AES

ECE 3300

By: Jason Moya, Bianca Chavez, Kathleen Mach, Ramiro Ascencio

What is AES?

- The Advanced Encryption Standard (AES)
  - serves to provide robust and secure encryption standards for the information exchanged, and serves to protect the integrity of sensitive information.
  - symmetrical block cipher algorithm
- The response to the Data Encryption Standard (DES), which was the main form of encryption
  - striving to improve on what DES falls short on, to becoming a standard in cryptography.
- Uses plain text in blocks of 128 bits and converts them to ciphertext using keys of 128, 192, and 256 bits.
  - 128 bit key is 10 rounds, 192 bit key is 12 rounds, and 256 bit key is 14 rounds

History of AES

- AES is a crucial development of cryptography in the early 2000s
- Main purpose of its development is to replace Data Encryption Standard (DES) when National Institute of Standards and Technology (NIST) requested it in the 1970s
- One of the block cipher encryption algorithm that was published by National Institute of Standards and technology (NIST)
- First examples of open collaboration in cryptographic standard selection
- It was adopted fairly easily in symmetric key cryptography by both government and private sector applications.
    - various applications like secure file transfer protocols, VPNs, disk encryption systems, and more

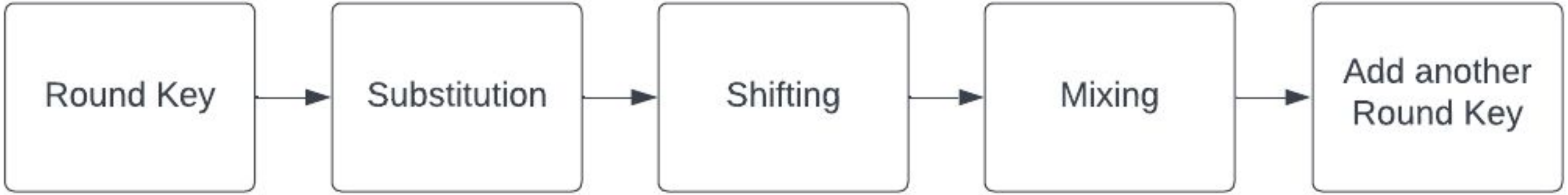
Nexys A7 Board

- Nexys A7 is a powerful and versatile FPGA (Field-Programmable Gate Array) board.
    - Its main features are its processing speed, memory capacity, and I/O options.
- AES involves numerous operations that can be processed in parallel. The Nexys A7, excels in parallel processing, allowing multiple stages of AES to be processed simultaneously. This capability significantly speeds up the encryption and decryption processes compared to sequential processing used in traditional CPUs.
- Advantages
    - AES on the Nexys A7 allows for significant customization.
        - Able to choose specific version of AES, whether it's AES-128, AES-192, or AES-256.
- Real-World Applications
    - Nexys A7 can be tested and upgrading any kind of AES implementation in real-time.
        - Crucial for performance tuning and debugging, allowing you to optimize the encryption process and ensure it meets the required security standards.

AES Uses

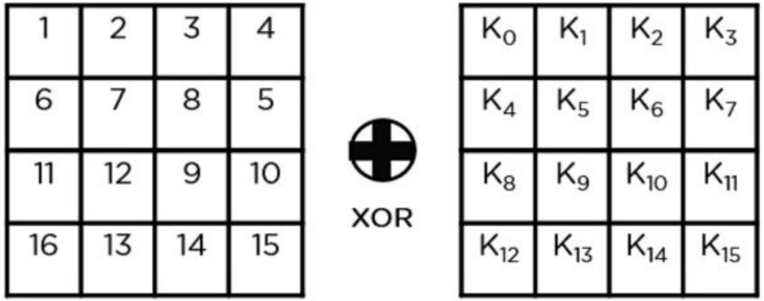
- AES is used to encrypt data
    - Self-encrypting disk drivers
    - Database encryption
    - Storage encryption
    - Secure Communication
- Used by many in the private sector
    - NSA to secure their systems
    - Military their technology that is used in the field
- Used by big corporations
    - Google’s cloud network
    - AWS network
    - Oracle to store data
    - IBM in their data privacy

Steps Of AES


Round Key
Substitution
Shifting
Mixing
Add another Round Key

Round Key

- First step of AES
- Round keys play a crucial role in the effectiveness of the entire encryption process.
- Before undergoing the AES algorithm, the plaintext is converted into Hex. In each round, the round key is XORed to the current state by using the operation, AddRoundKey.
- Takes the state array from the text, and performs an XOR operation of the state array to pass onto the next step of substitution where the AES algorithm starts.
- After the Mixing step, the current state array is XOR'd with the previous key and then repeats until the last round where the resulting roundkey becomes the ciphertext.



