Assignment 4: AES Process Explanation

SubBytes:

This step involves a non-linear substitution where each byte is replaced with another according to a fixed table, the S-box. It provides security against attacks by making the relationship between the plaintext and the ciphertext complex.

ShiftRows:

This operation provides diffusion in AES. Bytes in each row of the state are shifted cyclically to the left. The number of positions each row is shifted varies; the first row is not shifted, the second row is shifted one position, the third two positions, and the fourth three positions.

MixColumns:

This transformation treats each column of the state as a four-term polynomial. These columns are multiplied modulo x^4+1 with a fixed polynomial 03x^3 + 01x^2 + 01x + 02, which mixes the bytes within each column.

AddRoundKey:

Each byte of the state is combined with the round key using bitwise XOR. This step adds the key into the AES process. The round keys are derived from the initial AES key using the key schedule.

SubBytes:

This step involves a non-linear substitution where each byte is replaced with another according to a fixed table, the S-box. It provides security against attacks by making the relationship between the plaintext and the ciphertext complex.

ShiftRows:

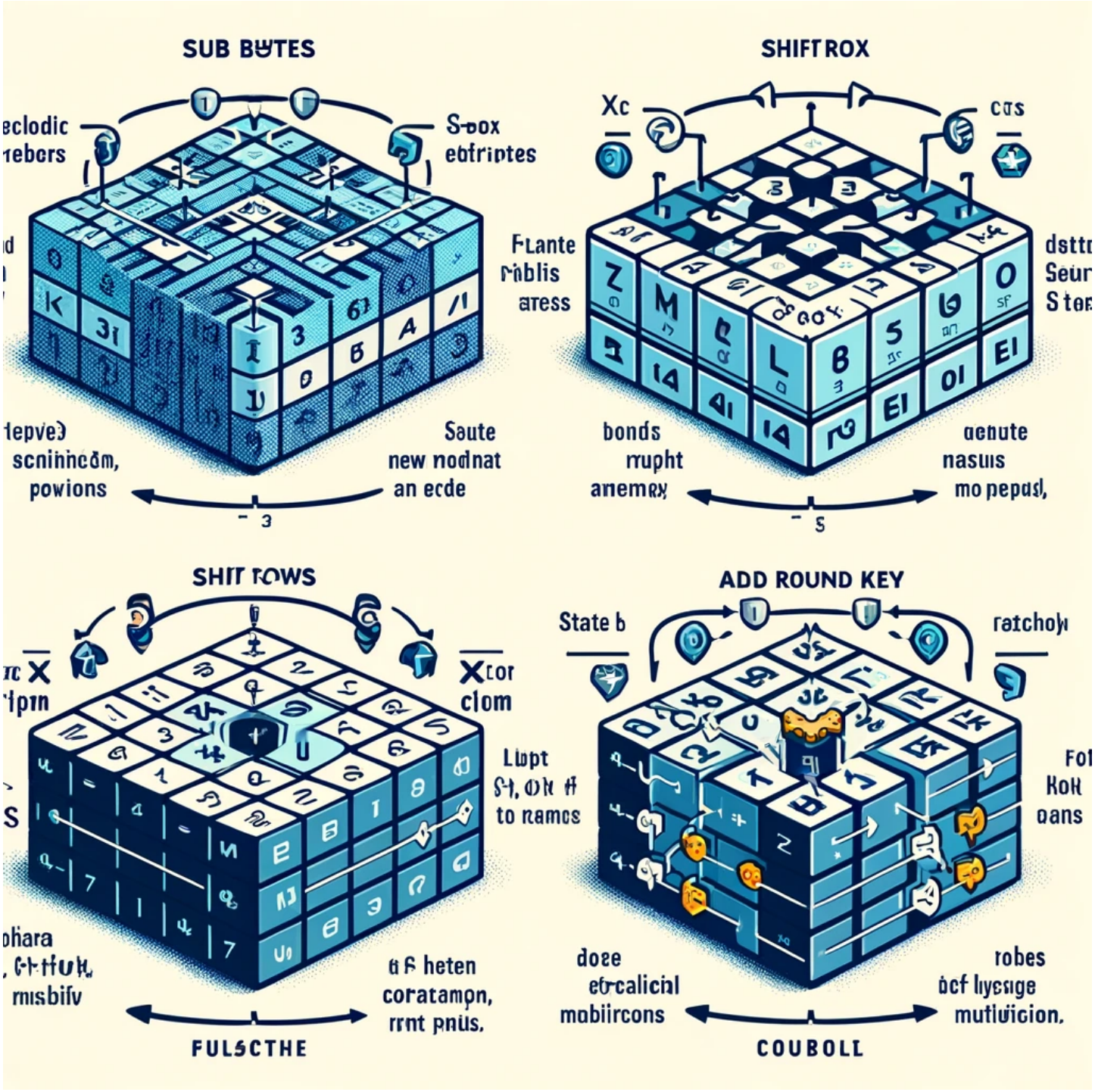
This operation provides diffusion in AES. Bytes in each row of the state are shifted cyclically to the left. The number of positions each row is shifted varies; the first row is not shifted, the second row is shifted one position, the third two positions, and the fourth three positions.

MixColumns:

This transformation treats each column of the state as a four-term polynomial. These columns are multiplied modulo x^4+1 with a fixed polynomial 03x^3 + 01x^2 + 01x + 02, which mixes the bytes within each column.

AddRoundKey:

Each byte of the state is combined with the round key using bitwise XOR. This step adds the key into the AES process. The round keys are derived from the initial AES key using the key schedule.


SUB BYTES
SHIFT ROX
SHIFT ROWS
ADD ROUND KEY
COUBOLL