НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені Ігоря СІКОРСЬКОГО»
Навчально-науковий фізико-технічний інститут
Кафедра математичних методів захисту інформації

ДКР
Варіант №3

Роботу виконав:
Юрчук Олексій, ФІ-52мн

27 листопада 2025 р.
м. Київ

Завдання № 1

Умова:

1. Перевірити, що набір публічних параметрів $(N, p, q, d) = (7, 3, 41, 2)$ криптосистеми NTRUCrypt є коректним;
2. Використовуючи публічний ключ:

$$pk = 18x^6 + 6x^5 - 11x^4 + 3x^3 - 15x^2 - 2x - 2 = h(x)$$

зашифрувати повідомлення $m = -x^5 - x^4 - x^2 - x + 1$.

Розв'язання:

Спершу перевіримо, що набір параметрів є коректним. Це робиться дуже просто. Треба усього лиш перевірити, що виконується наступна рівність: $q > (6d + 1)p$.
У нас задано:

- $N = 7$;
- $p = 3$;
- $q = 41$;
- $d = 2$.

Маємо: $41 > (6 \cdot 2 + 1) \cdot 3 = 39$. Справді, $41 > 39$, то ж система NTRUCrypt є коректною.

Далі займемося зашифруванням повідомлення. Для цього нам необхідно спершу обчислити центральне підняття m. В нашому випадку саме повідомлення $m = -x^5 - x^4 - x^2 - x + 1$ і буде центральним підняттям, оскільки коефіцієнти вже лежать у напівінтервалі $(-41/2, 41/2]$, тобто в проміжку $(-20, 20]$.

Наступним нашим кроком є обрання випадкового многочлена $\mathbf{r}$ з множини тернарних многочленів $\mathcal{T}(d, d)$. В нас це $\mathcal{T}(2, 2)$ – де перша двійка вказує на кількість коефіцієнтів 1, а друга відповідно коефіцієнтів -1.

Нехай це буде многочлен $\mathbf{r} = x^6 - x^5 + x - 1$. Щоб отримати шифротекст $\mathbf{e}(x)$ необхідно обчислити:

$$\mathbf{e}(x) = p \cdot \mathbf{r}(x) \star \mathbf{h}(x) + \mathbf{m}(x)$$

Зробимо покроково. Спершу обчислимо добуток a.k.a. згортковий многочлен:

$$\mathbf{r}(x) \star \mathbf{h}(x) = (x^6 - x^5 + x - 1) \star (18x^6 + 6x^5 - 11x^4 + 3x^3 - 15x^2 - 2x - 2)$$

Для цього необхідно обчислити результуючі коефіцієнти. Скористаємось формулою:

$$c_k = \sum_{i+j \equiv k \pmod N} a_i \cdot b_j, \quad 0 \le k \le N-1$$

Для нашої задачі $N = 7$, тому формула матиме вигляд:

$$c_k = \sum_{i+j \equiv k \pmod 7} a_i \cdot b_j, \quad 0 \le k \le 6$$

Обчислимо коефіцієнти $c_0, \dots, c_6$, маючи

$$a_0 = -1,\ a_1 = 1,\ a_2 = 0,\ a_3 = 0,\ a_4 = 0,\ a_5 = -1,\ a_6 = 1$$
$$b_0 = -2,\ b_1 = -2,\ b_2 = -15,\ b_3 = 3,\ b_4 = -11,\ b_5 = 6,\ b_6 = 18$$

