1) Cho hệ mã RSA, với n = 323, khóa để mã hóa là e=31.

a) Tiến hành xác định khóa bí mật d.

b) Tiến hành mã hóa P=30

c) Tiến hành giải mã C=40

2) Áp dụng chữ ký số trong RSA để ký thông điệp sau M = 1024 với khóa dùng để ký e=3, n=141? Trình bày lần lượt các bước.

Bài giải:

1)

+ Khóa công khai (n, e) = (323, 31)

+ Phân tích n thành thừa số nguyên tố: 323 = 17.19 (p=17, q=19)

+ Tìm phi $\phi(n) = (p-1)(q-1) = 16.18 = 288$

+ Tính khóa bí mật $d = e^{-1} \bmod \phi(n) = 31^{-1} \bmod 288$ ➔ sử dụng Euclipe mở rộng :

Bước	**m**	**a**	**r**	**q**	**y0**	**y1**	**y**
1	288	31	9	9	0	1	-9
2	31	9	4	3	1	-9	28
3	9	4	1	2	-9	28	-65
4	4	1	0				

Dựa vào bảng trên $d = -65 + k.288 \equiv 223 \bmod 288$

b) mã hóa:

$$y = p^e \bmod n = 30^{31} \bmod 323 = 106$$

c) Giải mã:

$$x = 40^{223} \bmod 323 = 71$$

Nháp: x = 30, n=31, M=323:

```
int pow(int x, int n, int M) {
    int res = 1;
    int temp = x;
    while (n > 0) {
        if (n & 1) res = res * temp % M;
        n >>= 1;
        temp = temp * temp % M;
    }
    return res;
}
```

1024 = 000100 00000000 = [4^31 mod 323, 0^31 mod 323] = [47 0]

47^223 mod 323 = 4

0^223 mod 323 = 0

l: độ dài của chuỗi con lớn nhất sao cho 2^l < n (323) ➔ l = 8