Hệ mã bất đối xứng

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.

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: $M = C^d \bmod n = 349^7 \bmod 527 = 2$

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 $d = 5$.

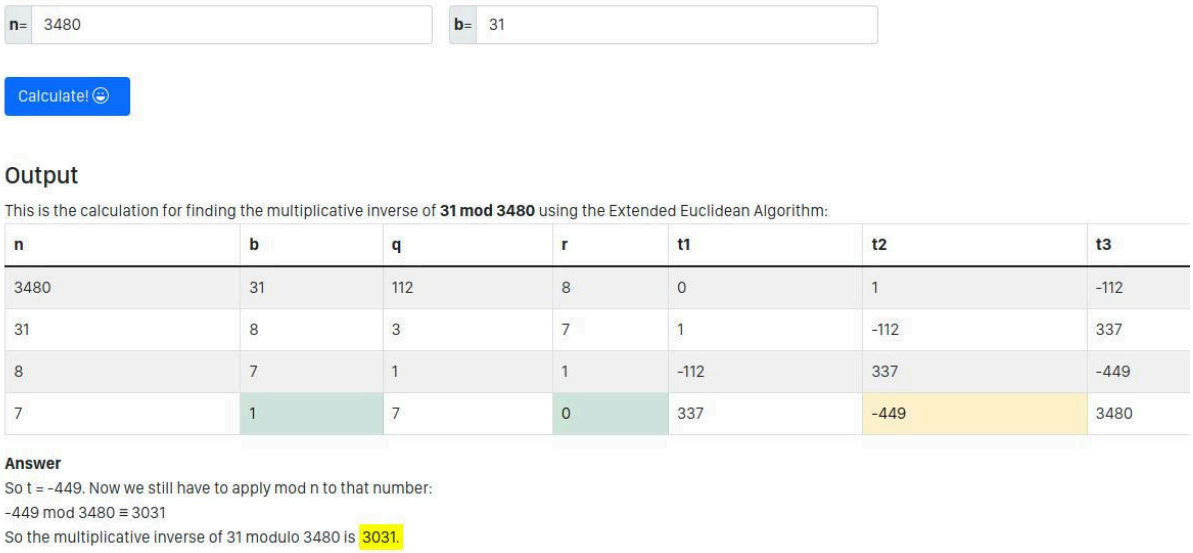
Vậy, private key là: (d, n) = (5, 35) $\Longrightarrow M = C^d \bmod n = 10^5 \bmod 35 = 5$.

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).