Homework #2

Linear Cryptanalysis of a 4-round SPN

Consider a 5-round SPN as studied in the class (also refer to tutorial paper) and perform linear cryptanalysis. The permutation and key mixing steps remains to be same. However, you have to choose a customary 4x4 S-box. (In page 98 of the textbook, 8 standard 6x4 S-boxes for DES are given. Pick one row—other than the first row of the first S-box—to generate the look-up table for substitution.) Generate each sub-key as the three-bit shifted version of the master-key.

Your work should include the following steps.

- Linear approximation of the custom S-box.
- Selection of the best linear approximation.
- Linear approximation of the SPN. (Note that the linear approximations derived in the class and the textbook both rely on the particular selection of S-box.)
- Estimation of the linear probability bias.

Implementation Aspects: Design the SPN and pick a (16bit) key in random, and generate many plaintext-ciphertext pairs using the selected key, and delete the key without seeing it.

Goal:

- Extract the key using the studied linear cryptanalysis methodology using the known plaintext-ciphertext pairs.
- Present your results in the form of a written report which we will include all the analysis, and experimental results.
- Include the necessary reasoning you have made and provide a discussion on the problems you encountered.

If you have any questions contact me via tahs@isis.poly.edu or drop by the room LC-115 before Friday.