CSE 130 – INTRO TO CRYPTOGRAPHY

Spring 2025 Homework 1

Historical Ciphers:

1. Say you are given a ciphertext that corresponds to English-language text that was encrypted using either the *shift cipher* or the *Vigènere cipher* with period (length of the key) greater than 1? How could you tell which was the case?

2. The index of coincidence method relies on a known value for the sum of the *squares* of plaintext-letter frequencies (cf. Equation (1.1) in pg. 12). Why would it not work using the sum $\sum_i p_i$ itself?

3. The attack on the Vigènere cipher has two steps: (a) find the key length by identifying τ with $S_\tau \approx 0.065$ (cf. equation in pg. 15) and (b) for each character of the key, find j maximizing I_j (cf. equation in pg. 13), using $\{p_i\}$ corresponding to English text. What happens in each case if the underlying plaintext is on a language other than English.

Modern Cryptography, Perfect Secrecy and One Time Pad:

1. Prove or refute: For every perfectly secret encryption scheme it hols that for every distribution on the message space $\mathcal{M}$, every $m, m' \in \mathcal{M}$, and every $c \in \mathcal{C}$:

$$\Pr[M = m | C = c] = \Pr[M = m' | C = c].$$

2. What is the ciphertext that results when the plaintext `0x012345` (written in hex) is encrypted using the one-time pad with the key `0xFFEEDD`?

3. In each of the following schemes, $\mathsf{Enc}_k(m) = [m + k \mod 3]$. State in each case whether the scheme is perfectly secret, and justify your answers.

   (a) The message space is $\mathcal{M} = \{0, 1\}$, and Gen chooses a uniform key from the key space $\mathcal{K} = \{0, 1\}$.

   (b) The message space is $\mathcal{M} = \{0, 1, 2\}$, and Gen chooses a uniform key from the key space $\mathcal{K} = \{0, 1, 2\}$.

   (c) The message space is $\mathcal{M} = \{0, 1\}$, and Gen chooses a uniform key from the key space $\mathcal{K} = \{0, 1, 2\}$.

4. The following questions concern the message space $\mathcal{M} = \{0, 1\}^{\leq l}$, the set of all nonempty binary strings of length at most l.

   (a) Consider the encryption scheme in which Gen chooses a uniform key from $\mathcal{K} = \{0, 1\}^l$, and $\mathsf{Enc}_k(m)$ outputs $k_{|m|} \oplus m$, where k_t denotes the first t bits of k. Show that this scheme is not perfectly secret for message space $\mathcal{M}$.

   (b) Design a perfectly secret encryption scheme for message space $\mathcal{M}$.

5. Let Π denote the Vigenère cipher where the message space consists of all 3-character strings (over the English alphabet), and the period t is fixed to 2 (and so the key is uniform string of length 2). Define $\mathcal{A}$ as follows: $\mathcal{A}$ outputs $m_0 = \mathtt{aaa}$ and $m_1 = \mathtt{aab}$. When given a ciphertext c, it outputs 0 if the first character of c is the same as the third character of c, and outputs 1 otherwise. Compute $\Pr[\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi} = 1]$.

6. The following questions concern multiple encryptions of single-character ASCII plaintexts with the one-time pad using the same 8-bit key. You may assume that the plaintexts are either (upper- or lower-case) English letters or the space character.

   (a) Say you see the ciphertext 1011 0111 and 1110 0111. What can you deduce about the plaintext characters these correspond to?

(b) Say you see three ciphertexts 0110 0110, 0011 0010, and 0010 0011. What can you deduce about the plaintext characters these correspond to?

Your submission must contain the following:

- Title that states "CSE 130 Homework 1 Solutions (Spring 2025)".
- Your full name (as it appears on CatCourses).
- The question number associated with each answer.
- Page numbers on each page. If submitting a handwritten scanned document (see below), your page numbers must be in the following format (1 of n, 2 of n, etc.), where n indicates the total number of pages.

The submission format is PDF. You may use the following to write your solutions:

- LaTeX: You may use the Overleaf online editor.
- Markdown: You may use VS Code for this (supports it natively). Please use the Print extension to save your rendered Markdown file as PDF.
- MS Word: You may use the built-in Equation Editor. Please make sure to save your Word file as PDF before submitting.
- Pen and Paper: Please make sure to scan your work as PDF before submitting (image formats like JPEG **will not be accepted**). Please make sure that your scanned document is **clearly legible** before submitting.