1	2	3	4
6	7	8	5
11	12	9	10
16	13	14	15

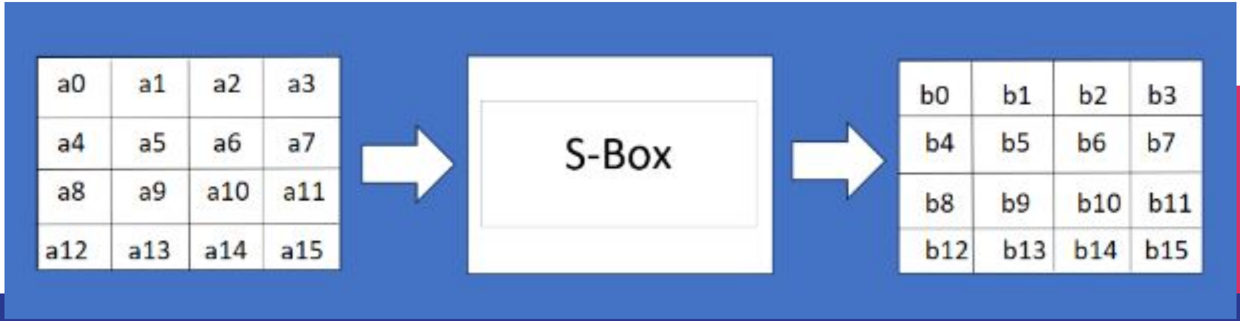
$\oplus$

XOR

K_0	K_1	K_2	K_3
K_4	K_5	K_6	K_7
K_8	K_9	K_{10}	K_{11}
K_{12}	K_{13}	K_{14}	K_{15}

Substitution

- The next step in the AES process which helps with the encryption process by changing the bytes in the array which helps with the encryption portion of AES.
- It takes the state array from the past step and transforms every byte independently in the past state array into a hexadecimal byte for the encryption.
  - Uses the AES lookup table that takes the bytes into it and transforms it into another state array
- It can help with making it more difficult for people to hack into the system.
  - Has a s-box which is a lookup table that is created by an algorithm to create confusion if it gets attacked

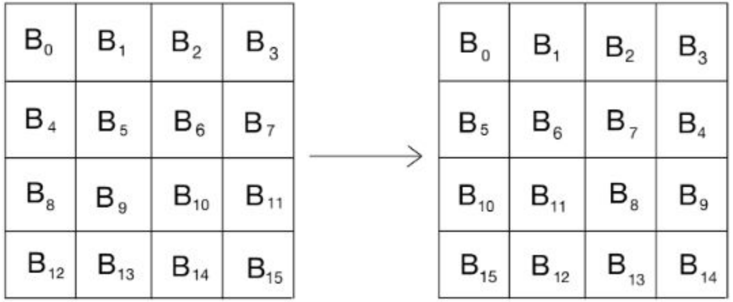


a0	a1	a2	a3
a4	a5	a6	a7
a8	a9	a10	a11
a12	a13	a14	a15

b0	b1	b2	b3
b4	b5	b6	b7
b8	b9	b10	b11
b12	b13	b14	b15

Shifting

- The third step of AES
- The main purpose of this step is to shuffle the bytes within each row to increase the confusion and complexity between the input and output.
- This procedure is done by shifting the rows in the array to the left. Each row holds bytes which are shifted a particular number of times.
- The first row is always unchanged, while the consecutive rows are shifted
    - For example, the second row is shifted once to the left, the third is shifted twice, the fourth is shifted three times, and the pattern continues depending on the number of rows in the system.
- After each shift in the row, there is a new arrangement of bytes that can prevent the attacker from recognizing patterns.

