ĐẠI HỌC QUỐC GIA THÀNH PHỐ HỒ CHÍ MINH
TRƯỜNG ĐẠI HỌC BÁCH KHOA
KHOA KHOA HỌC VÀ KỸ THUẬT MÁY TÍNH

Mật mã và An ninh mạng (TN) - CO3070

Báo cáo

BÀI THỰC HÀNH SỐ 3

Giảng viên hướng dẫn: ThS. Nguyễn Cao Đạt

Sinh viên thực hiện: 2014486 - Đậu Xuân Thành

TP. Hồ Chí Minh, 04/2024

Mục lục

Danh mục hình ảnh

1. Hệ mã bất đối xứng

1.1. Câu 1: Cho biết vai trò của the public và private key trong hệ mã khoá công khai với ứng dụng mã hoá?

- *Private key*: khóa riêng dùng để giải mã dữ liệu ai đó đã mã hóa bằng khóa công khai của chính mình và gửi dữ liệu đó cho mình.
- *Public key*: Khóa công khai để tiến hành mã hóa thông điệp muốn gửi cho người khác và khóa công khai có được là của người nhận dữ liệu.

1.2. Câu 2: Thực hiện tính toán: mã hoá và giải mã thông điệp sử dụng giải thuật RSA cho các câu bên dưới:

a) $p = 3; q = 11, e = 7; M = 5$

- $n = n * q = 3 * 11 = 33$
- $\varphi(n) = (p - 1) * (q - 1) = 20$
- $e = 7$
- $d = 3$ thỏa mãn $(d * e) \bmod \varphi(n) = 1$
- public key: (e, n = 7, 33)
- private key: (d, n = 3, 33)

Mã hóa: $C = M^e \bmod n = 5^7 \bmod 33 = 14$
Giải mã: $M = C^d \bmod n = 14^3 \bmod 33 = 5$

b) $p = 5; q = 11, e = 3; M = 9$

- $n = n * q = 5 * 11 = 55$
- $\varphi(n) = (p - 1) * (q - 1) = 40$
- $e = 3$
- $d = 27$ thỏa mãn $(d * e) \bmod \varphi(n) = 1$
- public key: (e, n = 3, 55)
- private key: (d, n = 27, 55)

Mã hóa: $C = M^e \bmod n = 9^3 \bmod 55 = 14$
Giải mã: $M = C^d \bmod n = 14^{27} \bmod 55 = 9$

c) $p = 7; q = 11, e = 17; M = 8$

- $n = n * q = 7 * 11 = 77$
- $\varphi(n) = (p - 1) * (q - 1) = 60$
- $e = 17$
- $d = 53$ thỏa mãn $(d * e) \bmod \varphi(n) = 1$
- public key: (e, n = 17, 77)
- private key: (d, n = 53, 77)

Mã hóa: $C = M^e \bmod n = 8^{17} \bmod 77 = 57$
Giải mã: $M = C^d \bmod n = 57^{27} \bmod 77 = 8$

d) $p = 11; q = 13, e = 11; M = 7$

- public key: (e, n = 11, 143)
- private key: (d, n = 11, 143)

Mã hóa: $C = M^e \bmod n = 7^{11} \bmod 143 = 106$
Giải mã: $M = C^d \bmod n = 106^{11} \bmod 143 = 7$

e) $p = 17; q = 31, e = 7; M = 2$

- public key: (e, n = 343, 527)
- private key: (d, n = 7, 527)

Mã hóa: $C = M^e \bmod n = 2^{343} \bmod 527 = 349$
Giải mã: $M = C^d \bmod n = 349^7 \bmod 527 = 2$

1.3. Câu 3: Giả sử trong hệ mã khoá công khai sử dụng RSA, bạn biết được một ciphertext C = 10 được gởi đến một người có public key là e = 5, n = 35.

Chúng ta có thể sử dụng được các thông tin như trên để giải mã được thông điệp gốc (M) được không, nêu từng bước thực hiện và giải thích?

