Problem 1: (a) Show that for all $K \in \{0, 1\}^{56}$ and $x \in \{0, 1\}^{64}$

$$DES_K(x) = \overline{DES_{\overline{K}}(\overline{x})}$$

This is called the key-complementation property of DES

(b) Show how to use the key-complementation property of DES to speed up exhaustive key search by a factor of two. Explain any assumptions that you make.

Problem 2: Find a key $K$ such that

$$DES_K(x) = DES_K^{-1}(y), \forall x, y$$

Such a key is sometimes called a “weak” key. How many weak keys can you find? To solve this problem you need to look up the exact key schedule generation algorithm for DES. For details refer to http://www.itl.nist.gov/fipspubs/fip46-2.htm Show your work or you will receive zero credit!

Problem 3: An important property which makes DES secure is that the S-boxes are nonlinear. Verify the nonlinearity of the S-boxes by computing the output of box $S_1$, for several pairs of inputs. Show that

$$S_1(x_1) \oplus S_1(x_2) \neq S_1(x_1 \oplus x_2)$$

for

a. $x_1 = 000000$, $x_2 = 000001$

b. $x_1 = 111111$, $x_2 = 100000$

c. $x_1 = 101010$, $x_2 = 010101$

Problem 4: What is the output of the first round of DES when the plaintext and the key are both all zeros? What if the plaintext and the key are all ones?

Problem 5: Assume that bit 57 of a 64 plaintext block is 1 with all other bits equal to zero. Let the key be all zeros.

a. How many S-boxes get different inputs compared to the case of an all-zero plaintext, in the first round of DES?

b. What is the number of output bits which are different compared to the input after the first round?

c. How many output bits have actually changed after the first round compared to the case of an all-zero plaintext (consider only one round). Does DES exhibit the avalanche effect (small changes in the plaintext yield significant changes in the ciphertext)?

Do not forget to apply the initial permutation on the plaintext before passing it through the DES round.

Problem 6: Problem 3.2 from your book.

Due Feb 16th in class