31.5-1

$$x \equiv 4 \pmod{5} \quad x \equiv 5 \pmod{11}$$

$$N = 5 \cdot 11 = 55$$

b_i	N_i	x_i	$b_i N_i x_i$
4	11	1	44
5	5	9	225

$11x_1 \equiv 1 \mod 5$ $\qquad$ $5x_2 \equiv 1 \pmod{11}$

$x_1 \equiv 1 \mod 5$ $\qquad$ $x \equiv 9 \pmod{11}$

$$a \equiv 44+225 \pmod{55}$$

$$\equiv 265 \pmod{55}$$

$$\equiv 49 \pmod{55}$$

31.5.2

$X \equiv 1 \pmod 9$

$X \equiv 2 \pmod 8$

$X \equiv 3 \pmod 7$

$63 x_2 \equiv 1 \pmod 8$

$7 x_2 \equiv 1 \pmod 8$

$x_2 \equiv 7 \pmod 8$

$N = 7 \cdot 8 \cdot 9 = 504$

b_i	N_i	x_i	$b_i N_i x_i$
1	56	5	280
2	63	7	882
3	72	4	864

$56 x_1 \equiv 1 \pmod 9$

$2 x_1 \equiv 1 \pmod 9$

$x_1 \equiv 5 \pmod 9$

$72 x_3 \equiv 1 \pmod 7$

$2 x_3 \equiv 1 \pmod 7$

$x_3 \equiv 4 \pmod 7$

$X \equiv (280 + 882 + 864) \pmod{504}$

$\equiv 10 \pmod{504}$

31-5.3

According to corollary 31.29

$X_i \equiv a_i \pmod{n}$ $X \equiv a \pmod{n}$

To show $X_i \equiv a_i^{-1} \pmod{n_i}$

we have

$(ax) \bmod n \leftrightarrow (a_i X_i \bmod n_i)$

Because $X_i \equiv a_i \pmod{n}$

$X_i \equiv a_i^{-1} \pmod{n}$

$(ax) \bmod n = 1 \bmod n$

$a_i X_i \pmod{n_i} = (1 \pmod{n_i})$

$a_i x_i = 1 \pmod{n_i} \Rightarrow X_i = a_i^{-1} \pmod{n_i}$

31.6-1

$g = 2$

i	$2^i \bmod 11$	$3^i \bmod 11$	$4^i \bmod 11$	$5^i \bmod 11$	$6^i \bmod 11$	$7^i \bmod 11$	$8^i \bmod 11$	$9^i \bmod 11$	$10^i \bmod 11$
0	1	1	1	1	1	1	1	1	1
1	2	3	4	5	6	7	8	9	10
2	4	9	5	3	3	5	9	4	1
3	8	5	9	4	7	2	6	3	10
4	5	4	3	9	9	3	4	5	1
5	10	1	1	1	10	10	10	1	10
6	9	3	4	5	5	4	3	9	1
7	7	9	5	3	8	6	2	4	10
8	3	5	9	4	4	9	5	3	1
9	6	4	3	9	2	8	7	5	10
10	1	1	1	1	1	1	1	1	1
11	2	3	4	5	6	7	8	9	10

31.6-2

```
Modular-exponentiation (a, b, n)
    V = 1
    while true:
        if b mod 2 = 1:
            V = (V · a) mod n
            b = b/2
        if b == 0:
            break
        else:
            a = a^2 mod n
    return V
```

31-6-3

$$X^{\phi(n)} \equiv 1 \pmod{n}$$

$$X \equiv a^{-1} \pmod{n}$$

$$aX = a \cdot a^{-1} \pmod{n} = 1 \bmod n$$

According to Fermat theorem,

$$a^{(n-1)} = 1 \pmod{n}$$

$$aX = a^{(n-1)} \Rightarrow X = a^{(n-2)}$$

Therefore, we can find solution with

$\phi(n)$

31.7-3

$$P_A(M_1) P_A(M_2)$$

$$= M_1^e \bmod n \quad M_2^e \bmod n$$

$$= (M_1 M_2)^e \bmod n$$

$$= P_A(M_1 M_2)$$

To produce efficient decrypt of 1% message, we can put the M into algorithm to see if we get a successful hit. If not we generate a random message and add them together. and do the above procedures again Since the value space is cyclic. If this is repeated large number of times. we will have a great confidence on the result.

31.8-3

x is non-trivial square root of 1

we have $(x-1)(x+1) = 0$

$\gcd(x^2-1, n) = \gcd(x^2-1 \bmod n, n)$

$= \gcd(n, 0)$,

we get

$\gcd(x+1, n) \cdot \gcd(x-1, n) \geq n$

It implies $x+1 \nmid n$ and $x-1 \nmid n$

Also $1 < x-1 < x+1 < n$

So $x-1$ and $x+1$ are both

non trivial divisors.