

Names: Yasar Azimi, Shahzada Masood Asir, Maryam Zakare

Group Project

Dr.Abdalrahman Alfagi

Class: ITC 370

2023/12/13

**Table of Contents**

**Introduction ---------------------------------------------------------------------------------------- Page 3**

**Main Body ---------------------------------------------------------------------------------------- Page 3**

**Add Round key ---------------------------------------------------------------------------------------- Page 3**

**Substitue Key ---------------------------------------------------------------------------------------- Page 4**

**Shift Rows ---------------------------------------------------------------------------------------- Page 6**

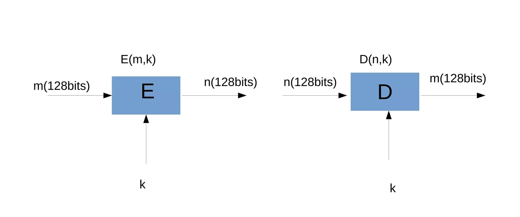
**Mix Columns ---------------------------------------------------------------------------------------- Page 7**

**Add Round Key ---------------------------------------------------------------------------------------- Page 8**

**Introduction:**

AES (Advanced encryption standard) a symmetric block cipher adopted by NIST in 2001, was designed to replace DES as the approved standard for a wide range of applications. It is characterized by its complex structure and stronger security base. AES is a private key symmetric block cipher, operating on 128-bit data with key lengths of 128, 192, or 256 bits, and it is stronger and faster than Triple-DES. The number of rounds in encryption and decryption depends on the key length:

1. 128-bit key: 10 rounds
2. 192-bit key: 12 rounds
3. 256-bit key: 14 rounds



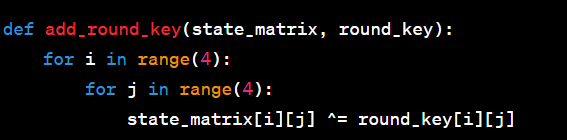
With real-world implementations ranging from VPNs to web browsers, AES plays a vital role in securing digital communications. AES treats the 128 bits of a plaintext block as 16 bytes, allowing for efficient processing. AES is much more powerful and faster, which is why its used in WIFI, OS system, Web browser, Mob Applications. The number of encryption and decryption rounds varies based on the chosen key length, demonstrating the adaptability and robustness of the algorithm.

**Main Body:**

In this project we are going to be studying in details the different steps involved in AES Transformation, the five main steps: Add Round Key, Substitute Bytes, Shift Rows, Mix Columns, and Add Round Key. Below is a detailed explanation of each step along with a flowchart and code snippets

1. **Add round key**:

In this step, each byte of the state matrix is XOR’ed with the corresponding byte from the round key. This step involves adding a layer of security by introducing the round key, derived from the original key, to the state matrix. So basically XOR each byte of the state matrix with the corresponding byte of the round key, and the round key is taken from the main/original encryption key using a key schedule/matrix/algorithm.

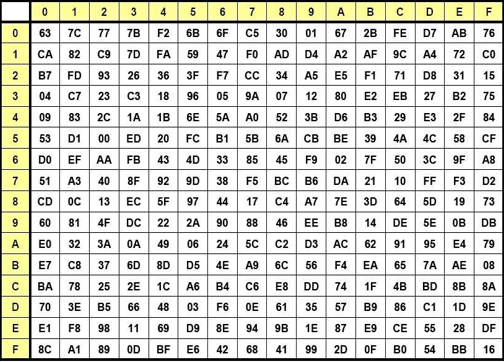


1. **Substitute bytes**:

This step involves replacing each byte in the state matrix with its corresponding value in the S-Box, a predefined substitution table. The Substitution provides non-linearity to the algorithm, enhancing its resistance to cryptographic attacks. In this step we have a 16 x 16 matrix of byte values, called an S-box, which contains a permutation of all possible 156 8-bit values.

