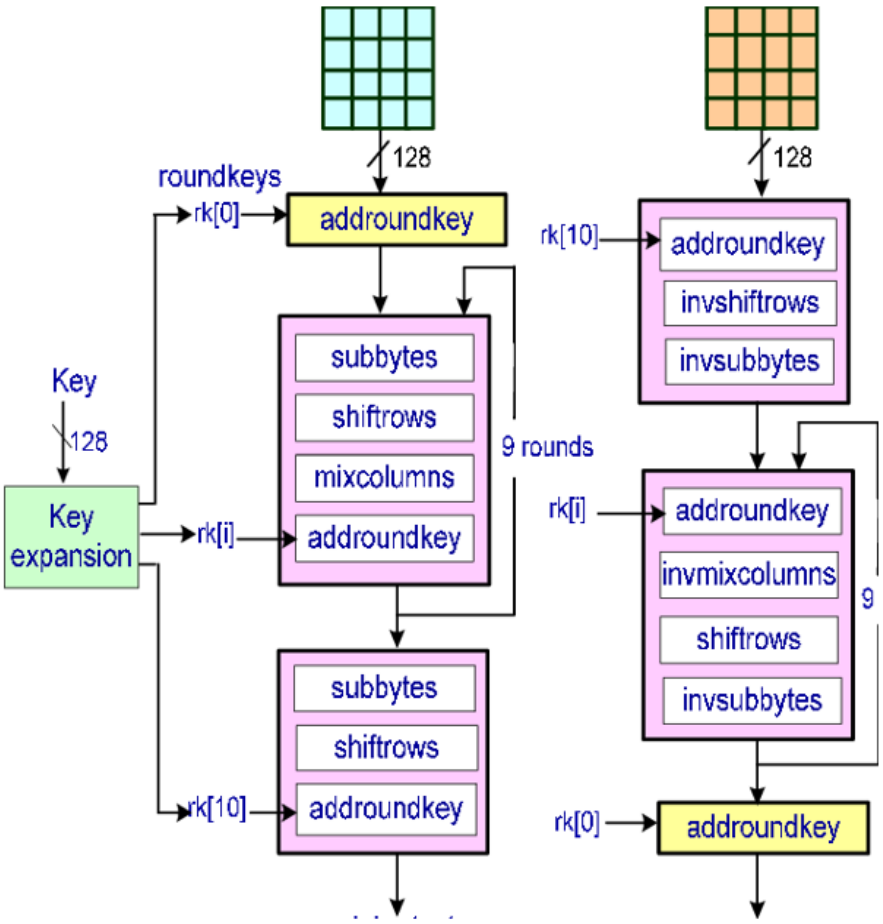
Assignment 1: Symmetric Cryptography

The advanced Encryption Standard, is also known by its original name Rijndael. In Advanced Encryption Standard, inputs are parsed in 128-bits, 192-bist and 256-bits block cipher. In basic 128-bit accepted. Aes is 12 bit block cipher that means it takes 128-bits of message and encrypts it into 128 bits of cipher text with some key. These keys that gives you just varying amounts of security. Also symmetric key ciphers use the same key for encrypting and decrypting. The sender and the receiver must both know and use the same secret key.

That are 10 rounds for 128-bits keys. A round consist of several processing steps that include substitution, transposition and mixing of the input plaintext to transform it into the final output of ciphertext.



In the above picture, you ca see how the process is proceeded.

1- Key Expansion

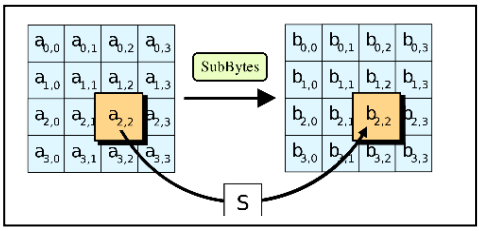
In key Expansion round keys are derived from the cipher key using the AES key schedule. AES requires a separate 128-bit round key block for each round plus one more.

2- Initial Round Key Addition

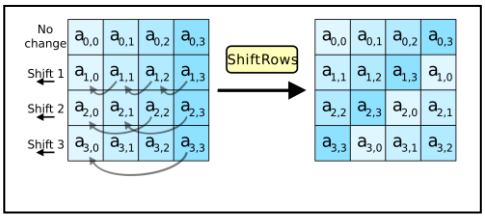
In first AddRoundKey , each byte of the state is combined with a byte of the round key using bitwise xor.

3- For 128-bits 9, for 192-bits 11, for 256-bits 13 rounds:

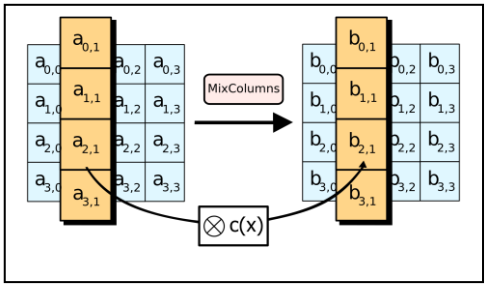
- **SubBytes:** In this step each byte in the state array is replaced with SubByte using 8-bits substation box.



- **ShiftRows:** The ShiftRows step operates on the rows of the state; it cyclically shifts the bytes in each row by a certain offset. For AES, the first row is left unchanged. Each byte of the second row is shifted one to the left. Similarly, the third and fourth rows are shifted by offsets of two and three respectively.



- **MixColumns:** During this operation, each column is transformed using a fixed matrix. Matrix multiplication is composed of multiplication and addition of the entries.



- **AddRoundKey:** The subkey is combined with the state. For each round, a subkey is derived from the main key using Rijndael's key schedule. The subkey is added by combining each byte of the state with the corresponding byte of the subkey using bitwise XOR.