CSCI471/971
Modern Cryptography

Workshop

Question-1

Question 1. Please show that the following encryption scheme is not IND-CCA secure, where Enc is a secure blockcipher:

1. Choose a random IV.
2. Run $W \leftarrow Enc(K, IV)$
3. Compute $C = W \oplus M$
4. Output $CT = (IV, C)$

Question-2

Question 2. Please show that the following encryption scheme is not IND-CCA secure, where Enc is a secure blockcipher:

1. Choose a random IV.
2. Compute $M' = IV \oplus M$
3. Run $C \leftarrow Enc(K, M')$
4. Output $CT = (IV, C)$

END