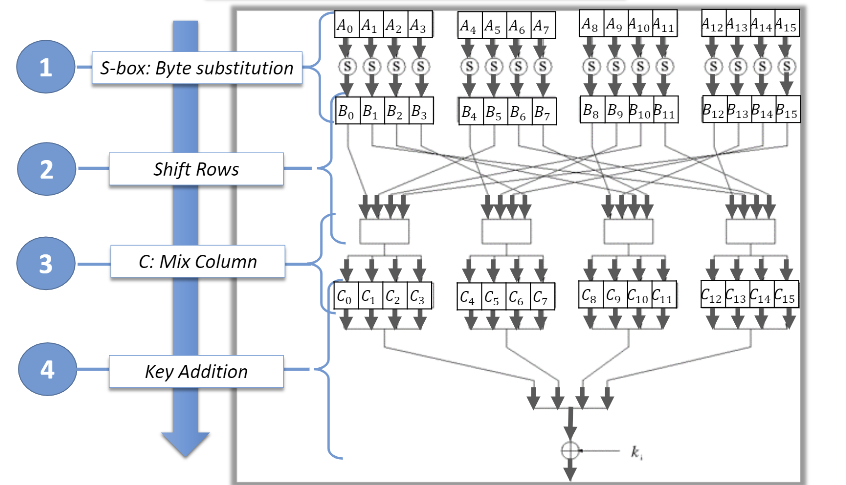
Homework2

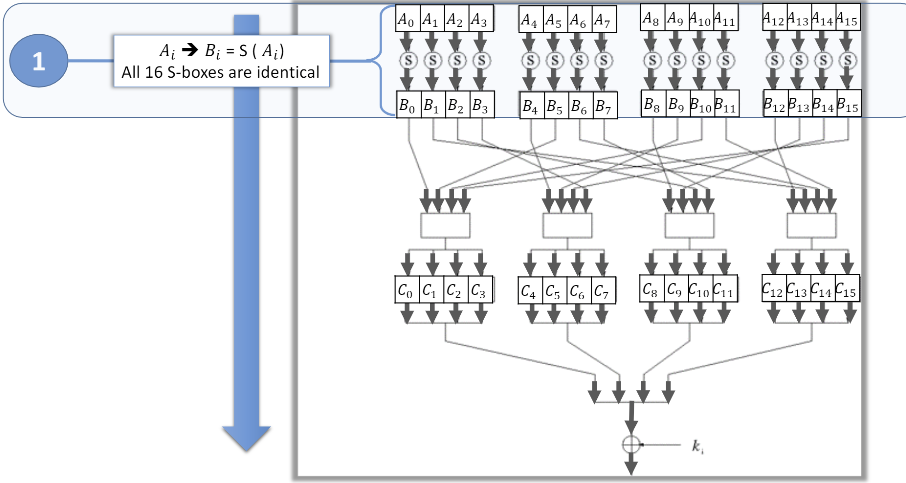
Back to back comparison DES versus AES:

