**ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ  
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ   
«ВЫСШАЯ ШКОЛА ЭКОНОМИКИ»**

Факультет компьютерных наук

Департамент программной инженерии

|  |  |
| --- | --- |
| СОГЛАСОВАНО  Доцент департамента программной инженерии факультета компьютерных наук, канд. физ.-мат. наук.  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ А.А.Набебин  «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_ 2015 г. | УТВЕРЖДАЮ  Академический руководитель образовательной программы «Программная инженерия»  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ В.В. Шилов  «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_2015 г. |
| |  |  | | --- | --- | | ***Подп. и дата*** |  | | ***Инв. № дубл.*** |  | | ***Взам. Инв. №*** |  | | ***Подп. и дата*** |  | | ***Инв. № подл.*** | RU.17701729.501430-01 33 01-1-ЛУ | | **Библиотека A5-1\_Lib**  **Руководство программиста**  **ЛИСТ УТВЕРЖДЕНИЯ**  **RU.17701729.501430-01 33 01-1-ЛУ**  Исполнитель  студент группы 102 ПИ  \_\_\_\_\_\_\_\_\_\_\_/Берюхов А.С./  «\_\_\_»\_\_\_\_\_\_\_\_\_\_2015 г.  **2015** | | |  |

УТВЕРЖДЕНО

RU.17701729.501430-01 33 01-1-ЛУ

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  | | --- | --- | | ***Подп. и дата*** |  | | ***Инв. № дубл.*** |  | | ***Взам. Инв. №*** |  | | ***Подп. и дата*** |  | | ***Инв. № подл.*** | RU.17701729.501430-01 33 01-1 | | **Библиотека A5-1\_Lib**  Руководство программиста  RU.17701729.501430-01 33 01-1  **Листов 11**  **2015** |  |

**АННОТАЦИЯ**

Документ «Руководство программиста» адресован программистам, желающим использовать данную библиотеку в своих программах. В нем содержится информация об основных функциях, реализованных в библиотеке, а также способах работы с ними.

Руководство программиста состоит из пяти основных частей.

В разделе Назначение и условия применения библиотеки описаны назначение, функционал и минимальные требования библиотеки.

В разделе Характеристики библиотеки указаны её качественные характеристики.

В разделе Обращение к библиотеке содержится информация по подключению библиотеки и использованию ее методов в новых программах.

В разделе Входные и выходные данные описаны форматы входных и выходных данных, с которыми работают методы библиотеки.

В разделе Сообщения содержатся возможные ошибки и исключительные ситуации, возникающие при работе с библиотекой.

**СОДЕРЖАНИЕ**

[1. Назначение и условия применения библиотеки 4](#_Toc419497771)

[1.1. Назначение библиотеки 4](#_Toc419497772)

[1.2. Функции, выполняемые библиотекой 4](#_Toc419497773)

[1.3. Условия, необходимые для выполнения библиотеки 4](#_Toc419497774)

[1.3.1. Требования к составу и параметрам технических средств 4](#_Toc419497775)

[1.3.2. Требования к программным средствам 4](#_Toc419497776)

[2. Характеристики библиотеки 5](#_Toc419497777)

[2.1. Средства контроля правильности исполнения 5](#_Toc419497778)

[3. Обращение к библиотеке 6](#_Toc419497779)

[3.1. Инициализация объекта-сессии 6](#_Toc419497780)

[3.2. Установка ключа и номера фрейма 6](#_Toc419497781)

[3.3. Получение двух 114-битных последовательностей 6](#_Toc419497782)

[3.4. Получение 228-битной последовательности 7](#_Toc419497783)

[4.Входные и выходные данные 8](#_Toc419497784)

[4.1. Входные данные 8](#_Toc419497785)

[4.2. Выходные данные 8](#_Toc419497786)

[5. Сообщения 9](#_Toc419497787)

[6. Приложения 10](#_Toc419497788)

[6.1. Список используемой литературы 10](#_Toc419497789)

# 1. Назначение и условия применения библиотеки

## 1.1. Назначение библиотеки

Библиотека предназначена для генерации последовательности, необходимой для шифрования / дешифрования.

## 1.2. Функции, выполняемые библиотекой

1. Инициализация объекта-сессии.
2. Установка ключа и номера фрейма.
3. Получение 228-битной последовательности для одностороннего шифрования.
4. Получение двух 114-битных последовательностей для двустороннего шифрования (применимо для шифрования мобильной связи, когда одновременно шифруется выходной сигнал и дешифруется входной).

