Homework 3

1. **Security of encryption schemes (8+8+8+10 points).** For each encryption scheme below, state whether the scheme is secure or not. Justify your answer in each case.

   (a) The message space is $\mathcal{M} = \{0, 1, \ldots, 12\}$. Algorithm Gen chooses a uniform key from the key space $\mathcal{K} = \{1, \ldots, 12\}$. The encryption algorithm $\mathsf{Enc}_{sk}(m)$ returns $(sk + m) \mod 13$, and the decryption algorithm $\mathsf{Dec}_{sk}(m)$ returns $(c - sk) \mod 13$.

   Solution.

   According to the Shannon theorem stated in the class, if a private key encryption scheme is correct and secure, then the size of its key space is not smaller than the size of its message space, i.e. $|\mathcal{K}| \geqslant |\mathcal{M}|$.

   The given encryption scheme is correct because

   $$\begin{aligned} \mathsf{Dec}_{sk}(\mathsf{Enc}_{sk}(m)) &= (\mathsf{Enc}_{sk}(m) - sk) \pmod{13} \\ &= (((sk + m) \mod 13) - sk) \pmod{13} \\ &= m \pmod{13} \end{aligned}$$

   However, $|\mathcal{K}| = 12$ and $|\mathcal{M}| = 13$ which implies that it is not secure.

   Alternative Solution: Give a counter example.

   We shall use graph representation to show that the given encryption scheme is not secure. For a scheme to be secure, for any $c \in \mathcal{C}, \mathrm{wt}(m, c) = \mathrm{wt}(m', c)$, where $\mathrm{wt}(m, c)$ is the number of witnesses (secret keys) to the mapping from message m to cipher text c for all $m, m' \in \mathcal{M}$.

   Let $c = 3, m = 0, m' = 3$, then $\mathrm{wt}(m, c) = 1$ because for $\mathsf{sk} = 3$, we have $\mathsf{Enc}_{\mathsf{sk}}(m) = c$. However, $\mathrm{wt}(m', c) = 0$ because there is no witness (secret key, because $0 \notin \mathcal{K}$) that $\mathsf{Enc}_{\mathsf{sk}}(m') = c$ holds.

   Since $\mathrm{wt}(m, c) \neq \mathrm{wt}(m', c)$, we conclude that the encryption scheme is not secure.

(b) The message space is $\mathcal{M} = \{0, 1, \ldots, 12\}$. Algorithm Gen chooses a uniform key from the key space $\mathcal{K} = \{0, 1, \ldots, 13\}$. The encryption algorithm $\mathsf{Enc}_{sk}(m)$ returns $(sk + m) \mod 13$, and the decryption algorithm $\mathsf{Dec}_{sk}(m)$ returns $(c - sk) \mod 13$.

Solution.

We shall use graph representation to prove that the scheme is not secure.

Let $c = 6$, $m = 6$ and $m' = 5$.

Then, $\mathrm{wt}(m, c) = 2$ because for $\mathsf{sk} \in \{0, 13\}$, we have $\mathsf{Enc}_{sk}(m) = c$. And $\mathrm{wt}(m', c) = 1$ because for only $\mathsf{sk} = 1$, we have $\mathsf{Enc}_{sk}(m') = c$.

Since $\mathrm{wt}(m, c) \neq \mathrm{wt}(m', c)$, we conclude that the encryption scheme is not secure.

(c) The message space is $\mathcal{M} = \{1, 3, 5, \ldots, 2019, 2021, 2023\}$. Algorithm Gen chooses a uniform key from the key space $\mathcal{K} = \{0, 2, 4, 6, \ldots, 2022\}$. The encryption algorithm $\mathsf{Enc}_{sk}(m)$ returns $(sk + m) \mod 2024$, and the decryption algorithm $\mathsf{Dec}_{sk}(m)$ returns $(c - sk) \mod 2024$.

Solution.

We shall use graph representation to prove that the scheme is secure.

The message space is the set of odd integers less than or equal to 2023 and the key space is the set of even integers less than or equal to 2022 and the summation of an even and an odd integer modulo 2024 is an odd integer. Thus, the cipher text space is $\mathcal{C} = \{1, 3, 5, \ldots, 2023\}$.

Let $c = 2j - 1$ for some j in the set $\{1, 2, \ldots, 1012\}$ and $m = 2i - 1$ for some $i \in \{1, 2, \ldots, 1012\}$. Then, $\mathrm{wt}(m, c) = 1$ because the only key $\mathsf{sk} \in \mathcal{K}$ for which $\mathsf{Enc}_{sk}(m) = c$ is $\mathrm{sk} = 2(j-i) \mod 2024$ (if $j \geqslant i$ then $2(j-i)$ is the key and if $j < i$, then $2(j-i)+2024$ is the key) which is an even integer less than 2022 and the key space contains that(note that this is important to make sure that this key exists in the key space).

Since for each m and c, $\mathrm{wt}(m, c) = 1$, the encryption scheme is secure.

