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 ≡ 1 mod 987.