*Encryption Step*

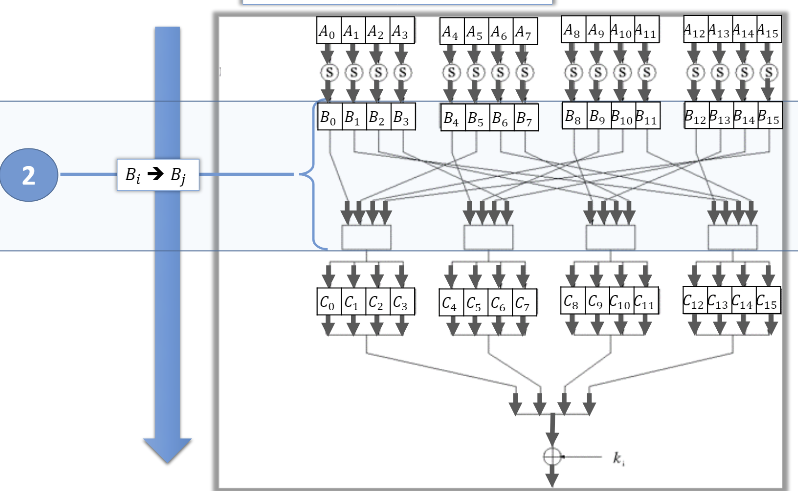
***AES***



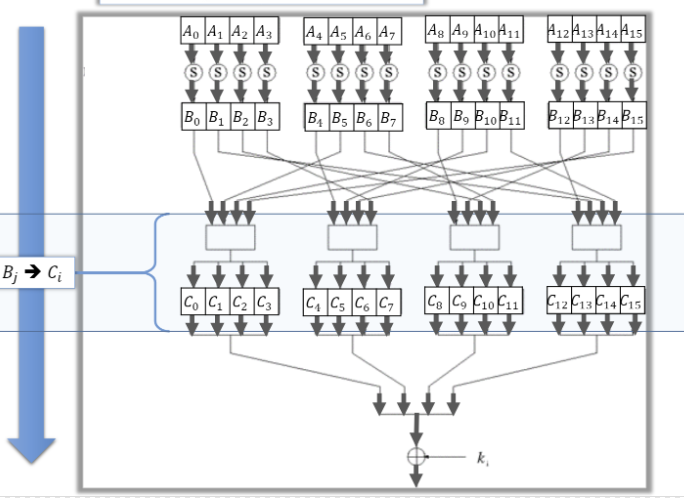
***Byte Substitution (Sub Bytes)***



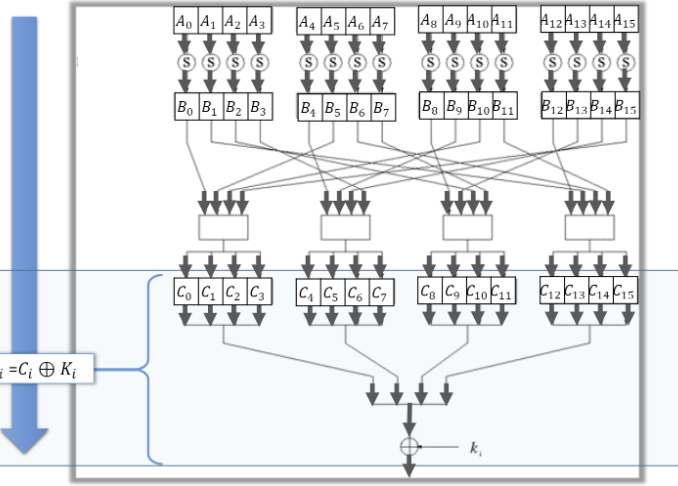
***Shift rows***



***Mix Column***



***Key addition***



***Key length is 56 bits in DES.***

***DES involves 16 rounds of identical operations***

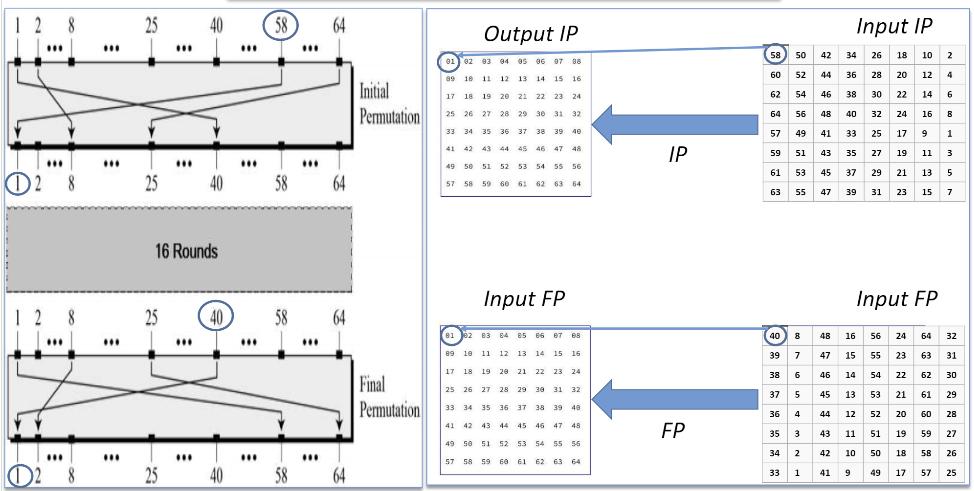
***The rounds in DES are: Expansion, XOR operation with round key, Substitution and Permutation***

***DES can encrypt 64 bits of plaintext.***

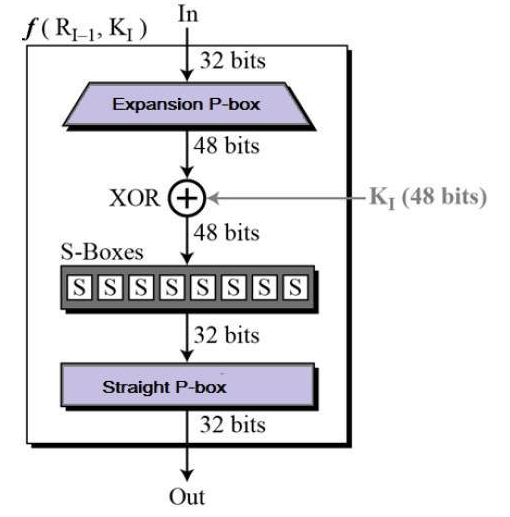
***DES cipher is derived from Lucifer cipher.***

