Университет ИТМО
Факультет ПИиКТ
Информационная безопасность

Лабораторная работа №5
«Шифрование открытого текста на основе эллиптических кривых»

Вербовой Александр
Группа P3400
Вариант 4

Санкт-Петербург
2021

Цель работы

зашифровать открытый текст, используя алфавит, приведенный в [4], в подразделе «Задачи к лабораторным работам по криптографии на эллиптических кривых (используется кривая $E_{751}(-1,1)$ – и генерирующая точка $G = (0, 1)$)».

Задание (вариант 4)

№ Варианта	Открытый текст	Открытый ключ B	Значение случайных чисел K для букв открытого текста
4	симметрия	(179,275)	11,17,18,19,16,6,12,8,2

Описание:

```
class Point:
    def __init__(self, x, y):
        self.x = x
        self.y = y
    def __eq__(self, other):
        if isinstance(other, Point):
            return self.x == other.x and self.y == other.y
        return False

a = 0
b = -1
c = 1
modp = 751
```

Правило сложение точек элептической кривой

$$x_3 = \lambda^2 - x_1 - x_2 (modp)$$

$$y_3 = \lambda(x_1 - x_3) - y_1 (modp)$$

```
def summ(p1: Point, p2: Point):
    lambd = lam(p1, p2)
    x = int((lambd * lambd - a - p1.x - p2.x) % modp)
    y = int((lambd * (p1.x - x) - p1.y) % modp)
    return Point(x, y)
```

Нахождение λ для сложения точек элептической кривой

$$\lambda = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1}, \text{если} P \neq Q \\ \frac{3x_1^2 + a}{2y_1}, \text{если} P = Q \end{cases}$$

```python
def lam(p1: Point, p2: Point):
    if(p1 == p2):
        nom = 3 * p1.x * p1.x + 2 * a * p1.x + b
        denom = 2 * p1.y
    else:
        nom = p2.y - p1.y
        denom = p2.x - p1.x

    # Нахождение модульноего обратного числа
    #
    # Модульные обратные числа A (mod C) это A^-1 такое что
    # (A * A^-1) ≡ 1 (mod C) или эквивалентное (A * A^-1) mod C = 1
    for i in range(modp):
        if ((denom * i) % modp == 1):
            denom = i
            break
    return (nom * denom) % modp
```

```python
pointB = Point(179,275)
k = [11,17,18,19,16,6,12,8,2]
g = Point(0,1)
text_points = [
    Point(243, 664), # С
    Point(236, 39),  # И
    Point(238, 175), # М
    Point(238, 175), # М
    Point(234, 587), # Е
    Point(247, 266), # Т
    Point(243, 87),  # Р
    Point(236, 39),  # И
    Point(257, 458)  # Я
]
```

```
i = 0
for point in text_points:
    prev_B = pointB
    prev_G = g
    for _ in range(k[i]-1):
        prev_B = summ(pointB, prev_B)
        prev_G = summ(g, prev_G)
    result = summ(point, prev_B)
    i+=1

    print("Cm = ({x1}, {y1}), ({x2}, {y2}) ".format(x1 = prev_G.x, y1 =
```

```
Cm = (179, 275), (383, 411)
Cm = (440, 539), (229, 151)
Cm = (618, 206), (466, 214)
Cm = (568, 355), (156, 704)
Cm = (72, 254), (564, 38)
Cm = (725, 195), (145, 143)
Cm = (286, 136), (176, 413)
Cm = (346, 242), (12, 314)
Cm = (188, 93), (275, 456)
```

Вывод

В ходе лабораторной работы был зашифрован открытый текст с помощью метода шифрования на основе эллиптических кривых