Tấn công chữ ký số Elgamal

NHÓM 13
Trần Viết Tài - 20185402
Hỏa Ngọc Phương - 20184301
Nguyễn Anh Đức - 20161092
Bùi Hữu Thành - 20173585
Nguyễn Sĩ Linh - 20185373

Viện Toán ứng dụng và Tin học, ĐHBK Hà Nội

Hà Nội, tháng 5 năm 2021

Công việc của thành viên trong nhóm

Họ và tên	Công việc
Nguyễn Anh Đức	Tìm tài liệu phân loại chữ ký số, làm slide, lập trình
Bùi Hữu Thành	Tìm tài liệu tấn công chữ ký số phương pháp xác định khóa bí mật
Nguyễn Sĩ Linh	Tìm tài liệu phần giới thiệu, sơ đồ chữ ký số, sơ đồ chữ ký số Elgamal
Trần Việt Tài	Tìm tài liệu tấn công chữ ký số phương pháp giả mạo chữ ký cùng tài liệu được ký
Hỏa Ngọc Phương	Tìm tài liệu tấn công chữ ký số phương pháp giả mạo chữ ký không cùng tài liệu được ký

Tổng quan

- Phần 1. Hệ mật mã Elgamal
- Phần 2. Tổng quan về chữ ký số
  - Giới thiệu chữ ký số
  - Sơ đồ chữ ký số
  - Phân loại chữ ký số
- Phần 3. Chữ ký số Elgamal
  - Sơ đồ chữ ký số Elgamal
  - Ví dụ
- Phần 4. Phương pháp tấn công chữ ký số Elgamal
  - Phương pháp 1: Xác định khóa bí mật
  - Phương pháp 2: Giả mạo chữ ký số

Hệ mật mã Elgamal

- Hệ Elgamal là một hệ mật mã khóa công khai.
- Hệ Elgamal dựa trên bài toán logarit rời rạc. Tính an toàn của hệ mật phụ thuộc vào độ phức tạp của bài toán logarit rời rạc.
- Hệ Elgamal là một biến thể của sơ đồ phân phối khóa Diffie-Hellman và được đưa ra vào năm 1984.

Bài toán logarit rời rạc: Cho $I = (n, \alpha, \beta)$, trong đó n là số nguyên tố, $\alpha \in Z_n$ là phần tử nguyên thủy và $\beta \in Z_n^*$. Tìm một số nguyên $a,\ 0 \leq a \leq n-2$ sao cho:

$$\alpha^a \equiv \beta (mod\ n)$$

Hệ mật mã Elgamal

Mã hóa và giải mã:

Chọn n là số nguyên tố sao cho bài toán logarit rời rạc trong Z_n khó giải và chọn 2 số nguyên tố nhỏ hơn n là α (một phần tử nguyên thủy Z_n^*) và a(khóa bí mật của người nhận) sau đó tính khóa công khai:

$$\beta \equiv \alpha^a (mod\ n)$$

Định nghĩa tập khóa:

$$K = \{(n, \alpha, a, \beta) : \beta \equiv \alpha^a (mod\ n)\}$$

Công khai giá trị n, α, β và giữ bí mật a.

- Để mã hóa một thông điệp x, người gửi chọn ngẫu nhiên một số $k \in Z_{n-1}$ và tính cặp bản mã:

$$y_1 = \alpha^k mod\ n$$
$$y_2 = x\beta^k mod\ n$$

Và giử (y_1, y_2) đi (sau đó k sẽ bị hủy đi)

- Thông điệp x được giải mã theo công thức: $x = y_2 * (y_1^a)^{-1}$

Với $(y_1^a)^{-1} mod\ n \equiv (y_1^{n-1-a})\ mod\ n$

Giới thiệu chữ ký số

- Những năm 80 của thế kỷ 20, các nhà khoa học đã phát minh ra "chữ ký số" để chứng thực một "tài liệu số".
- Người ta tạo ra "chữ ký số" (chữ ký điện tử) trên "tài liệu số" giống như tạo ra "bản mã" của 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 như không biết "khóa lập mã".
- Để kiểm tra một "chữ ký số" thuộc về một "tài liệu số", người ta phải giải mã "chữ ký số" bằng "khóa giải mã", và so sánh với tài liệu gốc. Ngoài ý nghĩa để chứng thực nguồn gốc hay hiệu lực của các tài liệu số hóa,"chữ ký số" còn dùng để kiểm tra tính toàn vẹn của tài liệu gốc.

