1. Module 1

7 варіант

1.1. 1

1. Схема RSA. Повідомлення: m = 17; параметри: p = 3 , q = 7, e = 17.

Знайти d, зашифрувати m (тобто знайти c), розшифрувати c.

$$\begin{cases} p = 3 \\ q = 7 \\ e = 17 \\ m = 17 \end{cases}$$

$$n = 21$$

$$\bmod \varphi(n) = 12$$

$$17d = 1 \bmod 12$$

Need to calculate **modular multiplicative inverse**

$$d = 17^{-1} \bmod 12$$

Using extended Euclidean algorithm. Let's set: $x_0 = 1, x_1 = 0$

While a>1:

$$q = 1; (a, n) = (12, 5); (x_0, x_1) = (1, -1)$$

$$q = 2; (a, n) = (5, 2); (x_0, x_1) = (-1, 3)$$

$$q = 2; (a, n) = (2, 1); (x_0, x_1) = (3, 5)$$

$$q = 2; (a, n) = (1, 1); (x_0, x_1) = (5, ...)$$

$$a = 1, \text{stop}$$

$$x_0 = 5 \rightarrow x = 5$$

$$\text{Let's verify: } 17 * 5 \bmod 12 = 85 \bmod 12 = 1$$

$$d = 5$$

Public key = (n, e) = (21, 17)

The encrypted message is $y = 17^{17} \bmod 21$

The decrypted message is

$$m = 17^{17*d} \bmod 21$$

$$m = 17^{17*5} \bmod 21$$

$$\text{as we know } (17 * 5) = k12 + 1 = 84 + 1 = 85$$

$$m = 17^{7*\varphi(21)} 17 \bmod 21 = 17 \bmod 21$$

1.2. 2

2. Розв'язати порівняння за модулем:

Need to calculate **modular multiplicative inverse**

$$610x \equiv 1 \bmod 987$$

$$x \equiv 610^{-1} \bmod 987$$

$$610x - 987y = 1$$

Using extended Euclidean algorithm. Let's set: $x_0 = 1, x_1 = 0$

While a>1:

$$q = 0; (a, n) = (987, 610); (x_0, x_1) = (,)$$

$$q = 1; (a, n) = (610, 377); (x_0, x_1) = (,)$$

$$q = 1; (a, n) = (377, 233); (x_0, x_1) = (,)$$

$$q = 1; (a, n) = (233, 144); (x_0, x_1) = (,)$$

$$q = 1; (a, n) = (144, 89); (x_0, x_1) = (,)$$

$$q = 1; (a, n) = (89, 55); (x_0, x_1) = (,)$$

$$q = 1; (a, n) = (55, 34); (x_0, x_1) = (,)$$

$$q = 1; (a, n) = (34, 21); (x_0, x_1) = (,)$$

$$q = 1; (a, n) = (21, 13); (x_0, x_1) = (,)$$

$$q = 1; (a, n) = (13, 8); (x_0, x_1) = (,)$$

$$q = 1; (a, n) = (8, 7); (x_0, x_1) = (,)$$

$$q = 1; (a, n) = (7, 1); (x_0, x_1) = (,)$$

$$q = 7; (a, n) = (1,_{)}; (x_0, x_1) = (,)$$

1.3. 3

$$15^{3^{1000}} \bmod 17 =$$

$$3^{1000} \bmod 16 = 16^x + y$$

$$15^{16x+y} \bmod 17 = 15^y * 15^{16x} \bmod 17$$

За малою теоремою Ферма

$$15^{16x} \bmod 17 = \left(15^{16}\right)^x \bmod 17$$

$$\left(15^{p-1}\right)^x \bmod p = 1^x \bmod p \longrightarrow \left(15^{16}\right)^x \bmod 17 = 1 \bmod 17$$

Залишилось знайти y.

$$15^y \bmod 17 = 15^{3^{1000}} \bmod 17$$

16 is not prime. 3^1000 is not prime, but 3 and 16 is coprime -> we can apply Euler's theorem.

$$\varphi(n) = 8$$

$$3^{1000} \bmod 16 = \left(3^8\right)^{125} \bmod 16$$

By Euler's theorem:

$$a^{\varphi(n)} \equiv 1 \bmod n$$

$$3^8 \equiv 1 \bmod 16$$

$$\left(3^8\right)^{125} \equiv 1 \bmod 16$$

$$3^{1000} \bmod 16 = 1 \bmod 16$$

$$3^{1000} = 16^z + 1$$

Finally:

$$15^{16z} * 15 \bmod 17$$

$$15^{16z} \bmod 17 = 1 \bmod 17$$

$$1 * 1 * 15 \bmod 17 = 15 \bmod 17$$