CS 435: Introduction to Cryptography **Spring 2020**

Homework 4

Professor Somesh Jha **Due:** April 8

1. Show the decryption logic for the four modes of operations ECB, CBC, OFB, and CTR.
2. 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.
3. What is the effect of a single-bit error in the ciphertext when using the CBC, OFB, and CTR modes of operation?
4. Let F be a pseudorandom permutation. Consider the mode of operation in which a uniform value $ctr \in \{0,1\}^n$ is chosen, and the ith ciphertext block c_i is computed as $c_i := F_k(ctr + i + m_i)$. Show that this scheme does not have indistinguishable encryptions in the presence of an eavesdropper.