*Выполнил студент ПК-12-2, Бекленищев Владислав*

# Описание программы

## Общие сведения

Программа “Aes cipher” является результатом выполнения лабораторной работы для курса “Методы защиты информации” и создана только в учебных целях, для демонстрации зашифровывания / расшифровывания различных текстовых сообщений.

Для запуска программы необходимо следующее программное обеспечение:

* Операционная система Windows 7, 8, 8.1;
* Библиотека .NET Framework версии 4.5.

Данная программа была написана с помощью средств языка C# на платформе .NET Framework в среде Microsoft Visual Studio 2012.

## Функциональное назначение

Приложение предназначено для расшифровывания / зашифровывания текстовых сообщений разной длины с помощью симметричного алгоритма шифрования AES (Advanced encryptional standard).

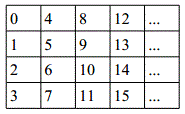
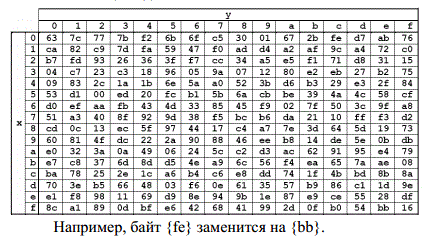
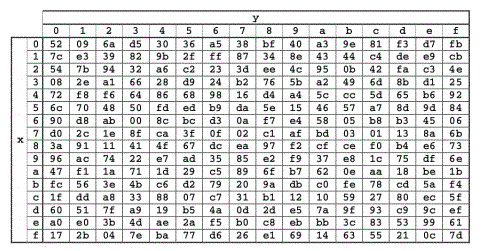
Программа позволяет шифровать используя ключи разной длины (128 бит, 192 бит и 256 бит) при фиксированном размере блока (128 бит).

## Описание логической структуры

Как уже было сказано выше, в основе программы “Aes cipher” лежит алгоритм шифрования AES.

Advanced Encryption Standard (AES), также известный как Rijndael (произносится [rɛindaːl] (Рэндал)) — симметричный алгоритм блочного шифрования (размер блока 128 бит, ключ 128/192/256 бит), принятый в качестве стандарта шифрования правительством США по результатам конкурса AES.

### Важные определения

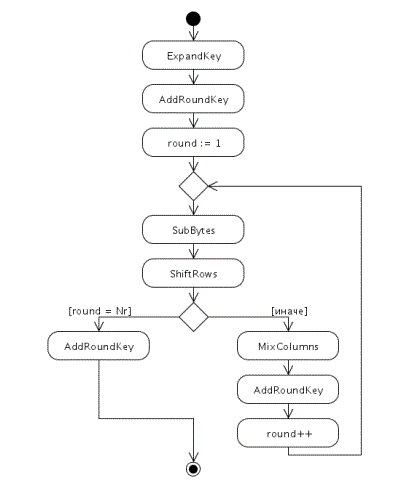
* **State** (форма) - матрица байтов расположенная таким образом:
* **Round** (раунд) - итерация цикла преобразования над State (формой). Чем больше длина ключа, тем больше итераций.
* **Round key** (раундовый ключ) - уникальный ключ, который применяется в каждом отдельном раунде.
* **Sbox** (таблица подстановок) - таблица, которая задаёт отображение одного байта в другой (биективное отображение):
* **InvSbox** (Обратная таблица подстановок) - таблица, которая аналогично SBox, задаёт обратное отображение:

### Этапы шифрования

Шифрование состоит из следующих функций преобразования:

1. ExpandKey — функция для вычисления всех раундовых ключей;
2. SubBytes — функция для подстановки байтов, использующая таблицу подстановок;
3. ShiftRows — функция, обеспечивающая циклический сдвиг в форме на различные величины;
4. MixColumns — функция, которая смешивает данные внутри каждого столбца формы;
5. AddRoundKey — сложение ключа раунда с формой.

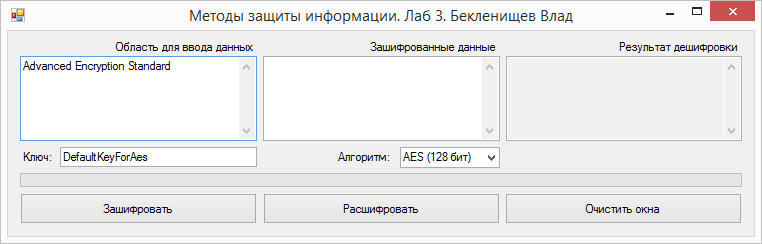
Весь алгоритм шифрования можно отобразить на следующей блок-схеме:



## Вызов и загрузка

Так как программа является приложением под операционные системы Windows 7, 8, 8.1, 10 её можно запустить либо из меню “Пуск” либо же с помощью ярлыка на рабочем столе.

После запуска появится главное окно приложения:



## Входные данные

Входными данными являются текстовые сообщения, которые можно вводить либо в поле “Область для ввода данных” либо в поле “Зашифрованные данные”.

Также пользователю предоставляется возможности самостоятельно ввести значение ключа и выбрать метод шифрования. По умолчанию, в программе ключ имеет длину 16 байт (128 бит), а в качестве метода шифрования выбран 128 битный AES алгоритм. Примечание: при выборе другого значения в комбобоксе “Алгоритм” длина ключа будет либо увеличиваться либо уменьшаться. Таким образом, пользователь может даже не изменять значение ключа - оно будет подстраиваться под выбранный алгоритм.

Если пользователь решит изменить значение ключа вручную, то программа его предупредит если значение ключа будет не соответствовать 16, 24 или 32 байтам. При вводе ключа вручную, его длина **должна** соответствовать выбранному алгоритму:

* Длина 16 символов - должен быть выбран алгоритм AES 128 bit;
* Длина 24 символов - должен быть выбран алгоритм AES 192 bit;
* Длина 32 символов - должен быть выбран алгоритм AES 256 bit;

## Выходные данные

Результатом работы программы будет:

* зашифрованный текст во втором поле (после нажатия на кнопку “Зашифровать”)
* расшифрованный текст в третьем поле (после нажатия на кнопку “Расшифровать”)

Текст в третьем поле будет однозначно соответствовать тексту из первого поля.

Также пользователь может очистить все поля сразу нажав кнопку “Очистить окна”. При этом нужно учесть, что нельзя сделать операции шифрования над пустыми полями (1 и 2). Если пользователь попытается это сделать, программа выдаст предупреждение.