CS 435: Intro to Cryptography **Fall 2020**

Homework 4

Professor Somesh Jha **Due:** Nov 5, 2020

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. Towards the end of LectureLet-16 we covered timing attacks for MACs. Let us say a message m has tag t which has m bytes, Let it take T milliseconds(ms) to compare equality of two bytes. In LectureLet-16 we only explained how to get two bytes of the tag t. Describe the full attack (i.e. recovering all the m bytes of the tag t). How much time in ms does the attack take?