều nếu với giá trị băm z, ta không có khả năng tìm ra thông điệp x sao cho $h(x) = z$.
- Có rất nhiều hàm băm thông dụng, bài thuyết trình này sẽ sử dụng hàm băm **SHA-256**.

  Vậy tại sao lại là **SHA-256**???

Tại sao lại là SHA-256???

- **SHA-256** là tiêu chuẩn hàng đầu của ngành bảo mật và được sử dụng rộng rãi.
- **Rất khó xảy ra xung đột:** Có thể có 2^{256} giá trị băm khi sử dụng **SHA-256**, điều này khiến cho 2 tài liệu khác nhau gần như không thể tình cờ có cùng giá trị băm giống nhau.
- **Hiệu ứng tuyết lở:** Không giống như các hàm băm cũ hơn, ngay cả một thay đổi rất nhỏ đối với thông tin ban đầu cũng làm thay đổi hoàn toàn giá trị băm — cái được gọi là hiệu ứng tuyết lở.


Tâm
Hiếu
RIP
COOL!
Hacker Đăng giấu tên

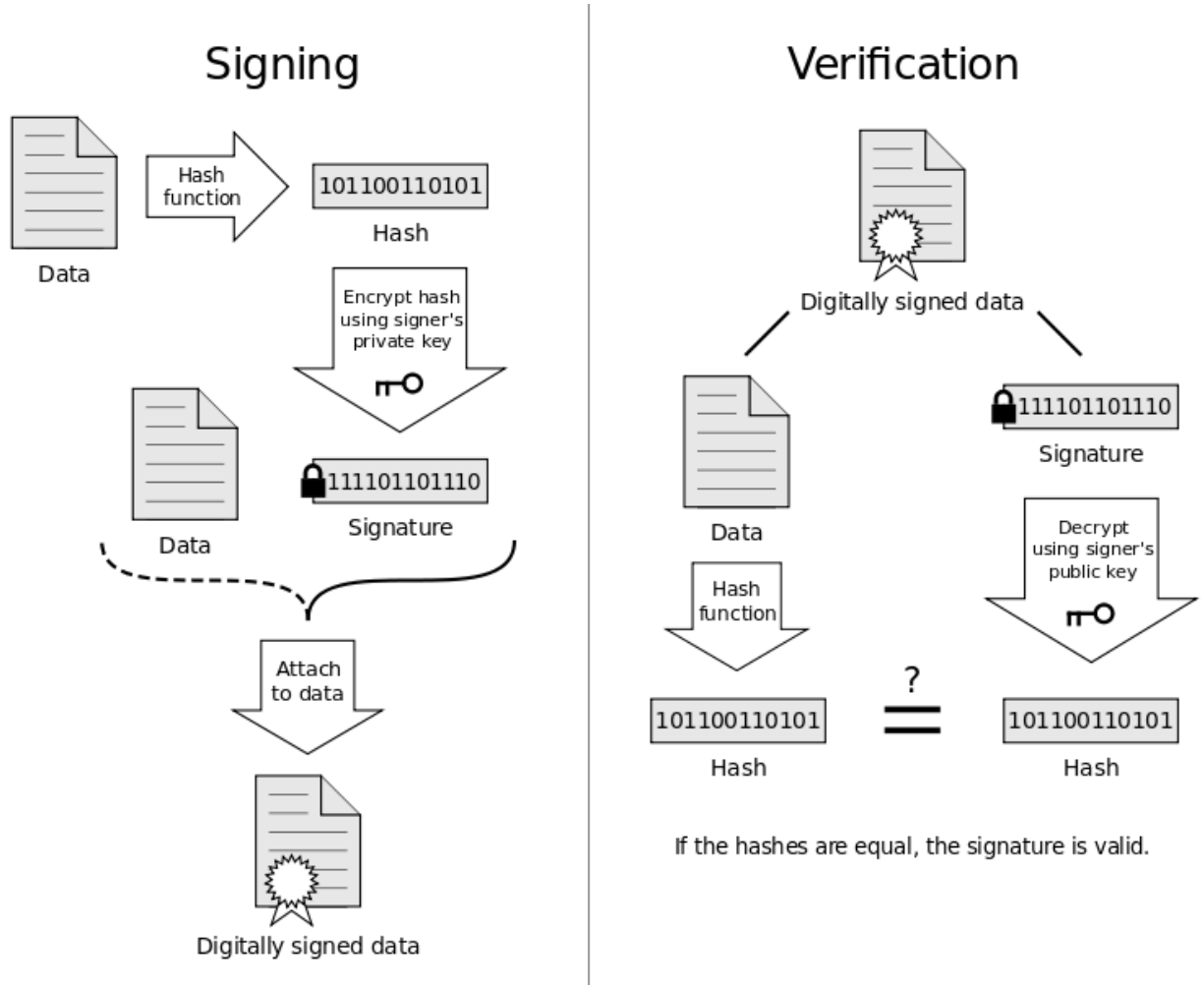
Nội dung

Sơ đồ chữ ký số RSA

Sơ đồ chữ ký RSA gồm 3 bước sau:

1. **Tạo khóa**
2. **Tạo chữ ký**
3. **Kiểm tra chữ ký**

Quá trình ký số với RSA



Tạo khóa

1. Chọn 2 số nguyên tố p và q
2. Tính $N = pq$ và $\phi(N) = (p-1)(q-1)$.
3. Chọn ngẫu nhiên một số nguyên e, $1 < e < \phi(N)$ sao cho $(e, \phi(N)) = 1$.
4. Tính số nguyên $d(1 < d < \phi(N))$, sao cho $ed \equiv 1(mod\ \phi(N))$.
5. Khóa công khai (public key) sẽ là cặp số (N, e) và khóa bí mật (private key) sẽ là cặp số (N, d).

Chúng ta cần giữ private key thật cẩn thận cũng như các số nguyên tố p, q vì từ đó có thể tính toán các khóa rất dễ dàng.

Tạo khóa

Ví dụ 1: Hãy giúp Tâm sinh khóa để tạo chữ ký số.

Tạo chữ ký số

1. Băm dữ liệu đầu vào bằng SHA-256, ta thu được mã hash h có độ dài 256 bit.

