FCC Assignment 01 Q2 Brainstorming 01/04/2022

Implementing DES

Overview:

Input: - key of any length (padding or chopping)
- plaintext file for encryption

Output: encrypted text (cipher text) file.
& decrypted ~~text~~ cipher text file.

-DES.py
- encrypt() method.
↳ permutation() ①
* after this there's 16 rounds of feistal operations:
↳ key schedule() ②
↳ ffunction() ③
↳ inverse Permutation ④ ()
= ciphertext

} For loop 16 times

decrypt() method.
↳ permutation()
↳ keySchedule()
↳ ffunction()
↳ inverse perm..()
= recovered plaintext.

① permutation() & ④ inversePerm..()
uses a substitution table & reverses that.

keyschedule()

② The key inputted is (padded or chopped) then it is scheduled for each round of the feistal network operation with left shift → BY TAKING ROUND # into account!! 1, 2, 9, 16 shift by 1 other rounds by 2.

③ fFunction()
? - should keyschedule() be called here??
→ expansion() expands 32 bits to 48 XOR'D with key i
→ sbox() or array?? storing numbers then reducing each 6 bits to 4, then permuting this; permutation() or sBoxPerm..()??