

## CSE 794Q Homework 2

Due: Thursday, February 5 by class time

1. Consider a Feistel cipher composed 16 rounds. Suppose that, for a given key  $k$ , the key scheduling algorithm determines the first 8 round keys,  $k_1, k_2, k_3, \dots, k_8$ , and then set  $k_9 = k_8, k_{10} = k_7, k_{11} = k_6, \dots, k_{16} = k_1$ . Suppose that you have access to an encryption oracle. Explain how you can easily decrypt any ciphertext which was encrypted with this cipher.
2. A student proposes a variant of DES, called DES', which is the same as DES except that the last step  $IP^{-1}$  is omitted. Will DES' work correctly as a block cipher? Is there any disadvantage of DES' compared with DES?
3. Suppose the DES F function mapped every 32-bit input R, regardless of the value of the round key, to 32 bits of ones. What function would DES then compute? (Hint:  $x \oplus 1 = \bar{x}$ .)
4. Let G be a pseudorandom generator that, given a string of length  $n$ , outputs a string of length  $2n$ . Define  $f_k(x) = G(k) \oplus x$ , where  $k \in \{0,1\}^n$  and  $x \in \{0,1\}^{2n}$ . Is  $\{f_k : k \in \{0,1\}^n\}$  a family of pseudorandom functions? Justify your answer.

## CSE 794Q Homework 3

Due: Thursday, February 5 by class time

Note: This homework will not be returned to you, so please separate it from Homework 2.

1. List all slides which you do not quite understand, and tell me your doubts/questions. (If you have no questions about any slide, that is OK, just say so.)
2. Propose three questions which you would like to ask in an exam if you were the instructor of this course.