Белорусский государственный университет
Механико-математический факультет
Кафедра дифференциальных уравнений и системного анализа

Аннотация к дипломной работе «Обобщение криптосистемы Эль-Гамаля»

Пацанюк Андрей Вячеславович,

руководитель Липницкий Валерий Антонович

2014

Дипломная работа содержит:

- 28 страницы.
- 2 иллюстрации(рисунка)
- 1 приложение
- 6 использованных источника

Ключевые слова: КОНЕЧНОЕ ПОЛЕ Z/PZ, ЦИКЛИЧЕСКАЯ ГРУППА, КРИПТОСТОЙКОСТЬ, ПРОБЛЕМА ДИСКРЕТНОГО ЛОГАРИФМА, ЭЛЛИПТИЧЕСКАЯ КРИВАЯ

В дипломной работе рассматривается криптосистема Эль-Гамаля, алгоритмы шифрования/расшифрование, криптостойкость криптосистемы.

Цель дипломной работы рассмотреть обобщения схемы Эль-Гамаля, повышающие ее криптостойкость, построить схемы полученных обобщений.

В дипломной работе получены следующие результаты:

1. Схема Эль-Гамаля в квадратичном расширении конечного поля Z/pZ
2. Схема Эль-Гамаля, построенная на эллиптической кривой.
3. Анализ полученных результатов на трудоемкость реализации и сложность взлома.
4. Рассмотрены несколько примеров работы, полученных обобщений.

Новизна результатов состоит в переносе схемы на другие циклические группы.

Дипломная работа носит теоретический и практический характер. Все результаты дипломной работы строго доказаны в соответствии с принятыми в математике правилами. Обоснованность и достоверность полученных результатов обусловлена согласованностью с результатами, известными ранее для конкретных частных случаев.

Дипломная работа выполнена автором самостоятельно.

Thesis project includes::

- 28 pages
- 2 picture
- 1 application
- 6 used source

Keywords: FINITE FIELD Z / PZ, CYCLIC GROUPS, CRYPTOGRAPHICALLY STRONG, DISCRETE LOGARITHM PROBLEM, ELLIPTIC CURVES

In the thesis project is considered ElGamal cryptosystem, encryption / decryption, cryptographic cryptosystem.

Purpose of the thesis consider generalizations ElGamal scheme, increasing its cryptographically strong, construct scheme obtained generalizations. The main results of the thesis projects are as follows:

ElGamal scheme in a quadratic extension of a finite field Z / pZ

1. Scheme ElGamal, built on an elliptic curve.
2. Analysis of the results on the complexity of the implementation and complexity of hacking.
3. Consider a few examples of the work produced generalizations.

The novelty of the results is to transfer the scheme to other cyclic groups.

Thesis project is theoretical and practical. All results of the thesis project rigorously proved in accordance with the rules of mathematics. Validity and reliability of the results obtained due to consistency with the results previously known for certain special cases.

The thesis project was done solely by the author.