CS 6222, Homework 1

Instructor: Wei-Kai Lin

Total points: 30. Points are noted after each problem.

Problem 1 (Monty Hall's problem, 1pt each)**.** This problem considers a game between a player and a host. There are n doors, and there is at most 1 car behind each door, where the total number of cars is $m \leq n - p$ for some positive integer $p < n$. The host knows which door has a car, but the player does not. The player picks 1 door, then the host opens other p doors that have no car, and then the player can finalize on any unopened door. If the finalized door has a car, the player wins. When the player finalizes with the following strategies, calculate the winning probability of the player (as functions of in n, m, p).

(a) Always finalize on the picked door.

(b) Finalize on an unopened door that is sampled uniformly.

(c) Finalize on an unopened door that is sampled uniformly but is not the picked one.

Problem 2 (Chernoff's inequality, 2pt each)**.** Let $X_1, X_2, ..., X_n$ be independent random variables in $[0, 1]$. Let $X := \sum_{i \in [n]} X_i$ and $\mu := \mathbb{E}[X]$. In this problem, we will prove that

$$\Pr[X \geq (1+\delta)\mu] \leq \left(\frac{e^\delta}{(1+\delta)^{1+\delta}}\right)^\mu.$$

Assume the random variables are discrete for simplicity.

(a) Show the following by Markov's inequality:

$$\Pr[X \geq a] \leq \frac{\mathbb{E}[e^{sX}]}{e^{sa}}$$

(b) Let Y be a random variable taking values in $[0, 1]$, and let $\mu_Y = \mathbb{E}[Y]$. Prove for any real s,

$$\mathbb{E}[e^{sY}] \leq 1 + \mu_Y \cdot (e^s - 1).$$

Note the RHS is $\leq e^{\mu_Y(e^s-1)}$ by $1 + x \leq e^x$.

(c) Use independence of X_i's and the above bound, show that

$$\mathbb{E}[e^{sX}] \leq e^{\mu(e^s-1)}.$$

(d) Complete the proof by putting the above together and then minimizing s on the exponent.

$$\Pr[X \geq (1+\delta)\mu] \leq \left(\frac{e^\delta}{(1+\delta)^{1+\delta}}\right)^\mu.$$

Note: for all $\delta > 0$, $e^{-\frac{\delta^2}{2+\delta}\mu}$ bounds the RHS and is often easier to use.

Problem 3 (Shannon's secrecy implies perfect secrecy, 1pt each)**.** This exercise will complete the equivalence between two definitions. Let $m_0, m_1 \in \mathcal{M}$ be any two messages. Let D be the distribution that samples m_b with probability $1/2$ for each $b = 0, 1$, that is,

$$\Pr[m \leftarrow D : m = m_b] = 1/2.$$

(a) Let $Q := \{\mathsf{Enc}_k(m) : k \in \mathcal{K}, m \in \{m_0, m_1\}\}$. Show that for all $c \notin Q$,

$$\Pr_k[\mathsf{Enc}_k(m_0) = c] = \Pr_k[\mathsf{Enc}_k(m_1) = c].$$

(b) Show that for all $c \in Q$,

$$\Pr_{k,m\leftarrow D}[m = m_0 | \mathsf{Enc}_k(m) = c] = 1/2.$$

(c) Show that the above conditional probability is equivalent to

$$\frac{\Pr_{m\leftarrow D}[m = m_0] \cdot \Pr_k[\mathsf{Enc}_k(m_0) = c]}{\Pr_{k,m\leftarrow D}[\mathsf{Enc}_k(m) = c]}.$$

(d) Obtain perfect secrecy by putting together the above equations.

Problem 4 (Vigenère cipher, 3pt each)**.** Let the strings of capital letters $\{A, B, ..., Z\}^*$ be the messages space and the keyspace. Vigenère cipher shifts each letter of the message according to the key as described in [KL21, page 11]:

> The key is viewed as a string of letters; encryption is done by shifting each plaintext character by the amount indicated by the next character of the key, wrapping around in the key when necessary.

In this problem, you are encouraged to read [KL21, Section 1.3].

(a) Implement the Enc and Dec algorithms of Vigenère cipher over the 26 capital letters. Verify your implementation is correct using the following:

```
key:     UVACS
message: COMPUTERSCIENCEANIMATESOURWORLDDRIVINGKNOWLEDGECREATIONANDINNOVATION
cipher:  WJMRMNZRUUCZNEWUIIOSNZSQMLROTDXYRKNCIGMFIRLGVAZCTWUOIQFUIDKFHJVCLCJN
```

Copy your code snippet to PDF and explain it.

(b) Recover the plaintext of "cipher (b)" in "hw1.txt".

(c) If we encrypt a message *twice* using Vigenère cipher, is it secure? That is to encrypt a message m by $\mathsf{Enc}_{k_2}(\mathsf{Enc}_{k_1}(m))$, where Enc is the Vigenère encryption, $k := (k_1, k_2)$ are two keys. Implement and verify your new encryption scheme using the following:

```
key:     (UVACS,ENGINEERING)
message: COMPUTERSCIENCEANIMATESOURWORLDDRIVINGKNOWLEDGECREATIONANDINNOVATION
cipher:  AWSZZRDICHIDAKEHMMFAAFWDSTESXUFLXOAIQTQJZZYMZNFKGAYFQDLYVJSSLNMKYINA
```

Recover the plaintext of "cipher (c)" in "hw1.txt". Note: composing the encryption is applied to increase the security in ealier standards, such as triple DES [MH81].

(d) Cipher-Block-Chaining (CBC) is used in practice with block ciphers (see [KL21, Section 3.6.2]). We can compose Vigenère using CBC as

$$c_i \leftarrow \mathsf{Enc}_k(m_i \oplus c_{i-1}),$$

where $m := m_1 m_2 ... m_\ell$ is the message, $\oplus$ means character-wise shifting, each message block m_i is fixed in size, c_i is the i-th cihper block, and c_0 is the initial vector. Here, let the block size be 256 and the initial vector be an all 'A' block. Is this encryption secure? Recover the plaintext of "cipher (d)" in "hw1.txt".

(e) If the length of the ciphertext is short, it is harder to recover the plaintext. Try to recover the plaintext of "cipher (e)" in "hw1.txt".

Explain your attack in detail, for example, the algorithm, the calculated numbers, and the time complexity. Estimate the success probability of your attack, e.g., calculate the probability as a function of the ciphertext length by Chernoff's Inequality.

References

[KL21] Jonathan Katz and Yehuda Lindell. *Introduction to Modern Cryptography.* CRC Press, Massachusetts, 3 edition, 2021.

[MH81] Ralph C. Merkle and Martin E. Hellman. On the security of multiple encryption. *Commun. ACM*, 24(7):465–467, jul 1981.