**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)**

**Техническое задание**

Инв. № дубл.

**ЛИСТ УТВЕРЖДЕНИЯ**

**RU.17701729. 501430-01 ТЗ 01-1**

Взам. инв. №

Исполнитель:

студент группы БПИ 165

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

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

Подп. и дата

Инв. № подл

RU.17701729.

501430-01

ТЗ 01-1

**2017**

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

**КРИПТОСИСТЕМА РАБИНА  
(RABIN CRYPTOSYSTEM)**

**Техническое задание**

**RU.17701729. 501430-01 ТЗ 01-1**

Подп. и дата

Инв. № дубл.

Взам. инв. №

**Листов 21**

Подп. и дата

Инв. № подл

RU.17701729.

501430-01

ТЗ 01-1

**2017**

**АННОТАЦИЯ**

Техническое задание – это основной документ, оговаривающий набор требований и порядок создания программного продукта, в соответствии с которым производится разработка программы, ее тестирование и приемка.

Настоящее Техническое задание на разработку «Криптосистема Рабина (Rabin Cryptosystem)» содержит следующие разделы: «Введение», «Основание для разработки», «Назначение разработки», «Требования к программе», «Требования к программным документам», «Технико-экономические показатели», «Стадии и этапы разработки», «Порядок контроля и приемки» и приложения.  
 В разделе «Введение» указано наименование и краткая характеристика области применения программы.  
 В разделе «Основания для разработки» указан документ, на основании которого ведется разработка и наименование темы разработки.  
 В разделе «Назначение разработки» указано функциональное и эксплуатационное назначение программного продукта.   
 Раздел «Требования к программе» содержит основные требования к функциональным характеристикам, к надежности, к условиям эксплуатации, к составу и параметрам технических средств, к информационной и программной совместимости, к маркировке и упаковке, к транспортировке и хранению, а также специальные требования.  
 Раздел «Требования к программным документам» содержит предварительный состав программной документации и специальные требования к ней.  
 Раздел «Технико-экономические показатели» содержит ориентировочную экономическую эффективность, предполагаемую годовую потребность, экономические преимущества разработки программы.  
 Раздел «Стадии и этапы разработки» содержит стадии разработки, этапы и содержание работ.  
 В разделе «Порядок контроля и приемки» указаны общие требования к приемке работы.  
 Настоящий документ разработан в соответствии с требованиями:

* ГОСТ 19.101-77 Виды программ и программных документов [1];
* ГОСТ 19.102-77 Стадии разработки [2];
* ГОСТ 19.103-77 Обозначения программ и программных документов [2];
* ГОСТ 19.104-78 Основные надписи [4];
* ГОСТ 19.105-78 Общие требования к программным документам [5];
* ГОСТ 19.106-78 Требования к программным документам, выполненным печатным способом [6];
* ГОСТ 19.201-78 Техническое задание. Требования к содержанию и оформлению [7].

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

СОДЕРЖАНИЕ

[1. ВВЕДЕНИЕ 5](#_Toc483414804)

[1.1. Наименование программы 5](#_Toc483414805)

[1.2. Краткая характеристика области применения 5](#_Toc483414806)

[1.3. Объект, в котором используют программу 5](#_Toc483414807)

[2. ОСНОВАНИЯ ДЛЯ РАЗРАБОТКИ 6](#_Toc483414808)

[3. НАЗНАЧЕНИЕ РАЗРАБОТКИ 7](#_Toc483414809)

[3.1. Функциональное назначение 7](#_Toc483414810)

[3.2 Эксплуатационное назначение 7](#_Toc483414811)

[4. ТРЕБОВАНИЕ К ПРОГРАММЕ 8](#_Toc483414812)

[4.1. Требование к функциональным характеристикам 8](#_Toc483414813)

[4.1.1. Требование к составу выполняемых функций 8](#_Toc483414814)

[4.1.2. Требование к организации входных данных 9](#_Toc483414815)

[4.1.3. Требование к организации выходных данных 9](#_Toc483414816)

[4.2. Требования к интерфейсу 9](#_Toc483414817)

[4.2.1. Требования к GUI интерфейсу 9](#_Toc483414818)

[4.2.2. Требования к API интерфейсу 9](#_Toc483414819)

[4.3 Требования к надежности 10](#_Toc483414820)

[4.3.1. Отказы из-за некорректных действий оператора 10](#_Toc483414821)

[4.3.2. Время восстановления после отказа 10](#_Toc483414822)

[4.4. Условия эксплуатации 10](#_Toc483414823)

[4.5. Требование к составу и параметрам технических средств 10](#_Toc483414824)

[4.6 Требование к информационной и программной совместимости 11](#_Toc483414825)

[4.6.1. Требования к программным средствам, используемым программой. 11](#_Toc483414826)

[4.6.2. Требование к исходным кодам и языкам программирования 11](#_Toc483414827)

[4.7. Требования к маркировке и упаковке 11](#_Toc483414828)

[4.8. Требования к транспортировке и хранению 11](#_Toc483414829)

[4.8.1. Требования к хранению и транспортировке компакт-дисков 11](#_Toc483414830)

[4.8.2. Требования к хранению и транспортировке флеш-драйвов 12](#_Toc483414831)

[4.8.3. Требования для хранения программной документации, представляемой в печатном виде 12](#_Toc483414832)

[5. ТРЕБОВАНИЯ К ПРОГРАММНОЙ ДОКУМЕНТАЦИИ 13](#_Toc483414833)

[5.1. Предварительный состав программной документации 13](#_Toc483414834)

[5.2. Специальные требования к программной документации 13](#_Toc483414835)

[6. ТЕХНИКО-ЭКОНОМИЧЕСКИЕ ПОКАЗАТЕЛИ 14](#_Toc483414836)

[6.1. Ориентированная экономическая эффективность 14](#_Toc483414837)

[6.2. Предполагаемая потребность 14](#_Toc483414838)

[6.3. Экономические преимущества разработки по сравнению с другими образцами и аналогами 14](#_Toc483414839)

[7. СТАДИИ И ЭТАПЫ РАЗРАБОТКИ 15](#_Toc483414840)

[8. ПОРЯДОК КОНТРОЛЯ И ПРИЕМКИ 17](#_Toc483414841)

[9. ЛИТЕРАТУРА 18](#_Toc483414842)

[ПРИЛОЖЕНИЕ 1 19](#_Toc483414843)

[СОКРАЩЕНИЯ И ОБОЗНАЧЕНИЯ 19](#_Toc483414844)

[ПРИЛОЖЕНИЕ 2 20](#_Toc483414845)

[ОПИСАНИЕ ФОРМАТА .publicKey 20](#_Toc483414846)

[ОПИСАНИЕ ФОРМАТА .privateKey 20](#_Toc483414847)

[ОПИСАНИЕ ФОРМАТА .encrypted 20](#_Toc483414848)

# 1. ВВЕДЕНИЕ

## **1.1. Наименование программы**

Наименование программы **-** «Криптосистема Рабина (Rabin Cryptosystem)».

## **1.2. Краткая характеристика области применения**

«Криптосистема Рабина (Rabin Cryptosystem)» предназначена для кодирования и декодирования текста, чисел и всевозможных файлов, используя криптосистему Рабина, основанную на сложности факторизации больших целых чисел, с использованием открытого ключа. Позволяет кодировать информацию всевозможного размера, представленную в файле с любым расширением, сохранять зашифрованный файл и соответствующие ему ключи, и расшифровывать при верном закрытом ключе.

## **1.3. Объект, в котором используют программу**

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

# 2. ОСНОВАНИЯ ДЛЯ РАЗРАБОТКИ

Документом, на основании которого ведется разработка является приказ об утверждении тем, руководителей курсовых работ студентов образовательной программы Программная инженерия факультета компьютерных наук № 2.3-02/0812-01 от 08.12.2016.

Программа выполняется в рамках темы курсовой работы в соответствии с учебным планом подготовки бакалавров по направлению 09.03.04 «Программная инженерия».

Организация, утвердившая документ: Национальный Исследовательский Университет «Высшая школа экономики», факультет компьютерных наук, отделение программной инженерии.

# 3. НАЗНАЧЕНИЕ РАЗРАБОТКИ

## **3.1. Функциональное назначение**

Программное обеспечение «Криптосистема Рабина (Rabin Cryptosystem)» предназначено для криптографической защиты информации. Программа должна обеспечивать надежную защиту закодированной информации от различных попыток взлома и рассекречивания зашифрованного текста.

## **3.2 Эксплуатационное назначение**

К функциональным возможностям программы относятся:

* Генерация открытого ключа для шифрования;
* Генерация закрытого ключа для дешифрования;
* Кодирование любых файлов, хранящихся на диске компьютера;
* Декодирование файлов, зашифрованных в данной программе.

# 4. ТРЕБОВАНИЕ К ПРОГРАММЕ

## **4.1. Требование к функциональным характеристикам**

### **4.1.1. Требование к составу выполняемых функций**

Программа должна обеспечивать возможность выполнения перечисленных ниже функций:

* Получение ключа
* Генерация закрытого ключа по указанной пользователем бинарной длине (пара простых чисел [17], дающих остаток 3 по модулю 4);
* Вычисление открытого ключа (произведение двух простых чисел [17], дающих остаток 3 по модулю 4);
* Запись открытого ключа в файл с расширением .publicKey [Приложение 2] и закрытого ключа в файл с расширением .privateKey [Приложение 2] 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 файла с использованием открытого ключа [16];
* Кодирование группы файла с использованием открытого ключа;
* Запись закодированного файла с расширением .encrypted [Приложение 2] на жесткий диск компьютера.
* Декодирование файла
* Выбор закрытого ключа для дешифрования;
* Используя закрытый ключ, декодирование [16] зашифрованного файла с расширением .encrypted [Приложение 2];
* Используя закрытый ключ, декодирование группы зашифрованных файлов с расширением .encrypted [Приложение 2];
* 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.

### **4.1.2. Требование к организации входных данных**

Программа должна иметь возможность получать на вход файлы следующего формата:

* Файлы с любым расширением (шифруемый файл)
* Файлы с расширением .publicKey [Приложение 2] и .privateKey [Приложение 2] (открытый и закрытый ключи соответственно)
* Файл с расширением .encrypted [Приложение 2] (зашифрованный файл)

### **4.1.3. Требование к организации выходных данных**

Программа должна иметь возможность выдавать на выходе файлы следующего формата:

* Файлы с любым расширением (расшифрованный файл)
* Файлы с расширением .publicKey [Приложение 2] и .privateKey [Приложение 2] (открытый и закрытый ключи соответственно)
* Файл с расширением .encrypted [Приложение 2] (зашифрованный файл)

## **4.2. Требования к интерфейсу**

### **4.2.1. Требования к GUI интерфейсу**

Данный программный продукт должен иметь Windows-интерфейс. На интерфейсе должны располагаться компоненты, позволяющие пользователю выполнять все операции, описанные в пункте 4.1.1.

### **4.2.2. Требования к API интерфейсу**

Программный интерфейс приложения должен обеспечивать генерацию открытого и закрытого ключей при полученной бинарной длине открытого ключа.

Должен обеспечивать свободное кодирование и декодирование информации представленной в формате String [Приложение 1], BigInteger [Приложение 1] и любого наследника класса Stream [Приложение 1].

## **4.3 Требования к надежности**

### **4.3.1. Отказы из-за некорректных действий оператора**

Программа не должна завершаться аварийно, при некорректных действиях пользователя, программа должна выводить сообщение с соответствующей ошибкой и дальнейшими указаниями.

### **4.3.2. Время восстановления после отказа**

В случае возникновения сбоя, вызванного внешними факторами (непредвиденное выключение источника питания) время восстановления программы не должно превышать суммарно затраченного времени на решение проблем с техническими средствами (перезагрузка операционной системы компьютера).

## **4.4. Условия эксплуатации**

Пользователь программы не должен обладать какими-либо особыми знаниями или навыками, за исключением беглого понимания, работы криптосистемы с открытым ключом. Для корректной работоспособности программы, пользователь должен располагать в наличии компьютерной мышью или устройством заменяющим ее, и иметь в наличии клавиатуру.

## **4.5. Требование к составу и параметрам технических средств**

Необходимые требования и минимальные характеристики для надежной и бесперебойной работы программы требуется следующий состав технических средств:

* 32-разрядный (x86) или 64-разрядный (x64) процессор с тактовой частотой 1 ГГц [Приложение 1] или выше.
* 1 ГБ [Приложение 1] (для 32-разрядного процессора) или 2 ГБ (для 64-разрядного процессора) ОЗУ.
* 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 1] 1.0 или более поздней версии.
* Мышь или совместимое указывающее устройство.
* Клавиатура.
* CD-ROM Drive
* USB-порт

## **4.6 Требование к информационной и программной совместимости**

### **4.6.1. Требования к программным средствам, используемым программой.**

Для работы программы необходим следующий состав программных средств:

* Операционная система Microsoft Windows 7 или более поздняя версия.
* Microsoft .NET Framework 4.5.2.

### **4.6.2. Требование к исходным кодам и языкам программирования**

Программа должна быть написана на языке программирования C#. В качестве интегрированной среды разработки программы должна быть использована среда Microsoft Visual Studio 2015.

## **4.7. Требования к маркировке и упаковке**

Программа поставляется в виде программного изделия на внешнем носителе информации – компакт-диске (Приложение 1) или флеш-драйве (Приложение 1), на котором должны содержаться программная документация, приложение (исполняемые файлы, два примера задачи и прочие необходимые для работы программы файлы) и презентация проекта.

Программное изделие должно иметь маркировку с обозначением наименования изделия, темы разработки, фамилии, имени и отчества исполнителя и руководителя разработки, учебной группы и года выпуска изделия.

## **4.8. Требования к транспортировке и хранению**

### **4.8.1. Требования к хранению и транспортировке компакт-дисков**

Требования к транспортировке и хранению компакт-дисков с программным обеспечением являются стандартными и должны соответствовать требованиям [10]:

* Допустимая температура воздуха от 10°С до 20°С и относительная влажность воздуха от 20% до 65%.
* Максимальные суточные колебания температуры 2°С и относительной влажности воздуха - 5 %.
* Хранить вдали от тепла и влаги.
* Компакт-диски хранят в темноте или при освещении рассеянным светом, не содержащим ультрафиолетовое излучение.
* Транспортировка производится вертикально в специальных маркированных контейнерах из безопасных материалов с применением мер по предотвращению ударов контейнеров, перемещению и вибрации компакт-дисков внутри контейнеров, а также проникновения влаги, вредных газов, пыли, солнечных лучей и образованию конденсата внутри контейнеров.
* Очистка компакт-диска производится путем протирания чистым мягким хлопчатобумажным тампоном без длинного ворса, пропитанным водой, этиловым или изопропиловым спиртом.

### **4.8.2. Требования к хранению и транспортировке флеш-драйвов**

* Хранить вдали от влаги и легко воспламеняющихся источников.
* Не хранить вблизи ядовитых веществ и агрессивных реагентов.

### **4.8.3. Требования для хранения программной документации, представляемой в печатном виде**

* Допустимая температура воздуха от 10°С до 30°С и относительная влажность воздуха от 40% до 60%.
* Хранить вдали от влаги и легко воспламеняющихся источников.
* Не хранить вблизи ядовитых веществ и агрессивных реагентов.

# 5. ТРЕБОВАНИЯ К ПРОГРАММНОЙ ДОКУМЕНТАЦИИ

## **5.1. Предварительный состав программной документации**

* «Криптосистема Рабина (Rabin Cryptosystem)» Техническое задание [7].
* «Криптосистема Рабина (Rabin Cryptosystem)». Программа и методика испытаний [11].
* «Криптосистема Рабина (Rabin Cryptosystem)». Текст программы [12].
* «Криптосистема Рабина (Rabin Cryptosystem)». Пояснительная записка [13].
* «Криптосистема Рабина (Rabin Cryptosystem)». Руководство оператора [14].
* «Криптосистема Рабина (Rabin Cryptosystem)». Руководство программиста [15].

## **5.2. Специальные требования к программной документации**

* Все документы должны быть сделаны в соответствии с ГОСТ [см. раздел 9] к этому виду документа.
* Документация сдается в печатном виде с подписями руководителя организации, утвердившей разработку, руководителя разработки и разработчика.
* Вся документация также сдается в электронном виде в формате .pdf или .docx. в архиве формата .rar. Все документы должны быть загружены в LMS в личном кабинете во вкладке «Проекты» - «Курсовая работа».

# 6. ТЕХНИКО-ЭКОНОМИЧЕСКИЕ ПОКАЗАТЕЛИ

## **6.1. Ориентированная экономическая эффективность**

В рамках данной курсовой работы расчет экономической эффективности не предусмотрен.

## **6.2. Предполагаемая потребность**

Данная программа ориентирована на людей, испытывающих потребность в безопасном использовании информации, представленной в цифровом виде. Которая позволяет любому желающему человеку безопасно зашифровать/расшифровать секретную информацию, представленную в цифровом виде.

