UNLV
HOWARD R. HUGHES
COLLEGE OF
ENGINEERING

# AES Encryption/Decryption
## (Hardware)

Dayton Flores
Joseph Sharp Halpin
Advisor: Dr. Ming Zhu

## Introduction:

AES (Advanced Encryption Standard) is a subset of the Rijndael block cipher, and it was established by the U.S. NIST (National Institute of Standards and Technology) in 2001. This algorithm can work with differing key lengths of 128, 192, or 256 bits. It is a symmetric-key algorithm, meaning it uses the same key for both encryption and decryption. AES replaced DES (Data Encryption Standard) as the NSA-approved federal government standard in 2002.

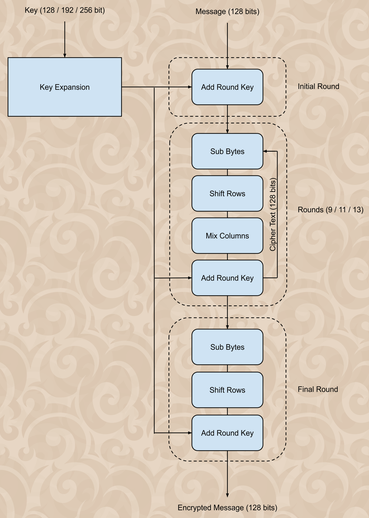
## Motivation:

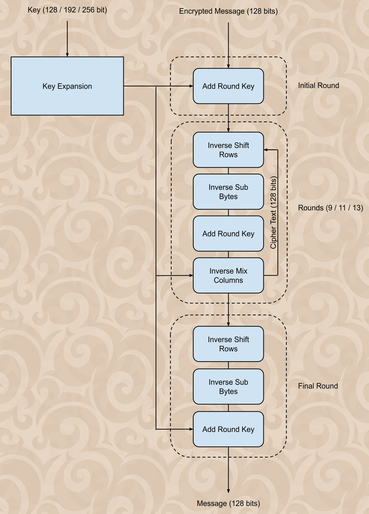
AES is traditionally applied in software due to its ease of implementation. Administering in hardware requires complex analysis, but is beneficial due to the following: more efficient (AES module is independent of CPU), much safer (key is built directly into hardware), and substantially faster (with a fast enough clock speed).

## Monetization:

If converted into an IC, this synthesis could be mass produced using an RNG (random number generator) for each key & sold for ≈ $1 each (based on current market).

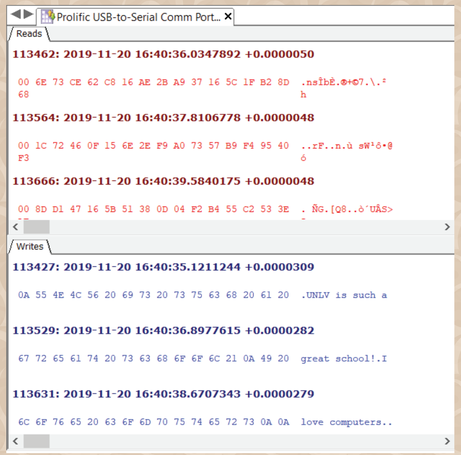
## AES Algorithm:

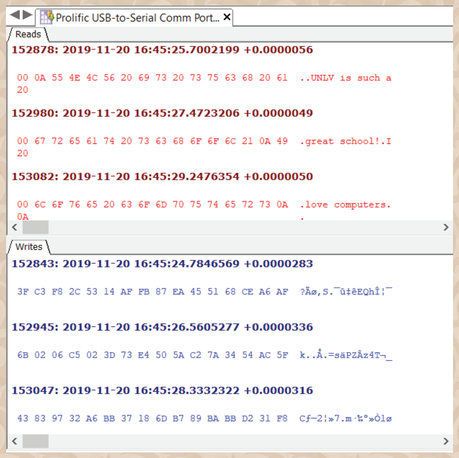



## Encrypt/Decrypt:

The user gives the AES module three inputs: key length (128 / 192 / 256 bits), actual key (128-bits), and a block of data (16 bytes). The Key Expansion module will create an expanded key (based on the key length) of sizes: 1408-bits, 1664-bits, or 1920-bits. Add Round Key will XOR the block of data with 128-bits of the expanded key. Sub Bytes will use the lower 4 bits of each byte as a column parameter and the upper 4 bits of each byte as a row parameter. Shift Rows will rotate each column down by n bytes. Mixed Columns will use matrix multiplication on each row. Sub Bytes and Mix Columns use given matrices for calculations. Decryption uses the same steps but with different given matrices for calculations. The Initial Rounds of encryption and decryption only use Add Round Key. The Final Rounds of encryption and decryption don't use Mixed Columns.




## Future Improvements:

Given more time, we would have also implemented an external server (using Raspberry Pi) to send and receive the encrypted files via internet. We would have also interfaced our FPGA with an Arduino (or any other microcontoller) to allow for file transfer via Bluetooth, WiFi, and SPI (e.g. SD card). We also would have fabricated the AES algorithm onto an IC (integrated circuit).

## Technical Details:

Our entire AES was implemented with Verilog 2001, Quartus v16.1, while using an Altera DE2-115. The AES synthesis requires 24,375 logic elements, 3,605 registers, 8 user I/O, and 8,192 memory bits. The program used for file transfer was coded in C++ 17 and used Code-Blocks IDE v17.12. We used an external library to handle serial port communication called "SerialPort.h".

## Conclusion:

Both being Computer Engineering majors, this project helped us learn about cryptography and file security. We gained valuable experience using FPGAs and serial communication.