**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)**

**Руководство оператора**

Инв. № дубл.

**ЛИСТ УТВЕРЖДЕНИЯ**

**RU.17701729. 501430-01 34 01-1**

Взам. инв. №

Исполнитель:

студент группы БПИ 165

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

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

Подп. и дата

Инв. № подл

RU.17701729.

501430-01

34 01-1

**2017**

УТВЕРЖДЕН  
RU.17701729. 501430-01 34 01-1-ЛУ

**КРИПТОСИСТЕМА РАБИНА  
(RABIN CRYPTOSYSTEM)**

**Руководство оператора**

**RU.17701729. 501430-01 34 01-1**

Подп. и дата

Инв. № дубл.

Взам. инв. №

**Листов 37**

Подп. и дата

Инв. № подл

RU.17701729.

501430-01

34 01-1

**2017**

**АННОТАЦИЯ**

Руководство оператора – это документ, назначение которого — предоставить людям помощь в использовании некоторого программного продукта.

Настоящее Руководство оператора предназначено для правильной организации работы с программой «Криптосистема Рабина (Rabin Cryptosystem)». Руководство оператора для «Криптосистема Рабина (Rabin Cryptosystem)» содержит следующие разделы: «Назначение программы», «Условия выполнения программы», «Выполнение программы», «Сообщения оператору» и приложения [7].

В разделе «Назначение программы» указаны сведения о назначении программы и информация о функциях и принципе эксплуатации программы.

Раздел «Условия выполнения программы» содержит информацию об условиях, необходимых для выполнения данной программы (минимальный состав аппаратурных и программных средств).

Раздел «Выполнение программы» содержит последовательность действий оператора, обеспечивающих загрузку, запуск, выполнение и завершение программы, описание функций, формата и возможных вариантов команд, с помощью которых оператор осуществляет загрузку и управляет выполнением программы, а также ответы программы на эти команды.

В разделе «Сообщения оператору» указаны тексты сообщений, выдаваемые в ходе выполнения программы, описание их содержания и соответствующие действия оператора.

Настоящий документ разработан в соответствии с требованиями:

1) ГОСТ 19.101-77 Виды программ и программных документов [1];

2) ГОСТ 19.102-77 Стадии разработки [2];

3) ГОСТ 19.103-77 Обозначения программ и программных документов [3];

4) ГОСТ 19.104-78 Основные надписи [4];

5) ГОСТ 19.105-78 Общие требования к программным документам [5];

6) ГОСТ 19.106-78 Требования к программным документам, выполненным печатным способом [6];

7) ГОСТ 19.505-79 Руководство оператора. Требования к содержанию и оформлению [7].

Изменения к данному Руководству оператора оформляются согласно ГОСТ 19.603-78 [8], ГОСТ 19.604-78 [9].

СОДЕРЖАНИЕ

[1. НАЗНАЧЕНИЕ ПРОГРАММЫ 4](#_Toc482811459)

[1.1. Функциональное назначение 4](#_Toc482811460)

[1.2. Эксплуатационное назначение 4](#_Toc482811461)

[1.3. Состав функций 4](#_Toc482811462)

[2. УСЛОВИЯ ВЫПОЛНЕНИЯ ПРОГРАММЫ 6](#_Toc482811463)

[2.1. Минимальный состав аппаратурных средств 6](#_Toc482811464)

[2.2. Минимальный состав программных средств 6](#_Toc482811465)

[2.3. Требования к персоналу (пользователю) 6](#_Toc482811466)

[3. ВЫПОЛНЕНИЕ ПРОГРАММЫ 7](#_Toc482811467)

[3.1. Инсталяция и запуск программы 7](#_Toc482811468)

[3.2. Выполнение программы 10](#_Toc482811469)

[3.2.1. Получение ключей 11](#_Toc482811470)

[3.2.1.1. Генерация ключей 11](#_Toc482811471)

[3.2.1.2 Добавление в программу ключей 14](#_Toc482811472)

[3.2.1.3. Выбор ключа для шифрования или дешифрования 16](#_Toc482811473)

[3.2.2. Работа с файлом 18](#_Toc482811474)

[3.2.2.1. Добавление файла в программу 18](#_Toc482811475)

[3.2.2.2. Открытие файла из самой программы 20](#_Toc482811476)

[3.2.2.3. Перемещение и удаление файла 20](#_Toc482811477)

[3.2.3. Шифрование файла 22](#_Toc482811478)

[3.2.4. Дешифрование файла 25](#_Toc482811479)

[3.3. Завершение работы с программой 27](#_Toc482811480)

[4. СООБЩЕНИЕ ОПЕРАТОРУ 28](#_Toc482811481)

[ПРИЛОЖЕНИЕ 1 34](#_Toc482811482)

[ЛИТЕРАТУРА 34](#_Toc482811483)

[ПРИЛОЖЕНИЕ 2 35](#_Toc482811484)

[СОКРАЩЕНИЯ И ОБОЗНАЧЕНИЯ 35](#_Toc482811485)

[ПРИЛОЖЕНИЕ 3 36](#_Toc482811486)

[ОПИСАНИЕ ФОРМАТА .publicKey 36](#_Toc482811487)

[ОПИСАНИЕ ФОРМАТА .privateKey 36](#_Toc482811488)

[ОПИСАНИЕ ФОРМАТА .encrypted 36](#_Toc482811489)

# **1. НАЗНАЧЕНИЕ ПРОГРАММЫ**

## **1.1. Функциональное назначение**

Данная программа предназначена для шифровки и дешифровки любых файлов, представленных в цифровом виде, реализуя алгоритм криптосистемы Рабина.  
 Программа генерирует ключи для шифрования/дешифрования и сохраняет их в указанный пользователем файл. Используя ключи шифрует/дешифрует указанный файл и сохраняет результат в указанное пользователем место.

## **1.2. Эксплуатационное назначение**

Скрытая передача важной информации является востребованной задачей на сегодняшний момент. Программное обеспечение «Криптосистема Рабина (Rabin Cryptosystem)» может быть использована для передачи и получения секретной информации в следующих сферах деятельности:

* В банковской сфере
* На закрытых предприятиях
* На военных действиях
* Любым человеком, заботящимся о безопасности своих личных данных

## **1.3. Состав функций**

Программа обеспечивает возможность выполнения перечисленных функций:

* Получение ключа
* Генерация закрытого ключа [Приложение 2] по указанной пользователем бинарной длине (пара простых чисел [11], дающих остаток 3 по модулю 4);
* Вычисление открытого ключа [Приложение 2] (произведение двух простых чисел [11], дающих остаток 3 по модулю 4);
* Запись открытого ключа в файл с расширением .publicKey [Приложение 3] и закрытого ключа в файл с расширением .privateKey [Приложение 3] на жесткий диск компьютера;
* Добавление в программу ключей, по указанному пользователем пути;
* Удаление ключа из списка ключей в программе.
* Кодирование файла
* Выбор открытого ключа для шифрования;
* Кодирование [10] файла с использованием открытого ключа;
* Кодирование группы файла с использованием открытого ключа;
* Запись закодированного файла с расширением .encrypted [Приложение 3] на жесткий диск компьютера.
* Декодирование файла
* Выбор закрытого ключа для дешифрования;
* Используя закрытый ключ, декодирование [10] зашифрованного файла с расширением .encrypted [Приложение 3];
* Используя закрытый ключ, декодирование группы зашифрованных файлов с расширением .encrypted [Приложение 3];
* Запись раскодированного файла на жесткий диск компьютера.
* Работа с файлом
* Добавление файла в программу, по указанному пользователем пути;
* Открытие файла по умолчанию из самой программы;
* Удаление файла из списка файлов в программе.

**2. УСЛОВИЯ ВЫПОЛНЕНИЯ ПРОГРАММЫ**

## **2.1. Минимальный состав аппаратурных средств**

Для надёжной и бесперебойной работы программы требуется следующий состав аппаратурных средств:

* 32-разрядный (x86) или 64-разрядный (x64) процессор с тактовой частотой 1 ГГц [Приложение 2] или выше.
* 1 ГБ [Приложение 2] (для 32-разрядного процессора) или 2 ГБ (для 64-разрядного процессора) ОЗУ [Приложение 2].
* 16 ГБ (для 32-разрядной системы) или 20 ГБ (для 64-разрядной системы) свободного места на жестком диске.
* Графическое устройство DirectX 9 с драйвером WDDM [Приложение 2] 1.0 или более поздней версии.
* Мышь или совместимое указывающее устройство.
* Клавиатура.
* CD-ROM Drive
* USB-порт

## **2.2. Минимальный состав программных средств**

Для надёжной и бесперебойной работы программы требуется следующий состав программных средств:

* Операционная система Microsoft Windows 7 [12] или более поздняя версия.
* Microsoft .NET Framework 4.5.2. [13]

**2.3. Требования к персоналу (пользователю)**

Минимальное количество персонала, требуемого для работы программы, должно составлять не менее 1 штатной единицы:

* конечный пользователь – оператор ЭВМ.

Оператор ЭВМ должен:

* иметь образование не ниже среднего (полного) общего;
* обладать практическими навыками работы с пользовательским интерфейсом операционной системы.
* иметь поверхностные знания о криптосистемах с открытым ключом.

# **3. ВЫПОЛНЕНИЕ ПРОГРАММЫ**

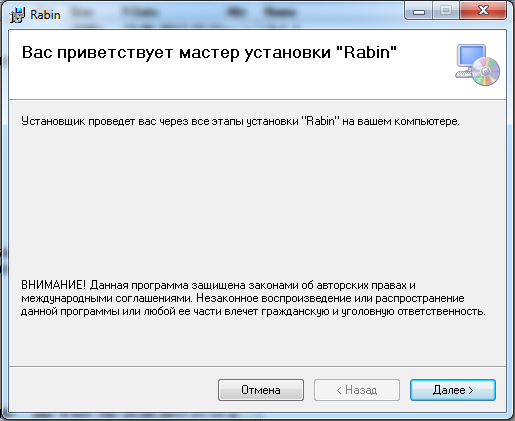
В данном разделе описан пример работы с программой и указано назначение элементов интерфейса.

## **3.1. Инсталляция и запуск программы**

Программное обеспечение «Rabin» поставляется на CD-диске.

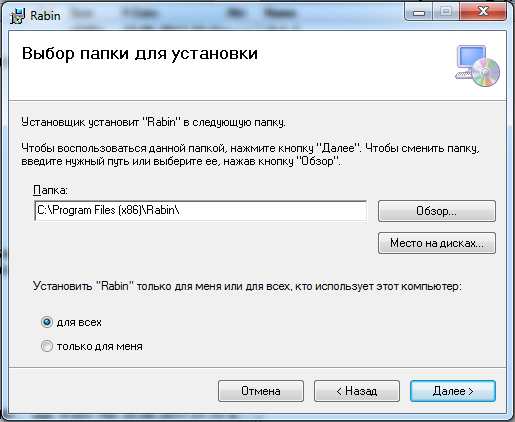
В комплект поставки программы входит CD-диск, который содержит файлы примеров к программе, техническую документацию и презентацию проекта.

При запуске диска необходимо открыть папку «Установка» и запустить пакет установщика Windows Rabin\_Setup.msi. После запуска появится следующее диалоговое окно (рис. 1):



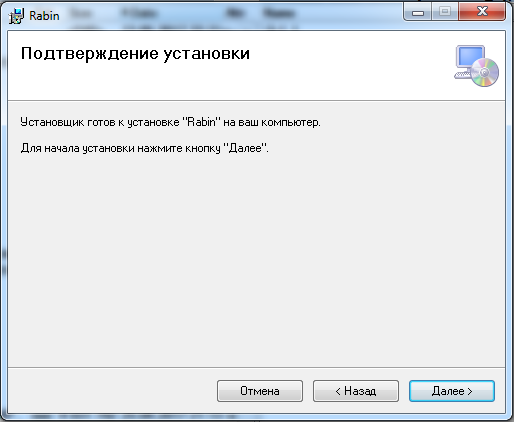
*Рисунок 1*

В этом окне (рис. 1) необходимо после прочтения информации нажать кнопку «Далее». После этого окна последует окно (рис. 2):



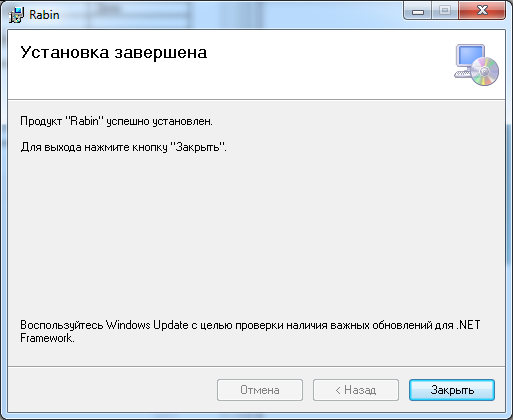
*Рисунок 2*

В поле «Папка» необходимо указать папку, в которую будет установлена программа. Также необходимо выбрать какие пользователи смогут пользоваться этой программой. Нажать «Далее». Появится окно (рис. 3):



*Рисунок 3*

Снова нажать «Далее», появится окно установки, а потом последует окно, сообщающее о завершении установки программы (рис. 4):



