Университет ИТМО

Факультет ПИиКТ

Информационная безопасность

Лабораторная работа №5

«Шифрование открытого текста на основе эллиптических кривых»

Вербовой Александр

Группа P3400

Вариант 4

**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:**

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 зашифрован открытый текст с помощью метода шифрования на основе эллиптических кривых