Secure & Dependable Systems
Spring 2017
Assignment 06

Humza Abid

May 9, 2017

Problem 6.3 *Theory: Security Analysis*

1. The substitution boxes change any bit of the input byte to at least two bits of the output byte, all the while sending the output bits to different sub-blocks. Thus changing one bit of the plaintext results in at least a two bit different in the output of one of the blocks in the first round. The mixing permutation sends the two bits to different blocks in each subsequent round, increasing the different in the number of bits. Although there are cases where collisions occur, the net effect achieved is that of changing (on average) half of the bits of the resulting ciphertext block.

Even in the cas eof only one round, the inversion of the permutations, then the S-boxes and then finally that for the key, render it comp-ind secure if probability distribution functions for frequencies cannot be approximated.

2. The adversary can easily (for the single round) determine the key by reverse engineering.