(d) The message space $\mathcal{M}$ is the set of all n bit strings ($\{0,1\}^n$) containing t 1s. The key space $\mathcal{K}$ is the set of all permutations of the n positions. Algorithm Gen chooses a key uniformly at random from the key space $\mathcal{K}$. The encryption algorithm $\mathsf{Enc}_{sk}(m)$ returns $\pi(m)$, and the decryption algorithm $\mathsf{Dec}_{sk}(m)$ returns $\pi^{-1}(m)$ where $\pi^{-1} \circ \pi = \mathbb{1}$, $\mathbb{1}$ is the identity permutation.

For example, when $n = 3, t = 2$, let $\mathcal{M} = \{110, 101, 011\}$ be the set of all 3 bit strings with two 1s. Let $m = 101 \in \mathcal{M}$ be a message. Let $\pi : \mathcal{M} \to \mathcal{M}, \pi \in \mathcal{K}$ be a permutation of the 3 positions such that $\pi(b_1b_2b_3) = b_2b_3b_1$, i.e. $\pi(101) = 011$.

Note: This encryption scheme shows that the witness for an encryption does not have to be unique.

Solution.

The message space $\mathcal{M}$ is the set of all n bit strings ($\{0,1\}^n$) containing t 1s and the key space $\mathcal{K}$ is the set of all permutations of the n positions. Thus, the cipher text space is $\mathcal{C} = \mathcal{M}$ and $|\mathcal{C}| = |\mathcal{M}| = \binom{n}{t} = \frac{n!}{t!(n-t)!}$

The given encryption scheme is correct because

$$\begin{aligned}\mathsf{Dec}_{sk}(\mathsf{Enc}_{sk}(m)) &= \pi^{-1}(\mathsf{Enc}_{sk}(m)) \\ &= \pi^{-1}(\pi(m)) \\ &= \pi^{-1} \circ \pi(m) \\ &= m\end{aligned}$$

For a scheme to be secure, for any cipher text $c \in \mathcal{C}$, $\mathrm{wt}(m, c) = \mathrm{wt}(m', c)$, where $\mathrm{wt}(m, c)$ is the number of witnesses (secret keys) to the mapping from message m to cipher text c for all $m, m' \in \mathcal{M}$.

Equivalently, we will show that for any arbitrary $c \in \mathcal{C}$ and $m \in \mathcal{M}$, there exists $(n-t)!t!$ different permutations (secret keys) π such that $\mathsf{Enc}_{sk}(m) = \pi(m) = c$, i.e. $wt(m, c) = (n-t)!t!$.

Case 1: $c = m$.

When $c = m$, we have $\mathsf{Enc}_{sk}(m) = \pi(m) = m$. All valid permutations π permute all 1's positions and all 0's positions among themselves, i.e. π does not swap the position of any 0 and 1. There are $t!$ ways to permute all 1's position and $(n-t)!$ ways to permute all 0's positions. Therefore, there are $(n-t)!t!$ different permutations such that $\pi(m) = m$ holds.

Case 2: $c \neq m$.

First, we will show that there always exists a permutation π_1 such that $\pi_1(m) = c$. Let

$$m = (b_1, b_2, \cdots, b_n)$$

$$c = (c_1, c_2, \cdots, c_n).$$

Claim 1. *The number of* 1*'s positions in* $m \oplus c$*, i.e. the number of bits where* $b_i \neq c_i$*, must be an even number between* 2 *and* $2t$*.*

Idea: If there are p positions that stores 1 in m and 0 in c, then there must exist $q = p$ positions that stores 0 in m and 1 in c. Otherwise, c and m have different number of 1's which contradicts the definition of a permutation function.

Proof. Let $I = \{i_1, i_2, \cdots, i_p\}$ be the set of indices such that $b_{i_1} = 1, b_{i_2} = 1, \cdots, b_{i_p} = 1$ and $c_{i_1} = 0, c_{i_2} = 0, \cdots, c_{i_p} = 0$.
Let $J = \{j_1, j_2, \cdots, j_q\}$ be the set of indices such that $b_{j_1} = 0, b_{j_2} = 0, \cdots, b_{j_q} = 0$ and $c_{j_1} = 1, c_{j_2} = 1, \cdots, c_{j_q} = 1$.
x can be either 0 or 1 as long as there are only t total 1's in m and c.
For example,

$$m: \ \mathsf{x}\cdots\mathsf{x}\underset{\uparrow b_{j_1}}{0}\mathsf{x}\cdots\mathsf{x}\underset{\uparrow b_{i_1}}{1}\mathsf{x}\cdots\mathsf{x}\underset{\uparrow b_{i_2}}{1}\mathsf{x}\cdots\mathsf{x}\underset{\uparrow b_{j_2}}{0}\mathsf{x}\cdots\mathsf{x}\underset{\uparrow b_{j_q}}{0}\mathsf{x}\cdots\mathsf{x}\underset{\uparrow b_{i_p}}{1}\mathsf{x}\cdots$$

$$c: \ \mathsf{x}\cdots\mathsf{x}\underset{\uparrow c_{j_1}}{1}\mathsf{x}\cdots\mathsf{x}\underset{\uparrow c_{i_1}}{0}\mathsf{x}\cdots\mathsf{x}\underset{\uparrow c_{i_2}}{0}\mathsf{x}\cdots\mathsf{x}\underset{\uparrow c_{j_2}}{1}\mathsf{x}\cdots\mathsf{x}\underset{\uparrow c_{j_q}}{1}\mathsf{x}\cdots\mathsf{x}\underset{\uparrow c_{i_p}}{0}\mathsf{x}\cdots$$