Phân tích thừa số nguyên tố: $n = 5 * 7 \Longrightarrow \varphi(n) = (5-1) * (7-1) = 24$

Ta có: $(d * e) \bmod \varphi(n) = 1 \Longrightarrow$ Ta cần giải phương trình $(d * 5) \bmod 24 = 1$.

Sử dụng giải thuật **Extended Euclidean** ta có $d = 5$.

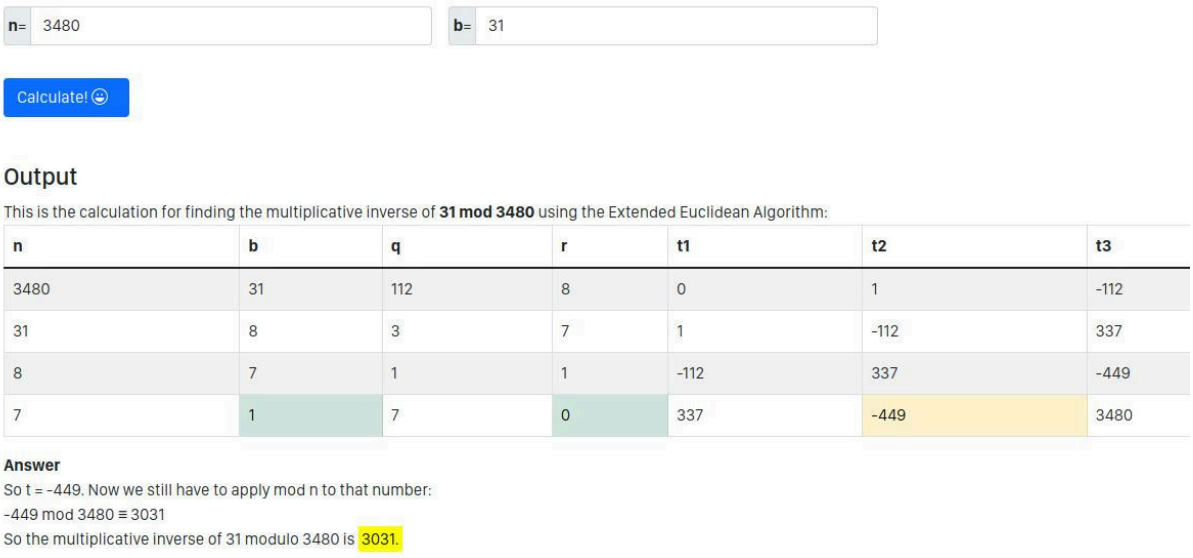
Vậy, private key là: (d, n) = (5, 35) $\Longrightarrow M = C^d \bmod n = 10^5 \bmod 35 = 5$.

1.4. Câu 4: Trong ứng dụng với hệ mã khoá công khai sử dụng RSA, chúng ta biết được một thành viên đang dùng public key là e = 31, n = 3599. Chúng ta có thể tìm được private key của thành viên nói trên được hay không, nêu từng bước thực hiện và giải thích?

Ta thực hiện thử sai với các số nguyên tố nhỏ hơn 60, kết quả cho thấy ta phân tích được: $n = 3599 = 59 * 61$. Vậy (p, q) sẽ là $(59, 61)$ hoặc $(61, 59)$.

Ta có: $\varphi(n) = (p-1) * (q-1) = 3480$. Để tìm d, ta cần giải phương trình: $(31 * d) \bmod 3480 = 1$.

Sử dụng thuật toán **Extended Euclidean** để tìm d, ta được $d = 3031$.



Vậy, private key của thành viên nói trên là: (3031, 3599).

2. Hashing

2.1. Câu 1: Hàm một chiều (one-way function) là gì?

Hàm một chiều là hàm mà rất dễ mã hóa nhưng không giải mã được, ta không thể tính lại được bản gốc khi có bản mã.

2.2. Câu 2: Cho một ví dụ để minh hoạ việc sử dụng hàm băm có thể giúp kiểm tra tính toàn vẹn của thông điệp.

Gợi ý: mã hoá thông điệp, tạo ra thay đổi trên ciphertext và sử dụng hàm băm để kiểm tra thông điệp được giải mã có thay đổi so với thông điệp gốc ban đầu.

