CS 435: Introduction to Cryptography **Fall 2016-17**

Homework 4

Professor Somesh Jha **Due:** November 10

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

2. Let F be a pseudorandome permutation. Consider the mode of operation in which a uniform value $\texttt{ctr} \in \{0,1\}^n$ is chosen, and the ith ciphertext block c_i is computed as $c_i := F_k(\texttt{ctr} + i + m_i)$. Show that this scheme does not have indistinguishable encryptions in the presence of an eavesdropper.

3. Consider a variant of CBC-mode encryption where the sender simply increment 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.

4. Present formulas for decryption of all the different modes of encryption we have seen. For which modes can decryption be parallelized?