Note that $p, q \leqslant t$ and $p + q \leqslant n$. There are same number of 1's in both m and c because $\pi_1(m) = c$ is a permutation.
Since there are p positions that stores 1 in m and 0 in c and there are in total t positions in m with 1, then there are $(t - p)$ positions in both m and c that have 1 at the same place, i.e. there are $(t - p)$ such k that $b_k = c_k = 1$. Similarly, because there are q positions that stores 0 in m and 1 in c and there are in total t positions in c with 1, then there are $(t - q)$ positions in both m and c that have 1 at the same place, i.e. there are $(t - q)$ such k that $b_k = c_k = 1$. Therefore,

$$(t - p) = (t - q) \implies p = q.$$

Thus, if there are p positions that stores 1 in m and 0 in c, then there must exist $q = p$ positions that stores 0 in m and 1 in c. There are $2p$ positions that $b_i \neq c_i$.
So we conclude that the number of bits where $b_i \neq c_i$ must be an even number between 2 and $2t$. □

We construct a permutation π_1 that swaps the i_kth bit with the j_kth bit in message m and the remaining positions stay the same.

$$\pi_1(i_1) = j_1, \pi_1(i_2) = j_2, \cdots, \pi_1(i_p) = j_p.$$

Such permutation exists because of Claim 1 above.
Observe that $\pi_1(m) = c$ holds.

Claim 2. *For $c \neq m$, there exists $(n - t)!t!$ different permutations (secret keys) π such that $\mathsf{Enc}_{sk}(m) = \pi(m) = c$, i.e. $wt(m, c) = (n - t)!t!$.*

Proof. Fix $m \in \mathcal{M}$ and $c \in \mathcal{C}$. Let π_1 be the permutation constructed as above and $\pi_1(m) = c$ holds.
In case 1, we have shown that if $m = c$, then there exists $(n-t)!t!$ different permutations that $\pi_2(c) = c$.
Then, $\pi = \pi_2 \circ \pi_1$ where $\pi_1(m) = c$ and $\pi_2(c) = c$ forms **all** permutations that $\pi(m) = c$.
If there exists a permutation $\pi \neq \pi_2 \circ \pi_1$ for all possible $\pi_2(c) = c$, then by the argument used Claim 1, π permutes a bit position outside the index set $I \cup J$ with a bit position inside $I \cup J$ in which case $\pi(m) = c$ no longer holds.
Therefore, there are $(n - t)!t!$ possible permutations that $\pi(m) = c$ holds. □

An alternative proof for Claim 2 provided by a student is as follows

Proof.
- $wt(m, c) \geqslant (n-t)!t!$.
  In case 1, we have shown that if $m = c$, then there exists $(n-t)!t!$ different permutations that $\pi_2(c) = c$. So far, we have constructed a π_1 such that $\pi_1(m) = c$. Then,
  $$\pi_2 \circ \pi_1(m) = \pi_2(\pi_1(m)) = \pi_2(c) = c.$$
  There are $(n-t)!t!$ different possible π_2 implies there are at least $(n-t)!t!$ different possible $\pi = \pi_2 \circ \pi_1$, i.e. $wt(m, c) \geqslant (n-t)!t!$.
- $wt(m, c) \leqslant (n-t)!t!$.
  For any permutation $\pi(m) = c$, and the permutation $\pi_1(m) = c$ as constructed above, there exists a permutation $\pi_2(c) = c$ such that $\pi = \pi_2 \circ \pi_1$. Since there are $(n-t)!t!$ different possible π_2, then there can be at most $(n-t)!t!$ distinct π.

□

Combining the two case, we have for each m and c, $\mathrm{wt}(m, c) = (n-t)!t!$, the encryption scheme is secure.

2. **Equivalent definition of Perfect Secrecy (15 points).** In the lecture, we defined the perfect security for any private-key encryption scheme $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ as follows. For any message m, cipher-text c, and apriori probability distribution $\mathbb{M}$ over the set of messages, we have:

$$\mathbb{P}\left[\mathbb{M} = m | \mathbb{C} = c\right] = \mathbb{P}\left[\mathbb{M} = m\right]$$

Show that the above definition is equivalent to the following alternative definition. For all messages m, m', cipher-text c, and apriori probability distribution $\mathbb{M}$ over the set of messages, we have:

$$\mathbb{P}\left[\mathbb{C} = c | \mathbb{M} = m\right] = \mathbb{P}\left[\mathbb{C} = c | \mathbb{M} = m'\right],$$

Remarks:

(a) Proving equivalence means that you have to show that the first definition implies the second definition. And the second definition also implies the first definition.

