**ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ**

**«ВЫСШАЯ ШКОЛА ЭКОНОМИКИ»**

Факультет компьютерных наук  
Департамент программной инженерии

СОГЛАСОВАНО

Профессор департамента

программной инженерии факультета компьютерных наук, к.т.н.

\_\_\_\_\_\_\_\_\_\_\_\_ С.М. Авдошин

«\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_ 2017 г.

УТВЕРЖДАЮ

|  |
| --- |
| Академический руководитель образовательной программы «Программная инженерия», к.т.н. |

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ В.В. Шилов

«\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_ 2017 г.

Подп. и дата

**КРИПТОСИСТЕМА РАБИНА  
(RABIN CRYPTOSYSTEM)**

**Текст программы**

Инв. № дубл.

**ЛИСТ УТВЕРЖДЕНИЯ**

**RU.17701729. 501430-01 12 01-1**

Взам. инв. №

Исполнитель:

студент группы БПИ 165

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ И. С. Чуев

«\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 2017 г.

Подп. и дата

Инв. № подл

RU.17701729.

501430-01

12 01-1

**2017**

УТВЕРЖДЕН  
RU.17701729. 501430-01 12 01-1-ЛУ

**КРИПТОСИСТЕМА РАБИНА  
(RABIN CRYPTOSYSTEM)**

**Текст программы**

**RU.17701729. 501430-01 12 01-1**

Подп. и дата

Инв. № дубл.

Взам. инв. №

**Листов 51**

Подп. и дата

Инв. № подл

RU.17701729.

501430-01

12 01-1

**2017**

**АННОТАЦИЯ**

В данном программном документе приведет текст «Криптосистема Рабина (Rabin Cryptosystem)». Текст программы реализован в виде символической записи на исходном языке. Исходным языком данной разработки является C# 5.0. Среда разработки - Microsoft Visual Studio 2015 Enterprise (локализованная русская версия).

Данное программное обеспечение предназначено для защищенной передачи важных файлов. Программа, реализуя алгоритм криптосистемы Рабина, способна кодировать и декодировать информацию, представленную в бинарном виде с использованием открытого и закрытого ключа.

Программа состоит из 10 классов.

В связи с большим количеством строк кода, текст программы на исходном языке находится на сдаваемом CD-диске в директории «Coursework 1 course\Documentation» название файла «Текст программы».

СОДЕРЖАНИЕ

[1. БИБЛИОТЕКА RABIN.LIB 4](#_Toc482814287)

[1.1. Rabin.cs 4](#_Toc482814288)

[1.2. RabinEncoding.cs 15](#_Toc482814289)

[1.3. ProgressInfo.cs 20](#_Toc482814290)

[2. ТЕКСТ ПРОГРАММЫ RABIN CRYPTOSYSTEM 20](#_Toc482814291)

[2.1. Rabin\_Cryptosystem.cs 20](#_Toc482814292)

[2.2. Rabin\_Cryptosystem.Designer.cs 33](#_Toc482814293)

[2.3. GenKey.cs 43](#_Toc482814294)

[2.4. GenKey.Designer.cs 45](#_Toc482814295)

[2.5. Program.cs 48](#_Toc482814296)

[2.6. ReachProgressBar.cs 48](#_Toc482814297)

[2.7. ProgressBarForManyProcesses.cs 49](#_Toc482814298)

**ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Лист регистрации изменений | | | | | | | | | |
| Номера листов (страниц) | | | | | Всего листов (страниц в докум.) | № документа | Входящий № сопроводительного докум. и дата | Подп. | Дата |
| Изм. | Измененных | Замененных | Новых | Аннулированх |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |