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

Homework 1

Professor Somesh Jha **Due:** Sept 24, 2020

1. Use definition 2 of perfect secrecy (Lemma 2.4 of the textbook) to prove that the mono-alphabetic substitution cipher is not perfectly secret.

   $$\Pr[\mathsf{Enc}_K(m) = c] = \Pr[\mathsf{Enc}_K(m') = c] \tag{2.1}$$

   Lemma 2.4. *An encryption scheme* $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ *with message space* $\mathcal{M}$ *is perfectly secret if and only if Equation (2.1) holds for every* $m, m' \in \mathcal{M}$ *and every* $c \in \mathcal{C}$.

2. Consider a variant of the Vigenère cipher where instead of a word or short phrase, the key instead consists of a book or some other English-language text that is much longer than the message to be encrypted. Using this cipher, the key is never repeated, so our standard methods for retrieving the key length will fail. Now assume that Bob is a sleeper agent and Alice is his handler. Alice, using this cipher, has sent Bob a ciphertext that reads

   ```
   YVBCXGJRYHHRCJIUL
   ```

   The plaintext is known to contain the day of the week that Bob is supposed to receive the dead drop, followed by the day of the week he is supposed to flee the country. Determine which plaintext Alice sent to Bob, and explain how you reached your answer.

   Note. Each ciphertext character c_i is equal to $m_i + k_i \pmod{26}$, where m_i is the i-th character of the plaintext message and k_i is the i-th character of the key. In particular, the alphabet is indexed from 0, so 'a' corresponds to 0, 'b' corresponds to 1, and so on.

3. a. Assume an attacker knows that a user's password is one of these: pqrs, mnop, svux, jmlo. Say the user encrypts his password using the shift cipher, and the attacker sees the resulting ciphertext. Show how the attacker can determine the user's password, or explain why this is not possible.

   b. The attacker has somehow narrowed down the passwords to pqrs or jmlo but now the user encrypts his password by Vigenère cipher. Show how the attacker can determine the user's password, or explain why this is not possible. Do this using period 2, using period 3, and using period 4.

4. For each of the following encryption schemes, state whether the scheme is perfectly secret. Justify your answer in each case.

a. The message space $\mathcal{M}$ is $\{0, \ldots, 4\}$. Algorithm Gen chooses a uniform key k from the key space $\{0, \ldots, 5\}$. $\mathsf{Enc}_k(m) = [k + m \mod 5]$.

b. The message space $\mathcal{M}$ is $\{0, 1\}^{2n}$. Gen chooses an uniform key k from $\{0, 1\}^n$. $\mathsf{Enc}_k(x) = \langle x_{1\ldots n} \oplus k, x_{n+1\ldots 2n} \oplus k \rangle$, where $\oplus$ denotes the bitwise XOR.