Giới thiệu chữ ký số

- Mặt mạnh của "chữ ký số" hơn "chữ ký tay" còn là ở chỗ người ta có thể "ký" vào tài liệu từ rất xa (trên mạng công khai). Hơn thế nữa, có thể "ký" bằng các thiết bị cầm tay (điện thoại di động) tại khắp mọi nơi, miễn là kết nối được vào mạng. Giảm thời gian, sức lực, chi phí.
- "Ký số" th c hiện trên từng bit tài liệu, nên độ dài của "chữ ký số" ít nhất cũng bằng độ dài của tài liệu. Do đó thay vì ký trên tài liệu dài, người ta thường dùng "hàm băm" để tạo "đại diện" cho tài liệu, sau đó mới "ký số" lên "đại diện" này.

Sơ đồ chữ ký số

Sơ đồ chữ ký là bộ năm (P, A, K, S, V), trong đó:

- P là tập hữu hạn các văn bản có thể.
- A là tập hữu hạn các chữ ký có thể.
- K là tập hữu hạn các khoá có thể.
- S là tập các thuật toán ký.
- V là tập các thuật toán kiểm thử.

Sơ đồ chữ ký số

Với mỗi khóa $k \in K$, có thuật toán ký $Sig_k \in S, Sig_k : P \to A$, có thuật toán kiểm tra chữ ký $Ver_k \in V, Ver_k : P \times A \to$ {đúng, sai}, thỏa mãn điều kiện sau với mọi $x \in P, y \in A$:

$$Ver_k(x, y) = \begin{bmatrix} \text{Đúng, nếu } y = Sig_k(x) \\ \text{Sai, nếu } y \neq Sig_k(x) \end{bmatrix}$$

** Chú ý:*

- Người ta thường dùng hệ mã hóa khóa công khai để lập "sơ đồ chữ ký số".
- Khóa bí mật a dùng làm khóa "ký", khóa công khai b dùng làm khóa kiểm tra "chữ ký". Ngược lại với việc mã hóa, dùng khóa công khai b để lập mã, dùng khóa bí mật a để giải mã.

Phân loại chữ ký số

Có nhiều loại chữ ký tùy theo cách phân loại, sau đây xin giới thiệu một số cách.

1. Phân loại chữ ký theo khả năng khôi phục thông điệp gốc

- *Chữ ký có thể khôi phục thông điệp gốc*: Là loại chữ ký, trong đó người nhận có thể khôi phục lại được thông điệp gốc, đã được "ký" bởi "chữ ký" này.

  Ví dụ: Chữ ký RSA

- *Chữ ký không thể khôi phục thông điệp gốc*: Là loại chữ ký, trong đó người nhận không thể khôi phục lại được thông điệp gốc, đã được "ký" bởi "chữ ký" này.

  Ví dụ: Chữ ký Elgamal

Phân loại chữ ký số

2. Phân loại chữ ký theo mức an toàn

- *Chữ ký "không thể phủ nhận"*: Để tránh việc chối bỏ chữ ký hay nhân bản chữ ký để sử dụng nhiều lần, người gửi chữ ký cũng tham gia trực tiếp vào việc kiểm thử chữ ký. Điều đó được thực hiện bằng một giao thức kiểm thử, dưới dạng một giao thức mời hỏi và trả lời.
- *Chữ ký "một lần"*: Để bảo đảm an toàn, "khóa ký" chỉ dùng một lần trên một tài liệu.

