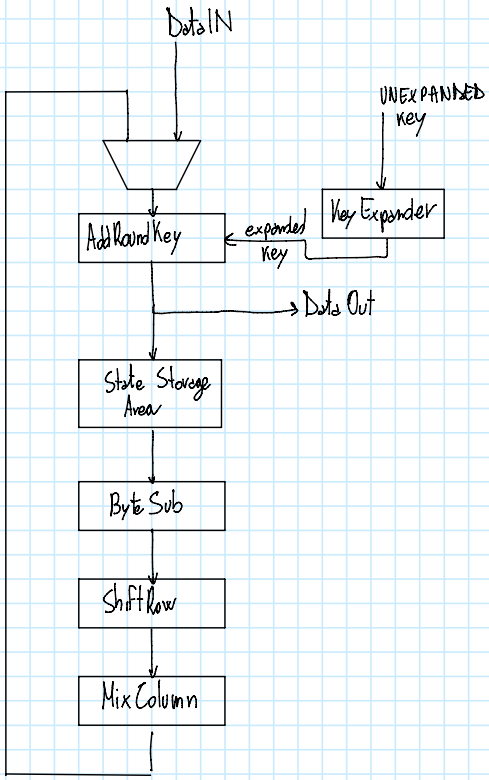
Project

martedì 30 maggio 2023 11:20



	Key Length (Nk words) (bits)	Block Size (Nb words) (bits)	Number of Rounds (Nr)
AES-128	4 (128)	4 (128)	10
AES-192	6 (192)		12
AES-256	8 (256)		14

1. Key Expansion: The original key, typically a 256-bit secret key, undergoes a key expansion process to generate a set of round keys. These round keys are used in each round of the encryption and decryption process.
2. Initial Round (AddRoundKey): In the initial round, the plaintext is combined with the first round key. This operation, called "AddRoundKey," involves a bitwise XOR (exclusive OR) operation between each byte of the plaintext and the corresponding byte of the round key.
3. Rounds (SubBytes, ShiftRows, MixColumns, AddRoundKey): After the initial round, a series of rounds is performed. Each round consists of four distinct operations:
   a. SubBytes: Each byte of the state (the intermediate result of the previous round) is substituted with a corresponding byte from the S-box lookup table, providing a nonlinear transformation.
   b. ShiftRows: The bytes in each row of the state are shifted cyclically to the left. This step ensures that the bytes in the same column are spread across different rows.
   c. MixColumns: The columns of the state are mixed using a matrix multiplication operation. This step provides diffusion and introduces further nonlinearities.
   d. AddRoundKey: The round key for the current round is combined with the state using bitwise XOR, similar to the initial round.
4. Final Round (SubBytes, ShiftRows, AddRoundKey): The final round is similar to the regular rounds but lacks the MixColumns operation.
5. Finalization: After the final round, the resulting state is the encrypted ciphertext or decrypted plaintext.