***DES***

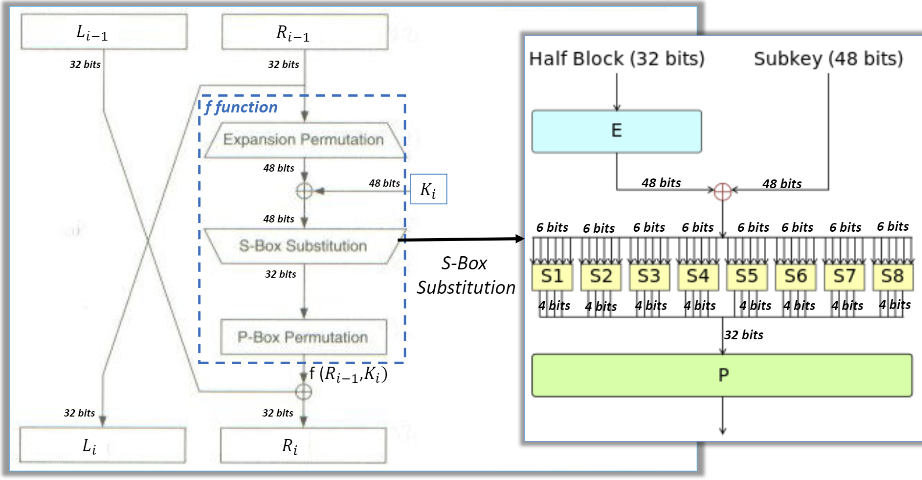
***1. Initial and Final Permutation***



***2.Round Function***



***S-Box***



***Key length can be of 128-bits, 192-bits and 256-bits.***

***Number of rounds depends on key length: 10(128-bits), 12(192-bits) or 14(256-bits)***

***The rounds in AES are: Byte Substitution, Shift Row, Mix Column and Key Addition***

***AES can encrypt 128 bits of plaintext.***

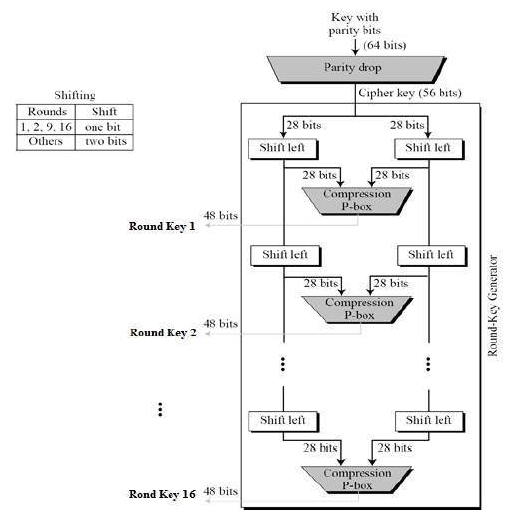
***AES cipher is derived from square cipher.***

