Midterm I

Name:

SID:

Do not turn this page until your instructor tells you to do so.

- After the exam starts, write your name on every odd-numbered page. We reserve the right to deduct points if you do not, and you will not be allowed to do so after time is called.
- For short question, your answers must be written clearly inside the box region. Any answer outside the box will not be graded. For longer questions, if you run out of space, you must clearly mention in the space provided for the question if part of your answers is elsewhere.
- Try to answer all questions. Not all parts of a problem are weighted equally. Before you answer any question, read the problem carefully. Be precise and concise in your answers.
- You may consult at most *20 sheets of notes*. Apart from that, you may not look at books, notes, etc. Calculators, phones, computers, and other electronic devices are NOT permitted.
- There are **10** pages on the exam (counting this one). Notify a proctor immediately if a page is missing.
- **You have 80 minutes: there are 5 questions on this exam worth a total of 100 points.**

1 True/False (20 points)

Bubble in the right answer. No explanation needed. +2 points for correct answer and ***-1 points for wrong answers!*** *If you leave a question unanswered, then there is no penalty. This part will be graded automatically. Please mark your answer clearly.*

1. Let $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ be a pseudorandom function. Then, $f'_k(x,y) = f_k(x) \| f_k(x \oplus y)$ is a pseudorandom function.

   ○ True

   ○ False

   Solution: False

2. Let $p(n)$ be a negligible function. Then, $f(n) = 2^{\log^2 n} \cdot p(n)$ can be a non-negligible function.

   ○ True

   ○ False

   Solution: True

3. Consider an encryption scheme that leaks the first half of the secret key as part of each ciphertext. Then, the scheme can be CPA-secure.

   ○ True

   ○ False

   Solution: True

4. A CCA-secure encryption scheme is also CPA-secure.

   ○ True

   ○ False

   Solution: True

5. Consider a variant of the CPA security definition where the adversary has limited number of phase-2 queries. Then, the definition where adversary is allowed at most k phase-2 queries is not equivalent to the definition where the adversary is allowed $k+1$ phase-2 queries.

   ○ True

   ○ False

   Solution: False

6. The number of possible functions from $\{0,1\}^n$ to $\{0,1\}^{2n}$ is given by $(2^n)^{2^n}$.

   ○ True

   ○ False

   Solution: False

7. The encryption algorithm for a perfectly secure encryption scheme must necessarily be randomized.

   ○ True

   ○ False

   Solution: False

8. Let $g : \{0,1\}^\ell \rightarrow \{0,1\}^m, f : \{0,1\}^m \rightarrow \{0,1\}^n$ be two pseudorandom generators. Then, $f(g(\cdot))$ is a pseudorandom generator.

   ○ True

   ○ False

   Solution: True

9. The number of possible keys for a Vigenère cipher with period length t is $26^t \cdot 26!$

   ○ True

   ○ False

   Solution: False

10. A pseudorandom permutation is also a pseudorandom function.

    ○ True

    ○ False

    Solution: True

2 Pseudorandom Functions (20 points)

Let $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ be a pseudorandom function and $g : \{0,1\}^{n-1} \to \{0,1\}^n$ be a pseudorandom generator. Consider the function $f'_k(x) := f_k(g(x))$. We are going to show that f'_k is *not* necessarily pseudorandom. (We will show this by constructing a pseudorandom generator g for which f'_k is not a pseudorandom function)

1. Using a pseudorandom generator h, we first construct a pseudorandom generator g such that for some $x_1, x_2 \in \{0,1\}^{n-1}$:

$$g(x) = \begin{cases} \boxed{\textbf{Solution: } h(x_1)} & \text{if } x = x_2 \\ \boxed{\textbf{Solution: } h(x)} & \text{otherwise} \end{cases}$$

2. Show that g is a PRG assuming that h is a PRG.

Solution: As $g(x) = h(x)$ for every x except x_2, with probability $\frac{1}{2^{n-1}}$ $x \neq x_2$ and hence g is also a PRG.

3. Now, to show that $f'_k(x) = f_k(g(x))$ is not a pseudorandom function, we construct an adversary $\mathcal{A}$ that distinguishes between the function $f'_k(\cdot)$ and a random function $R(\cdot)$ (given only oracle access to one of these functions). Towards this goal, $\mathcal{A}$ makes queries for input values $\boxed{\textbf{Solution: } x_1}$ and $\boxed{\textbf{Solution: } x_2}$

Let y_1 and y_2 be the responses obtained. $\mathcal{A}$ outputs 1 if and only if

Solution: $y_1 = y_2$

4. $\Pr[\mathcal{A}^{f'_k(\cdot)}(1^n) = 1] =$ **Solution:** 1 and $\Pr[\mathcal{A}^{R(\cdot)}(1^n) = 1] =$ **Solution:** $1/2^n$.

3 Perfectly Secure Encryption (15 points)

Consider the following encryption scheme with message space equal to $\mathbb{Z}_5$.

- Gen: Choose a random vector $\mathbf{k}' \overset{\$}{\leftarrow} \mathbb{Z}_5^{n-1}$ and set $\mathbf{k} = (1, \mathbf{k}')$. That is, the first coordinate of the $\mathbf{k}$ is 1 and the rest of the cooridinates are given by $\mathbf{k}'$.
- $\mathsf{Enc}(\mathbf{k}, m)$: Choose a uniform $\mathbf{c} \in \mathbb{Z}_5^n$ such that $\langle \mathbf{c}, \mathbf{k} \rangle = m$ where $\langle \cdot, \cdot \rangle$ denotes the inner product and is defined below. If such a $\mathbf{c}$ does not exist, output error.