(b) Additionally, in this problem, for simplicity, assume that in the probability expressions, no "division by error" occurs.

Solution.

Forward direction : We are given that for any message m, cipher-text c, and a priori probability distribution $\mathbb{M}$ over the set of messages, we have:

$$\mathbb{P}\left[\mathbb{M} = m | \mathbb{C} = c\right] = \mathbb{P}\left[\mathbb{M} = m\right]$$

We can use Baye's rule to do the following manipulation :

$$\begin{aligned}
\Pr[\mathbb{M} = m | \mathbb{C} = c] &= \Pr[\mathbb{M} = m] \\
\frac{\Pr[\mathbb{M} = m, \mathbb{C} = c]}{\Pr[\mathbb{C} = c]} &= \Pr[\mathbb{M} = m] \\
\frac{\Pr[\mathbb{M} = m, \mathbb{C} = c]}{\Pr[\mathbb{M} = m]} &= \Pr[\mathbb{C} = c] \\
\Pr[\mathbb{C} = c | \mathbb{M} = m] &= \Pr[\mathbb{C} = c]
\end{aligned}$$

Since the RHS is independent of $\mathbb{M} = m$, the above expression must be true for any $\mathbb{M} = m$, so we can write $\Pr[\mathbb{C} = c | \mathbb{M} = m'] = \Pr[\mathbb{C} = c]$. Therefore we have that $\Pr[\mathbb{C} = c | \mathbb{M} = m] = \Pr[\mathbb{C} = c | \mathbb{M} = m']$.

Backward direction : We are given that for all messages m, m', cipher-text c, and a priori probability distribution $\mathbb{M}$ over the set of messages, we have:

$$\mathbb{P}\left[\mathbb{C} = c | \mathbb{M} = m\right] = \mathbb{P}\left[\mathbb{C} = c | \mathbb{M} = m'\right] = \alpha \text{ (say)}$$

Observe that

$$\begin{aligned}
\Pr[\mathbb{C} = c] &= \sum_{m \in \mathcal{M}} \Pr[\mathbb{C} = c, \mathbb{M} = m] \\
&= \sum_{m \in \mathcal{M}} \Pr[\mathbb{C} = c | \mathbb{M} = m] \Pr[\mathbb{M} = m] \\
&= \sum_{m \in \mathcal{M}} \alpha \Pr[\mathbb{M} = m] \\
&= \alpha \sum_{m \in \mathcal{M}} \Pr[\mathbb{M} = m] \\
&= \alpha \times 1 = \alpha
\end{aligned} \tag{1}$$

Consider the LHS of the expression that we have to prove

$$\begin{aligned}
\Pr[\mathbb{M} = m | \mathbb{C} = c] &= \frac{\Pr[\mathbb{M} = m, \mathbb{C} = c]}{\Pr[\mathbb{C} = c]} \\
&= \frac{\Pr[\mathbb{C} = c | \mathbb{M} = m] \Pr[\mathbb{M} = m]}{\Pr[\mathbb{C} = c]} \\
&= \frac{\alpha \Pr[\mathbb{M} = m]}{\alpha} \\
&= \Pr[\mathbb{M} = m]
\end{aligned}$$

3. **Defining Perfect Security from Ciphertexts (15 points).** An upstart in the field of cryptography has proposed a new definition for perfect security of private-key encryption schemes. According to this new definition, a private-key encryption scheme $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ is perfectly secure if, for all apriori distribution $\mathbb{M}$ over the message space, and any two ciphertexts c and c', we have the following identity.

$$\mathbb{P}\left[\mathbb{C} = c\right] = \mathbb{P}\left[\mathbb{C} = c'\right]$$

Show that the definition in the class does not imply this new definition.

Remark. You need to construct a private-key encryption scheme that is secure according to the definition we learned in class. However, this scheme does not satisfy the new definition.

Solution.