Tạo chữ ký số

1. Băm dữ liệu đầu vào bằng SHA-256, ta thu được mã hash h có độ dài 256 bit.
2. Dùng khóa bí mật $K^{-}(N, d)$ sinh được để tạo chữ ký số s

$$s = h^d \ mod \ N$$

Bản chất của việc ký số vào tài liệu số là việc mã hóa chúng bằng thuật toán RSA.

Câu hỏi: Hãy mã hóa và tạo chữ ký số với nội dung tin nhắn Tâm gửi "Lớp Toán tin K63".

Kiểm tra chữ ký, xác thực tin nhắn

1. Mã hóa dữ liệu nhận được bằng hàm băm SHA-256 thu được mã hash $h^{'}$.
2. Giải mã chữ ký số s nhận được bằng khóa công khai $K^{+}(N, e)$ thu được mã hash:

$$h = s^{e} \ mod \ N$$

3. Nếu $h = h^{'}$ thì dữ liệu nhận được đúng từ bên gửi chưa bị sửa đổi trong quá trình truyền.

Ví dụ

Sau khi gửi đi tin nhắn, giả sử Hiếu sẽ nhận được tin nhắn là "Lớp Toán tin K64" và chữ ký số s đi kèm.
Hãy xác thực tin nhắn đó có phải đúng là Tâm gửi hay không?

Nội dung

Ứng dụng của chữ ký số

- Chứng thực kê khai nộp thuế trực tuyến, kê khai hải quan điện tử, giao dịch ngân hàng điện tử, giao dịch chứng khoán điện tử, cổng thông tin một cửa quốc gia, cơ quan hành chính
- Dùng để ký hợp đồng với các đối tác làm ăn trực tuyến
- Chữ ký số dùng trong các giao dịch thư điện tử, ký vào các email để các đối tác, khách hàng của bạn biết có phải bạn là người gửi thư không.
- Chữ ký số để đầu tư chứng khoán trực tuyến, mua bán hàng trực tuyến, có thể dùng để thanh toán online, chuyển tiền trực tuyến mà không sợ bị mất cắp tiền như với đối với các tài khoản VISA, Master.
- Xác nhận đăng nhập vào một số Cổng giao dịch trực tuyến

