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.

   The scheme above is not secure.
   For a scheme to be secure, it must fulfill two conditions - it must be private and must be correct.
   Furthermore, the theorem mentioned in Lecture 8 mentions that a correct and private private-key encryption scheme has $|K| \geqslant |M|$.
   However, the case here for the given encryption scheme above is that $|M| = 13$, while $|K| = 12$, which means that $|K| \leqslant |M|$. This means that there $\exists$ two distinct messages m_i and m_j, such that $sk_i = sk_j$ in the message to ciphertext mappings, violating the correctness property.
   Hence, the 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.

The scheme is not secure, and we can prove using a counterexample which shows that for a given ciphertext and 2 distinct messages, $wt(m, c) \neq wt(m', c)$, and thus, encryption scheme is not private and thus not secure.

Let $m = 12$, $m' = 10$, and $c = 12$. Thus, $wt(m, c) = 2$ because only $sk \in \{0, 12\}$ will $Enc_{sk}(m) = c$. However, $wt(m', c) = 1$ because only $sk \in \{2\}$ will $Enc_{sk}(m') = c$. Hence, this shows that $wt(m, c) \neq wt(m', c)$ and thus, encryption scheme is not private and hence 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.

The scheme is secure because it is private and correct.
First, the message space M is the set of all odd integers up till 2023 and the key space K is the set of all even integers up till 2022. Furthermore, the ciphertext space, $C = \{1, 3, 5, ..., 2021, 2023\}$, because $Enc_{sk}(m) = (sk + m)\ mod\ 2024$ and the fact that the summation of an even integer with an odd integer yields an odd integer as the result.

Next, since C and M contains only odd integers, let an arbitrary ciphertext $c = 2i - 1$, for some $i \in \{1, 2, ..., 1011, 1012\}$ and let an arbitrary message $m = 2j - 1$ such that $Enc_{sk}(m) = c$, for some $j \in \{1, 2, ..., 1011, 1012\}$. Then, since $Enc_{sk}(m) = c, \exists\ only\ 1\ sk \in K$, because $sk = 2(i - j)\ mod\ 24$.
This means that there are 2 cases, when $i \geqslant j$ or when $i < j$.
1. Case $i \geqslant j$: The key sk would be equal to $2(i - j)$.
2. Case $i < j$: The key sk would be equal to $2(i - j) + 2024$ because $(i - j)$ would be negative and thus, would result in an even integer which is strictly less than 2024.
In both of these cases, the key $sk \in K$. This is because the $1 \leqslant sk \leqslant 2023$. Then, this means that $wt(m, c) = 1,\ \forall m, c \in M, C$ respectively, because there is only 1 key $sk \in K$ such that $Enc_{sk}(m) = c$. Hence, since $\forall m, c,\ wt(m, c) = 1$, encryption scheme is both private and correct, making it a secure scheme.

(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 scheme is secure because it is private and correct.
Firstly, the scheme is correct because the ciphertext space consists of permutations of the message space. This means that the ciphertext space is essentially also bounded by n(number of bits) and t(number of 1's), resulting in $|C| = |M|$. Thus, by the theorem discussed in lecture, this would mean that $|C| \geqslant |M|$ and hence, this implies that this encryption scheme is correct.

Secondly, the scheme is private because given two distinct messages m, m' with both containing n bits and t number of 1s, and ciphertext c such that $Enc_{sk}(m) = Enc_{sk}(m') = c$, we can note that since 1's and 0's are identical in value, i.e. if $b_0 = 1, b_1 = 1, then b_0 = b_1$. Thus, there $\exists$ at most one $sk \in K$ such that $Enc_{sk}(m) = c$. This would mean that there may be multiple witnesses for an encryption of a message as well. However, since c is also bounded by the constraints of n and t, this implies that $\text{weight}(m, c) = \text{weight}(m', c)$. Thus, making the scheme private.

Furthermore, since from above we can note that $|K| \geqslant |M|$ from the argument that there are multiple witnesses for the encryption of a message. Thus, as $|K| \geqslant |M|$, from theorem discussed in lecture, the encryption scheme is therefore private and correct. Hence, this makes the encryption scheme 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.

