Cryptography: Homework 8

(Deadline: 10am, 2021/12/03)

1. (15 points) Show that DES has the property that $\mathsf{DES}_k(x) = \overline{\mathsf{DES}_{\bar{k}}(\bar{x})}$ for every key k and input x (where $\bar{z}$ denotes the bitwise complement of z. For example, $\overline{101} = 010$).

2. (35 points) Implement the encryption algorithm of AES.