Divij Singh March 5, 2019

CS-302 Problem Set 2

Collaborators: *Aditya*

Problem 1-1

(a) 20 words would have been consumed.
(b) w_{32} to w_{35} will be used.

Problem 1-2

(a) 33 times
(b) 30 times
(c) 30 times
(d) 27 times

Problem 1-3

(a) 11100110 (E6)
(b) 81ee66326c5078165c35b5a756cf120b
(c) There were 4 blocks of plaintext to convert (as there are 128 characters of hexadecimal) Additionally, one block of plaintext is repeated, as there are two similar blocks of ciphertext.

Problem 1-4

PFA code

Problem 1-5

The S-Boxes of DES were chosen specifically to prevent any access via a backdoor attack. Even a small change to the S-Boxes significantly weakens DES.

Problem 1-6

The final step involves the rearranging of 32 bits from the S-boxes according to a given permutation. This is done so that the output bits from an S-box are spread across different S-boxes for the next round, as part of the confusion and diffusion concept.

Problem 1-7

PFA code and README