БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

МЕХАНИКО-МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ

Кафедра дифференциальных уравнений и системного анализа

Аннотация к дипломной работе

«Криптосистема NTRU»

Шубенок Виктория Дмитриевна

Научный руководитель:
кандидат физ.-мат. наук,
доцент Д. Н. Чергинец

2014

В дипломной работе 33 страниц, 2 иллюстрации, 16 источников, 10 приложений.

КРИПТОСИСТЕМА, NTRU, РЕШЕТКИ, ИНФОРМАЦИОННЫЕ СИСТЕМЫ, ОБРАТНЫЙ ПОЛИНОМ, КОЛЬЦО УСЕЧЕННЫХ МНОГОЧЛЕНОВ.

В разделе 1.1 описываются кольца многочленов $Z[x]/\,(x^{\,N}-1)$ и $Z_p[x]/\,(x^{\,N}-1)$. Составляется вероятностный критерий обратимости. Описываются алгоритмы поиска обратного элемента в кольцах $Z[x]/\,(x^{\,N}-1)$ и $Z_p[x]/\,(x^{\,N}-1)$.

В разделе 1.2 изучаются алгоритмы криптосистемы NTRU, выполняется их реализация, описывается алгоритм выбора правильных параметров для заданного уровня безопасности зашифрованного сообщения.

В разделе 1.3 выполняется криптоанализ шифра. Происходит поиск уязвимостей криптосистемы и взлом шифрованного сообщения.

В разделе 1.4 происходит реализация атаки на основе решеток, которая заключается в построении решетки и поиске кратчайших векторов в ней.

Новизна результатов состоит в реализации алгоритмов поиска обратного элемента, криптосистемы NTRU и атак на нее в mathematica.

Дипломная работа носит практический характер. Ее результаты могут быть использованы в дальнейших исследованиях данной криптосистемы.

Все результаты дипломной работы строго доказаны в соответствии с принятыми в математике правилами. Обоснованность и достоверность полученных результатов обусловлена строгими математическими доказательствами сформулированных в работе лемм и теорем и согласованностью с результатами, известными ранее для конкретных частных случаев.

Дипломная работа выполнена автором совместно с руководителем.

There are 33 pages, 2 illustrations, 16 sources, 10 applications in the thesis work.

CRYPTOSYSTEM, NTRU, LATTICE, INFORMATION SYSTEMS, REVERSE POLYNOMIAL, RING TRUNCATED POLYNOMIALS.

Section 1.1 describes the polynomial rings $Z[x]/\,(x^{\,N}-1)$ and $Z_p[x]/\,(x^{\,N}-1)$. Composed probabilistic criterion of reversibility. Presents the algorithms search inverse element in the ring $Z[x]/\,(x^{\,N}-1)$ and $Z_p[x]/\,(x^{\,N}-1)$.

In Section 1.2 we study algorithms cryptosystem NTRU, performed their implementation, describe an algorithm for selecting the correct parameters for a given level of security encrypted message.

In Section 1.3 is performed cipher cryptanalysis. There is a search cryptosystem vulnerabilities and hacking encrypted message in this section.

In Section 1.4, we implement an attack based on lattices which consists in constructing a lattice, and finding the shortest vectors in it.

The novelty of the results is to implement an inverse element of search algorithms, NTRU cryptosystem and attacks her in mathematica.

Diploma work is practical. Its results can be used in further studies of this cryptosystem.

All results of the thesis rigorously proved in accordance with the rules of mathematics. Validity and reliability of the results is due to the strict mathematical proofs formulated in the lemmas and theorems and consistency with the results previously known for certain special cases.

Diploma work performed by the author together with the supervisor.