Университет ИТМО
Факультет ПИиКТ
Информационная безопасность

Лабораторная работа №9
«Получение ЭЦП на основе эллиптических кривых»

Вербовой Александр
Группа P3400
Вариант 4

Санкт-Петербург
2021

Цель работы

сгенерировать ЭЦП для сообщения с известным значением хэш-свертки e, зная секретный ключ подписи d при данном значении выбираемого случайным образом числа k. Используется эллиптическая кривая $E_{751}(-1,1)$ и генерирующая точка G = (416, 55) порядка n =13.

Задание (вариант 4)

№ варианта	e	d	k
4	3	4	7

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

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

```
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
```

```
g = Point(416, 55)
n = 13 # порядок точки
e = 3 # хэш свертка
d = 4 # секретный ключ подписи
k = 7 # случайное число

# Считает kG
prev_G = g
for _ in range(k):
    prev_G = summ(g, prev_G)
kG = prev_G

r = kG.x % n

# Нахождение модульноего обратного числа k^-1
z = k
for i in range(n):
    if ((z)% n == 1):
        z = i
        break

s = z*(e + d*r) % n
r, s
```

```
(3, 1)
```

Вывод

В ходе лабораторной работы был сгенерирована ЭЦП для сообщения с известным значением хэш-свертки e, зная секретный ключ подписи d при данном значении выбираемого случайным образом числа k.