*Finished student PC 12-2 Beklenischev Vladislav*

# Program Description

## General

Program "Aes cipher" is the result of the laboratory work for the course "Methods of protection of information" and created only for educational purposes to demonstrate the encrypting / decrypting the various text messages.

To run the program you need th e following software:

* Windows 7, 8, 8.1,
* Library .NET Framework version 4.5.

This program was written by means of C # on the .NET Framework in the environment Microsoft Visual Studio 2012.

## Functional purpose

Application is designed to decrypt / encrypt text messages of varying length using a symmetric encryption algorithm, AES (Advanced encryptional standard).

The program can encrypt using keys of different lengths (128 bits, 192 bits and 256 bits) with a fixed size block (128 bits).

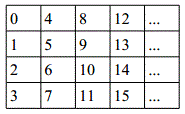
## Description logical structure

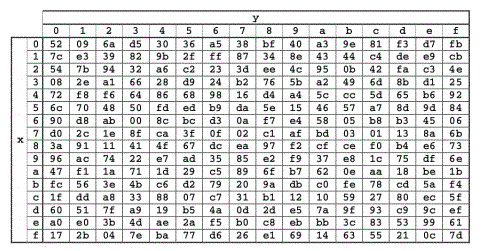
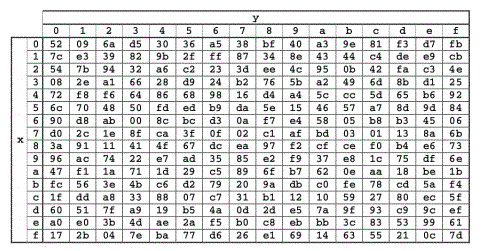
As mentioned above, program "Aes cipher" is based on the AES algorithm.

Advanced Encryption Standard (AES),also known as Rijndael (pronounced [rɛindaːl](Randal)) - it’s a symmetric algorithm block encryption (128-bit block size, 128/192/256 bit key), adopted as an encryption standard by the US government as a result of competition AES.

### Important definitions

* **State (form)** - matrix of bytes located



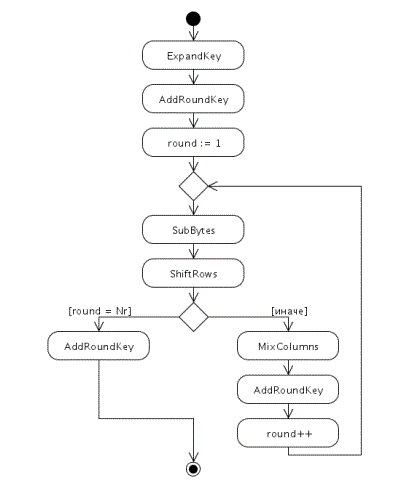
* **Round** - iteration of the transformation of the State (the form). The longer the key, the more counts of iterations.
* **Round key** - the unique key that is used in each round.
* **Sbox** (table permutations) - is a table that defines the mapping of bytes to another (bijection) 
* **InvSbox** (inverse table substitutions) - table which is similar to SBox and sets the inverse mapping:

### Steps for encryption

Encryption consists of the following conversions:

1. ExpandKey - function to compute all round keys;
2. SubBytes - function to insert bytes, using substitutions table;
3. ShiftRows - function, providing cyclic shift in the form for various values;
4. MixColumns - function that mixes the data within each column of the form;
5. AddRoundKey - the addition of a key round to the form.

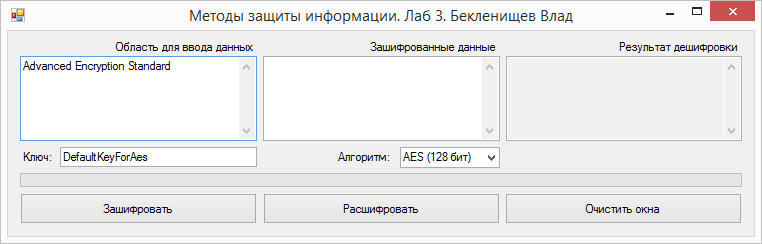
All the encryption algorithm can be displayed in the following flowchart:



## Call and load

The program is an application for Windows operating systems 7, 8, 8.1, 10. It can be run from the "Start" menu or by using the shortcut on the desktop.

After starting the main application window will appear:



## Input

Input data are text messages that can be administered in the field "Field data entry" or in the field "encrypted data".

Also, the user can manually enter the value of the key and select the encryption method. By default, the program key has a length of 16 bytes (128 bits), and as the encryption method selected 128-bit AES algorithm. Note: when you select a different value in the combo box "algorithm" key length will increase or decrease. Thus, the user can leave the key value as it was - it will adapt to the selected algorithm.

If the user decides to change the key manually, the program will warn him if the key value will not match the 16, 24 or 32 bytes. When the user enter the key manually, key’s **length** mustmatch the chosen algorithm:

* Length 16 characters - must be selected the “AES 128-bit” algorithm;
* Length 24 characters - must be selected the “AES 192 bit” algorithm;
* Length 32 characters - must be selected the “AES 256-bit” algorithm;

## Output

Result of the program will be:

* encrypted text in the second field (after pressing the "Зашифровать")
* decrypted text in the third field (after you clicking the “Расшифровать”)

The text in the third field will be correspond to the text of the first field.

The user can clear all fields at once by clicking the "Очистить окна". It should take into account that you can not make encryption operations over the empty fields (1 and 2). If a user attempts to do this, the program will give a warning.