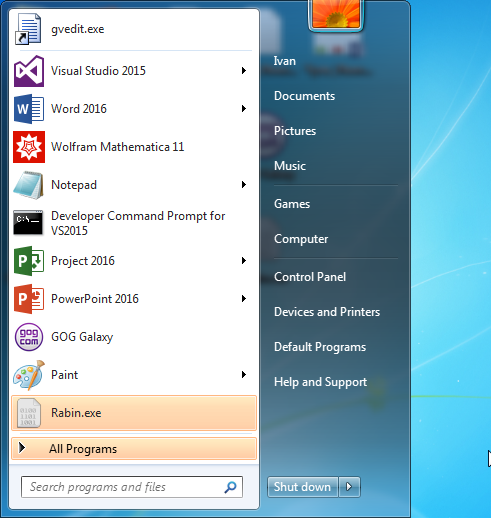
*Рисунок 4*

Нажать кнопку «Закрыть». На рабочем столе компьютера появился ярлык для запуска программы «Rabin» (рис. 5):

C:\Users\Ivan\Documents\ShareX\Screenshots\2017-05\explorer_2017-05-13_22-58-26.png

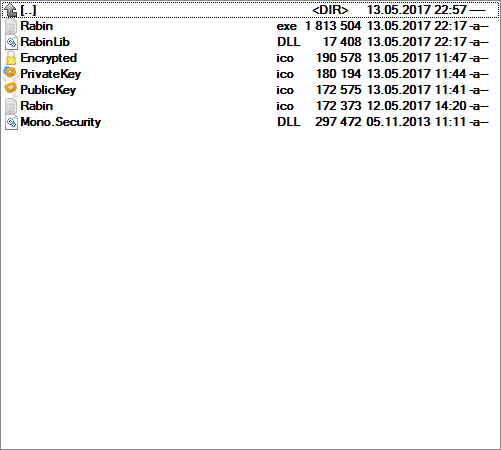
*Рисунок 5*

Также ярлык для программы «Rabin» можно найти в меню «Пуск» (рис. 6):



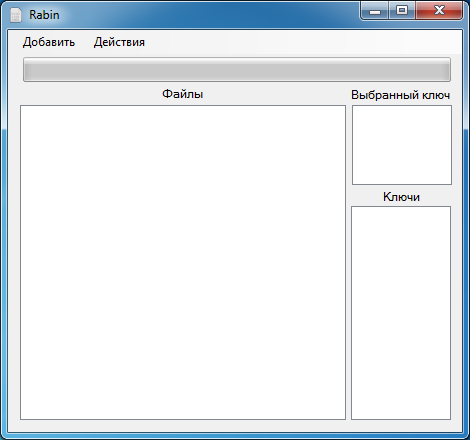
*Рисунок 6*

В папке, куда была установлена программа, должен появиться следующий состав файлов (рис. 7):



*Рисунок 7*

После установки программы выполняется ее открытие, нужно два раза кликнуть на иконку, которая появилась на рабочем столе, или на иконку в меню «Пуск» (Программу можно открыть также и из папки, в которую была выполнена установка. Необходимо два раза кликнуть по приложению Rabin). В случае успешного запуска появится следующее окно (рис. 8):

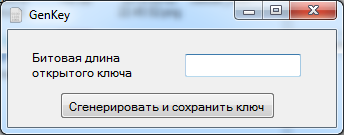


*Рисунок 8*

## **3.2. Выполнение программы**

Интерфейс программы состоит из двух окон:

1. Основное окно (рис. 8)
2. Окно для генерации ключей (рис. 9)



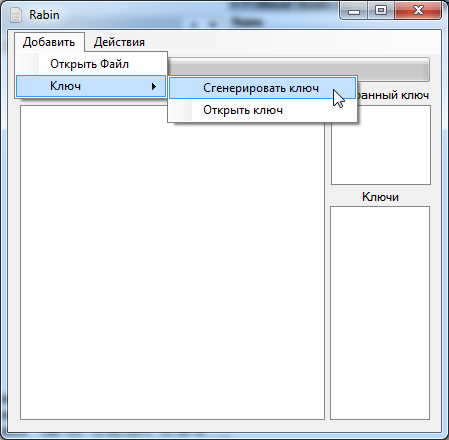
*Рисунок 9*

Данное программное обеспечение имеет Windows интерфейс. На главном окне программы управление реализовано с помощью главного и контекстного меню, выделены поля для файлов, ключей и выбранного ключа. Также вверху располагается ProgressBar, который описывает прогресс. Управление окном генерации ключей осуществляется с помощью системы кнопочного типа. И выделено окно для записи бинарной длины открытого ключа.

### **3.2.1. Получение ключей**

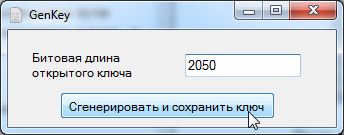
**3.2.1.1. Генерация ключей**

Чтобы сгенерировать новый ключ надо идти по следующему пути «Добавить\Ключ\Сгенерировать ключ» (рис. 10)



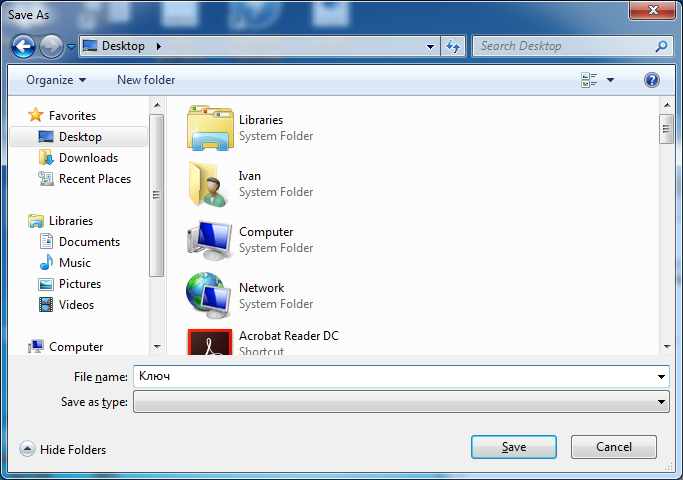
*Рисунок 10*

После данных действий откроется окно генерации ключа (рис. 9). В поле для введения следует вести необходимую бинарную длину открытого ключа и нажать кнопку «Сгенерировать и сохранить ключ». (рис. 11)



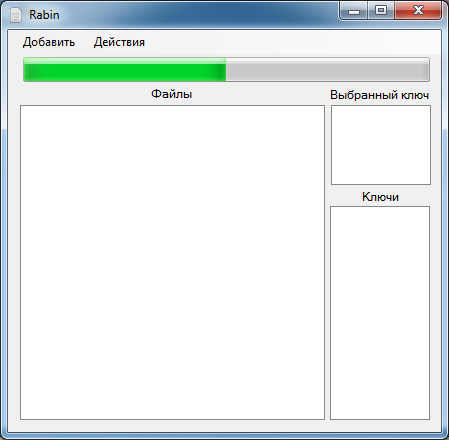
*Рисунок 11*

Далее откроется диалог для выбора места сохранения ключей. (рис. 12) Следует выбрать место для сохранения и названия ключей открытого и закрытого.