## 1.3. Условия, необходимые для выполнения библиотеки

### 1.3.1. Требования к составу и параметрам технических средств

Компьютер, со следующими свойствами:

1. Процессор Pentium с частотой 233 МГц или более быстрый (рекомендуется не менее 300 МГц).
2. Не менее 64 МБ оперативной памяти (рекомендуется не менее 128 МБ).
3. Не менее 1,5 ГБ свободного места на жестком диске.
4. Дисковод для компакт- или DVD-дисков.
5. Клавиатура, мышь Microsoft Mouse или совместимое указывающее устройство.
6. Видеокарта и монитор, поддерживающие режим Super VGA с разрешением не менее чем 800x600 точек. [1]

### 1.3.2. Требования к программным средствам

1. операционная система Microsoft Windows XP и новее;
2. установленный Microsoft .NET Framework 2.0.

# 2. Характеристики библиотеки

## 2.1. Средства контроля правильности исполнения

Правильность исполнения проверяется двукратным применением побитового сложения выходной последовательности и массива данных (массив данных и последовательность, полученный массив и последовательность) и получением исходного массива данных.

Правильность получения выходной последовательности проверяется многократным получением одной и той же последовательности на основе одинаковых значений ключа и номера фрейма.

# 3. Обращение к библиотеке

Для использования методов библиотеки A5-1\_Lib необходимо подключить её в соответствующем проекте.

## 3.1. Инициализация объекта-сессии

Для использования основных методов библиотеки необходимо создать объект-сессию, задать ключ и номер фрейма. За создание объекта отвечает конструктор умолчания класса A5\_1 *public A5\_1()*, создаваемый языком по умолчанию.

## 3.2. Установка ключа и номера фрейма

Для установки ключа и номера фрейма предусмотрен открытый метод *public void keysetup(uint[] key, uint frame).*

Этот метод принимает на вход ключ в виде массива из восьми целых положительных чисел uint и номер фрейма в виде целого положительного числа uint.

Метод осуществляет инициализацию регистров обратной связи с учетом ключа и номера фрейма.

Метод не имеет возвращаемого значения.

## 3.3. Получение двух 114-битных последовательностей

Для генерации двух выходных последовательностей для шифрования и дешифрования предусмотрен открытый метод *public void TwoStreams(out uint[] AtoBkeystream, out uint[] BtoAkeystream).*

Этот метод не имеет входных параметров, а работает с текущим состоянием регистров объекта, для которого он вызван.

Метод производит 228 тактов для регистров, управляемых специальным механизмом тактирования, и выводит их конечное состояние в качестве выходных последовательностей.

На выход метод возвращает по ссылкам *AtoBkeystream* и *BtoAkeystream* два массива с выходными последовательностями типа uint. Размер каждого массива – 15 элементов. В первом элементе используются 2 бита, в остальных 14 по 8 битов.

## 3.4. Получение 228-битной последовательности

Для получения одной 228-битной последовательности, применяемой при одностороннем шифровании, предусмотрен открытый метод *public bool[] Stream228()* и открытый статический метод *public static bool[] Stream228(uint[] AtoB, uint[] BtoA).*

Статический метод принимает на вход два массива, полученные от метода *TwoStreams* и формирует из них один массив типа bool.

Нестатический метод выполняет ту же функцию, но применим к объекту-сессии и не имеет входных параметров.

# 4.Входные и выходные данные

## 4.1. Входные данные

uint[] key – сеансовый ключ в виде массива из восьми целых положительных чисел uint.

uint frame – номер фрейма.

## 4.2. Выходные данные

uint[] AtoBkeystream – выходная последовательность для шифрования.

uint[] BtoAkeystream – выходная последовательность для дешифрования.

bool[] Stream228 – выходная «длинная» последовательность для шифрования / дешифрования.

# 5. Сообщения

Так как библиотека написана для использования с корректными входными данными, проверяемыми в основной программе, сообщения об ошибках не предусмотрены.

# 6. Приложения

## 6.1. Список используемой литературы

1. Системные требования для операционных систем Windows ХР [Электронный ресурс] / URL: <https://support.microsoft.com/ru-ru/kb/314865> (Дата обращения 20.02.2015, режим доступа: свободный).

2. A5. Материал из Википедии — свободной энциклопедии [Электронный ресурс] / URL: <https://ru.wikipedia.org/wiki/A5> (Дата обращения 14.04.2015, режим доступа: свободный).

3. Единая система программной документации – М.: ИПК Издательство стандартов, 2000 (ГОСТ 19.504-79).

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Лист регистрации изменений | | | | | | | | | |
| Изм. | Номера листов (страниц) | | | | Всего листов (страниц) в документе | № документа | Входящий № сопроводительного документа и дата | Подпись | Дата |
| измененных | Замененных | новых | аннулированных |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |