Homework 3

1. **One-time pad without the identity element in the key space (10 points).** Recall that in the lecture, we defined one-time pad encryption scheme over a group $(G, \circ)$. The encryption algorithm works as follows $\mathsf{Enc}_{\mathsf{sk}}(m) = m \circ \mathsf{sk}$. Let e be the identity element of the group G. One observes that when using the one-time pad key $\mathsf{sk} = e$, the ciphertext is identical to the plaintext because $c = \mathsf{Enc}_{\mathsf{sk}}(m) = m \circ e = m$.

   It has been, therefore, suggested to modify the scheme by only encrypting with $\mathsf{sk} \neq e$, in other words, to have Gen choose sk uniformly at random from the set of $G \setminus \{e\}$. Prove that this modified scheme is *not* secure.

   Solution.

2. **Security of encryption schemes (10+10 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 $\mathcal{M} = \{0, 1, \ldots, 6\}$. Algorithm Gen chooses a uniform key from the key space $\mathcal{K} = \{0, 1, \ldots, 7\}$. The encryption algorithm $\mathsf{Enc}_{sk}(m)$ returns $(sk + m)$ mod 7, and the decryption algorithm $\mathsf{Dec}_{sk}(m)$ returns $(c - sk) \mod 7$.

   Solution.

(b) The message space is $\mathcal{M} = \{1, 3, 5, \dots, 2019\}$. Algorithm Gen chooses a uniform key from the key space $\mathcal{K} = \{2, 4, 6, \dots, 2020\}$. 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.

3. **Equivalent definition of Perfect Secrecy (10 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.

4. **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 <u>not</u> 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.

5. **One-time Pad for 3-Alphabet Words (5+5 points).** We interpret alphabets `a`, `b`, $\dots$, `z` as integers $0, 1, \dots, 25$, respectively. We will work over the group $(\mathbb{Z}_{26}^3, +)$, where $+$ is coordinate-wise integer sum $\mod 26$. For example, `abx` + `acd` = `ada`.

   Now, consider the one-time pad encryption scheme over the group $(\mathbb{Z}_{26}^3, +)$.

   (a) What is the probability that the encryption of the message `cat` is the cipher text `cat`?
   Solution.

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

6. **A Conjectured Private-key Encryption Scheme (15 points).** Consider the following encryption scheme.

   - The message space $\mathcal{M}$ is the set of all n-bit strings that have exactly t-ones in them.
   - The key space $\mathcal{K}$ is the set of all permutations from the set $\{1, 2, \dots, n\}$ to $\{1, 2, \dots, n\}$.
   - The set of all cipher-texts, represented by $\mathcal{C}$, is identical to $\mathcal{M}$.

   The private-key encryption scheme $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ is defined below.

   - $\mathsf{Gen}()$: Return a random permutation sk from $\{1, 2, \dots, n\}$ to $\{1, 2, \dots, n\}$.
   - $\mathsf{Enc}_{\mathsf{sk}}(m)$: Return c, where c is obtained by permuting the message m using the permutation sk. For example, if $m = m_1 m_2 \dots m_n$, then the permutation of m using sk is the string $c = c_1 c_2 \dots c_n = m_{\mathsf{sk}(1)} m_{\mathsf{sk}(2)} \cdots m_{\mathsf{sk}(n)}$.
   - $\mathsf{Dec}_{\mathsf{sk}}(c)$: Return $\widetilde{m}$, where $\widetilde{m}$ is obtained from c by inverting the permutation sk. For example, if $c = c_1 c_2 \dots c_n$, then decoded message is $c_{\mathsf{sk}^{-1}(1)} c_{\mathsf{sk}^{-1}(2)} \cdots c_{\mathsf{sk}^{-1}(n)}$.

   Is this scheme perfectly secure? If yes, then provide a proof. If no, then give a counterexample.

   A worked-out example of the encryption algorithm. Let $n = 4$ and $t = 2$. Therefore, we have the set of messages $\mathcal{M} = \{1100, 1010, 1001, 0110, 0101, 0011\}$. Note that the size of the set $\mathcal{M}$ is $\binom{n}{t} = 6$. The set $\mathcal{K}$ is the set of all permutations from the set $\{1, 2, 3, 4\}$ to the set $\{1, 2, 3, 4\}$. Note that there are a total of $4! = 24$ such permutations.

   Suppose the $\mathsf{Gen}()$ algorithm picked the following permutation

   $$\mathsf{sk}(1) = 3, \mathsf{sk}(2) = 1, \mathsf{sk}(3) = 4, \mathsf{sk}(4) = 2$$

   Suppose Alice wants to encrypt the message $m = m_1 m_2 m_3 m_4 = 1010$ using the sk above. Then, the cipher-text is $c = m_{\mathsf{sk}(1)} m_{\mathsf{sk}(2)} m_{\mathsf{sk}(3)} m_{\mathsf{sk}(4)} = m_3 m_1 m_4 m_2 = 1100$. When Bob wants to decrypt the message $c = c_1 c_2 c_3 c_4 = 1100$, he outputs $\widetilde{m} = c_{\mathsf{sk}^{-1}(1)} c_{\mathsf{sk}^{-1}(2)} c_{\mathsf{sk}^{-1}(3)} \widetilde{c}_{\mathsf{sk}^{-1}(4)} = c_2 c_4 c_1 c_3 = 1010$.

   Note that in the example presented above, we recovered the original message! However, is this scheme secure?

   Solution.

7. **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.

8. **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 $s = 2$. The random polynomial of degree < 4 that is chosen during the secret sharing steps is $p(X) = X^3 + 3X + 2$.

   (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.

9. **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), $\dots$, 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), $\dots$, 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 :