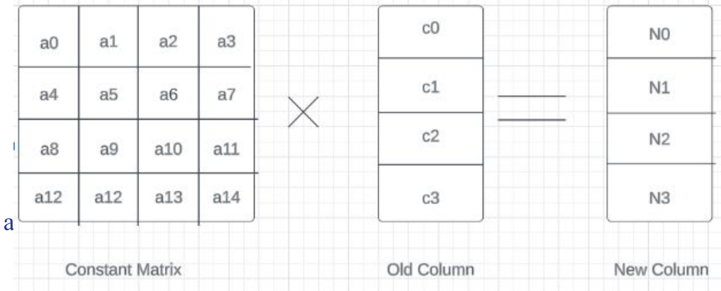


B_0	B_1	B_2	B_3
B_4	B_5	B_6	B_7
B_8	B_9	B_{10}	B_{11}
B_{12}	B_{13}	B_{14}	B_{15}

B_0	B_1	B_2	B_3
B_5	B_6	B_7	B_4
B_{10}	B_{11}	B_8	B_9
B_{15}	B_{12}	B_{13}	B_{14}

Mixing

- The next process of the AES is mixing which mixes up the bytes in each column to get a new column from the current state array which can help with encryption in systems.
- This helps with creating more confusion by multiplying the column of the array with a matrix that will create a new state array for the system
    - ○ Produces these new values for the state array by using the XOR to get the new bytes of each column.
- The mixing step helps with taking arrays into a multiplication step with a matrix which is made with a four term polynomial.
- Every column is put into through the matrix helps create another layer of security to help with securing the system and making it a lot more difficult to solve the key for the system.
- The process of mixing the column gives more complexity since a small input of the byte can influence a whole column in the array
    - ○ By creating this new state array for the security of the system it is used for the final step of AES



a0	a1	a2	a3
a4	a5	a6	a7
a8	a9	a10	a11
a12	a12	a13	a14

Example:

Let’s say we want to encrypt this line:

“Two▽One▽Nine▽Two”

In ASICII:

T	W	O	▽	O	N	E	▽
54	77	6F	20	4F	6E	65	20

N	I	N	E	▽	T	W	O
43	69	6E	25	20	54	77	6F

As a Matrix:

$$\begin{bmatrix} 54 & 77 & 6F & 20 \\ 4F & 6E & 65 & 20 \\ 43 & 69 & 6E & 25 \\ 20 & 54 & 77 & 6F \end{bmatrix}$$

Example continued:

Using this encryption key:

“Thats▽my▽kung▽fu”

In ASICII:

T	H	A	T	S	▽	M	Y
54	68	61	74	73	20	6D	79
▽	K	U	N	G	▽	F	U
20	4B	75	6E	67	20	46	75

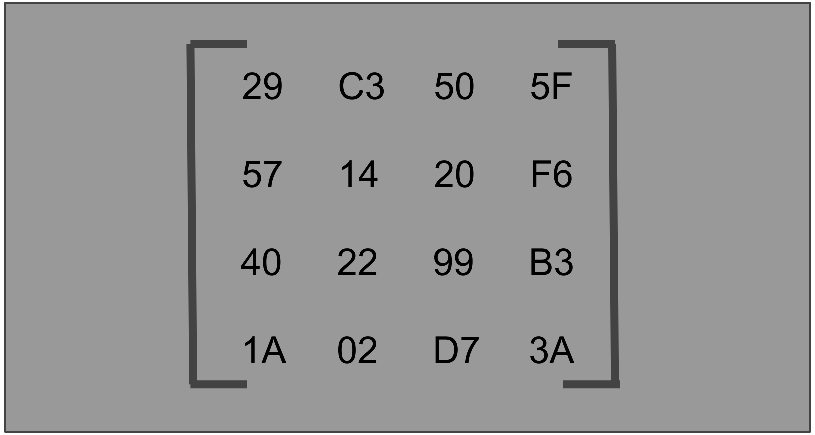
In Plain Text:

$$\begin{bmatrix} 54 & 68 & 61 & 74 \\ 73 & 20 & 6D & 79 \\ 20 & 4B & 75 & 6E \\ 67 & 20 & 46 & 75 \end{bmatrix}$$

Example continued:

Result after Round 10:

In Plain Text:



$$\begin{bmatrix} 29 & C3 & 50 & 5F \\ 57 & 14 & 20 & F6 \\ 40 & 22 & 99 & B3 \\ 1A & 02 & D7 & 3A \end{bmatrix}$$

Conclusion

- In our project, we successfully implemented the Advanced Encryption Standard (AES) using Verilog on the Nexys A7 board.
- Round Key Generation: Enhances encryption strength.
- Data Substitution: Increases complexity.
- Shifting & Mixing Columns: Further secures encryption.
- Employed Nexys A7's VGA output to dynamically display each step of the AES encryption process.
- Significantly strengthens data protection in the digital era through robust AES encryption.
- Represents a milestone in integrating hardware (Nexys A7) with advanced cryptographic methods.
- Sets a foundation for further innovations in hardware-based encryption and cybersecurity education.