

An 8086 Implementation of a 128bit Advanced Encryption Standard (AES) **(Deadline:)**

The **Advanced Encryption Standard** or **AES** is a symmetric block cipher used by the U.S. government to protect classified information and is implemented in software and hardware throughout the world to **encrypt** sensitive data. The AES operates on a 128 bit bursts as well as 128 bits key. The complete standard is shown in the document below:

<http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf>

Also a good description for the standard is shown in this flash video:

https://formaestudio.com/rijndaelinspector/archivos/Rijndael_Animation_v4_eng-html5.html

Project Requirements

The implementation of one cycle of AES algorithm as follows:

- 1) Build two Procedures based on interrupts that reads 128 bits from the user and prints the result on the screen. (Not covered in lecture yet)
- 2) Use Macros to implement **SubBytes()**, **ShiftRows()**, **MixColumns()**, **AddRoundKey()** modules, all work on 128 bits.
- 3) **MixColumns** is a bit tough, and needs extra work its clear description is available in this document. Try to start with others first to get better feeling:
http://www.angelfire.com/biz7/atleast/mix_columns.pdf
- 4) Your main program should use the above Macros and subroutines to read the data from the user and finalize 10 stages of AES and print the result on the screen.
- 5) For groups of 4 students, we need to build the Key Schedule as well. Groups smaller than 4 (it will be considered a bonus to build it)
- 6) The usage of EMU8086 as an emulator for this project is encouraged if you prefer using any other 8086 emulator it is acceptable:
<http://www.emu8086.com>
- 7) Please use the KEY & INPUT that is provided by the Standard as your test case.