  Ví dụ: Chữ ký một lần Lamport.

Phân loại chữ ký số

3. Phân loại chữ ký theo ứng dụng đặc trưng

- Chữ ký "mù" (Blind Signature): được David Chaum giới thiệu vào năm 1983, là một loại chữ ký số trong đó nội dung của thông điệp bị "che" đi trước khi nó được ký.
- Chữ ký "nhóm" (Group Signature): được David Chaum và Van Heyst giới thiệu vào năm 1991, là một loại chữ ký số nhằm mục đích cho phép người dùng ký một thông điệp thay mặt cho một nhóm.
- Chữ ký "bội" (Multy Signature): là một loại chữ ký số chữ ký số cho phép một nhóm người dùng cùng ký vào một tài liệu. Chữ ký "bội" lần đầu tiên cho được áp dụng cho Bitcoin.
- Chữ ký "mù nhóm" (Blind Group Signature): kết hợp các tính chất của chữ ký mù và chữ ký nhóm.
- Chữ ký "mù bội" (Blind Multy Signature): kết hợp các tính chất của chữ ký mù và chữ ký bội.

Sơ đồ chữ ký số Elgamal

*** Tạo cặp khóa (bí mật, công khai) (a, h)**

- Chọn số nguyên tố p sao cho bài toán logarit rời rạc trong Z_p là "khó" giải.
- Chọn phần tử nguyên thủy $g \in Z_p^*$.
- Chọn khóa bí mật $a \in Z_p^*$. Tính khóa công khai $h \equiv g^a mod\ p$.
- Định nghĩa tập khóa: $K = \{(p, g, a, h) : h \equiv g^a mod\ p\}$.
- Các giá trị (p, g, h) được công khai. Còn giá trị a được giữ bí mật.

Sơ đồ chữ ký số Elgamal

*** Ký số**

- Dùng 2 khóa ký: khóa a và khóa ngẫu nhiên bí mật $r \in Z_{p-1}^*$
  (Vì $r \in Z_{p-1}^*$, nên số nguyên tố cùng nhau với $p-1$, do đó tồn tại $r^{-1} mod\ (p-1)$).
- Chữ ký trên $x \in Z_p^*$ là $y = Sig_a(x, r) = (\gamma, \delta), y \in Z_p \times Z_{p-1}$

Trong đó:

$\gamma \in Z_p^*, \delta \in Z_{p-1}$

$\gamma = g^r mod\ p$ và $\delta = (x - a * \gamma) * r^{-1} mod\ (p-1)$

Sơ đồ chữ ký số Elgamal

*** Kiểm tra chữ ký**

$Ver_k(x, \gamma, \delta) =$ đúng $\Leftrightarrow h^\gamma * \gamma^\delta \equiv g^x mod\ p$

Chú ý: Nếu chữ ký được tính đúng, kiểm thử sẽ thành công vì:

$h^\gamma * \gamma^\delta \equiv g^{a\gamma} * g^{r\delta} mod\ p \equiv g^{a\gamma + r\delta} mod\ p \equiv g^x mod\ p$

Do $\delta = (x - a * \gamma) * r^{-1} mod\ (p-1)$ nên $(a * \gamma + r * \delta) \equiv x mod\ (p-1)$

Ví dụ

Ví dụ: Chữ ký Elgamal trên dữ liệu $x = 15$

*** Tạo cặp khóa (bí mật, công khai) (a, h)**

Chọn số nguyên tố $p = 19$

Chọn phần tử nguyên thủy $g = 2 \in Z_p^*$

Chọn khóa bí mật $a = 5 \in Z_p^*$

Tính khóa công khai $h \equiv g^a mod\ p \equiv 2^5 mod\ 19 = 13$

Định nghĩa tập khóa $K = \{p, g, a, h\} = \{19, 2, 5, 13\}$

Các giá trị (p, g, h) công khai, giá trị a được giữ bí mật

Ví dụ

*** Ký số**

Chọn ngẫu nhiên bí mật $r = 7$

Khóa ký là $(a, r) = (5, 7)$

Chữ ký trên dữ liệu $x = 15$ là (γ, δ)