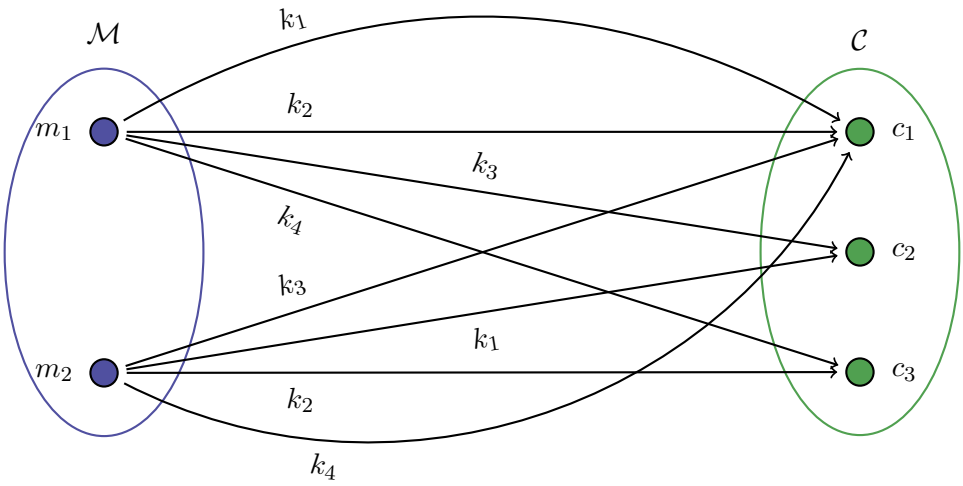

Figure 1: Corresponding graph of encryption scheme Π

Let $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ denote the encryption scheme defined on message space $\mathcal{M} = \{m_1, m_2\}$ such that encryption algorithm Gen chooses a key from set $\{k_1, k_2, k_3, k_4\}$ uniformly at random and the ciphertext space is defined as $\mathcal{C} := \{c_1, c_2, c_3\}$. Encryption scheme is defined in the following table.

	m_1	m_2
k_1	c_1	c_2
k_2	c_1	c_3
k_3	c_2	c_1
k_4	c_3	c_1

The corresponding graph for encryption scheme Π is given in figure 1.

We have

$$\Pr[\mathbb{C} = c_1 | \mathbb{M} = m_1] = \Pr[\mathbb{K} \in \{k_1, k_2\} | \mathbb{M} = m_1] = \Pr[\mathbb{K} \in \{k_1, k_2\}] = \frac{2}{4} = \frac{1}{2}$$

$$\Pr[\mathbb{C} = c_1 | \mathbb{M} = m_2] = \Pr[\mathbb{K} \in \{k_3, k_4\} | \mathbb{M} = m_2] = \Pr[\mathbb{K} \in \{k_3, k_4\}] = \frac{2}{4} = \frac{1}{2}$$

$$\Pr[\mathbb{C} = c_2 | \mathbb{M} = m_1] = \Pr[\mathbb{K} = k_3 | \mathbb{M} = m_1] = \Pr[\mathbb{K} = k_3] = \frac{1}{4}$$
$$\Pr[\mathbb{C} = c_2 | \mathbb{M} = m_2] = \Pr[\mathbb{K} = k_1 | \mathbb{M} = m_2] = \Pr[\mathbb{K} = k_1] = \frac{1}{4}$$
$$\Pr[\mathbb{C} = c_3 | \mathbb{M} = m_1] = \Pr[\mathbb{K} = k_4 | \mathbb{M} = m_1] = \Pr[\mathbb{K} = k_4] = \frac{1}{4}$$
$$\Pr[\mathbb{C} = c_3 | \mathbb{M} = m_2] = \Pr[\mathbb{K} = k_2 | \mathbb{M} = m_2] = \Pr[\mathbb{K} = k_2] = \frac{1}{4}$$

Therefore, for any $c \in \mathcal{C}$, we have $\Pr[\mathbb{C} = c | \mathbb{M} = m_1] = \Pr[\mathbb{C} = c | \mathbb{M} = m_2]$ which according to question 1, implies that $\Pr[\mathbb{M} = m | \mathbb{C} = c] = \Pr[\mathbb{M} = m]$ for any chipertext c, any message m and any probability distribution $\mathbb{M}$ over message space. Note that if we want to prove $\Pr[\mathbb{M} = m | \mathbb{C} = c] = \Pr[\mathbb{M} = m]$ directly, then we need to prove it for any arbitrary probability distribution $\mathbb{M}$ not only uniform distribution. However,we have:

$$\Pr[\mathbb{C} = c_1] = \Pr[\mathbb{C} = c_1 | \mathbb{M} = m_1] \Pr[\mathbb{M} = m_1] + \Pr[\mathbb{C} = c_1 | \mathbb{M} = m_2] \Pr[\mathbb{M} = m_2] \quad (2)$$
$$= \frac{1}{2} \times \Pr[\mathbb{M} = m_1] + \frac{1}{2} \times \Pr[\mathbb{M} = m_2] = \frac{1}{2} \quad (3)$$

and

$$\Pr[\mathbb{C} = c_2] = \Pr[\mathbb{C} = c_2 | \mathbb{M} = m_1] \Pr[\mathbb{M} = m_1] + \Pr[\mathbb{C} = c_2 | \mathbb{M} = m_2] \Pr[\mathbb{M} = m_2] \quad (4)$$
$$= \frac{1}{4} \times \Pr[\mathbb{M} = m_1] + \frac{1}{4} \times \Pr[\mathbb{M} = m_2] = \frac{1}{4} \quad (5)$$

So, $\Pr[\mathbb{C} = c_1] \neq \Pr[\mathbb{C} = c_2]$ which means that the definition in the class does not imply the definition introduced in the question.

4. **One-time Pad for 4-Alphabet Words (8+8 points).** We interpret alphabets $\mathtt{a}, \mathtt{b}, \ldots, \mathtt{z}$ as integers $0, 1, \ldots, 25$, respectively. We will work over the group $(\mathbb{Z}_{26}^4, +)$, where $+$ is coordinate-wise integer sum $\mod 26$. For example, $\mathtt{abcx} + \mathtt{aczd} = \mathtt{adba}$.