Nội dung

Tấn công lược đồ chữ ký số RSA

Tấn công dạng 1: Tìm cách xác định khóa bí mật

Có các trường hợp sau:

1. Bị lộ một trong các giá trị: $p, q, \phi(n)$
2. Tấn công dựa theo khóa công khai $K^+(N, e)$ của người ký
3. Khi nhiều người cùng sử dụng chung "modulo N"
4. Sử dụng giá trị "modulo N" nhỏ
5. Sử dụng các tham số $(p-1)$ hoặc $(q-1)$ có các ước nguyên tố nhỏ

Tấn công dạng 1: Tìm cách xác định khóa bí mật

Bị lộ một trong các giá trị: $p, q, \phi(n)$

- Bị lộ q hoặc p $\Longrightarrow$ suy ra p hoặc q từ n.
- Bị lộ $\phi(n)$ $\Longrightarrow$ Tính d theo $d * e \equiv 1 \ (mod \ \phi(n))$

Khắc phục:
Tạo p,q một cách kín đáo.Tạo xong khóa bí mật d thì nên tiêu hủy p,q.

Tấn công dạng 1: Tìm cách xác định khóa bí mật

Tấn công dựa theo khóa công khai $K^+(N, e)$ của người ký

Thuật toán phân tích thừa số nguyên tố (Integer Factorization):
Input: n
Output: p, q

1. Khởi tạo $i = 2$.
2. Nếu $n \equiv 0 \bmod i, n = n/i$.
3. $i = i + 1$.
4. Nếu $n = 1$ thì dừng thuật toán, không thì quay lại lại bước 2.

Tấn công dạng 1: Tìm cách xác định khóa bí mật

Tấn công dựa theo khóa công khai $K^+(N, e)$ của người ký

Khắc phục Chọn 2 số nguyên tố p, q đủ lớn, khoảng 512 bit.

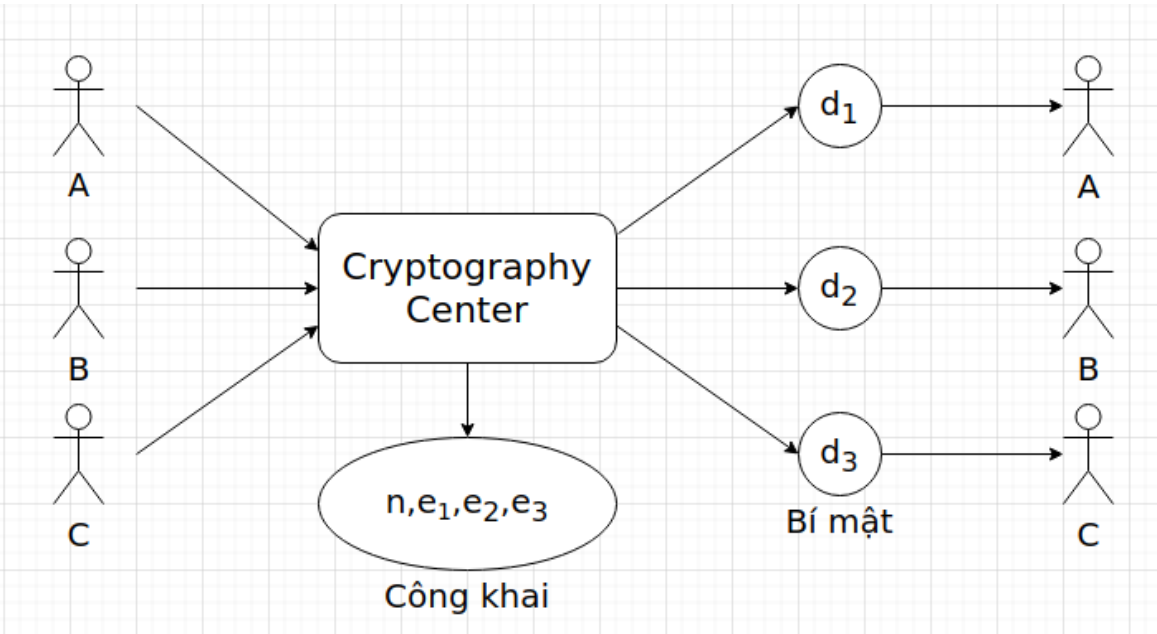
Số lượng bit	Có thể crack
256	Người thường
384	Đại học & cộng đồng mật mã
512	Chính phủ
768	Bảo mật trong ngắn hạn
1024	Bảo mật trong tương lai gần
2048	Bảo mật trong vài thập kỷ?

