Project Title: AES Encryption/Decryption

Team members: Anna Griffin, Grace Montagnino

Description of project: (1-3 paragraphs)

The Advanced Encryption Standard (AES) is a block cipher implemented in hardware and software that is the default algorithm used to protect information. The algorithm uses the same key for encrypting and decrypting (symmetric key), thus requiring that the sender and receiver both know the code. The algorithm works by first expanding the given key using Rijndael's key schedule and then using a "XOR" to add the round key to message. Then it launches into rounds of the following steps: it takes the numerically represented data and substitutes in values from a substitution table; next it shifts the rows of data, before next mixing the columns; finally a "XOR" is used on each column with a different part of the encryption key to again add the round keys. The shift rows and mix columns work to just add another layer of complication to the encryption by transforming both vertically and horizontally. The substitution changes the data in a non-linear way to add further complicate the relationship between the message and the ciphertext. Finally, the key expansion/xor step allows the algorithm to be harder to crack by generating a different round key to add during each round.

Data encryption in hardware has advantages over implementing it in software. The processor is able to execute tasks simultaneously which improves the speed and efficiency of the encryption process. Additionally, having hardware dedicated to encryption, it is less susceptible to getting hacked by software, adding a layer of protection. The design and architecture of AES is very relevant to what is happening around us today and faults in it can have major consequences.

For this project, we want to explore AES to get a better understanding of its significance and to learn how it works. It is used by the US government as a standard as well as many other countries. Using what we have learned thus far in this course, we want to get a good grasp on the encryption process and try to implement it.

References: (2 to 3)

https://www.comparitech.com/blog/information-security/what-is-aes-encryption/

https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf

https://searchsecurity.techtarget.com/definition/Advanced-Encryption-Standard

https://www.researchgate.net/publication/261459636_Successful_implementation_of_AES_algorithm_in_hardware

https://iopscience.iop.org/article/10.1088/1757-899X/263/5/052030/pdf

https://pdfs.semanticscholar.org/f63b/c7fa269a15c2fce294e3f9fea2ac98ed2c9a.pdf

Deliverables plan:

> **Minimum:** Thorough research paper and schematics of how to implement AES and the circuit needed/explained in a walk through.
>
> **Planned:** Verilog Implementation of AES + report
>
> **Stretch:** FPGA + verilog + report

Work Plan:

11/19 Update work plan after meeting with Ben during class

11/22 Have finished initial research, begin looking at how to implement this

11/25 - 11/29 Write draft of report, start outlining poster

12/4 Have a circuit diagram/plan for implementation in verilog

12/9 Finish verilog by today, finalize report, and finalize presentation plan

12/10 Project DUE