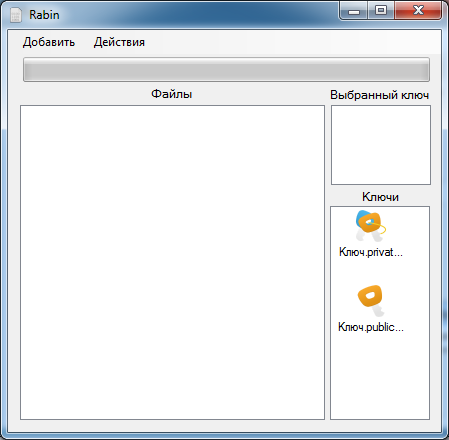
*Рисунок 12*

После этого запустится генерация ключей (рис. 13)



*Рисунок 13*

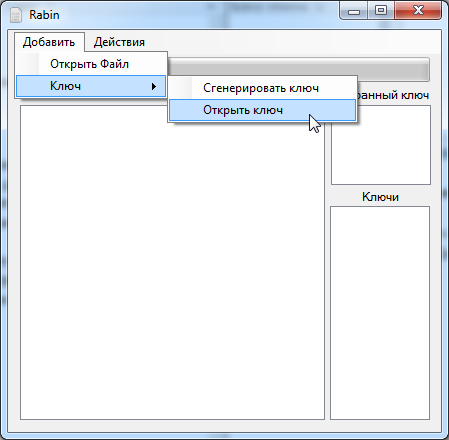
После того, как открытый и закрытый ключи успешно сгенерируются, они будут сохранены в указанном месте в одной папке. И также будут добавлены в коллекцию в список ключей. (рис. 14)



*Рисунок 14*

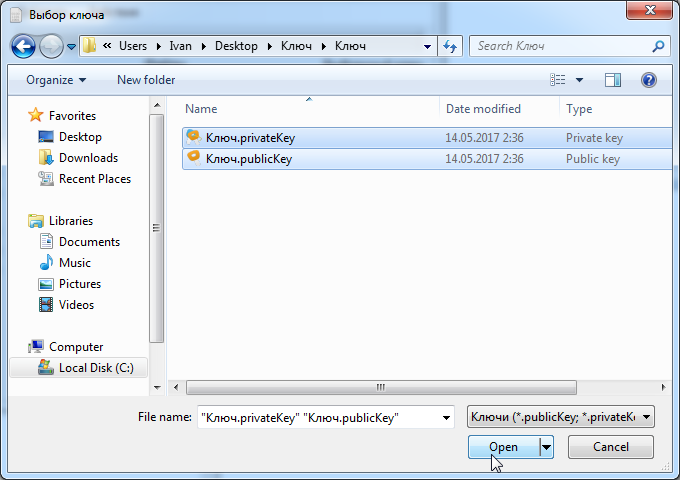
**3.2.1.2 Добавление в программу ключей**

Также можно добавить в программу уже существующие ключи выполняя следующие действия: идти по пути «Добавить\Ключ\Открыть ключ» (рис. 15)



*Рисунок 15*

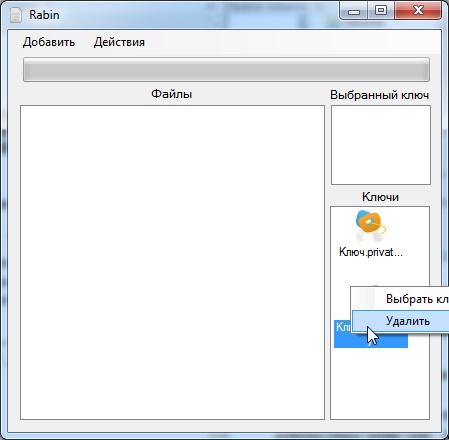
После этого откроется меню для выбора ключа. Где следует выбрать нужнее вам ключи и нажать кнопку «Open». (рис. 16)



*Рисунок 16*

После этого ключи добавятся в программу (рис. 14).

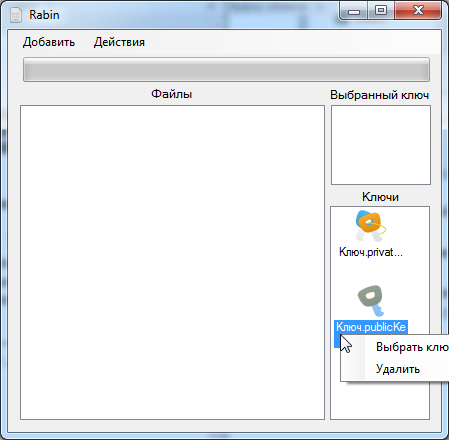
Чтобы удалить ключи из программы следует воспользоваться контекстным меню и нажать кнопку «Удалить». (рис. 17)



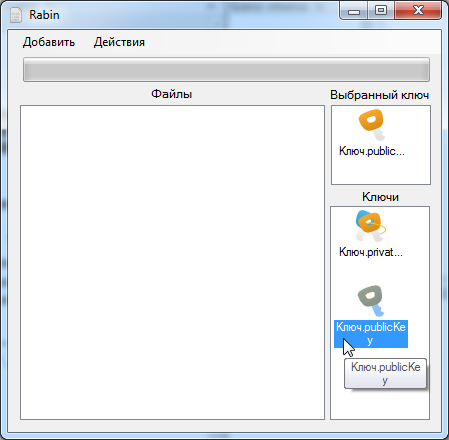
*Рисунок 17*

**3.2.1.3. Выбор ключа для шифрования или дешифрования**

Чтобы выбрать ключ нужно дважды кликнуть на ключ, или воспользовавшись контекстным меню (рис. 18), нажать кнопку «Выбрать ключ». После этого произойдет выбор ключа. (рис. 19).

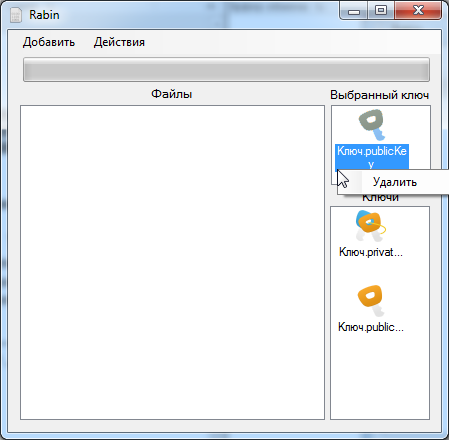


*Рисунок 18*



*Рисунок 19*

Чтобы удалить выбранный ключ, нужно воспользоваться контекстным меню и в нем нажать кнопу «Удалить». (рис. 20)