Tấn công dạng 1: Tìm cách xác định khóa bí mật

Khi nhiều người cùng sử dụng chung "modulo N"

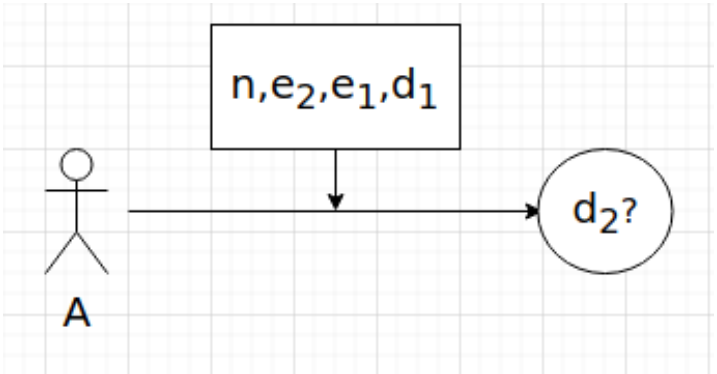
Đặt vấn đề

Giả sử có nhiều người cùng đăng ký sử dụng chữ ký số RSA tại một hệ thống cung cấp chữ ký số mà Tâm là khách hàng.
Khi đó hệ thống sẽ sinh ra 2 số nguyên tố p và q, và sinh ra tập các cặp khóa $\{e_i, d_i\}$
Hệ thống cung cấp cho người đăng kí thứ i khóa bí mật d_i, đại lượng n và tập các khóa công khai tương ứng $\{e_i\}$



Tấn công dạng 1: Tìm cách xác định khóa bí mật

Khi nhiều người cùng sử dụng chung "modulo N"

