# Homework 3

1. **Security of encryption schemes (8+8+8 points).** For each of the encryption schemes 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 $\mathsf{Gen}$ 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.**

(b) The message space is $\mathcal{M} = \{1, 3, 5, \ldots, 99, 101\}$. Algorithm $\mathsf{Gen}$ chooses a uniform key from the key space $\mathcal{K} = \{0, 2, 4, 6, \ldots, 100\}$. The encryption algorithm $\mathsf{Enc}_{sk}(m)$ returns $(sk + m) \mod 102$, and the decryption algorithm $\mathsf{Dec}_{sk}(m)$ returns $(c - sk) \mod 102$.

**Solution.**

(c) The message space is $\mathcal{M} = \{0, 3, 6, \ldots, 3j, \ldots, 2019\}$. Algorithm $\mathsf{Gen}$ chooses a uniform key from the key space $\mathcal{K} = \{2, 5, 8, \ldots, 3j - 1, \ldots, 2018\}$. The encryption algorithm $\mathsf{Enc}_{sk}(m)$ returns $(sk + m) \mod 2020$, and the decryption algorithm $\mathsf{Dec}_{sk}(m)$ returns $(c - sk) \mod 2020$.
**Solution.**

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 a priori probability distribution $\mathbb{M}$ over the set of messages, we have:

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

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

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

Remarks: (1) 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.

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

**Solution.**

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 a priori distribution $\mathbb{M}$ over the message space, and any two cipher-texts $c$ 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 the class. However, this scheme does not satisfy the new definition.

**Solution.**

4. **One-time Pad for 4-Alphabet Words (8+8 points).** We interpret alphabets $\texttt{a}, \texttt{b}, \dots, \texttt{z}$ as integers $0, 1, \dots, 25$, 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 `card` is the cipher text `card`?
   **Solution.**

   (b) What is the probability that the encryption of the message `card` is the cipher text `lime`?
   **Solution.**

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 $a \in \{0, \dots, p-1\}$ and $b \in \{0, \dots, q-1\}$. 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.**

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

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

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 such that any 4 parties can reconstruct the secret, but no subset of 3 parties gain any additional information about the secret.

   Suppose the secret is $s = 4$. The random polynomial of degree $< 4$ that is chosen during the secret sharing steps is $p(X) = X^3 + X + 4$.

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

(b) Suppose parties 1, 2, 5, and 6 are interested in reconstructing the secret. Run 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 $p_1(X)$, $p_2(X)$, $p_3(X)$, and $p_4(X)$.)

**Solution.**

(c) Suppose parties 1, 2, and 5 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 $q_0(X)$, $q_1(X)$, $\dots$, $q_6(X)$.
**Solution.**

7. **A bit of Counting (8+8+9 points).** In this problem, we will do a bit of 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.**

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

**Solution.**

(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 there are $p^{t-k}$ polynomials in $\mathcal{P}_t$ that pass through these $k$ points.

**Solution.**

**Collaborators :**