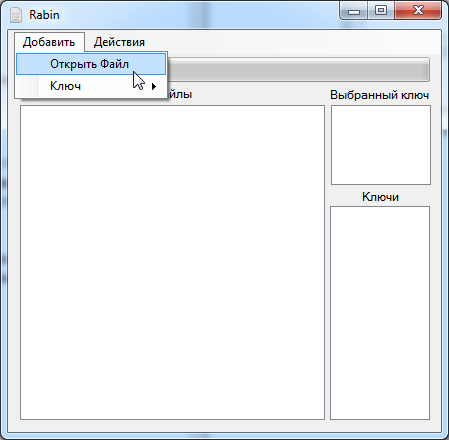


*Рисунок 20*

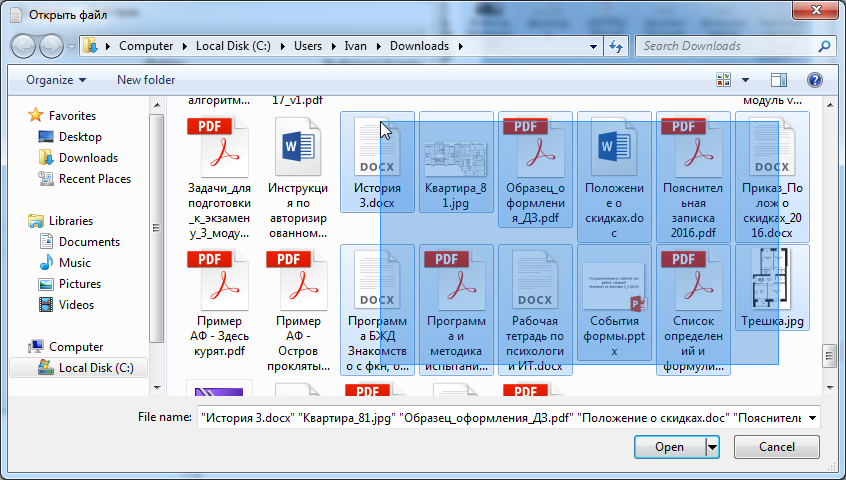
### **3.2.2. Работа с файлом**

#### **3.2.2.1. Добавление файла в программу**

Чтобы добавить кодируемый или декодируемый файл в программу, нужно воспользоваться главным меню и пройти по следующему пути: «Добавить\ Открыть Файл». (рис. 21)

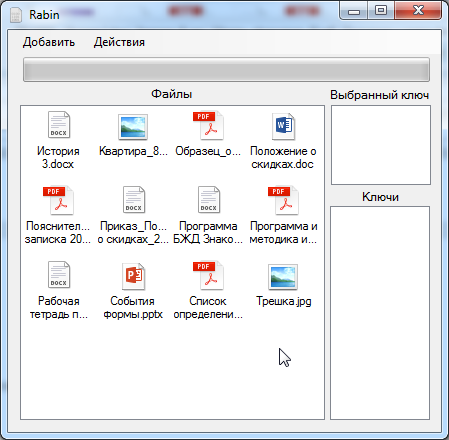


*Рисунок 21*

Далее откроется меню выбора файлов, в котором можно выбрать нужные файлы. (рис. 22)

*Рисунок 22*

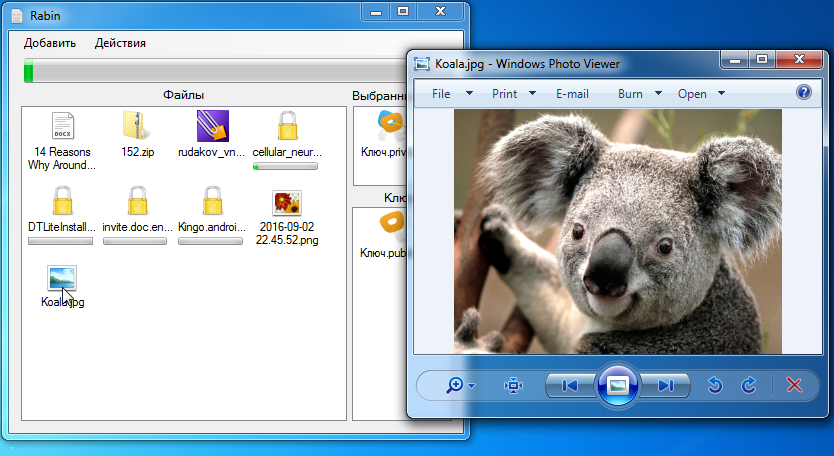
После нажатия кнопки «Open» файлы появятся в приложении (рис. 23)



*Рисунок 23*

#### **3.2.2.2. Открытие файла из самой программы**

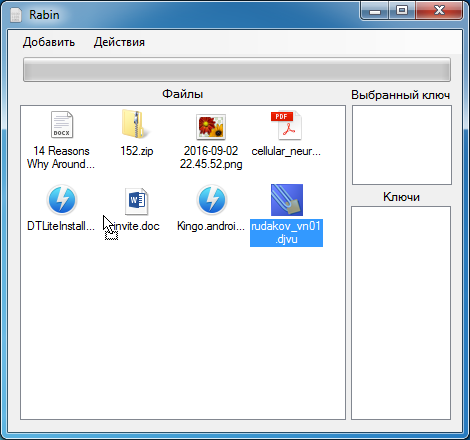
Чтобы открыть файл из программы для просмотра или редактирования следует нажать двойным кликом на его иконку. После этого произойдет открытия файла. (рис. 24)



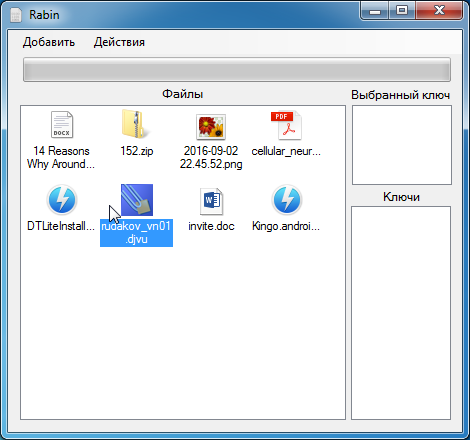
*Рисунок 24*

#### **3.2.2.3. Перемещение и удаление файла**

Чтобы переместить файл или группу файлов следует выбрать нужные файлы и перетащить в желаемое место. (рис. 25 и рис. 26)

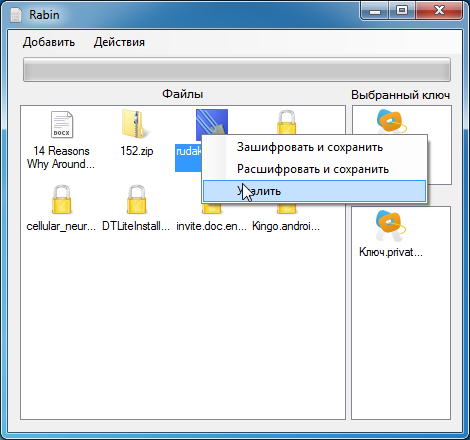


*Рисунок 25*



*Рисунок 26*

Для того, чтобы удалить файл из программы, следует в всплывающем контекстном меню нажать кнопку «Удалить». (рис. 27)



