**МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ**

**УО «БЕЛОРУСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»**

**МЕХАНИКО – МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ**

**Кафедра математической кибернетики**

ДУБРОВСКИЙ

Даниил Васильевич

**Аппаратная реализация алгоритма шифрования RSA**

Дипломная работа

 Научный руководитель:

 кандидат техн. наук,

 доцент А. А. Дерюшев

Допущен к защите

«\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_ 2022 г.

Зав. кафедрой математической кибернетики

доктор физико-математических наук А.Л. Гладков

МИНСК 2022

**ОГЛАВЛЕНИЕ**

**РЕФЕРАТ ДИПЛОМНОЙ РАБОТЫ** 3

**ВВЕДЕНИЕ** 6

**Глава 1. Шифрование информации** 7

**1.1 Понятие шифрования и его типы** 7

**1.2 Пример математических алгоритмов** 7

**1.2.1 Система остаточных классов** 8

**1.3 Симметричное шифрование** 10

**1.4 Алгоритмы симметричного типа шифрования** 11

**1.4.1 DES-алгоритм симметричного шифрования** 12

**1.4.2 Алгоритм симметричного шифрования 3DES** 12

**1.4.3 Алгоритм симметричного шифрования AES** 13

**1.5 Асимметричное шифрование** 13

**1.6 Основные типы алгоритмов асимметричного шифрования** 14

**1.6.1 Алгоритм асимметричного шифрования RSA** 15

**1.6.2 Алгоритм асимметричного шифрования ECC** 15

**1.7 Гибридное шифрование** 18

**Глава 2. Практическая часть** 21

**2.1** **Описание практической части** 21

**2.2** **Подготовка ключей** 21

**2.3** **Шифрование** 22

**2.4** **Расшифровка** 23

**2.5** **Оценка быстродействия** 23

**2.6 Преобразование в синтезируемые языки** 26

**2.7 Сравнение двух реализаций синтезируемых кодов** 27

**ЗАКЛЮЧЕНИЕ** 29

**СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ** 30

**ПРИЛОЖЕНИЯ** 31

**РЕФЕРАТ**

Дипломная работа по теме «Аппаратная реализация алгоритма шифрования RSA» содержит:

* 31 страница,
* 18 иллюстраций (рисунков),
* 1 таблицу,
* 3 приложения,
* 6 использованных источников.

Используются следующие ключевые слова: криптография с открытым ключом, RSA алгоритм, шифрование.

Целью дипломной работы является разработка синтезируемой программы RSA алгоритма, для реализации и анализа ассиметричного метода шифрования.

В дипломной работе получены следующие результаты:

1) Определены типы шифрования, их положительные и негативные стороны.

2) Рассмотрены алгоритмы, используемые в актуальном шифровании, а также устаревшие алгоритмы.

3) Проведён краткий анализ устаревания алгоритмов.

4) Получены программная реализация алгоритма на языке программирования С#, C++, SystemVerilog.

5) Проведено сравнение эффективности разработанных алгоритмов.

Дипломная работа выполнена автором самостоятельно.

\_\_\_\_\_\_\_\_\_\_\_\_\_

(Подпись студента)

 **РЭФЕРАТ**

Дыпломная работа па тэме "Апаратная рэалізацыя алгарытму шыфравання RSA" змяшчае:

• 31 старонка,

• 18 ілюстрацый (малюнкаў),

• 1 табліцу,

• 3 прыкладанні,

• 6 выкарыстаных крыніц.

Выкарыстоўваюцца наступныя ключавыя словы: крыптаграфія з адкрытым ключом, RSA алгарытм, шыфраванне.

Мэтай дыпломнай працы з'яўляецца распрацоўка сінтэзаванай праграмы RSA алгарытму, для рэалізацыі і аналізу асіметрычнага метаду шыфравання.

У дыпломнай рабоце атрыманы наступныя вынікі:

1) Вызначаны тыпы шыфравання, іх станоўчыя і негатыўныя бакі.

2) Разгледжаны алгарытмы, якія выкарыстоўваюцца ў актуальным шыфраванні, а таксама састарэлыя алгарытмы.

3) Праведзены кароткі аналіз састарэння алгарытмаў.

4) Атрыманы праграмная рэалізацыя алгарытму на мове праграмавання З#, C++, SystemVerilog.

5) Праведзена параўнанне эфектыўнасці распрацаваных алгарытмаў.

Дыпломная работа выканана аўтарам самастойна.

\_\_\_\_\_\_\_\_\_\_\_\_\_

(Подпіс студэнта)

**ANNOTATION**

The thesis on the topic "Hardware implementation of the RSA encryption algorithm" contains:

• 31 pages,

• 18 illustrations (drawings),

• 1 table,

• 3 applications,

• 6 sources used.

The following keywords are used: public key cryptography, RSA algorithm, encryption.

The purpose of the thesis is to develop a synthesized RSA algorithm program for the implementation and analysis of an asymmetric encryption method.

The following results were obtained in the thesis work:

1) The types of encryption, their positive and negative aspects are determined.

2) The algorithms used in the current encryption, as well as outdated algorithms, are considered.

3) A brief analysis of the obsolescence of algorithms was carried out.

4) A software implementation of the algorithm in the C#, C++, SystemVerilog programming languages ​​has been obtained.

5) The efficiency of the developed algorithms was compared.

The thesis work was done by the author independently.

\_\_\_\_\_\_\_\_\_\_\_\_\_

(Student's signature)