An 8086 Implementation of a 128bit Advanced Encyption Standard (AES)
(Deadline: 4/12/2019)

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:
http://www.formaestudio.com/rijndaelinspector/archivos/Rijndael_Animation_v4_eng.swf

Project Requirements

The implementation of one cycle of AES algorithm as follows:

1) Use Macros and Procedures based on interrupts that reads 128 bits from the user and prints the result on the screen.
2) Use Macros & Procedures to implement **SubBytes(), ShiftRows(), MixColumns(), AddRoundKey()** modules, all work on 128 bits.
3) Your main program should use the above Macros and procedures to read the data from the user and perform **10** AES cycles and print the result on the screen
4) For the first cycle in AddRoundkey module consider the key of **FF FF FF FF FF FF FF FF FF FF FF FF.** For the rest of the cycles, you should generate the keys.
5) **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
6) The usage of EMU8086 as an emulator for this project is encouraged if you prefer using any other 8086 emulator it is acceptable: https://download.cnet.com/Emu8086-Microprocessor-Emulator/3000-2069_4-10392690.html
7) The project consists of groups of **4** students.