*Рисунок 27*

### **3.2.3. Шифрование файла**

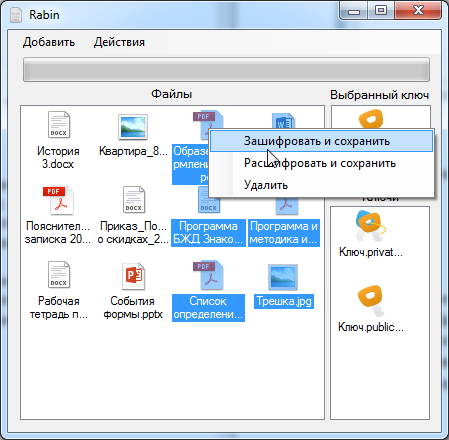
Для того, чтобы начать шифрование, следует выбрать открытый ключ (рис. 28). 

*Рисунок 28*

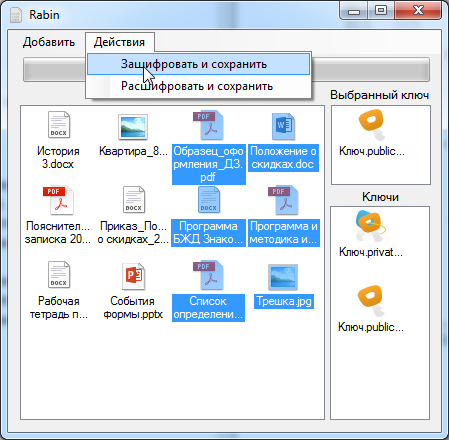
Это можно сделать по инструкции в п. 6.3.1.3.

После того, как выбран открытый ключ, можно переходить к шифрованию.

Чтобы зашифровать файл или группу файлов, следует выделить нужные файлы, воспользовавшись всплывающим контекстным меню, нажать кнопку «Зашифровать и сохранить». (рис. 29) Или пройти по пути в главном меню: «Действия\ Зашифровать и сохранить». (рис. 30)

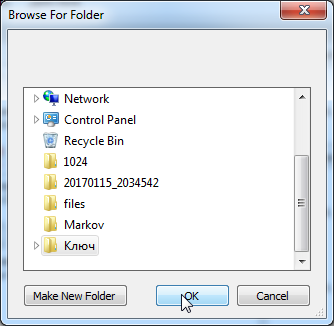


*Рисунок 29*



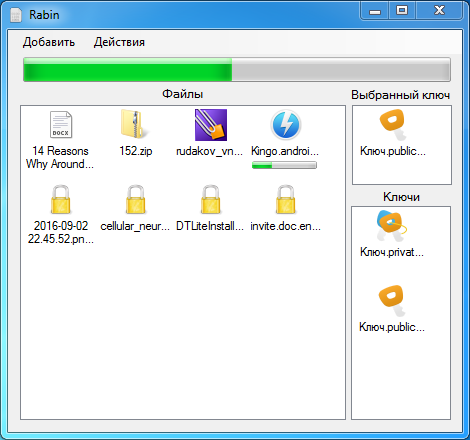
*Рисунок 30*

После этого появится диалог выбора папки, в которую следует сохранить зашифрованные файлы.



*Рисунок 31*

После выбора папки начнется кодирование файлов. (рис. 32)



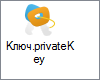
*Рисунок 32*

После этого, в окне с файлами вместо шифруемых файлов появятся зашифрованные файлы. (рис. 33)



*Рисунок 33*

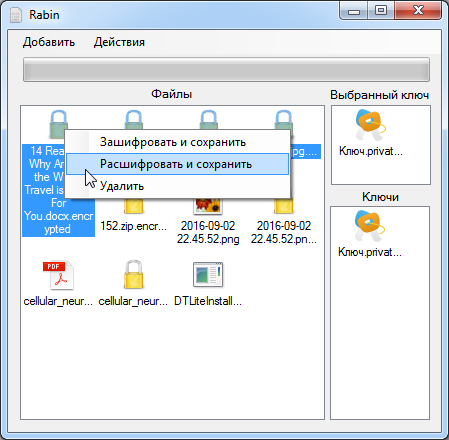
### **3.2.4. Дешифрование файла**

Для того, чтобы начать дешифрование, следует выбрать закрытый ключ (рис. 34). 

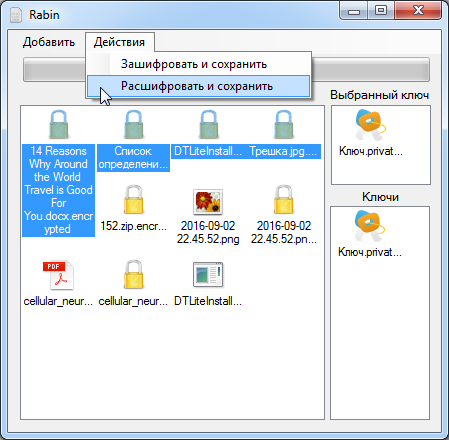
*Рисунок 34*

Это можно сделать по инструкции в п. 3.2.1.3.

После того, как выбран закрытый ключ, можно переходить к дешифрованию. Чтобы расшифровать файл или группу файлов, следует выделить нужные файлы, воспользовавшись всплывающим контекстным меню, нажать кнопку «Расшифровать и сохранить». (рис. 35) Или пройти по пути в главном меню: «Действия\ Расшифровать и сохранить». (рис. 36) Но программа может расшифровывыть только зашифрованные файлы (рис. 33)



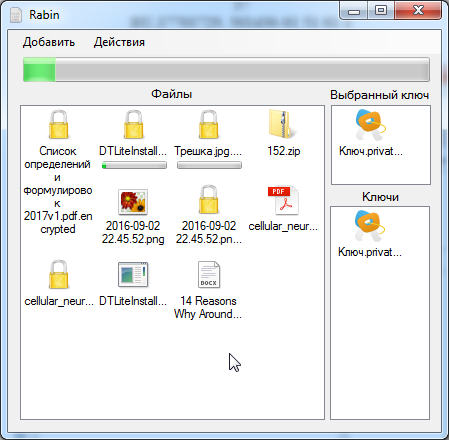
*Рисунок 35*

**

*Рисунок 36*

После этого появится диалог выбора папки, в которую следует сохранить расшифрованные файлы. (рис. 31)

После выбора папки начнется декодирование файлов. (рис. 37)



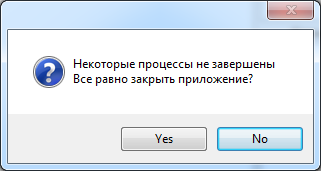
*Рисунок 37*

После этого, в окне с файлами вместо дешифруемых файлов появятся расшифрованные файлы. (рис. 33)

## **3.3. Завершение работы с программой**

При попытке завершения программы проверяется выполнение процессов.

