

**Лабораторные работы по разделу
«Криптографические системы с открытым ключом»**

Лабораторная работа № 10

Проверка ЭЦП на основе эллиптических кривых

Цель работы: проверить подлинность ЭЦП (r,s) для сообщения с известным значением хэш-свертки e , зная открытый ключ проверки подписи Q . Используется эллиптическая кривая $E_{751}(-1,1)$ и генерирующая точка $G = (562, 89)$ порядка $n = 13$.

Ход работы:

– ознакомиться с теорией в учебном пособии «Криптография», а также в учебно-методическом пособии к выполнению лабораторного практикума по дисциплине «Криптография»;

- получить вариант задания у преподавателя;
- проверить подлинность ЭЦП для сообщения;
- результаты и промежуточные вычисления оформить в виде отчета.

Пример генерации и проверки подписи

Пусть используется эллиптическая кривая $E_{751}(-1,1)$ – и генерирующая точка $G = (384, 475)$ порядка $n = 13$ (13 – наибольший из делителей порядка кривой $N = 728$). Предположим, абонент подписывает личным секретным ключом $d = 12$ сообщение, хэш-свертка которого равна $e = 12$.

Пусть абонент, подписывающий сообщение, выбрал случайное $k = 3$. Тогда он вычисляет $kG = (x,y) = 3 \cdot (384, 475) = (596, 318)$ и затем $r = x \bmod n = 596 \bmod 13 = 11$. Используя расширенный алгоритм Евклида, определяем $z = k^{-1} \bmod n = 3^{-1} \bmod 13 = 9$ (так как $3 \cdot 9 = 27 \equiv 1 \pmod{13}$). Наконец, $s = z(e + dr) \bmod n = 9 \cdot (12 + 12 \cdot 11) \bmod 13 = 9$. Таким образом, $(r, s) = (11, 9)$ – цифровая подпись данного абонента для сообщения.

Пусть теперь необходимо проверить подлинность данной подписи. Открытый ключ абонента, подписавшего сообщение, равен $Q = dG = 12 \cdot (384, 475) = (384, 276)$. Проверка подписи начинается с проверки условий $1 \leq r \leq n-1$, $1 \leq s \leq n-1$ – в данном случае они соблюдаются. Затем последовательно вычисляем $v = s^{-1} \bmod n = 9^{-1} \bmod 13 = 3$, $u_1 = ev \bmod n = 12 \cdot 3 \bmod 13 = 10$ и $u_2 = 11 \cdot 3 \bmod 13 = 7$. Находим точку $X = u_1 \cdot G + u_2 \cdot Q = 10 \cdot (384, 475) + 7 \cdot (384, 276) = (596, 318)$. Наконец, сравниваем значения $r = 11$ и $x \bmod n = 596 \bmod 13 = 11$ – они совпадают, следовательно, подпись действительная.

Варианты заданий

№ варианта	e	Q	(r, s)
1	4	(596, 318)	(11, 4)
2	5	(455, 368)	(3, 7)
3	6	(135, 669)	(5, 7)
4	6	(562, 662)	(5, 7)
5	2	(135, 669)	(7, 6)
6	8	(135, 82)	(11, 10)
7	4	(384, 475)	(11, 9)
8	7	(596, 433)	(11, 1)
9	7	(455, 368)	(11, 11)
10	7	(384, 475)	(5, 5)