Shweta Prasad March 19, 2021

CS 2362 Problem Set 2

Collaborators: *Saloni Mehta*

Problem 1-9

The real question here is: why is the Initial Permutation needed in DES? The Final Permutation is just an inverse to the Initial Permutation, after which the encrypted message can be obtained. Additionally, since we use the same functional machinery to do the decryption of the ciphertext in DES, the Final Permutation needs to be in place if the Initial Permutation is, so that the message itself can be recovered.

The IP and FP both don't add any security to DES. These are both known permutations, and are engineering artefacts from the time when $8-$bit registers were used. The 'permutations' were necessary to reduce the spatial requirements of cross wiring needed to deal with the $64-$bit blocks on $8-$bit registers. The creators of DES decided to do away with the wiring and let the configuration be, and called it an Initial Permutation.

Problem 1-11

(a)

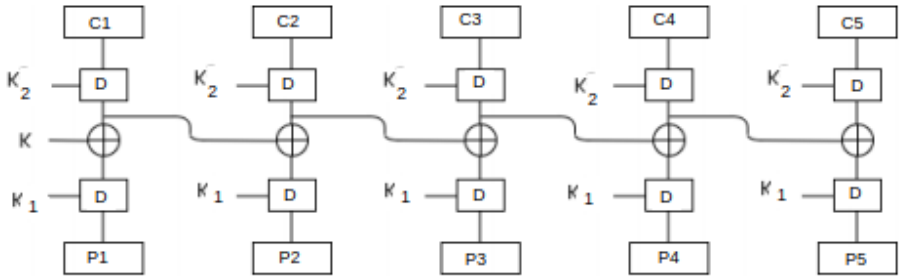

Figure 1: The Decryption Algorithm

The above image is an illustration of the decryption algorithm for the given encryption

scheme. K_1, K_2 are 56 bits long, as they should be to be used with the DES decryption function. K is 64 bits long as it has to be XORed with the 64 bit output of DES decryption.