CS 171: Discussion Section 1 (Jan 22)

1. Formal definitions

Provide formal definitions of $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ for the shift, substitution, and Vigenère ciphers. (You can use $\mathbb{Z}_n$ to denote the set of numbers $\{0, 1, \ldots, n-1\}$ and identify the letters of the English alphabet with $\mathbb{Z}_{26}$.)

2. Exploiting Partial Information About the Message

Setting: Let's say that a user wants to send one of two values over unsecured channels. For example, these could correspond to `Attack by land` and `Attack by sea`, or `abcd` and `ehgj`, or even something else. They will encrypt their message before sending it using one of the encryption schemes above and hope that an adversary who can see the ciphertext cannot figure out which message they sent.

In more general terms:

1. Assume that an adversary knows that a user's message is one of two values, m_A or m_B.
2. Say the user encrypts their message, and the adversary sees the resulting ciphertext.
3. Can the adversary figure out which message, m_A or m_B, was encrypted?

The answer depends on the particular values of m_A and m_B.

Questions:

(a) Say the user encrypts their message with the shift cipher, and say the message is either $m_A =$ `abcd` or $m_B =$ `ehgj`. Show how the adversary can determine the user's message, or show that this is not possible.

(b) Now say the user encrypts their message with the substitution cipher. If the message is either $m_A =$ `abcd` or $m_B =$ `ehgj`, can the adversary learn the message? If so, show how the adversary can do so. If not, find different values for m_A and m_B such that the adversary can learn the message.

(c) Say the user encrypts their message with the Vigenère cipher, and say the message is either $m_A =$ `abcd` or $m_B =$ `ehgj`. Show how the adversary can determine the user's password, or explain why this is not possible. Consider Vigenère ciphers that use period 2, period 3, and period 4.