Faculty of Information Engineering and Technology

(IET)

CSIS 402 Computer Organization & system programming

Project

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

(Deadline: 8/12/2024)

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

Requirements

Implement 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.
2) Use Macros to implement **SubBytes() and ShiftRows()** modules, all work on 128 bits.
3) Use Macros to implement one cycle of **MixColumns() and AddRoundKey()** modules, all work on 128 bits.
4) For the AddRoundkey module consider the used key of **F F F F F F F F F F F F F F F F.**
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) Your main program should use the above Macros and subroutines to **read the data from the user, finalize 10 stages of AES and print the result on the screen.**

- **Teams Submission (Deadline 7/11/2024)**
  https://docs.google.com/forms/d/e/1FAIpQLSejVDfKub8XaouINcepS_N5So5VOZHVNRpewlssu0Hb1_K-WA/viewform?usp=sf_link

- **Milestone (1): (Deadline 23/11/2024)**
  SubBytes() and ShiftRows() modules without macros, procedures or interrupts.

- **Milestone (2): (Deadline 8/12/2024)**
  The rest of the requirements

Remarks:

- The usage of **EMU8086** as an emulator for this project is encouraged (available online). If you prefer using any other 8086 emulators, it is acceptable.
- Groups up to 4 members (maximum) are acceptable.
- Groups could have members with different TAs.
- Evaluation method will be announced later.