   Now, consider the one-time pad encryption scheme over the group $(\mathbb{Z}_{26}^4, +)$.

   (a) What is the probability that the encryption of the message $\mathtt{nope}$ is the cipher text $\mathtt{nope}$?
   Solution.

$$\begin{aligned}\Pr[\mathsf{Enc}_{\mathsf{sk}}(\mathtt{nope}) = \mathtt{nope}] &= \Pr[\mathbb{C} = \mathtt{nope} | \mathbb{M} = \mathtt{nope}] \\ &= \Pr[\mathbb{SK} = aaaa | \mathbb{M} = \mathtt{nope}] \\ &= \Pr[\mathbb{SK} = aaaa] \quad \text{(key is chosen independent of message)} \\ &= \frac{1}{26^4} \quad \text{(key is chosen uniformly at random)}\end{aligned}$$

   (b) What is the probability that the encryption of the message $\mathtt{nope}$ is the cipher text $\mathtt{mice}$?
   Solution.

$$\begin{aligned}\Pr[\mathsf{Enc}_{\mathsf{sk}}(\mathtt{nope}) = \mathtt{mice}] &= \Pr[\mathbb{C} = \mathtt{mice} | \mathbb{M} = \mathtt{nope}] \\ &= \Pr[\mathbb{SK} = \text{zuna} | \mathbb{M} = \mathtt{nope}] \\ &= \Pr[\mathbb{SK} = \text{zuna}] \quad \text{(key is chosen independent of message)} \\ &= \frac{1}{26^4} \quad \text{(key is chosen uniformly at random)}\end{aligned}$$

5. **Lagrange Interpolation(7+7+6 points).** We want to derive a part of the Chinese Remainder Theorem using principles of Lagrange Interpolation. Our goal is the following

Suppose p and q are two distinct primes. Suppose $a \in \{0, \ldots, p-1\}$ and $b \in \{0, \ldots, q-1\}$. We want to find a natural number x such that $$x \pmod p = a \text{ and } x \pmod q = b$$

We shall proceed towards this objective incrementally (similar to the approach of Lagrange interpolation).

(a) Find a natural number x_p satisfying $x_p \pmod p = 1$, and $x_p \pmod q = 0$.

Solution.

In order for x_p to satisfy $x_p \pmod q = 0$, we know it has to be a multiple of q. Furthermore, using the result from Homework 2, we know that $x^{p-1} = 1 \mod p$, for any integer x that is not divisible by p. So, one value of x that we can choose is q (because p and q are distinct primes). Therefore, $x_p = q^{p-1}$ simultaneously satisfies $x_p = 0 \mod q$ and $x_p = 1 \mod p$.

(b) Find a natural number x_q satisfying $x_q \pmod{p} = 0$ and $x_q \pmod{q} = 1$.

Solution.

Similar to part (a) of our solution, we conclude that $x_q = p^{q-1}$ satisfies $x_q = 0 \mod p$ and $x_q = 1 \mod q$.

(c) Find a natural number x satisfying $x \pmod{p} = a$ and $x \pmod{q} = b$.

Solution.

We use parts (a) and (b) to claim that $x = ax_p + bx_q$ satisfies

$$x \mod p = ax_p \mod p + bx_q \mod p = a \times 1 + b \times 0 = a \mod p$$

and

$$x \mod q = ax_p \mod q + bx_q \mod q = a \times 0 + b \times 1 = b \mod q.$$

6. **An Illustrative Execution of Shamir's Secret Sharing Scheme (6+10+9 points).** We shall work over the field $(\mathbb{Z}_7, +, \times)$. We are interested in sharing a secret among 6 parties so that any 3 parties can reconstruct the secret, but no subset of 2 parties gain additional information about the secret.

   Suppose the secret is $s = 1$. The random polynomial of degree < 3 chosen during the secret sharing steps is $p(X) = 3X^2 + 2X + 1$.

   (a) What are the respective secret shares of parties 1, 2, 3, 4, 5, and 6?

   Solution.

   Recall that the secret share of party i is the evaluation of the polynomial $p(X)$ at $X = i$. Therefore, the secret shares of parties $1, 2, 3, 4, 5, 6$ are $6, 3, 6, 1, 2, 2$, respectively. We calculate one of them as an example:

   $$p(3) \mod 7 = 3 * 3^2 + 2 \times 3 + 1 \mod 7 = 27 + 6 + 1 \mod 7 = 34 \mod 7 = 6$$

(b) Suppose parties 1, 3, and 5 are interested in reconstructing the secret. Run the Lagrange Interpolation algorithm as explained in the class.

(*Remark:* It is essential to show the step-wise reconstruction procedure to score full points. In particular, you need to write down the polynomials $p_1(X)$, $p_3(X)$, and $p_5(X)$.)

