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

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) 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) For the AddRoundkey module consider the used key of **FF FF FF FF FF FF FF FF FF FF**
4) **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
5) Your main program should use the above Macros and subroutines to read the data from the used and finalize ONE AES cycle and print the result on the screen.
6) For groups of 3 or 4 students, we need to build the whole 10 stages of AES using the above module. (mainly Extra loops and control work needed) (Bonus for smaller groups)
7) 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