Trong đó:

$\gamma = g^r mod\ p = 2^7 mod 19 = 14$

$\delta = (x - a * \gamma) * r^{-1} mod\ (p-1) = (15 - 5 * 14) * 7^{-1} mod 18 = 5$

Ví dụ

*** Kiểm tra chữ ký**

$Ver_k(x, \gamma, \delta) =$ đúng $\Leftrightarrow h^\gamma * \gamma^\delta \equiv g^x mod\ p$

$h^\gamma * \gamma^\delta = 13^{14} * 14^5 mod\ 19 = 12$
$g^x mod\ p = 2^{15} mod\ 19 = 12$

Hai giá trị đó bàng nhau, như vậy chữ ký là đúng.

Phương pháp 1: Xác định khóa bí mật

1. Số ngẫu nhiên r bị lộ

Nếu r bị lộ, kẻ thám mã sẽ tính được khoá mật

$$a = (x - r\delta)\gamma^{-1} mod\ (p-1)$$

$\Longrightarrow$ *Giải pháp phòng tránh*: Cẩn thận trong việc sử dụng số ngẫu nhiên r, không được để lộ số r được dùng.

Phương pháp 1: Xác định khóa bí mật

2. Dùng r cho 2 lần ký khác nhau

Giả sử dùng r cho 2 lần ký trên x_1 và x_2. Khi đó, (γ, δ_1) là chữ ký trên x_2 còn (γ, δ_2) là chữ ký trên x_2.

Kẻ thám mã có thể tính được giá trị a như sau:

$$\beta^{\gamma} * \gamma^{\delta_1} \equiv \alpha^{x_1} mod\ p$$
$$\beta^{\gamma} * \gamma^{\delta_2} \equiv \alpha^{x_1} mod\ p$$

Do đó ta có: $\alpha^{x_1 - x_2} \equiv \gamma^{\delta_1 - \delta_2} mod\ p$

Phương pháp 1: Xác định khóa bí mật

Đặt $\gamma = \alpha^r$

Ta có $\alpha^{x_1 - x_2} \equiv \gamma^{r*(\delta_1 - \delta_2)} (mod\ p) \Leftrightarrow x_1 - x_2 = r(\delta_1 - \delta_2) (mod\ p) \quad (1)$

Đặt $d = UCNN(\delta_1 - \delta_2)$ và $x' = \frac{x_1 - x_2}{d}, \delta' = \frac{\delta_1 - \delta 2}{2}, p' = \frac{p-1}{d}$

Khi đó đồng dư thức (1) trở thành: $x' \equiv r * \delta' (mod\ p')$

Vì $UCNN(\delta', p') = 1$, nên tính $\epsilon = (\delta' - 1) (mod\ p')$ và tính $r = x' * \epsilon mod\ p'$

$\Rightarrow r = (x' * \epsilon + i * p') mod\ (p-1)$, với i là giá trị nào đó, $0 \leq i \leq d-1$

Thử với giá trị nào đó, ta tìm được r(điều kiện để xác định r là: $\gamma = \alpha^r mod\ p$)

Tiếp theo sẽ tính được khóa bí mật a như trường hợp 1.

$\Longrightarrow$ *Giải pháp phòng tránh*: Mỗi lần ký sử dụng một số r khác nhau.

Phương pháp 1: Xác định khóa bí mật

3. Khóa bí mật a quá nhỏ

Nếu khóa bí mật a quá nhỏ thì bằng phương pháp dò tìm đơn giản, người ta có thể tính được nó.

$\Longrightarrow$ *Giải pháp phòng tránh*: chọn khóa bí mật a là những số nguyên lớn, có kích thước gần bằng số $modulo\ n$.