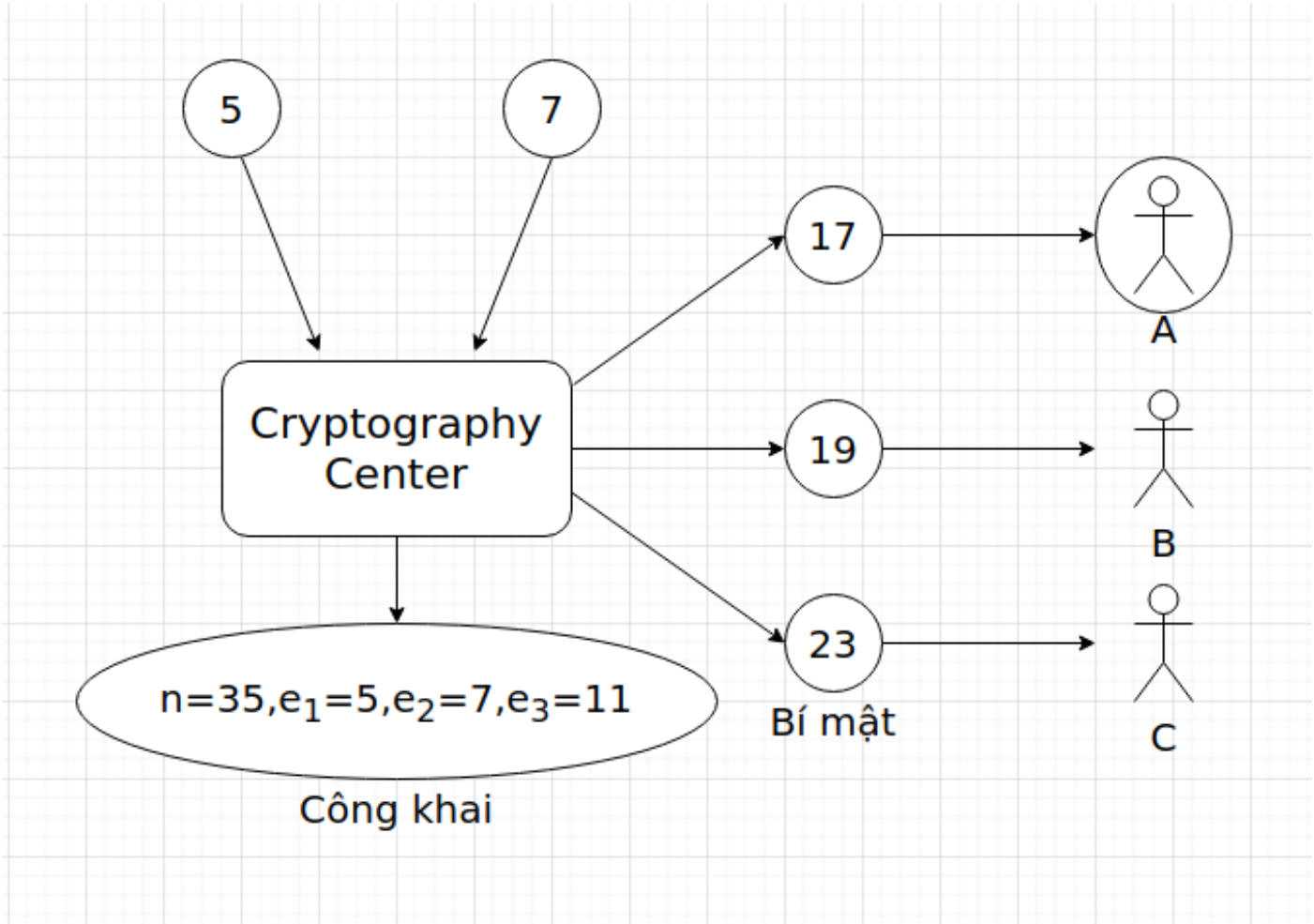


Thủ tục tìm d_2
Input: e_1, e_2, d_1
Output: d_2

1. Khởi tạo $t = e_1 d_1 - 1$.
2. S/d Euclid mở rộng tìm ƯCLN f của (e_2, t). Đồng thời tìm r,s t/m: $r.t + s.e_2 = f$
3. Nếu $f = 1$ thì đặt $d_1 = s$. Dừng thủ tục.
4. Nếu $f \neq 1$ thì đặt $t = t/f$, trở lại bước 2.

Tấn công dạng 1: Tìm cách xác định khóa bí mật

Khi nhiều người cùng sử dụng chung "modulo N"



Ví dụ

Tấn công dạng 1: Tìm cách xác định khóa bí mật

Khi nhiều người cùng sử dụng chung "modulo N"

Input: khóa công khai e của đối tượng và N
Thuật toán:

1. Tìm một căn bậc hai không tầm thường của 1 mod N, nghĩa là đi tìm một số b thỏa mãn $b^2 = 1 \text{ mod } N$
2. Tìm ước chung lớn nhất của $b + 1$ và N. ƯCLN này sẽ là p hoặc q
3. Tính đại lượng $\phi(N)$
4. Thực hiện tính toán khóa bí mật $d = e^{-1} mod \phi(N)$

Tấn công dạng 1: Tìm cách xác định khóa bí mật

Khi nhiều người cùng sử dụng chung "modulo N"

Ví dụ, với cặp số nguyên tố $p = 103$ và $q = 113$, ta có thể tạo ra từng này cặp khóa (d_i, e_i):

Private	Public	Private	Public
10865	8849	71	9815
5197	2917	2957	3365
6379	7459	7103	11231
7153	6481	1187	8171
5989	8269	11269	4717
3949	3781	3539	7163
10579	7963	6523	979
11297	1889	7253	2717
10103	10343	3187	7291
...	...	...	...

