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

26 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:

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

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

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.