CSA E0 235: Cryptography 13/09/2019

Tutorial 5

Instructor: Arpita Patra *Question Set*

1. Consider a stateful variant of CBC-mode encryption where the sender simply increments the IV by 1 each time a message is encrypted (rather than choosing IV at random each time). Show that the resulting scheme is not CPA-secure.

2. What is the effect of a single-bit error in the ciphertext when using the CBC, OFB, and CTR modes of operation?

3. What is the effect of a dropped ciphertext block (e.g., if the transmitted ciphertext $c_1, c_2, c_3, \ldots$ is received as $c_1, c_3, \ldots$) when using the CBC, OFB, and CTR modes of operation?

4. Show that the CBC, OFB, and CTR modes of operation do not yield CCA-secure encryption schemes (regardless of F).

5. What happens if the encryption scheme does not satisfy special correctness property in Yao's Scheme?