Homework #7

I. Lý thuyết

1. Nêu các thành phần chính của hệ mật mã khóa công khai?

Khóa công khai (public key): Được sử dụng để mã hóa dữ liệu và có thể được công bố rộng rãi.
Khóa bí mật (private key): Được sử dụng để giải mã dữ liệu đã được mã hóa và phải được bảo mật cẩn thận.

2. Vai trò của khóa công khai (publick key) và khóa bí mật (private key)?

Khóa công khai (public key): Dùng để mã hóa thông tin trước khi gửi đi, nó được phân phối rộng rãi và có thể được truy cập bởi bất kỳ ai.

Khóa bí mật (private key): Dùng để giải mã thông tin đã được mã hóa bằng khóa công khai tương ứng với nó. Khóa này phải được bảo mật cẩn thận và chỉ có chủ sở hữu mới biết.

II. Bài tập:

Mã hóa và giải mã theo phương pháp RSA cho các trường hợp sau:

1. Tính n: $n = p \times q$
2. Tính hàm Euler của n: $\phi(n) = (p-1) \times (q-1)$
3. Tìm khóa công khai (public key): e là số nguyên tố cùng nhau với $\phi(n)$
4. Tìm khóa bí mật (private key): $d \times e \equiv 1 \pmod{\phi(n)}$
5. Mã hóa: $C \equiv M^e \pmod{n}$
6. Giải mã: $M \equiv C^d \pmod{n}$

1. $n = p \times q = 3 \times 11 = 33$
2. $\phi(n) = (3-1) \times (11-1) = 2 \times 10 = 20$
3. Vì 7 là số nguyên tố cùng nhau với 20, nên $e = 7$ là khóa công khai.
4. Tìm d: $d \times 7 \equiv 1 \pmod{20}$. Giải phương trình này ta có $d = 3$.
5. Mã hóa: $C \equiv 5^7 \pmod{33} \equiv 18$
6. Giải mã: $M \equiv 18^3 \pmod{33} \equiv 5$

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

1. $n = p \times q = 5 \times 11 = 55$
2. $\phi(n) = (5 - 1) \times (11 - 1) = 4 \times 10 = 40$
3. $e = 3$ là khóa công khai vì $gcd(3, 40) = 1$
4. Tìm d: $d \times 3 \equiv 1 \pmod{40}$. Giải phương trình này ta có $d = 27$.
5. Mã hóa: $C \equiv 9^3 \pmod{55} \equiv 14$
6. Giải mã: $M \equiv 14^{27} \pmod{55} \equiv 9$

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

1. $n = p \times q = 7 \times 11 = 77$
2. $\phi(n) = (7 - 1) \times (11 - 1) = 6 \times 10 = 60$
3. $e = 17$ là khóa công khai vì $gcd(17, 60) = 1$
4. Tìm d: $d \times 17 \equiv 1 \pmod{60}$. Giải phương trình này ta có $d = 53$.
5. Mã hóa: $C \equiv 8^{17} \pmod{77} \equiv 27$
6. Giải mã: $M \equiv 27^{53} \pmod{77} \equiv 8$

d. $p = 11$; $q = 13$; $e = 11$; M=7

1. $n = p \times q = 11 \times 13 = 143$
2. $\phi(n) = (11 - 1) \times (13 - 1) = 10 \times 12 = 120$
3. $e = 11$ là khóa công khai vì $gcd(11, 120) = 1$
4. Tìm d: $d \times 11 \equiv 1 \pmod{120}$. Giải phương trình này ta có $d = 11$.
5. Mã hóa: $C \equiv 7^{11} \pmod{143} \equiv 11$
6. Giải mã: $M \equiv 11^{11} \pmod{143} \equiv 7$

e. p = 17 ; q = 31 ; e=7 ; M = 2

1. $n = p \times q = 17 \times 31 = 527$
2. $\phi(n) = (17 - 1) \times (31 - 1) = 16 \times 30 = 480$
3. $e = 7$ là khóa công khai vì $gcd(7, 480) = 1$
4. Tìm d: $d \times 7 \equiv 1 \pmod{480}$. Giải phương trình này ta có $d = 343$.
5. Mã hóa: $C \equiv 2^7 \pmod{527} \equiv 128$
6. Giải mã: $M \equiv 128^{343} \pmod{527} \equiv 2$