Phương pháp 1: Xác định khóa bí mật

4. Số ngẫu nhiên r quá nhỏ

Tương tự như đối với khóa bí mật a, số ngẫu nhiên r cũng phải bí mật. Trong trường hợp các tham số này quá nhỏ thì bằng phương pháp dò tìm đơn giản người ta cũng có thể tìm được chúng. Khi đó, sơ đồ chữ ký sẽ bị mất an toàn. Nếu r bị lộ, kẻ thám mã sẽ tính được khóa bí mật $a = (x - r\delta)\gamma^{-1} mod\ (p-1)$.

$\Longrightarrow$ *Giải pháp phòng tránh*: chọn số ngẫu nhiên r là những số nguyên lớn, có kích thước gần bằng số $modulo\ n$.

Phương pháp 2: Giả mạo chữ ký

1. Giả mạo chữ ký không cùng với tài liệu được ký

Tin tặc H cố gắng giả mạo chữ ký trên x mà không hề biết khóa bí mật a.

Như vậy, yêu cầu H phải tính được δ và γ.

- Nếu chọn trước γ, thì H phải tính δ qua đẳng thức $h^{\gamma} * \gamma^{\delta} \equiv g^{x} mod\ p$

Tức là $\gamma^{\delta} \equiv g^{x} h^{-\gamma} mod\ p$ hay $\delta \equiv log_{\gamma} g^{x} h^{-\gamma} mod\ p$

- Nếu chọn trước δ, thì H phải tính γ qua đẳng thức $h^{\gamma} * \gamma^{\delta} \equiv g^{x} mod\ p$

- Nếu chọn trước γ, δ sau đó tính x, thì tin tặc H sẽ phải đối mặt với bài toán logarit rời rạc

Ta có: $h^{\gamma} * \gamma^{\delta} \equiv g^{x} mod\ p$

Như vậy: $x \equiv log_{g} g^{x} \equiv log_{g} h^{\gamma} * \gamma^{\delta}$

Phương pháp 2: Giả mạo chữ ký

2. Giả mạo chữ ký cùng với tài liệu được ký

Tin tặc H có thể ký trên tài liệu ngẫu nhiên bằng cách chọn trước đồng thời x, γ, δ

Cách 1

- Chọn x, γ, δ thỏa mãn điều kiện thử như sau: Chọn các số nguyên i, j sao cho $0 \leq i, j \leq p-2,\ (j, p-1) = 1$ và tính:

$$\gamma = g^i h^j mod\ p$$
$$\delta = -\gamma j^{-1} mod\ (p-1)$$
$$x = \gamma i j^{-1} mod\ (p-1)$$

Trong đó, j^{-1} được tính theo $mod\ (p-1)$

- Chứng minh (γ, δ) là chữ ký trên x bằng cách kiểm tra điều kiện kiểm thử:

$$h^\gamma \gamma^\delta \equiv h^\gamma (g^i h^j)^{-\gamma . j^{-1}} mod\ p \equiv h^\gamma g^{-i.\gamma . j^{-1}} h^\gamma mod\ p \equiv g^x mod\ p$$

Phương pháp 2: Giả mạo chữ ký

Cách 2

Nếu (γ, δ) là chữ ký trên tài liệu x có từ trước, thì có thể giả mạo chữ ký trên tài liệu x' khác.

Chọn số nguyên k, i, j thỏa mãn

$0 \leq k, i, j \leq p-2, (k, p-1) = 1, (\gamma - j, p-1) = 1$ và tính:

$$\gamma' = \gamma^k g^i h^j mod\ p$$
$$\delta' = \delta\gamma'(k\gamma - j\delta)^{-1} mod\ (p-1)$$
$$x' = \gamma'(kx + i\delta)(k\gamma - j\delta)^{-1} mod\ (p-1)$$

(γ', δ') là chữ ký trên x' vì thỏa mãn điều kiện kiểm thử: $h^{\gamma'} \gamma'^{\delta'} \equiv g^{x'} mod\ p$

Thank you !!!