$=>$ Một người có thể dùng cặp khóa công khai và bí mật của mình, khi biết khóa công khai của người khác có thể cố tìm cách tìm ra khóa bí mật

Tấn công dạng 1: Tìm cách xác định khóa bí mật

Khi nhiều người cùng sử dụng chung "modulo N"

=> Giải pháp: Sử dụng các đại lượng n khác nhau cho từng khách hàng

Tấn công dạng 1: Tìm cách xác định khóa bí mật

Sử dụng giá trị "modulo N" nhỏ

Trong sơ đồ chữ ký RSA, công thức sinh chữ ký s theo mã hash h như sau:

$$s = h^d \ (mod\ N)$$

Người tấn công có thể tính được khóa bí mật d theo công thức:

$$d = \log_h s \ (mod\ N)$$

Đây là bài toán logarit rời rạc trên vành Z_N

Khắc phục:

Chọn p, q đủ lớn để việc giải bài toán logarit rời rạc trên vành Z_N khó có thể thực hiện trong thời gian thực.

Tấn công dạng 1: Tìm cách xác định khóa bí mật

Sử dụng các tham số $(p-1)$ hoặc $(q-1)$ có các ước nguyên tố nhỏ

Nếu chọn p và q sao cho $(p-1)$ hoặc $(q-1)$ có các ước nguyên tố nhỏ
$=>$ Có thể dùng thuật toán $(p-1)$ của Pollard để phân tích N thành thừa số.
Khắc phục:
Chọn p và q sao cho $(p-1)$ và $(q-1)$ có các ước nguyên tố lớn

Tấn công dạng 1: Tìm cách xác định khóa bí mật

Sử dụng các tham số $(p-1)$ hoặc $(q-1)$ có các ước nguyên tố nhỏ

Thuật toán $p-1$ của Pollard
Input: N
Output: Phân tích thừa số nguyên tố của N

1. Khởi tạo $a = 2$, $i = 2$.
2. $a := (a^i) \mod N$, $d := GCD(a-1, N)$
3. If $1 < d < n$ return d else $i := i + 1$
4. Đặt $d' := n/d$ và lặp lại thuật toán tới khi d' là số nguyên tố

Tấn công dạng 2: Giả mạo chữ ký (không tính trực tiếp khóa bí mật)

Xét quá trình A gửi tin nhắn cùng chữ ký s đến B có 2 cách xử lý:

1. Ký trước, mã hóa sau
   - A băm tin nhắn thành mã hash h rồi ký trước vào h bằng chữ ký $s = Sign_A(h)$
   - A mã hóa h và s thu được $z = e_A(h, s)$ rồi gửi z cho B.
   - Nhận được z, B giải mã z được h, s.
   - Kiểm tra chữ ký $Ver_B(h, s) = true$?
2. Mã hóa trước, ký sau
   - A băm dữ liệu thành mã hash h rồi mã hóa bằng $u = e_A(h)$
   - A ký vào u bằng chữ ký $v = Sign_A(u)$ rồi gửi cho B
   - Nhận được (u, v), B giải mã u nhận được h
   - B kiểm tra chữ ký $Ver_B(u, v) = true$?

Tấn công dạng 2: Giả mạo chữ ký (không tính trực tiếp khóa bí mật)

Giả sử H lấy trộm được thông tin trên đường truyền từ A $\rightarrow$ B

TH1 H lấy được z

- Để tấn công h hoặc s, H cần giải mã z

TH2 H lấy được (u, v)

- Để tấn công h, H cần giải mã (u, v)
- Để tấn công v, H thay thế v bằng chữ ký giả v' rồi gửi cho B. Trong trường hợp này, H có thể giả mạo chữ ký mà không cần giải mã

Khắc phục:
Ký trước, sau đó mã hóa cả chữ ký

Cảm ơn cô và các bạn đã lắng nghe!!!

Phân công, nhiệm vụ

Họ và tên	Công việc
Hoàng Phi Long	Phần 1: Giới thiệu bài toán Sơ đồ chữ ký số và tóm lược quá trình ký số Tạo khóa và code,chạy demo
Vũ Thị Tâm	Tạo chữ ký số và chạy demo Kiểm tra chữ ký và chạy demo Ứng dụng của chữ ký số
Nguyễn Hải Đăng	Tấn công dạng 1: Lộ một trong các giá trị Dựa theo khóa công khai Khi nhiều người sd chung modulo N (TH1) Code demo
Nguyễn Quang Hiếu	Tấn công dạng 1: TH2 của sd chung modulo N Code demo tấn công cho TH này
Phạm Huy Hoàng	Phần còn lại của tấn công dạng 1 Tấn công dạng 2