▓2 null bytes, 64 encoding? AAA=

▓Characteristics of Feistel Structure?

1. Divide input into two halves
2. Substitution+permutation
3. LE0 = RD16, RE0 = LD16, KE0 = KD16, reguardless of Feistel function

▓constrain of Feistel function? No

▓Why permutation expension? Let the 4-bit substitution be a function of previous and next segements

▓what happen if replace all the values in the S-boxes with 0s? because A OXR 0 = A, plaintext will be unchanged for every round and has no decryption

▓round key generation of DES?

▓diffusion and confusion in DES?