Если все не процессы завершили свою работу, то появится следующее окно с предупреждением для пользователя (рис. 38)

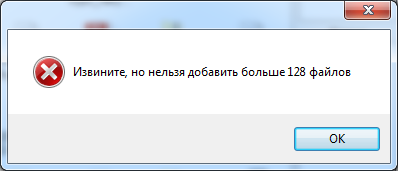


*Рисунок 38*

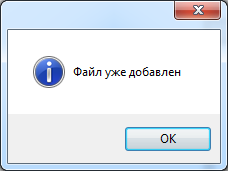
В противном случае произойдет обычное закрытие программы.

# **4. СООБЩЕНИЕ ОПЕРАТОРУ**

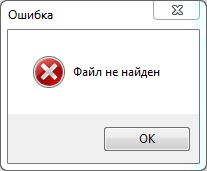
1) «Извините, но нельзя добавить больше 128 файлов». Возникает при попытке открыть более 128 файлов. При нажатии на кнопку «Ок» или «Закрыть» в верхнем левом углу данного окна происходит возврат в главное окно программы (см. рис. 8).



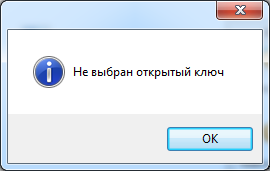
2) «Файл уже добавлен». Возникает при попытке добавить в программу один файл дважды. При нажатии на кнопку «Ок» или «Закрыть» в верхнем левом углу данного окна происходит возврат в главное окно программы (см. рис. 8).



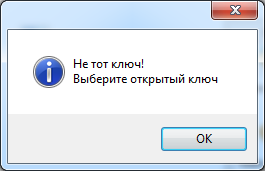
3) «Файл не найден». Возникает в то случае, когда добавленный файл был перемещен или удален. При нажатии на кнопку «Ок» или «Закрыть» в верхнем левом углу данного окна происходит возврат в главное окно программы (см. рис. 8) и файл удаляется из программы.



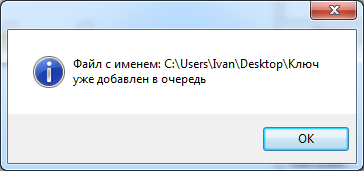
4) «Не выбран открытый ключ». Возникает при попытке зашифровать файл, не выбрав ключ. При нажатии на кнопку «Ок» или «Закрыть» в верхнем левом углу данного окна происходит возврат в главное окно программы (см. рис. 8)



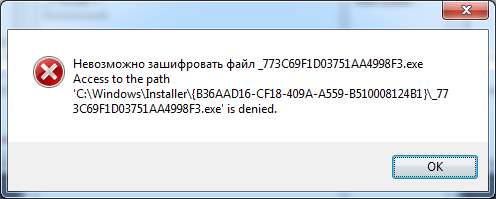
5) «Не тот ключ! Выберете открытый ключ». Возникает при попытке зашифровать файл открытым ключом. При нажатии на кнопку «Ок» или «Закрыть» в верхнем левом углу данного окна происходит возврат в главное окно программы (см. рис. 8)



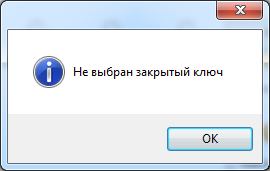
6) «Файл с именем: [Имя файла] уже добавлен в очередьзникает при попытке зашифровать файл открытым ключем.мещен или удален.». Возникает, когда пользователь пытается зашифровать один и тот же файл дважды одновременно. При нажатии на кнопку «Ок» или «Закрыть» в верхнем левом углу данного окна происходит возврат в главное окно программы (см. рис. 8)



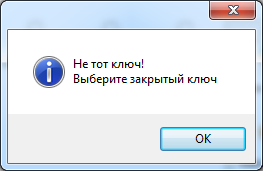
7) «Невозможно зашифровать файл [Имя файла] [Сообщение об ошибке]». Возникает, когда невозможно зашифровать файл. В основном это связано с проблемой доступа к файлу. При нажатии на кнопку «Ок» или «Закрыть» в верхнем левом углу данного окна происходит возврат в главное окно программы (см. рис. 8)



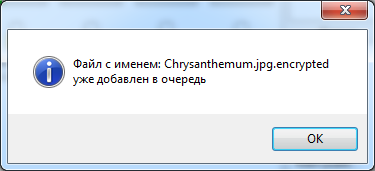
8) «Не выбран закрытый ключ». Возникает, когда пользователь пытается расшифровать файл, не выбрав закрытый ключ. При нажатии на кнопку «Ок» или «Закрыть» в верхнем левом углу данного окна происходит возврат в главное окно программы (см. рис. 8)



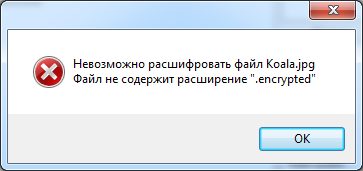
9) «Не тот ключ! Выберете закрытый ключ». Возникает, когда пользователь пытается расшифровать файл с использованием открытого ключа. При нажатии на кнопку «Ок» или «Закрыть» в верхнем левом углу данного окна происходит возврат в главное окно программы (см. рис. 8)



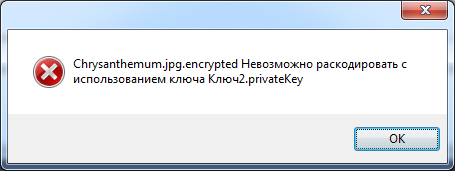
10) «Файл с именем: [Имя файла] уже добавлен в очередьзникает при попытке зашифровать файл открытым ключем.мещен или удален.». Возникает, когда пользователь пытается расшифровать один и тот же файл дважды одновременно. При нажатии на кнопку «Ок» или «Закрыть» в верхнем левом углу данного окна происходит возврат в главное окно программы (см. рис. 8)



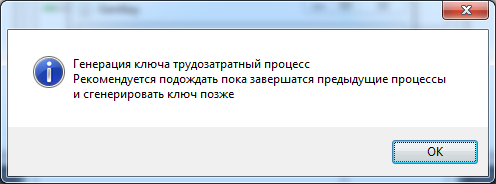
11) «Невозможно расшифровать файл [Имя файла] Файл не содержит расширение .encrypted». Возникает, когда пользователь пытается расшифровать незашифрованный файл. При нажатии на кнопку «Ок» или «Закрыть» в верхнем левом углу данного окна происходит возврат в главное окно программы (см. рис. 8)



