1 Information

ID	Name
21120566	Huu Thuan Nguyen

2 Problem statement

- **Trường hợp 1**: Giả sử nhóm $m \geq 2$ người dùng 1 hệ mã RSA cùng dùng chung giá trị n.
- **Trường hợp 2**: Nếu có k người ($2 \leq k \leq n$) cùng chọn khoá công khai là (e, n_i), (e như nhau, n_i khác nhau)

Nếu dùng hệ mã RSA như 1 trong 2 cách trên thì RSA có khả năng bị tấn công. Giải thích tại sao?

3 Solution

3.1 Trường hợp 1

3.1.1 Ví dụ

Lỗ hổng bảo mật trong trường hợp này được gọi là **Common-Modulus Attack**. Lỗ hổng này xảy ra khi một nhóm người dùng sử dụng các public key $Z_i = (e_i, n)$ với cùng một modulus n.

Cho Alice và Bob với các public key $Z_A = (e_A, n)$ và $Z_B = (e_B, n)$, và $e_A \neq e_B$. Giả sử plaintext m được mã hoá thành 2 ciphertext c_A và c_B để gửi cho Alice và Bob bằng cách sử dụng 2 public key trên:

$$
\begin{aligned}
c_A &= m^{e_A} \mod n \\
c_B &= m^{e_B} \mod n
\end{aligned}
$$

Khi đó, nếu Charlie biết được e_A, e_B và có được 2 ciphertext trên, anh ta có thể tính được plaintext m bằng cách sử dụng **Extended Euclidean Algorithm** như sau.

Vì $(e_A, e_B) = 1$, tồn tại x, y sao cho $xe_A + ye_B = 1$. Khi đó, ta có:

$$
\begin{aligned}
c_A^x \times c_B^y &= (m^{e_A})^x \times (m^{e_B})^y \\
&= m^{xe_A + ye_B} \\
&= m
\end{aligned}
$$

3.1.2 Tổng quát

Tấn công này áp dụng cho bất kì k người (với $k \geq 2$) bằng cách chứng minh tương tự như trên.

3.2 Trường hợp 2

3.2.1 Ví dụ

Trường hợp này không có lỗ hổng bảo mật nào. Hầu hết các hệ thống RSA hiện nay đều sử dụng chung một exponent $e = 65537$. Nếu có một loại tấn công trong trường hợp này, RSA đã không được sử dụng rộng rãi như hiện nay.

Tuy nhiên với một exponent e nhỏ, thì có thể tìm được plaintext m bằng cách sử dụng **Chinese Remainder Theorem**.

Lỗ hổng bảo mật trong trường hợp này được gọi là **Hastad's Broadcast Attack**. Lỗ hổng này xảy ra khi một nhóm người dùng sử dụng các public key $Z_i = (e, n_i)$ với cùng một exponent e.

Cho Alice và Bob với các public key $Z_A = (e, n_A)$ và $Z_B = (e, n_B)$, và $n_A \neq n_B$. Giả sử plaintext m được mã hoá thành 2 ciphertext c_A và c_B để gửi cho Alice và Bob bằng cách sử dụng 2 public key trên:

$$\begin{aligned} c_A &= m^e \mod n_A \\ c_B &= m^e \mod n_B \end{aligned}$$

Khi đó, nếu Charlie biết được n_A, n_B, e và có được 2 ciphertext trên, anh ta có thể tính được plaintext m bằng cách sử dụng **Chinese Remainder Theorem** như sau.

$$\begin{aligned} m^e &\equiv c_A \mod n_A \\ m^e &\equiv c_B \mod n_B \end{aligned}$$

Đặt:

$$\begin{aligned} x_A &= \Pi_{i \neq A} n_i \\ &= n_B \\ x_B &= \Pi_{i \neq B} n_i \\ &= n_A \end{aligned}$$

Ta có:

$$\begin{aligned} m^e &\equiv c_A \times x_A \times x_A^{-1} \mod \Pi n_i \\ &= c_A \times n_B \times n_B^{-1} \mod n_A \times n_B \\ m^e &\equiv c_B \times x_B \times x_B^{-1} \mod \Pi n_i \\ &= c_B \times n_A \times n_A^{-1} \mod n_A \times n_B \end{aligned}$$

Áp dụng **Chinese Remainder Theorem**:

$$m^e \equiv c_A \times n_B \times n_B^{-1} + c_B \times n_A \times n_A^{-1} \mod n_A \times n_B$$

Từ đây, ta có thể tính được plaintext m:

$$m = \sqrt[e]{m^e}$$

3.2.2 Tổng quát

Tấn công này áp dụng cho bất kì k người (với $k \geq 2$) bằng cách chứng minh tương tự như trên.