*Key Generation*

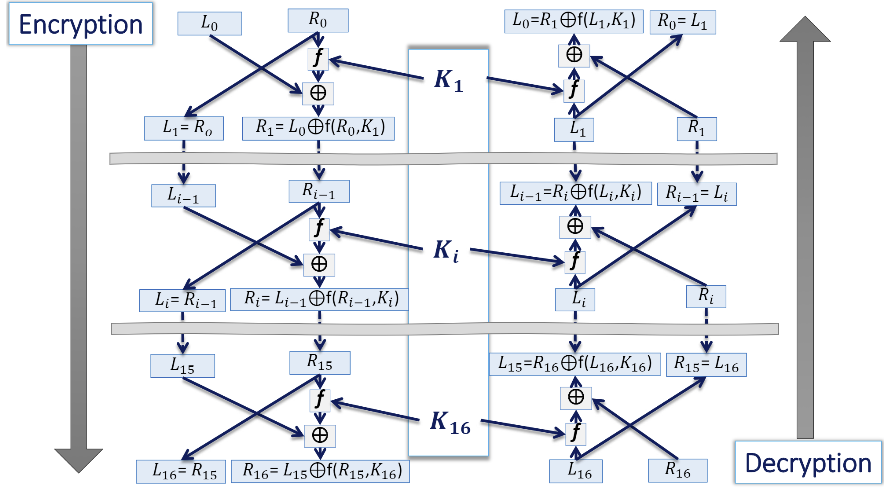
***DES***

***Key Generation***

*The round-key generator creates sixteen 48-bit keys out of a 56-bit cipher key*



***Decryption***

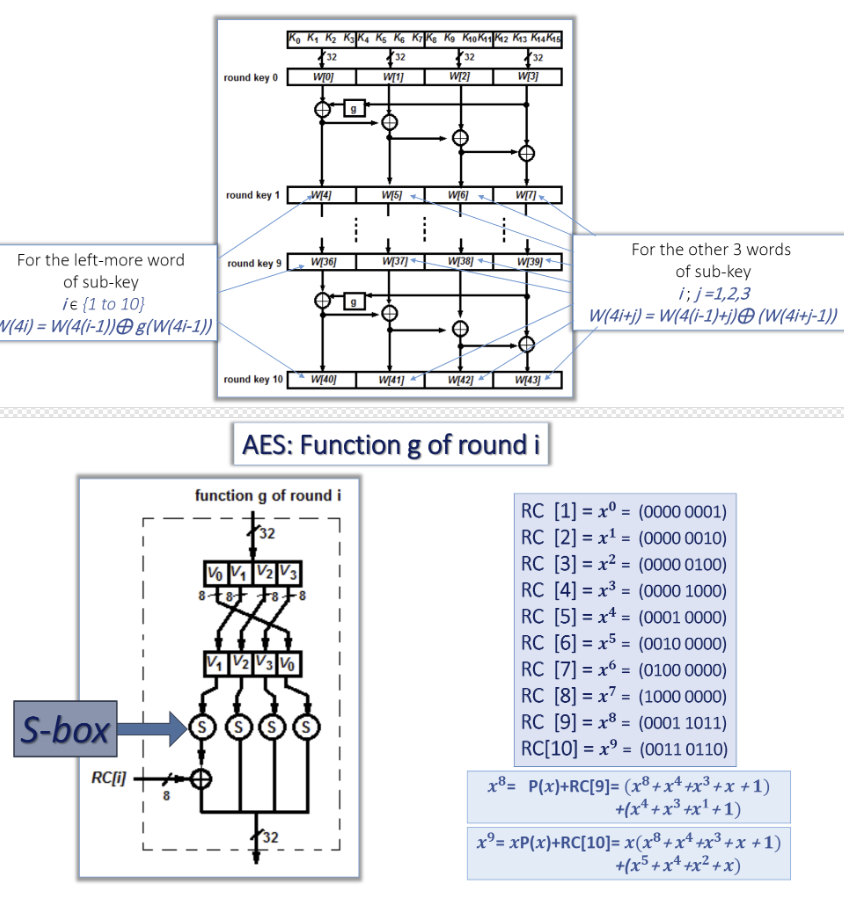


***Ultimately decryption is very similar to encryption, a common feature of Feistel ciphers in general. In fact, with some arrangements the only difference is the order of the subkeys, which is (or at least was) a big advantage as it makes implementation easier on limited devices, as you can mostly reuse the encryption code for decryption.***

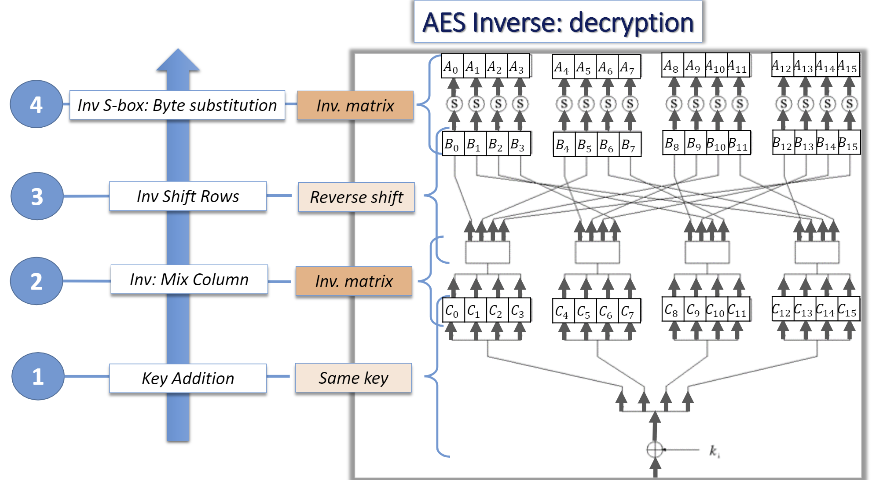
***AES***

***Key Generation***

***Key schedule for each round (128-bit size)***



***Decryption***



***The process of decryption of an AES ciphertext is similar to the encryption process in the reverse order. Each round consists of the four processes conducted in the reverse order −***

***Add round key***

***Mix columns***

***Shift rows***

***Byte substitution***