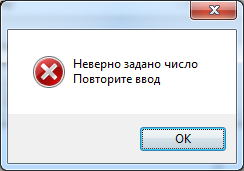
12) «[Имя файла] Невозможно раскодировать с использованием ключа [Имя ключа]». Возникает при попытке расшифровки файла несоответствующим ему ключом. При нажатии на кнопку «Ок» или «Закрыть» в верхнем левом углу данного окна происходит возврат в главное окно программы (см. рис. 8)



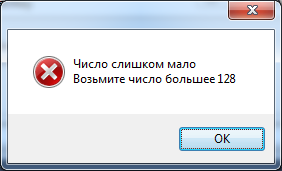
13) "Генерация ключа трудозатратный процесс. Рекомендуется подождать пока завершатся предыдущие процессы и сгенерировать ключ позже". Возникает при попытке сгенерировать ключ во время выполнения других процессов. При нажатии на кнопку «Ок» или «Закрыть» в верхнем левом углу данного окна происходит возврат в главное окно программы (см. рис. 8)



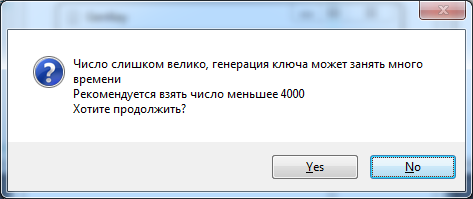
14) «Неверно задано число повторите ввод». Возникает при генерации ключей, когда введенное значение нельзя перевести к числовому виду. При нажатии на кнопку «Ок» или «Закрыть» в верхнем левом углу данного окна происходит возврат к окну генерации ключей (см. рис. 9). И введенное значение удаляется из окошка.



15) «Число слишком мало Возьмите большее 128». Возникает при попытке задать слишком малую длину открытого ключа. При нажатии на кнопку «Ок» или «Закрыть» в верхнем левом углу данного окна происходит возврат к окну генерации ключей (см. рис. 9). И введенное значение удаляется из окошка.



16) «Число слишком велико, генерация ключа может занять много времени. Рекомендуется взять число меньшее 4000. Хотите продолжить?». Возникает при попытке задать слишком большую бинарную длину открытого ключа. При нажатии на кнопку «No» происходит возврат к окну генерации ключей (см. рис. 9). И введенное значение удаляется из окошка. При нажатии на кнопку «Yes» происходит генерация ключа.



# **ПРИЛОЖЕНИЕ 1**

**ЛИТЕРАТУРА**

1. ГОСТ 19.101-77 Виды программ и программных документов. //Единая система программной документации. – М.: ИПК Издательство стандартов, 2001.
2. ГОСТ 19.102-77 Стадии разработки. //Единая система программной документации. – М.: ИПК Издательство стандартов, 2001.
3. ГОСТ 19.103-77 Обозначения программ и программных документов. //Единая система программной документации. – М.: ИПК Издательство стандартов, 2001.
4. ГОСТ 19.104-78 Основные надписи. //Единая система программной документации. – М.: ИПК Издательство стандартов, 2001.
5. ГОСТ 19.105-78 Общие требования к программным документам. //Единая система программной документации. – М.: ИПК Издательство стандартов, 2001.
6. ГОСТ 19.106-78 Требования к программным документам, выполненным печатным способом. //Единая система программной документации. – М.: ИПК Издательство стандартов, 2001.
7. ГОСТ 19.505-79 Руководство оператора. Требования к содержанию и оформлению. //Единая система программной документации. – М.: ИПК Издательство стандартов, 2001.
8. ГОСТ 19.603-78 Общие правила внесения изменений. //Единая система программной документации. – М.: ИПК Издательство стандартов, 2001.
9. ГОСТ 19.604-78 Правила внесения изменений в программные документы, выполненные печатным способом.
10. The Laws of Cryptography: Rabin’s Version of RSA [Электронный ресурс]. URL.: <http://www.cs.utsa.edu/~wagner/laws/Rabin.html> (даты обращения 5.01.2017 - 10.01.2017).
11. Mono Documentation [Электронный ресурс]. URL.: <http://docs.go-mono.com/?link=N%3aMono.Math> (дата обращения 9.01.2017).
12. Требования к системе для .NET Framework [Электронный ресурс]. URL.: <https://msdn.microsoft.com/ru-ru/library/8z6watww(v=vs.110).aspx> (дата обращения: 10.04.2017).
13. Системные требования для ОС Windows 7 [Электронный ресурс]. URL.: <https://support.microsoft.com/ru-ru/help/10737/windows-7-system-requirements>(дата обращения: 10.04.2017).

# **ПРИЛОЖЕНИЕ 2**

## **СОКРАЩЕНИЯ И ОБОЗНАЧЕНИЯ**

ГБ – Согласно ГОСТ 8.417—2002 термин гигабайт с обозначением «ГБ» равен 109 = 1 000 000 000 байт.

Гц – Единица частоты периодических процессов ( 1 Гц = 1 с-1 ).

ОЗУ – Оперативно запоминающее устройство

WDDM – это архитектура графических драйверов для видеокарты под управлением Microsoft Windows.

Компакт диск – Лазерный носитель информации в виде диска.

Флеш-драйв – запоминающее устройство, использующее в качестве носителя флеш-память и подключаемое считывающему устройству по USB.

Закрытый ключ – пара простых чисел P и Q, дающих остаток 3 при делении на 4. С помощью закрытого ключа производится дешифровка сообщения.

Открытый ключ – число N, численно равное произведению пары простых чисел P и Q. С помощью открытого ключа производится шифрования сообщения.

**ПРИЛОЖЕНИЕ 3**

**ОПИСАНИЕ ФОРМАТА .publicKey**

Файл формата .publicKey содержит открытый ключ записанный в кодировке RabinEncoding.

Преимуществами данной кодировки является уменьшение в 2 раза используемой памяти компьютера по сравнению со стандартной, UTF8Encoding. Кодировка также уменьшает читабельность информации другими программами, что повышает степень защиты от злоумышленников.

Корректно открыть файл .publicKey можно программой «Rabin».

**ОПИСАНИЕ ФОРМАТА .privateKey**

Файл формата .privateKey содержит закрытый ключ записанный в кодировке RabinEncoding.

Преимуществами данной кодировки является уменьшение в 2 раза используемой памяти компьютера по сравнению со стандартной, UTF8Encoding. Кодировка также уменьшает читабельность информации другими программами, что повышает степень защиты от злоумышленников.

Корректно открыть файл .privateKey можно программой «Rabin».

**ОПИСАНИЕ ФОРМАТА .encrypted**

Файл формата .encrypted содержит зашифрованный файл записанный в кодировке RabinEncoding.

Преимуществами данной кодировки является уменьшение в 2 раза используемой памяти компьютера по сравнению со стандартной, UTF8Encoding. Кодировка также уменьшает читабельность информации другими программами, что повышает степень защиты от злоумышленников.

Корректно открыть файл .encrypted можно программой «Rabin».

**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 |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |