# Introduction

This document describes the AES practical assignment for the course CRY.

# Software

Use the Visual Studio project CryAes (available on Sharepoint) as a starting point.

Short description of the classes:

* Key  
  the constructor implements the complete Key Schedule, and the Cipher Key and all Round Keys are available in property w  
  w is a 2-dim array; it has dimensions 4x44 for a 128 bit key, this represents the Cipher Key + 10 Round Keys. The layout of w is similar to slide 20 of Rijndael\_Animation\_v4\_eng.swf  
  no code has to be written for this class
* State  
  it contains the 4x4 byte state, together with the operations on a state  
  the encryption operations are already implemented, the decryption operations have to be written
* Sbox  
  contains the sbox, which is already initialized  
  code for the inverse sbox has to be written
* FormAes  
  a very simple GUI  
  it shows how a key in hexadecimal notation can be given, and how a message in ascii characters can be given  
  the test button prints the given key and the message in the Console  
  you have to extend the GUI according to your wishes
* UnitTestAes  
  module with only a few unit tests  
  you can extend it with your test cases

Data bytes are represented in hexadecimal notation because this facilitates the checking of all bitwise operations. Please refresh your binary and hexadecimal knowledge if you are less familiar with the notations.

# Assignment

To get a grade 6, the minimum functionality that your application offers is the following:

* full functional encoding and decoding of one block (16 bytes) with a 128 bits key in Electronic CodeBook mode

For a higher grade, the following enhancements are possible:

* longer data (e.g. a file containing a bitmap (where the header is not encrypted so it still can be viewed))
* 192 and 256 bit keys
* block cipher modes CBC, CFB and CTR (where your application shows their advantages and disadvantages as well)
* parallelism (e.g. with threads)
* ... (your own features)

# Testing

There are various online tools available such that you can check your hexadecimal result of your own plaintext encryption with your own key (and the decryption as well of course). We believe that the following sites give good results:

* <http://aes.online-domain-tools.com/>   
  (note: the CFB mode gives different results; it is because this site implements a CFB-8 mode, while our assignment has a CFB-128/192/256 mode)
* <http://www.inconteam.com/software-development/41-encryption/55-aes-test-vectors>

# Delivery

To be delivered in Canvas:

* source code of the project
* additional document describing your tests and your add-ons