Assignment 4

Submission Deadline: 2021.10.20, 12:00pm

1. Let m be a message consisting of t AES blocks (say t=100). Alice encrypts m using CBC mode and transmits the resulting ciphertext to Bob. Due to a network error, ciphertext block number t/2 is corrupted during transmission. All other ciphertext blocks are transmitted and received correctly. Once Bob decrypts the received ciphertext, how many plaintext blocks will be corrupted? Give your explanation.

2. Considering the nonce based CBC mode operation. Assume that the nonce is initialized to 0, and incremented by one for each message. The nonce will return to 0 when it reaches 100, and the procedure repeats. Please show by the challenger and adversary game that this encryption is not semantic secure under a CPA attack.

3. Let I=(S,V) be a MAC. Suppose an attacker is able to find $m_0 \neq m_1$ such that $S(k, m_0) = S(k, m_1)$ for ½ of the keys k in K. Please provide your argument using the challenger and adversary game about the security of the MAC.