

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ  
Федеральное государственное автономное  
образовательное учреждение высшего образования  
«Национальный исследовательский университет ИТМО»

**Факультет программной инженерии и компьютерной техники**

## **ЛАБОРАТОРНАЯ РАБОТА №4**

### **“Основы шифрования данных”**

по дисциплине

### **“Информационная безопасность”**

Вариант №16

**Студент:**

Миху Вадим Дмитриевич

Группа Р34301

**Преподаватель:**

Рыбаков Степан Дмитриевич

г. Санкт-Петербург

2024

## Цель работы:

Дан шифротекст, используя алфавит, приведенный в, в подразделе «Задачи к лабораторным работам по криптографии на эллиптических кривых (используется кривая  $E_{751}(-1,1)$  – и генерирующая точка  $G = (0,1)$ )» и зная секретный ключ  $n_b$ , найти открытый текст.

## Вариант 5:

| № Варианта | Секретный ключ $n_b$ | Шифртекст   |
|------------|----------------------|---|
| 16         | 48                   | $\{(16, 416), (724, 522)\}; \{(489, 468), (719, 538)\}; \{(56, 419), (205, 372)\}; \{(72, 254), (628, 293)\}; \{(188, 93), (594, 337)\}; \{(440, 539), (588, 707)\}; \{(568, 355), (707, 556)\}; \{(489, 468), (719, 538)\}; \{(16, 416), (590, 376)\}; \{(56, 419), (612, 329)\}; \{(188, 93), (594, 337)\}$ |

## Выполнение:

Пользователь для расшифровки сообщения должен провести следующие вычисления

$$P_m + kP_b - n_b(kG) - n_b(kG)$$

| Исходные точки           | Вычисленная точка | Символ |
|--------------------------|-------------------|--------|
| $(16, 416), (724, 522)$  | $(243, 87)$       | р      |
| $(489, 468), (719, 538)$ | $(228, 271)$      | а      |
| $(56, 419), (205, 372)$  | $(229, 151)$      | в      |
| $(72, 254), (628, 293)$  | $(238, 576)$      | н      |
| $(188, 93), (594, 337)$  | $(240, 309)$      | о      |
| $(440, 539), (588, 707)$ | $(235, 732)$      | з      |
| $(568, 355), (707, 556)$ | $(238, 576)$      | н      |
| $(489, 468), (719, 538)$ | $(228, 271)$      | а      |
| $(16, 416), (590, 376)$  | $(250, 737)$      | ч      |
| $(56, 419), (612, 329)$  | $(238, 576)$      | н      |
| $(188, 93), (594, 337)$  | $(240, 309)$      | о      |

## Листинг разработанной программы:

```
@main
def main(): Unit = {
    val a = -1
    val p = 751
    val nb = 48

    var message = ""
    for (point <- points) {
        var nb_kG = point._1
        for (_ <- 1 until nb) {
            nb_kG = addPoints(nb_kG, point._1, a, p)
        }
        val result = subPoints(point._2, nb_kG, a, p)
        message = message + alphabet(result)
    }
}
```

```
}  
  
println("Decrypted message: " + message)  
}
```

```
def addPoints(P: Point, Q: Point, a: Int, p: Int): Point = {  
    val (x1, y1) = (P.x, P.y)  
    val (x2, y2) = (Q.x, Q.y)  
  
    if (P == Point(0, 0)) return Q  
    if (Q == Point(0, 0)) return P  
  
    val lambda = if (P != Q) {  
        (y2 - y1) * modInverse(x2 - x1, p) % p  
    } else {  
        (3 * x1 * x1 + a) * modInverse(2 * y1, p) % p  
    }  
  
    val x3 = (lambda * lambda - x1 - x2) % p  
    val y3 = (lambda * (x1 - x3) - y1) % p  
    Point((x3 + p) % p, (y3 + p) % p)  
}  
  
def subPoints(P: Point, Q: Point, a: Int, p: Int): Point = {  
    addPoints(P, negatePoint(Q, p), a, p)  
}  
  
def negatePoint(P: Point, p: Int): Point = {  
    Point(P.x, (-P.y + p) % p)  
}  
  
def modInverse(value: Int, mod: Int): Int = {  
    BigInt(value).modInverse(mod).toInt  
}
```

## Результат работы программы:

```
Decrypted message: равнозначно
```

## Вывод:

В результате выполнения данной лабораторной работы я ознакомилась с тем, как, зная секретный ключ получателя сообщения, расшифровать криптограмму на основе эллиптических кривых. Кроме того, разработала скрипт для нахождения открытого текста посредством сложения, вычитания и умножения точек на эллиптических кривых.