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.

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

$n = 3 * 7 = 21$

$\varphi(n) = (p-1)(q-1) = 12 = N$

$de = 1 \bmod N$

$3d = 1 \bmod 12 \longrightarrow d = 37$

$C = E(m) = 17^{17} \bmod 21 = 5$

1.2. 2

2. Розв’язати порівняння за модулем:

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

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:

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

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

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