Each individual byte of State is mapped into a new byte where:

1. Leftmost 4 bits of the byte 🡪 Row value
2. Rightmost 4 bits of the byte 🡪 column value

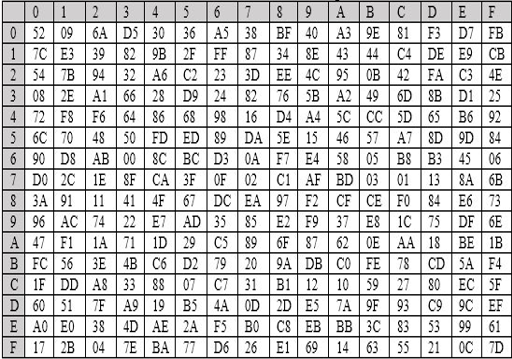


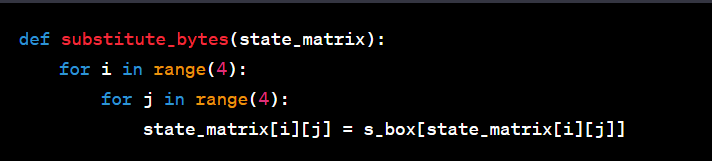
Example:

 🡪  🡪



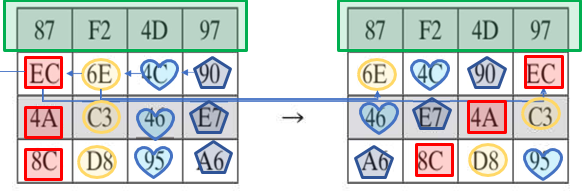
For the Decryption process we use the inverse S-box while the operation is the same.



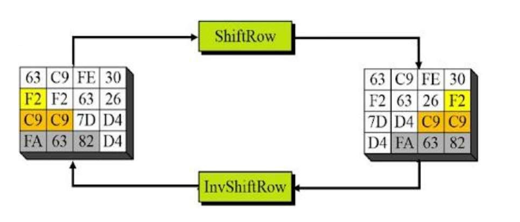


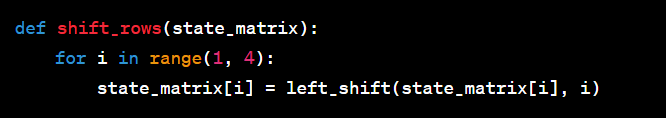
1. **Shift rows**

In this step, each row in the state matrix is shifted to the left by a certain offset, while the offset is determined by the row index. The first row is not shifted, the second row is shifted by one position to the left, the third row by two positions to the left, and the fourth row by three positions to the left. Shifting the rows ensures that each byte influences multiple bytes in the next round, contributing to diffusion.



For the decryption we use the inverse shift row transformation, called InvShiftRows, in the inverse transformations, the first row is not shifter, the second row is shifted by one to the right, the third row is shifted by two positions to the right, and the fourth row is shifted by three positions to the right.

