

Министерство образования и науки Российской Федерации

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
«САРАТОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИМЕНИ Н.Г. ЧЕРНЫШЕВСКОГО»

Кафедра компьютерной алгебры и
теории чисел

ЭЛЛИПТИЧЕСКИЕ КРИПТОСИСТЕМЫ

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА БАКАЛАВРА

Студента 4 курса 421 группы
направления 010200 — Математика и компьютерные науки
Механико-математического факультета
Каймашникова Всеволода Александровича

Научный руководитель
доцент, к. ф.-м. н.

В. В. Кривобок

Заведующий кафедрой
Профессор, доктор

В. Н. Кузнецов

Саратов 2015

Содержание

ВВЕДЕНИЕ	3
1 Секция 1	4
2 Секция 2	4
3 Секция 3	4
3.1 Подсекция 1	4
3.2 Подсекция 3	4
4 Заключение	4
СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ.....	4

ВВЕДЕНИЕ

Введение

1 Секция 1

2 Секция 2

3 Секция 3

3.1 Подсекция 1

3.2 Подсекция 3

4 Заключение

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

- 1 Кокс Д., Литтл Дж., О’Ши Д. «Идеалы, многообразия и алгоритмы. Введение в вычислительные аспекты алгебраической геометрии и коммутативной алгебры»: Пер. с англ. – М.: Мир, 2000. – 687 с., ил.
- 2 Курош А. Г. «Курс высшей алгебры» – М.: Наука, 1965. – 431 с.
- 3 Ван дер Варден Б. Л. «Алгебра» – М.: Мир, 1975 – 649 с.
- 4 Кострикин А. И. «Введение в алгебру. Часть 1» – ФИЗМАЛИТ, 2004 – 272 с
- 5 Михаев А.В., Панкратьев Е.В. «Компьютерная алгебра. Вычисления в дифференциальной и разностной алгебре: Учебное пособие» – М.: Изд-во МГУ, 1989 – 97 с.
- 6 Дэвенпорт Дж., Сирэ И., Турнье Э. «Компьютерная алгебра»: Пер. с франц. – М.: Мир, 1991 – 352 с., ил.
- 7 Аржанцев И. В., «Базисы Грёбнера и системы алгебраических уравнений» — М.: МЦНМО, 2003 – 68 с.