Solution. We want to construct a polynomial of degree at most 2 that passes through 3 points $(x_1, y_1) = (1, 6), (x_2, y_2) = (3, 6), (x_3, y_3) = (5, 2)$.

The sub-problem i is to construct a polynomial $p_i(X)$ of degree at most 2 that passes through (x_i, y_i) and $(x_j, 0)$ where $j \neq i$. The following is the formula of the polynomial $p_i(X)$.

$$p_i(X) = y_i \cdot \prod_{j \neq i} \frac{(X - x_j)}{(x_i - x_j)} = c_i \cdot \prod_{j \neq i} (X - x_j)$$

where $c_i \cdot \prod_{j \neq i}(x_i - x_j) = y_i \mod 7$.

i. Sub-problem 1: $c_1 \cdot (1-3)(1-5) = 6 \mod 7$, which implies $c_1 = 6$. Thus $p_1(X) = 6(X-3)(X-5) = 6X^2 + X + 6$.

ii. Sub-problem 2: $c_2 \cdot (3-1)(3-5) = 6 \mod 7$, which implies $c_2 = 2$. Thus $p_1(X) = 2(X-1)(X-5) = 2X^2 + 2X + 3$.

iii. Sub-problem 3: $c_3 \cdot (5-1)(5-3) = 2 \mod 7$, which implies $c_3 = 2$. Thus $p_1(X) = 2(X-1)(X-3) = 2X^2 + 6X + 6$.

Therefore, we have

$$\begin{aligned} & p(X) \\ &= p_1(X) + p_2(X) + p_3(X) \\ &= 6X^2 + X + 6 + 2X^2 + 2X + 3 + 2X^2 + 6X + 6 \\ &= 6X^2 + 2X^2 + 2X^2 + X + 2X + 6X + 6 + 3 + 6 \\ &= 3X^2 + 2X + 1 \end{aligned}$$

(c) Suppose parties 1, and 2 get together. Let $q_{\widetilde{s}}(X)$ be the polynomial that is consistent with their shares and the point $(0, \widetilde{s})$, for each $\widetilde{s} \in \mathbb{Z}_p$. Write down the polynomials $q_0(X)$, $q_1(X)$, $\ldots$, $q_6(X)$.

Solution.

Note that the polynomial, for $\widetilde{z} \in \mathbb{Z}_7$, is

$$q_{\widetilde{s}}(X) = c_{\widetilde{s}}(X-1)(X-2) + \alpha(X) + \beta(X) \text{ such that } q_{\widetilde{s}}(0) = \widetilde{s}$$

where the following constraints are satisfied for the polynomials $\alpha(X), \beta(X)$, and $\gamma(X)$.

$$\alpha(X) = c_1 X(X-2) \text{ such that } \alpha(1) = 6$$
$$\beta(X) = c_2 X(X-1) \text{ such that } \beta(2) = 3$$

Solving, we get $\alpha(X) = X(X-2) = X^2 + 5X$ and $\beta(X) = 5X(X-1) = 5X^2 + 2X$,. Since $q_{\widetilde{s}}(0) = \widetilde{s}$, we can find $c_{\widetilde{s}}$ using the following equation

$$c_{\widetilde{s}} \cdot 2 = \widetilde{s} \mod 7 \text{ for every } \widetilde{s} \in \mathbb{Z}_7.$$

Therefore, we have

$$q_0(X) = 0(X-1)(X-2) + \alpha(X) + \beta(X) = 0(X^2+4X+2) + 6X^2 = 6X^2$$
$$q_1(X) = 4(X-1)(X-2) + \alpha(X) + \beta(X) = 4(X^2+4X+2) + 6X^2 = 3X^2 + 2X + 1$$
$$q_2(X) = 1(X-1)(X-2) + \alpha(X) + \beta(X) = 1(X^2+4X+2) + 6X^2 = 4X + 2$$
$$q_3(X) = 5(X-1)(X-2) + \alpha(X) + \beta(X) = 5(X^2+4X+2) + 6X^2 = 4X^2 + 6X + 3$$
$$q_4(X) = 2(X-1)(X-2) + \alpha(X) + \beta(X) = 2(X^2+4X+2) + 6X^2 = X^2 + X + 4$$
$$q_5(X) = 6(X-1)(X-2) + \alpha(X) + \beta(X) = 6(X^2+4X+2) + 6X^2 = 5X^2 + 3X + 5$$
$$q_6(X) = 3(X-1)(X-2) + \alpha(X) + \beta(X) = 3(X^2+4X+2) + 6X^2 = 2X^2 + 5X + 6$$

7. **A bit of Counting (8+8+9 points).** In this problem, we will do some counting related to polynomials that pass through a given set of points in the plane. We already did this counting (slightly informally) in the class. Writing the solution for this problem shall make the solution's intuition more concrete.

   We are working over the field $(\mathbb{Z}_p, +, \times)$, where p is a prime number. Let $\mathcal{P}_t$ be the set of all polynomials in the indeterminate X with degree $< t$ and coefficients in $\mathbb{Z}_p$.