$$c_0 = \sum_{i+j \equiv 0 \pmod 7} a_i \cdot b_j = a_0 \cdot b_0 + a_1 \cdot b_6 + a_2 \cdot b_5 + a_3 \cdot b_4 + a_4 \cdot b_3 + a_5 \cdot b_2 + a_6 \cdot b_1 =$$
$$= a_0 \cdot b_0 + a_1 \cdot b_6 + a_5 \cdot b_2 + a_6 \cdot b_1 = (-1) \cdot (-2) + 1 \cdot 18 + (-1) \cdot (-15) + 1 \cdot (-2) =$$
$$= 33 \pmod{41}$$
$$c_1 = \sum_{i+j \equiv 1 \pmod 7} a_i \cdot b_j = a_0 \cdot b_1 + a_1 \cdot b_0 + a_2 \cdot b_6 + a_3 \cdot b_5 + a_4 \cdot b_4 + a_5 \cdot b_3 + a_6 \cdot b_2 =$$
$$= a_0 \cdot b_1 + a_1 \cdot b_0 + a_5 \cdot b_3 + a_6 \cdot b_2 = (-1) \cdot (-2) + 1 \cdot (-2) + (-1) \cdot 3 + 1 \cdot (-15) = -18 =$$
$$= 23 \pmod{41}$$
$$c_2 = \sum_{i+j \equiv 2 \pmod 7} a_i \cdot b_j = a_0 \cdot b_2 + a_1 \cdot b_1 + a_2 \cdot b_0 + a_3 \cdot b_6 + a_4 \cdot b_5 + a_5 \cdot b_4 + a_6 \cdot b_3 =$$
$$= a_0 \cdot b_2 + a_1 \cdot b_1 + a_5 \cdot b_4 + a_6 \cdot b_3 = (-1) \cdot (-15) + 1 \cdot (-2) + (-1) \cdot (-11) + 1 \cdot 3 =$$
$$= 27 \pmod{41}$$
$$c_3 = \sum_{i+j \equiv 3 \pmod 7} a_i \cdot b_j = a_0 \cdot b_3 + a_1 \cdot b_2 + a_2 \cdot b_1 + a_3 \cdot b_0 + a_4 \cdot b_6 + a_5 \cdot b_5 + a_6 \cdot b_4 =$$
$$= a_0 \cdot b_3 + a_1 \cdot b_2 + a_5 \cdot b_5 + a_6 \cdot b_4 = (-1) \cdot 3 + 1 \cdot (-15) + (-1) \cdot 6 + 1 \cdot (-11) = -35 =$$
$$= 6 \pmod{41}$$
$$c_4 = \sum_{i+j \equiv 4 \pmod 7} a_i \cdot b_j = a_0 \cdot b_4 + a_1 \cdot b_3 + a_2 \cdot b_2 + a_3 \cdot b_1 + a_4 \cdot b_0 + a_5 \cdot b_6 + a_6 \cdot b_5 =$$
$$= a_0 \cdot b_4 + a_1 \cdot b_3 + a_5 \cdot b_6 + a_6 \cdot b_5 = (-1) \cdot (-11) + 1 \cdot 3 + (-1) \cdot 18 + 1 \cdot 6 =$$
$$= 2 \pmod{41}$$
$$c_5 = \sum_{i+j \equiv 5 \pmod 7} a_i \cdot b_j = a_0 \cdot b_5 + a_1 \cdot b_4 + a_2 \cdot b_3 + a_3 \cdot b_2 + a_4 \cdot b_1 + a_5 \cdot b_0 + a_6 \cdot b_6 =$$
$$= a_0 \cdot b_5 + a_1 \cdot b_4 + a_5 \cdot b_0 + a_6 \cdot b_6 = (-1) \cdot 6 + 1 \cdot (-11) + (-1) \cdot (-2) + 1 \cdot 18 =$$
$$= 3 \pmod{41}$$
$$c_6 = \sum_{i+j \equiv 6 \pmod 7} a_i \cdot b_j = a_0 \cdot b_6 + a_1 \cdot b_5 + a_2 \cdot b_4 + a_3 \cdot b_3 + a_4 \cdot b_2 + a_5 \cdot b_1 + a_6 \cdot b_0 =$$
$$= a_0 \cdot b_6 + a_1 \cdot b_5 + a_5 \cdot b_1 + a_6 \cdot b_0 = (-1) \cdot 18 + 1 \cdot 6 + (-1) \cdot (-2) + 1 \cdot (-2) = -12 =$$
$$= 29 \pmod{41}$$

Отже маємо:

$$c(x) = \mathbf{r}(x) \star \mathbf{h}(x) = 29x^6 + 3x^5 + 2x^4 + 6x^3 + 27x^2 + 23x + 33$$

Далі помножимо на p:

$$p \cdot c(x) = 3 \cdot (29x^6 + 3x^5 + 2x^4 + 6x^3 + 27x^2 + 23x + 33) =$$
$$= 5x^6 + 9x^5 + 6x^4 + 18x^3 + 40x^2 + 28x + 17 \pmod{41}$$

Далі додамо $\mathbf{m}(x)$ і отримаємо зашифроване повідомлення:

$$p \cdot c(x) + \mathbf{m}(x) = 5x^6 + 9x^5 + 6x^4 + 18x^3 + 40x^2 + 28x + 17 - x^5 - x^4 - x^2 - x + 1 =$$
$$= 5x^6 + 8x^5 + 5x^4 + 18x^3 + 39x^2 + 27x + 18 \pmod{41}$$

Отриманий криптотекст має вигляд:

$$\mathbf{e}(x) = p \cdot \mathbf{r}(x) \star \mathbf{h}(x) + \mathbf{m}(x) = 5x^6 + 8x^5 + 5x^4 + 18x^3 + 39x^2 + 27x + 18$$

Завдання № 2

Умова:

Еліптична крива E над полем $\mathbb{F}_{631}$ задана рівнянням:

$$y^2 = x^3 + 30x + 34$$

1. Перевірити, що точки $P = (36, 571)$ та $Q = (420, 48)$ належать ЕК;
2. Перевірити, що обидві точки мають порядок 5 і породжують підгрупу точок експоненти 5
3. Обчислити значення спарювання Вейля $w_5(P, Q)$ та перевірити, що отримане значення є коренем 5 степеня з 1.

Розв'язання:

Перевірку, чи точки справді лежать на кривій ми можемо звичайною підстановкою у рівняння ЕК.
Для точки P:

$$\begin{aligned} &P(36, 571) \leftarrow y^2 = x^3 + 30x + 34 \\ &571^2 = 36^3 + 30 \cdot 36 + 34 \pmod{631} \\ &445 = 445 \pmod{631} \end{aligned}$$

та точки Q:

$$\begin{aligned} &Q(420, 48) \leftarrow y^2 = x^3 + 30x + 34 \\ &48^2 = 420^3 + 30 \cdot 420 + 34 \pmod{631} \\ &441 = 441 \pmod{631} \end{aligned}$$

Як бачимо, точки належать еліптичній кривій. Для перевірки порядку 5 цих точок, треба обчислити точки $2P$, $3P$, $4P$, $5P$ та $2Q$, $3Q$, $4Q$, $5Q$ відповідно і переконатися що $5P = 5Q = \mathcal{O}$. Для зручності обчислень покладемо точку на нескінченності рівною $(0, 0)$: $\mathcal{O} = (0, 0)$. Це нам ніщо не забороняє зробити, оскільки $(0, 0)$ не належить заданій ЕК.