University of Maryland
CMSC456 — Introduction to Cryptography
Professor Jonathan Katz

Homework 4

Due at the *beginning* of class on Nov. 8

1. (Exercise 5.4.) Consider a modified substitution-permutation network where instead of carrying out the key-mixing, substitution, and permutation steps in alternating order for r rounds, the cipher instead first applies r rounds of key mixing, then carries out r rounds of substitution, and finally applies r permutations. Analyze the security of this construction.

2. (Exercise 5.5.) 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.

3. (Exercise 5.10a.) Describe an attack on the following modification to DES: Each round sub-key is 32 bits long, and the mangler function simply XORs the round sub-key with the input to the round (i.e., $\hat{f}(k, R) = k_i \oplus R$). For this example, the key schedule is unimportant and you can treat the k_i as independent keys.

4. (Exercise 7.5.) Compute the final two (decimal) digits of 3^{1000} by hand.

5. (Exercise 7.6.) Compute $[101^{4,800,000,023} \bmod 35]$ by hand.