   (a) Let (x_1, y_1), (x_2, y_2), $\ldots$, and (x_t, y_t) be t points in the plane $\mathbb{Z}_p^2$. We have that $x_i \neq x_j$ for all $i \neq j$; that is, the first coordinates of the points are all distinct.

   Prove that there exists a *unique polynomial* in $\mathcal{P}_t$ that passes through these t points.

   (Hint: Use Lagrange Interpolation and Schwartz–Zippel Lemma.)

   Solution.

   Lagrange Interpolation demonstrates that there is at least one polynomial passing through these points that has degree at most $(t-1)$.

   Now, we want to show that there is at most one polynomial passing through these points. We shall prove this by contradiction. Assume that there are two distinct polynomials $A(X)$ and $B(X)$ of degree $< t$ such that both pass through all these points. Therefore, the polynomial $C(X) := A(X) - B(X)$ is not the zero polynomial (because $A(X)$ and $B(X)$ are distinct). Simultaneously, the polynomial $C(X)$ has $\{x_1, x_2, \ldots, x_t\}$ as its roots. By Schwartz–Zippel Lemma, the polynomial $C(X)$ must be the zero polynomial (because it has t roots and degree $< t$). Hence, contradiction.

(b) Let (x_1, y_1), (x_2, y_2), $\ldots$, and (x_{t-1}, y_{t-1}) be $(t-1)$ points in the plane $\mathbb{Z}_p^2$. We have that $x_i \neq x_j$ for all $i \neq j$; that is, the first coordinates of the points are all distinct.

Prove that p polynomials in $\mathcal{P}_t$ pass through these $(t-1)$ points.

Solution.

Let x_t be distinct from $\{x_1, \ldots, x_{t-1}\}$. Using part (a) of the result, there exists a unique polynomial passing through

$$\{(x_1, y_1), (x_2, y_2), \ldots, (x_{t-1}, y_{t-1}), (x_t, 0)\}$$

Similarly, there exists a unique polynomial passing through

$$\{(x_1, y_1), (x_2, y_2), \ldots, (x_{t-1}, y_{t-1}), (x_t, 1)\}$$

And this polynomial is different from the previous one (because they evaluate to different values at x_t).

Similarly, there exists a unique polynomial passing through

$$\{(x_1, y_1), (x_2, y_2), \ldots, (x_{t-1}, y_{t-1}), (x_t, 2)\}$$

that is different from all previous ones.

And so on...

Formally, we argue as follows. Considering each value of $y \in \{0, 1, \ldots, p-1\}$, we obtain a distinct polynomial that passes through the points

$$\{(x_1, y_1), (x_2, y_2), \ldots, (x_{t-1}, y_{t-1}), (x_t, y)\}$$

So, a total of p polynomials pass through

$$\{(x_1, y_1), (x_2, y_2), \ldots, (x_{t-1}, y_{t-1})\}$$

(c) Let (x_1, y_1), (x_2, y_2), $\ldots$, and (x_k, y_k) be k points in the plane $\mathbb{Z}_p^2$, where $k \leqslant t$. We have that $x_i \neq x_j$ for all $i \neq j$; that is, the first coordinates of the points are all distinct.
Prove that p^{t-k} polynomials in $\mathcal{P}_t$ pass through these k points.

Solution.

Following a similar counting argument as in part (b), consider the points

$$(x_1, y_1), \ldots, (x_k, y_k), (x_{k+1}, r_1), \ldots, (x_t, r_{t-k})$$

Where the first coordinates are all distinct from each other. Since each $r_i \in \{r_1, \ldots r_{t-k}\}$ can take p values ($\{0, 1, \ldots, p-1\}$), we obtain p^{t-k} polynomials.

8. **Monotone Circuits for Secret Sharing (15 points).** Recall that the *additive secret sharing* scheme secret-shares a secret among n parties that can be recovered when all parties are present. The *repetitive secret sharing* scheme secret-shares a secret among n parties that any party can recover. Intuitively, these two secret sharing schemes implement the atomic access structure accepted by the AND and the OR gates, respectively.

   Any monotone circuit can be expressed using AND and OR gates. A monotone circuit also accepts the threshold access structure. For example, consider the access structure of $n = 3$ parties where any $k = 2$ parties can reconstruct the secret. The following monotone circuit represents the access structure.

   $$(A \wedge B) \vee (A \wedge C) \vee (B \wedge C)$$

   Construct a secret sharing scheme for this access structure by recursively using additive and repetitive secret sharing schemes.

   Solution.

   First, the central authority shares the secret to each two party combination using repetitive secret sharing scheme (OR) such that any group of the two party combinations can reconstruct the secret.

   According to the access structure, the three possible combinations of a two party groups are $\{(A, B), (A, C), (B, C)\}$. To share the secret s among two parties, we uses the additive secret sharing scheme. First generate a random numbers r_1. Give r_1 to party 1 and $s - r_1$ to party 2.

   Every two parties can reconstruct the secret by summing their secret shares together.

Collaborators :