Applied Cryptography: Homework 4

(Deadline: 3:00pm, 2022/03/16)

Justify your answers with calculations, proofs, and programs.

1. (10 points, question 4.3, page 132 of the textbook) Let $DES(x, K)$ represent the encryption of plaintext x with key K using the DES cryptosystem. Suppose $y = DES(x, K)$ and $y' = DES(c(x), c(K))$, where $c(\cdot)$ denotes the bitwise complement of its argument. Prove that $y' = c(y)$ (i.e., if we complement the plaintext and the key, then the ciphertext is also complemented). Note that this can be proved using only the "high-level" description of DES—the actual structure of S-boxes and other components of the system are irrelevant.

2. (40 points) Implement the AES encryption algorithm. (key length = 128 bits) Your code must test the example (in hex) below and two other your own examples. Submit your code and result together.

   Example 1:

```
Input:
    PLAINTEXT:    32 43 f6 a8 88 5a 30 8d 31 31 98 a2 e0 37 07 34
    KEY:          2b 7e 15 16 28 ae d2 a6 ab f7 15 88 09 cf 4f 3c
Output:
    CIPHERTEXT:   39 25 84 1d 02 dc 09 fb dc 11 85 97 19 6a 0b 32
    DECIPHERTEXT: 32 43 f6 a8 88 5a 30 8d 31 31 98 a2 e0 37 07 34
```