Proving equivalence in the forward direction:
This means that we are proving $\mathbb{P}[\mathbb{M} = m|\mathbb{C} = c] = \mathbb{P}[\mathbb{M} = m]$ implies that $\mathbb{P}[\mathbb{C} = c|\mathbb{M} = m] = \mathbb{P}[\mathbb{C} = c|\mathbb{M} = m']$, as the forward direction.
Given any message m, cipher-text c, and apriori probability distribution $\mathbb{M}$ over the set of messages, $\mathbb{P}[\mathbb{M} = m|\mathbb{C} = c] = \mathbb{P}[\mathbb{M} = m]$.
First, using Bayes Rule,

$$\mathbb{P}[\mathbb{M} = m|\mathbb{C} = c] = \frac{\mathbb{P}[M = m, C = c]}{\mathbb{P}[C = c]}$$

This means that:

$$\frac{\mathbb{P}[M = m, C = c]}{\mathbb{P}[C = c]} = \mathbb{P}[M = m]$$

$$\frac{\mathbb{P}[M = m, C = c]}{\mathbb{P}[M = m]} = \mathbb{P}[C = c]$$

(by algebraic manipulation)

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

Since the right hand side of the expression is now implied to be independent of $\mathbb{M} = m$, this means that the above expression will be true for any $m \in M$, thus, this means that $\mathbb{P}[\mathbb{C} = c|\mathbb{M} = m'] = \mathbb{P}[\mathbb{C} = c] = \mathbb{P}[\mathbb{C} = c|\mathbb{M} = m]$.
Hence, this means that $\mathbb{P}[\mathbb{C} = c|\mathbb{M} = m] = \mathbb{P}[\mathbb{C} = c|\mathbb{M} = m']$.

Proving equivalence in the backward direction:
This means that we are proving $\mathbb{P}[\mathbb{C} = c|\mathbb{M} = m] = \mathbb{P}[\mathbb{C} = c|\mathbb{M} = m']$ implies that $\mathbb{P}[\mathbb{M} = m|\mathbb{C} = c] = \mathbb{P}[\mathbb{M} = m]$, as the backward direction.
Given any message $m, m' \in M$, cipher-text c, and apriori probability distribution $\mathbb{M}$ over the

set of messages, $\mathbb{P}[\mathbb{C} = c|\mathbb{M} = m] = \mathbb{P}[\mathbb{C} = c|\mathbb{M} = m']$.
First, suppose that the above equates to some value γ.
Then,

$$\mathbb{P}[\mathbb{C} = c] = \sum_{m \in M} \mathbb{P}[\mathbb{C} = c, \mathbb{M} = m]$$

(by definition of event space)

$$= \sum_{m \in M} \mathbb{P}[\mathbb{C} = c|\mathbb{M} = m] \cdot \mathbb{P}[\mathbb{M} = m]$$

(by Bayes Rule)

$$= \sum_{m \in M} \gamma \cdot \mathbb{P}[\mathbb{M} = m]$$

(since we let $\mathbb{P}[\mathbb{C} = c|\mathbb{M} = m] = \gamma$ above)

$$= \gamma \cdot \sum_{m \in M} \mathbb{P}[\mathbb{M} = m]$$

$$= \gamma \cdot 1$$

(by probability axiom that $\mathbb{P}(S) = 1$, where S is the sample space)

$$= \gamma$$

This means that $\mathbb{P}[\mathbb{C} = c] = \gamma$.
Next,

$$\mathbb{P}[\mathbb{M} = m|\mathbb{C} = c] = \frac{\mathbb{P}[\mathbb{M} = m, \mathbb{C} = c]}{\mathbb{P}[\mathbb{C} = c]}$$

(By definition of conditional probability)

$$= \frac{\mathbb{P}[\mathbb{C} = c|\mathbb{M} = m] \cdot \mathbb{P}[\mathbb{M} = m]}{\mathbb{P}[\mathbb{C} = c]}$$

(Using Bayes Rule)

$$= \frac{\gamma \cdot \mathbb{P}[\mathbb{M} = m]}{\gamma}$$

(From result derived above that $\mathbb{P}[\mathbb{C} = c|\mathbb{M} = m] = \mathbb{P}[\mathbb{C} = c] = \gamma$)

$$= \mathbb{P}[\mathbb{M} = m]$$

Thus, $\mathbb{P}[\mathbb{M} = m|\mathbb{C} = c] = \mathbb{P}[\mathbb{M} = m]$ and we are done showing the backward direction, where $\mathbb{P}[\mathbb{C} = c|\mathbb{M} = m] = \mathbb{P}[\mathbb{C} = c|\mathbb{M} = m']$ implies that $\mathbb{P}[\mathbb{M} = m|\mathbb{C} = c] = \mathbb{P}[\mathbb{M} = m]$.

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.

Let us define $\alpha = (Gen, Enc, Dec)$ as a private-key encryption scheme defined on message space $\mathbb{M} = \{m_1, m_2\}$, and that Gen chooses a key from the set $\mathbb{K} = \{k_1, k_2, k_3, k_4\}$ uniformly at random and the ciphertext space is defined as $\mathbb{C} = \{c_1, c_2, c_3\}$. Let us define the encryption as follows:

$$Enc_{k_1}(m_1) = c_1$$

$$Enc_{k_2}(m_1) = c_1$$

$$Enc_{k_3}(m_1) = c_2$$

$$Enc_{k_4}(m_1) = c_3$$

$$Enc_{k_1}(m_2) = c_3$$

$$Enc_{k_2}(m_2) = c_2$$

$$Enc_{k_3}(m_2) = c_1$$

$$Enc_{k_4}(m_2) = c_1$$

Thus, we get the following results:

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

(since key k is chosen independently from message m)

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

(since key k is chosen independently from message m)

$$P[\mathbb{C} = c_2|\mathbb{M} = m_1] = P[k \in \{k_3\}|\mathbb{M} = m_1] = P[k \in \{k_3\}] = \frac{1}{4}$$

$$P[\mathbb{C} = c_2|\mathbb{M} = m_2] = P[k \in \{k_2\}|\mathbb{M} = m_2] = P[k \in \{k_2\}] = \frac{1}{4}$$

$$P[\mathbb{C} = c_3|\mathbb{M} = m_1] = P[k \in \{k_4\}|\mathbb{M} = m_1] = P[k \in \{k_4\}] = \frac{1}{4}$$

$$P[\mathbb{C} = c_3|\mathbb{M} = m_2] = P[k \in \{k_1\}|\mathbb{M} = m_2] = P[k \in \{k_1\}] = \frac{1}{4}$$

Thus, we have verified that $\forall c \in \mathbb{C}$, $P[\mathbb{C} = c|\mathbb{M} = m_1] = P[\mathbb{C} = c|\mathbb{M} = m_2]$. We can then apply the result from question 2, which implies that $P[\mathbb{M} = m|\mathbb{C} = c] = P[\mathbb{M} = m]$, given any message m, ciphertext c, and apriori distribution $\mathbb{M}$ over the message space. This scheme is also correct because $|C| \geqslant |M|$ and it is also private because for any $c \in \mathbb{C}$ and the two distinct messages $m_1, m_2 \in M$, weight(m_1, c) = weight(m_2, c). Hence, since the scheme is correct and private, it is secure.
However, the problem here is that:

$$P[\mathbb{C} = c_1] = P[\mathbb{C} = c_1|\mathbb{M} = m_1]\cdot P[\mathbb{M} = m_1] + P[\mathbb{C} = c_1|\mathbb{M} = m_2]\cdot P[\mathbb{M} = m_2] = (\frac{1}{2}\cdot\frac{1}{2}) + (\frac{1}{2}\cdot\frac{1}{2}) = \frac{1}{2}$$

$$P[\mathbb{C} = c_2] = P[\mathbb{C} = c_2|\mathbb{M} = m_1]\cdot P[\mathbb{M} = m_1] + P[\mathbb{C} = c_2|\mathbb{M} = m_2]\cdot P[\mathbb{M} = m_2] = (\frac{1}{4}\cdot\frac{1}{2}) + (\frac{1}{4}\cdot\frac{1}{2}) = \frac{1}{4}(\neq \frac{1}{2})$$

Hence, we can note that $P[\mathbb{C} = c_1] \neq P[\mathbb{C} = c_2]$, which goes to show that the definition in the class does not imply this new definition that $P[\mathbb{C} = c] = P[\mathbb{C} = c']$.

4. **One-time Pad for 4-Alphabet Words (8+8 points).** We interpret alphabets $\texttt{a}, \texttt{b}, \ldots, \texttt{z}$ 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, $\texttt{abcx} + \texttt{aczd} = \texttt{adba}$.

   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 `nope` is the cipher text `nope`?
   Solution.
   Probability that encryption of the message `nope` is ciphertext `nope` =

$$\mathbb{P}[Enc_{sk}(nope)]$$

$$= \mathbb{P}[\mathbb{C} = nope | \mathbb{M} = nope]$$

$$= \mathbb{P}[SK = aaaa | \mathbb{M} = nope]$$

   (since ciphertext generated depends on SK if M is fixed)

$$= \mathbb{P}[SK = aaaa]$$

   (since key is chosen independently of message in $Gen()$)

$$= (\frac{1}{26}) \cdot (\frac{1}{26}) \cdot (\frac{1}{26}) \cdot (\frac{1}{26})$$

   (since there are 26 alphabets and only a is desired to obtain desired ciphertext)

$$= (\frac{1}{26})^4$$

   (b) What is the probability that the encryption of the message `nope` is the cipher text `mice`?
   Solution.

Since $\texttt{nope} + \texttt{zuna} = \texttt{mice}$,
Probability that encryption of the message `nope` is ciphertext `mice`

$$= \mathbb{P}[\mathbb{C} = mice | \mathbb{M} = nope]$$

$$= \mathbb{P}[SK = zuna | \mathbb{M} = nope]$$

(since ciphertext generated depends on SK if M is fixed)

$$= \mathbb{P}[SK = zuna]$$

(since key is chosen independently of message in $Gen()$)

$$= (\frac{1}{26})^4$$

(since key is chosen uniformly at random)

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.

First, We know that for $x_p \ (mod\ q) = 0$, x_p has to be a factor of q.
Next, using Fermat's Little Theorem in HW2, that $x^{p-1} = 1 \ (mod\ p)$, for any integer x not divisible by p, we can use this result and the fact that x_p has to be a factor of q and a natural number that satisfies $x_p \pmod p = 1$, and $x_p \pmod q = 0$ would be

$$x_p = q^{p-1}$$

, since q is also not divisible by p as they are distinct primes.

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

Solution.

Following part (a), we can note that x_q to satisfy $x_q \ (mod\ p) = 0$ and $x_q \ (mod\ q) = 1$, a natural number that satisfies would be:

$$x_q = p^{q-1}$$

, which would satisfy $x_q \ (mod\ p) = 0$ and $x_q \ (mod\ q) = 1$.

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

Solution.

Following answers to part (a) and part (b), we can note that

$$x = a \cdot x_p + b \cdot x_q$$

, would satisfy the constraints above:

$$x \ (mod\ p) = a \cdot x_p \ (mod\ p) + b \cdot x_q \ (mod\ p)$$

$$= a \cdot 1 + b \cdot 0$$

(since $x_p \ (mod\ p) = 1$ and $x_q \ (mod\ p) = 0$)

$$= a \ (mod\ p)$$

$$x \ (mod\ q) = a \cdot x_p \ (mod\ q) + b \cdot x_q \ (mod\ q)$$

$$= a \cdot 0 + b \cdot 1$$

(since $x_p \ (mod\ q) = 0$ and $x_q \ (mod\ q) = 1$

$$= b \ (mod\ q)$$

Thus, we can conclude that this natural number $x = a \cdot x_p + b \cdot x_q$ satisfies $x \ (mod\ p) = a$ and $x \ (mod\ q) = b$.

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.

   The respective secret shares of parties 1, 2, 3, 4, 5 and 6 are the evaluation of the polynomial when $X = i$, where i corresponds to the secret share of party i.

   1. Thus, the secret share of party $1 = 3 \cdot (1)^2 + 2 \cdot (1) + 1 \ (mod\ 7) = 6 \ (mod\ 7)$.
   2. The secret share of party $2 = 3 \cdot (2)^2 + 2 \cdot (2) + 1 \ (mod\ 7) = 3 \ (mod\ 7)$
   3. The secret share of party $3 = 3 \cdot (3)^2 + 2 \cdot (3) + 1 \ (mod\ 7) = 6 \ (mod\ 7)$
   4. The secret share of party $4 = 3 \cdot (4)^2 + 2 \cdot (4) + 1 \ (mod\ 7) = 1 \ (mod\ 7)$
   5. The secret share of party $5 = 3 \cdot (5)^2 + 2 \cdot (5) + 1 \ (mod\ 7) = 2 \ (mod\ 7)$
   6. The secret share of party $6 = 3 \cdot (6)^2 + 2 \cdot (6) + 1 \ (mod\ 7) = 2 \ (mod\ 7)$

(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.

1. First, we need to construct a polynomial $p(X)$ with degree < 3 that passes through $(x_1, y_1) = (1, 6)$, $(x_2, y_2) = (3, 6)$ and $(x_3, y_3) = (5, 2)$.
2. Then, we need to construct a polynomial $p_i(X)$ for i^{th} subproblem, of degree < 3 that passes through (x_i, y_i) and $(x_j, 0)$, where $j \neq i$.
3. This means that

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

, where c_i is a constant and that

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

, by algebraic manipulation.
4. Thus,

$$p_1(X) = 6 \cdot \frac{(X-3)(X-5)}{(1-3)(1-5)}$$

$$= 6 \cdot (X-3) \cdot (X-5)$$

5.

$$p_2(X) = 6 \cdot \frac{(X-1)(X-5)}{(3-1)(3-5)}$$

$$= 2 \cdot (X-1) \cdot (X-5)$$

6.

$$p_3(X) = 2 \cdot \frac{(X-1)(X-3)}{(5-1)(5-3)}$$

$$= 2 \cdot (X-1) \cdot (X-3)$$

7. Therefore, we have

$$p(X) = p_1(X) + p_2(X) + p_3(X)$$

$$= 6(X^2 - X + 1) + 2(X^2 + X + 5) + 2(X^2 + 3X + 3)$$

(simplification of polynomials here to work with smaller coefficients)

$$= 6X^2 - 6X + 6 + 2X^2 + 2X + 10 + 2X^2 + 6X + 6$$

$$= 3X^2 + 2X + 1$$

(after simplification and taking *mod* 7 on coefficients)

(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 $q_0(X)$, $q_1(X)$, ..., $q_6(X)$.

Solution.

The corresponding polynomial is:

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

, such that $q_{\widetilde{s}}(X) = 0$ by definition and front part of the polynomial is derived from part (b), and $\alpha(X)$ and $\beta(X)$ represents the polynomials construted for the subproblem respectively for party 1 and party 2, which satisfies the following constraints:
1.

$$\alpha(X) = c_1(X)(X-2)$$

such that $\alpha(1) = 6$ (because polynomial passes through $(x_1, 0)$ and (x_2, y_2)).
2.

$$\beta(X) = c_2(X)(X-1)$$

such that $\beta(2) = 3$
Then, solving for c_1 using $\alpha(1)$:
$c_1(1)(1-2) = 6$ $(mod\ 7)$
$6 \cdot c_1 = 6$ $(mod\ 7)$
$c_1 = 6 \cdot modinv(6)$ $(mod\ 7)$
$= 36$ $(mod\ 7)$
$= 1$ $(mod\ 7)$
Next, solving for c_2 using $\beta(2)$:
$c_2(2)(2-1) = 3$
$2 \cdot c_2 = 3$
$c_2 = 3 \cdot modinv(2)$ (modinv(2) = 4)
$= 12$ $(mod\ 7)$
$= 5$ $(mod\ 7)$
Hence, $\alpha(X) = X(X-2)$ and $\beta(X) = 5X(X-1)$.

Next, since $q_{\widetilde{s}}(0) = \widetilde{s}$, $c_{\widetilde{s}} \cdot 2 = \widetilde{s}\ mod\ 7$, for all $\widetilde{s} \in \mathbb{Z}_7$.
This means that $c_{\widetilde{s}} = \widetilde{s} \cdot modinv(2)$ $(mod\ 7) = 4 \cdot c_{\widetilde{s}}$ $(mod\ 7)$.

Therefore, we then have:

$$q_0(X) = 0(X-1)(X-2) + \alpha(X) + \beta(X)$$

$$= X(X-2) + 5X(X-1)$$

$$= X^2 - 2X + 5X^2 - 5X$$

$$= 6X^2$$

(after simplification of coefficients with mod 7)
Next,

$$q_1(X) = 4(X-1)(X-2) + \alpha(X) + \beta(X)$$

$$= 4(X^2 - 3X + 2) + X(X-2) + 5X(X-1)$$

$$= 4X^2 + 2X + 1 + X^2 - 2X + 5X^2 - 5X$$

$$= 3X^2 + 2X + 1$$

Next,

$$q_2(X) = 1(X-1)(X-2) + \alpha(X) + \beta(X)$$

$$= X^2 - 3X + 2 + X(X-2) + 5X(X-1)$$

$$= X^2 - 3X + 2 + X^2 - 2X + 5X^2 - 5X$$

$$= 4X + 2$$

Next,

$$q_3(X) = 5(X-1)(X-2) + \alpha(X) + \beta(X)$$

$$= 5(X^2 - 3X + 2) + X(X-2) + 5X(X-1)$$

$$= 5X^2 - 15X + 10 + X^2 - 2X + 5X^2 - 5X$$

$$= 4X^2 + 6X + 3$$

(after simplification of coefficients with mod 7)
Next,

$$q_4(X) = 2(X-1)(X-2) + \alpha(X) + \beta(X)$$

$$= 2(X^2 - 3X + 2) + X(X - 2) + 5X(X - 1)$$

$$= 2X^2 + X + 4 + X^2 - 2X + 5X^2 - 5X$$

$$= X^2 + 2X + 4$$

Next,

$$q_5(X) = 6(X - 1)(X - 2) + \alpha(X) + \beta(X)$$

$$= 6(X^2 - 3X + 2) + X(X - 2) + 5X(X - 1)$$

$$= 6X^2 + 3X + 5 + X^2 - 2X + 5X^2 - 5X$$

$$= 5X^2 + 3X + 5$$

Lastly,

$$q_6(X) = 3(X - 1)(X - 2) + \alpha(X) + \beta(X)$$

$$= 3(X^2 - 3X + 2) + X(X - 2) + 5X(X - 1)$$

$$= 3X^2 + 5X + 6 + X^2 - 2X + 5X^2 - 5X$$

$$= 2X^2 + 5X + 6$$

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), ..., 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.

   From lecture, we know that Lagrange Interpolation provides one polynomial of degree $\leqslant t-1$ that passes through all of these points $(x_1, y_1), (x_2, y_2), ..., (x_t, y_t)$.
   Next, to prove that the polynomial is unique in $\mathcal{P}_t$ that passes through these t points, we can do a proof by contradiction.
   First, suppose that there are indeed two distinct polynomials $p(X)$ and $p'(X)$ of degree $\leqslant t-1$, such that both polynomials passes through all t points.
   Then, let $p^*(X) := p(X) - p'(X)$. We then note that for $i \in \{1, 2, ..., t\}$, at $X = x_i$, both $p(X)$ and $p'(X)$ evaluates to y_i (by definition of polynomial from Lagrange Interpolation). Thus, the polynomial $p^*(X)$ evaluates to $y_i - y_i = 0$, at $X = x_i$. This would mean that the polynomial $p^*(X)$ would have roots $X = x_1, X = x_2, ..., X = x_t$. Then, this means that $p^*(X)$ is a polynomial with degree $\leqslant t-1$ that has at least t roots. Thus, this implies that the polynomial $p^*(X)$, by the Schwartz-Zippel Lemma, is the zero-polynomial and hence, $p(X) = p'(X)$. This forms a contradiction with the initial assumption that $p(X)$ and $p'(X)$ are two distinct polynomials.
   Henceforth, the polynomial in $\mathcal{P}_t$ that passes through these t points is unique and it exists.

(b) Let (x_1, y_1), (x_2, y_2), ..., 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.

From the question, the first coordinates of the points are all distinct.
First, let us consider x_t, which is distinct from $\{x_1, x_2, ..., x_{t-1}\}$. Then, we can use the result from part (a) to claim that there is a unique polynomial passing through $(x_1, y_1), (x_2, y_2), ..., (x_{t-1}, y_{t-1}, (x_t, 0))$. Then, we can extend this claim to all $y_t \in \{0, 1, ..., p-1\}$. Thus, since the cardinality of the set is p, we can conclude that a total of p polynomials in $\mathcal{P}_t$ passes through these $t-1$ points.

(c) Let (x_1, y_1), (x_2, y_2), ..., 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.

First, we can consider all t points where the first coordinates are all distinct and let α denote the y-value of the coordinate after k points:

$$\{(x_1, y_1), (x_2, y_2), ..., (x_k, y_k), (x_{k+1}, \alpha_1), ..., (x_t, \alpha_{t-k})\}$$

We can note that each $\alpha_i \in \{\alpha_1, ..., \alpha_{t-k}\}$ can take a value from $\{0, 1, ..., p-1\}$ (total of p values). Thus, applying the result from part (b), this means that we would be able to obtain p^{t-k} such polynomials in $\mathcal{P}_t$ that pass through these k points.

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.

   First, we can recursively split parties into groups of k. Then, for each group of k parties, we can make use of additive secret sharing, which means that each party would receive a share of the secret such that if k parties are present, they would be able to apply additive secret sharing such that they would be able to obtain the secret.

   Then, the repetitive secret sharing scheme here applies because across the groups of k parties, each group is able to reconstruct the secret by itself, independent of other groups. This would represent a secret sharing scheme for this access structure.

Collaborators : Josh Tseng, Rohan Purandare, Nate Johnson, Adam Nasr