Introduction to Cryptology ENEE459E/CMSC498R: Homework 7

Due by beginning of class on 4/7/2016.

1. In our attack on a one-round SPN, we considered a block length of 64 bits and 8 S-boxes, each taking an 8-bit input. Repeat the analysis for the case of 16 S-boxes, each taking a 4-bit input. What is the complexity of the attack now? Repeat the analysis again with a 128-bit block length and 16 S-boxes that each take an 8-bit input.

2. In this question we assume a three-round SPN with 64-bit block length. Assume independent 64-bit sub-keys are used in each round, so the master key is 256 bits long. Show a key-recovery attack using approximately $2 \cdot 128 \cdot 2^{128}$ time.

3. What is the output of an r-round Feistel network when the input is (L_0, R_0) in each of the following two cases:

   (a) Each round function outputs all 0s, regardless of the input.

   (b) Each round function is the identity function.

4. Let $\mathsf{Feistel}_{f_1,f_2}()$ denote a two-round Feistel network using functions f_1 and f_2 (in that order). Show that if $\mathsf{Feistel}_{f_1,f_2}(L_0, R_0) = (L_2, R_2)$, then $\mathsf{Feistel}_{f_2,f_1}(R_2, L_2) = (R_0, L_0)$.

5. **Extra Credit:** Consider implementing a three-round Feistel Network, where each round function f_1, f_2, f_3 is a pseudorandom function with independent key k_1, k_2, k_3, respectively. Show that this *does not* yield a *strong* pseudorandom permutation (i.e. it can be distinguished from a random permutation, when given oracle access to both the forward and inverse directions).