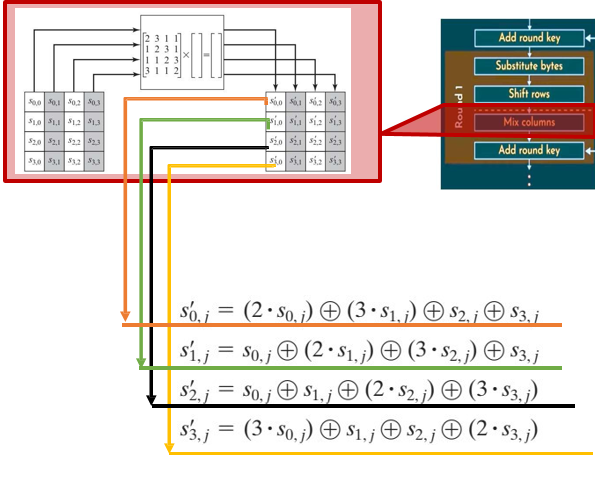


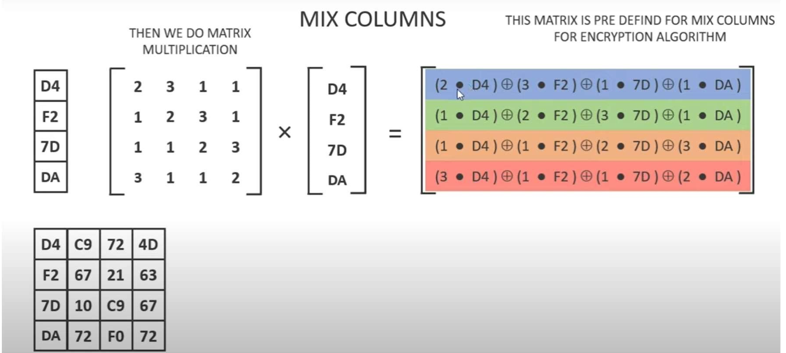


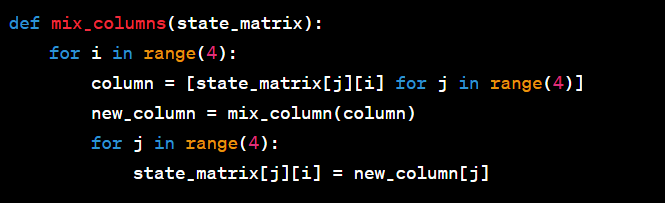
1. **Mix columns:**

This step introduces mixing and diffusion by combining the values in each column through matrix multiplication. It Mix’s the columns of the state matrix using a fixed matrix multiplication, and each column is treated as a polynomial and multiplied in the Galois Field. And just like row-shift it has a forward and an inverse.

1. The forward mix column transformation, called MixColumns Forward Transformations:
2. Each byte of a column is mapped into a new value that is a function of all four bytes in that column,
3. The transformation can be defined by the matrix multiplication on State.



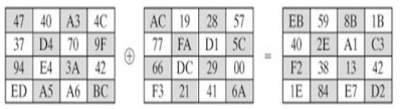


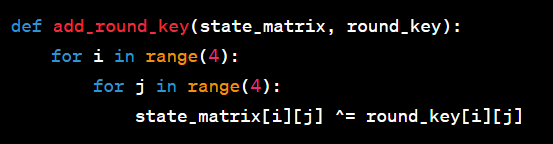


1. **Add round key**

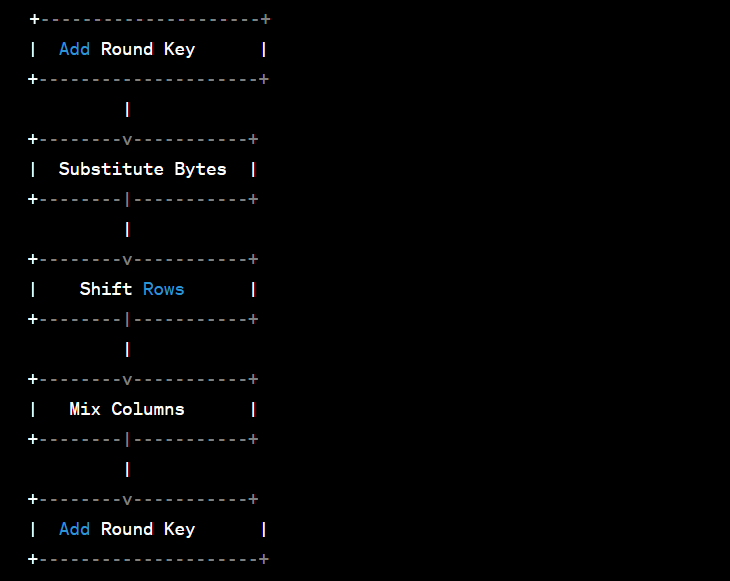
The final application of the round key ensures that each byte in the state matrix is influenced by the key at least twice, providing added security. Similar to Step 1, XOR each byte of the state matrix with the corresponding byte of the round key. And we have a Forward and Inverse Transformation for this round as well:

1. In the forward add round key transformation, called AddRoundKey, the 128 bits of State are bitwise XORed with the 128 bits of the round key.





**Flow chart:** This flowchart represents the logical flow of the AES single-round implementation.



**Conclusion:**

Implementing a single round of the Advanced Encryption Standard (AES) involves a sequence of steps: Add Round Key, Substitute Bytes, Shift Rows, Mix Columns, and a final Add Round Key. These steps collectively introduce non-linearity, confusion, and diffusion in the encryption process. The Add Round Key step XORs the state matrix with the encryption key, creating a unique combination. Substitute Bytes replaces each byte with values from a substitution table, enhancing non-linearity. Shifting Rows and Mixing Columns introduce diffusion through horizontal and mathematical operations, respectively.

The final Add Round Key operation ensures key material is recombined, reinforcing the encryption. The provided flowchart visually represents the logical flow. Note that the code snippets are illustrative, and a complete implementation requires additional functions and constants. The strength of AES lies in the combination of these steps across multiple rounds, providing a secure encryption scheme.