  For any two vectors, $\mathbf{a}, \mathbf{b} \in \mathbb{Z}_5^n$*, the inner product* $\langle \mathbf{a}, \mathbf{b} \rangle$ *is given by* $a_1 b_1 + \ldots + a_n b_n \mod 5$.
- $\mathsf{Dec}(\mathbf{k}, \mathbf{c})$: Compute $\langle \mathbf{c}, \mathbf{k} \rangle$.

1. For any message $m \in \mathbb{Z}_5$,

$$\Pr[\mathsf{Dec}(\mathbf{k}, \mathsf{Enc}(\mathbf{k}, m)) = m] = \boxed{\textbf{Solution: } 1}$$

2. Is the above encryption scheme perfectly secure? If yes, give an argument. Else, show an attack.

Solution: No. For $\mathbf{c} = 0^n$, $\Pr[\mathsf{Enc}(\mathbf{k}, 0) = \mathbf{c}] > 0$ but for $m \neq 0$, $\Pr[\mathsf{Enc}(\mathbf{k}, m) = \mathbf{c}] = 0$.

Name:

4 Private Key Encryption (20 points)

1. Consider a variant of the standard CPA security definition where there are no phase-1 queries allowed. Is this variant equivalent to the standard CPA security? If yes, give an argument. If no, show an encryption scheme that is secure according to the modified definition but is insecure with respect to the standard CPA security definition.

Solution: No. Let $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ be any CPA-secure encryption scheme. Consider the following encryption scheme.

- Gen' : Sample $k, m^* \leftarrow \mathsf{Gen}$.
- $\mathsf{Enc}'((k, m^*), m)$: If $m = m^*$, then output m^*. Else, output $(\mathsf{Enc}(k, m), m^*)$.
- $\mathsf{Dec}'((k, m^*), c)$: If $c = m^*$, then output m^*. Else, output $\mathsf{Dec}(k, c)$.

2. Let $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ be a CPA-secure encryption scheme. Consider an encryption scheme $(\mathsf{Gen}', \mathsf{Enc}', \mathsf{Dec}')$ defined as follows:

   - Gen' : Run Gen to get a key k.
   - $\mathsf{Enc}'(k, m)$: Output $(c_1, c_2) = \mathsf{Enc}(k, m) \| \mathsf{Enc}(k, m)$ where c_1, c_2 are generated using independent randomness.
   - $\mathsf{Dec}'(k, (c_1, c_2))$: Output $m = \mathsf{Dec}(k, c_1)$.

   Show that $(\mathsf{Gen}', \mathsf{Enc}', \mathsf{Dec}')$ is CPA secure.

   Solution: Hybrid 1: $\mathsf{Enc}(k, m_0), \mathsf{Enc}(k, m_0)$
   Hybrid 2: $\mathsf{Enc}(k, m_0), \mathsf{Enc}(k, m_1)$
   Hybrid 3: $\mathsf{Enc}(k, m_1), \mathsf{Enc}(k, m_1)$

5 Fill in the Blanks (25 points)

1. Let $g_1 : \{0,1\}^n \to \{0,1\}^{3n}$ and $g_2 : \{0,1\}^n \to \{0,1\}^{3n}$ be two pseudorandom generators of which only one of them is secure (and you don't know which one is secure). Construct a pseudorandom generator $g : \{0,1\}^{2n} \to \{0,1\}^{3n}$ that is always secure (no explanation needed).

   Solution: $g(x, y) = g_1(x) \oplus g_2(y)$

2. Consider two encryption schemes $(\mathsf{Gen}_1, \mathsf{Enc}_1, \mathsf{Dec}_1)$ and $(\mathsf{Gen}_2, \mathsf{Enc}_2, \mathsf{Dec}_2)$ such that only one of them is CPA-secure (and you don't know which one is secure). Construct an encryption scheme $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ that is always CPA-secure (no explanation needed).

   Solution: $\mathsf{Enc}((k_1, k_2), m) = (\mathsf{Enc1}(k_1, m_1), \mathsf{Enc}_2(k_2, m_2))$ where m_1, m_2 is chosen randomly subject to $m_1 \oplus m_2 = m$.

3. Show an attack against the CBC mode when the IV's are chosen as 1,2,. . . , etc.

   Solution: Query the encryption oracle for two messages 0^n and $0^{n-1}\|1$. Receive $(0^{n-1}\|1, c_1)$ and $(0^{n-2}\|10, c_2)$. Output $m_0 = 0^n$ and arbitrary m_1 as the challenge ciphertext. If m_0 was encrypted with $IV = 0^{n-2}\|11$, then $c^* = c_2$. To see why, notice that an encryption of m_0 will be given by $c = F_k(0^{n-2}\|11 \oplus m_0) = F_k((0^{n-2}\|10) \oplus (0^n - 1\|1)) = c_2$. On the other hand if

m_1 was encrypted the answer will not be equal to c_2 with overwhelming probability.

4. Give an example of a pseudorandom function $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ such that $f'_k(x) = f_k(x) \oplus k$ is not pseudorandom (no explanation needed).

Solution: $f_{k,b}(x) = \begin{cases} g_k(x)_{1,\ldots,n-1} \| b & \text{if } x = x^* \\ g_k(x) & otherwise \end{cases}$ where g is a PRF.

5. Give an unconditional construction of a pseudorandom function with input length $O(\log n)$, output length $O(n)$ and key size $p(n)$ where $p(\cdot)$ is a polynomial.

Solution: Choose the key as follows. For each point in the domain, choose a random string of length n. This will generate a table of length $p(n)$ where $p(\cdot)$ is some polynomial. Now, the function on any input just reads the corresponding entry from the row corresponding to this input and outputs the string.