Có thể dùng hàm băm để tạo chữ kí số giúp xác thực tính toàn vẹn của thông điệp cũng như xác minh được người gửi. Ví dụ với việc gửi thông điệp M. Bên gửi: sẽ gửi dùng hàm Hash để tính h = Hash(M), sau đó lấy h đi mã hóa bằng khóa riêng người gửi để được chữ ký số S. Người gửi sẽ gửi cả M và S.

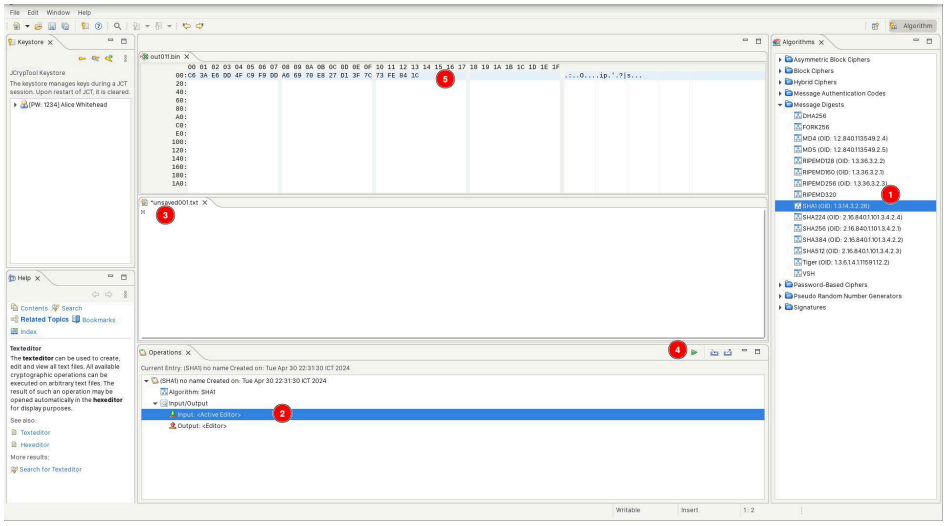
Bên nhân: lấy ra M và tính h = Hash(M), sau đó sẽ lấy khóa công khai người gửi để giải mã S ta được h'. Cuối cùng so trùng h = h' để xem tính toàn vẹn của dữ liệu.

2.3. Câu 3: Hàm băm H(·) là hàm có chức năng chuyển thông điệp có kích thước bất kì bất kỳ về kích thước cố định:

a) Xem xét giá trị hash được tạo ra bằng cách áp dụng giải thuật hash SHA-1 trên một ký tự trong bảng chữ cái tiếng Anh: C6 3A E6 DD 4F C9 F9 DD A6 69 70 E8 27 D1 3F 7C 73 FE 84 1C. Hãy tìm ký tự chữ cái tiếng anh được sử dụng và mô tả cách làm? (dùng công cụ CrypTool)

   NOTE: Ở đây sinh viên đang sử dụng hệ điều hành **ArchLinux** nên sử dụng phiên bàn Cryptool dành cho Linux.

   - Bước 1: Mở công cụ, và chọn vào phần Algorithms, và chọn giải thuật **SHA1**
   - Bước 2: Ở tab Operations > Input/Ouput, chọn Input là Active Editor
   - Bước 3: Nhập các ký tự cần thử để dùng giải thuật hashing và nhấn Execute
   - Bước 4: Ta theo dõi kết quả ở oupt editor



b) Giả sử bạn đã tìm ra được ký tự ở câu a, như vậy có thể kết luận hàm hash SHA-1 không thoả mãn tính chất một chiều (one-way) được hay không, giải thích câu trả lời? SHA-1 vẫn thỏa mãn

tính chất một chiều, chúng ta tìm được ký tự ban đầu dựa vào phép thử, và nếu message trở nên lớn hơn, rất khó để tìm ra được giá trị hash.

2.4. Câu 4: Thực hiện lại bước 3 cho các giải thuật hash khác và đánh giá giá trị hash nhận được với giá trị hash ban đầu.

•

Tài liệu tham khảo