Университет ИТМО

Факультет ПИиКТ

Информационная безопасность

Лабораторная работа №9

«Получение ЭЦП на основе эллиптических кривых»

Вербовой Александр

Группа P3400

Вариант 4

**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 E751(−1,1) и генерирующая точка *G* = (416, 55) порядка *n* =13.

**Задание (вариант 4)**

|  |  |  |  |
| --- | --- | --- | --- |
| № варианта | **e** | **d** | **k** |
| 4 | 3 | 4 | 7 |

**Описание:**

Изображение выглядит как текст

Автоматически созданное описание

**Изображение выглядит как текст

Автоматически созданное описание**

**Изображение выглядит как текст

Автоматически созданное описание**

**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.