

$$\equiv 1 \times 5 \pmod{12} \quad (\because 5^2 = 25 \equiv 1 \pmod{12})$$

$$\equiv 5 \pmod{12}.$$

(2)

$$x^e = 2^5 = 32 \equiv 11 \pmod{21}$$

より, $c = 11$.

(3)

$$c^d = 3^5 = 3^4 \times 3$$

$$\equiv (-3) \times 3 \pmod{12} \quad (\because 3^4 = 81 \equiv (-3) \pmod{21})$$

$$\equiv -9 \pmod{21}$$

$$\equiv 12 \pmod{21}$$

より, $x = 12$.

問2. 14

送信メッセージを x とする.

(1)

$$N = 13 \times 31 = 403, L = 12 \times 30 = 360 \text{ である.}$$

ユークリッドの互助法を用いて, d を求める.

割り算の計算は, 表記困難のため, 省略.

$$n = 360, a = 7, r_1 = 3, r_2 = 1 \text{ とすると,}$$

$$\gcd(a, n) = r_2 = a - 2r_1 = a - 2(n - 51a) = 103a - 2n = 103 \times 7 - 2 \times 360.$$

よって,

$$d = e^{-1} = 7^{-1} \equiv 103 \pmod{360}.$$

$$c^d = 87^{103} = (87^3)^{34} \times 87$$

$$\equiv 1^{34} \times 87 \pmod{403} \quad (\because 87^3 = 1634 \times 403 + 1 \equiv 1 \pmod{403})$$

$$\equiv 87 \pmod{403}$$

より, $x = 87$.

(2)

$$N = 13 \times 31 = 403, L = 12 \times 30 = 360 \text{ である.}$$

ユークリッドの互助法を用いて, d を求める.

割り算の計算は, 表記困難のため, 省略.

$$n = 360, a = 19, r_1 = 18, r_2 = 1 \text{ とすると,}$$

$$\gcd(a, n) = r_2 = a - r_1 = a - (n - 18a) = 19a - n = 19 \times 19 - 360.$$

よって,

$$d = e^{-1} = 19^{-1} \equiv 19 \pmod{360}.$$

$$c^d = 125^{19} = 5^{57} = (5^4)^{14} \times 5$$

$$\equiv 222^{14} \times 5 \pmod{403} \quad (\because 5^4 = 625 \equiv 222 \pmod{403})$$

$$\equiv (222^2)^7 \times 5 \pmod{403}$$

$$\equiv 118^7 \times 5 \pmod{403} \quad (\because 222^2 = 122 \times 403 + 118 \equiv 118 \pmod{403})$$