## **6.3. Экономические преимущества разработки по сравнению с другими образцами и аналогами**

Данная разработка обладает рядом преимуществ относительно других криптографических программ:

* В данной программе используется алгоритм криптосистемы Рабина с открытым ключом, о котором не известно многим злоумышленникам.
* В отличие от многих других программ, основанных на криптосистеме Рабина, сгенерированные ключи защищены от «метода Ферма» (этот метод позволяет довольно быстро по открытому ключу найти закрытый, и расшифровать сообщение).
* Позволяет зашифровать/расшифровать информацию неограниченного объема.

# 7. СТАДИИ И ЭТАПЫ РАЗРАБОТКИ

Стадии и этапы разработки с учетом [2]:

|  |  |  |
| --- | --- | --- |
| **Стадии разработки** | **Этапы разработки** | С**одержание работ по этапам** |
| 1. Техническое задание | Обоснование необходимости разработки программы | Формулировка цели.  Исследование материалов по теме поставленной задачи.  Определение требований к программному продукту |
| Научно-исследовательские работы | Определение структуры входных и выходных данных.  Выбор методов и алгоритмов решения задачи.  Определение требований к техническим средствам. |
| Разработка и утверждение технического задания | Определение требований к программе.  Определение стадий, этапов и сроков разработки. программы и документации на нее.  Определение языка программирования.  Согласование и утверждение технического задания. |
| 1. Технический проект | Разработка технического проекта | Поиск оптимальных алгоритмов решения поставленной задачи.  Изучение дополнительных материалов.  Разработка алгоритма решения задачи. |
| Подготовка пакета программной документации | Подготовка полного пакета программной документации, перечисленной в п. 5.1. |
| Утверждение технического проекта | Разработка плана мероприятий по разработке и внедрению программ.  Разработка пояснительной записки.  Согласование и учреждение технического проекта. |
| 1. Рабочий проект | Разработка программы | Разработка и отладка программного кода.  Реализация интерфейса для программы. |
|  | Разработка программной документации | Разработка программных документов в соответствии с требованиями [1]. |
|  | Испытание программы | Разработка, согласование и утверждение порядка и методики испытаний.  Испытание программы и поиск ошибок.  Корректировка программного кода и программной документации. |
| 1. Внедрение | Защита программного продукта | Согласование даты защиты программного продукта.  Утверждение программной документации.  Презентация программного продукта. |

# 8. ПОРЯДОК КОНТРОЛЯ И ПРИЕМКИ

Контроль и приемка разработки проводится в соответствии с программным документом «Криптосистема Рабина (Rabin Cryptosystem)». Программа и методика испытаний в соответствии с [11].

Программа принимается только при условии работоспособности программы при вводимых в нее различных данных; при соответствии требованиям технического задания и при наличии полного пакета документации.

# 9. 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 19.201-78 Техническое задание. 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. //Единая система программной документации. – М.: ИПК Издательство стандартов, 2001.
10. ГОСТ Р 7.02-2006 Консервация документов на компакт-дисках. Общие требования. – М.: ИПК Издательство стандартов, 2006.
11. ГОСТ 19.301-79 Программа и методика испытаний. Требования к содержанию и оформлению. //Единая система программной документации. – М.: ИПК Издательство стандартов, 2001.
12. ГОСТ 19.401-78 Текст программы. Требования к содержанию и оформлению. //Единая система программной документации. – М.: ИПК Издательство стандартов, 2001.
13. ГОСТ 19.404-79 Пояснительная записка. Требования к содержанию и оформлению. //Единая система программной документации. – М.: ИПК Издательство стандартов, 2001.
14. ГОСТ 19.505-79 Руководство оператора. Требования к содержанию и оформлению. //Единая система программной документации. – М.: ИПК Издательство стандартов, 2001.
15. ГОСТ 19.504-79 Руководство программиста //Единая система программной документации. – М.: ИПК Издательство стандартов, 2001.
16. 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).
17. Mono Documentation [Электронный ресурс]. URL.: <http://docs.go-mono.com/?link=N%3aMono.Math> (дата обращения 9.01.2017).

# ПРИЛОЖЕНИЕ 1

## **СОКРАЩЕНИЯ И ОБОЗНАЧЕНИЯ**

API интерфейс – Программный интерфейс приложения, интерфейс программирования приложений, интерфейс прикладного программирования.

GUI интерфейс – Графический интерфейс пользователя.

String – Вид информации представленный в текстовом виде.

BigInteger – Вид информации представленный в виде произвольно большого числа со знаком.

Stream – Универсальное представление последовательности байтов.

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.

# ПРИЛОЖЕНИЕ 2

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