

Instructions:

This is an optional assignment that you will not turn it. Please attempt to do it, because it will help you understand the notions of security for encryption schemes that were presented in class.

Problem 1. Consider the space of messages to consist of all 1-letter texts (i.e., a message is just one English letter). Show that the shift cipher is perfectly secure. Use version 1 of the definition in your proof.

Problem 2. Consider the space of messages to consist of all 2-letters texts. Show that the shift cipher is not perfectly secure. Hint: Think of some particular message m_1m_2 and ciphertext c_1c_2 such that it is obvious that $P(M = m_1m_2 \mid E_K(M) = c_1c_2) \neq P(M = m_1m_2)$.