Ashoka University, Sonipat
Department of Computer Science
CS-3610: Information Security
Assignment 4, Date: April 7, 2025

Due: 11:59 PM, April 9, 2025 Max Marks: 100

Assignment 4

1 You already know this.

1. Let $\Pi = (\mathcal{M}, \mathcal{K}, \mathcal{C}, \texttt{Enc}, \texttt{Dec})$ be a symmetric-key encryption scheme. Suppose $\xrightarrow{K} \mathcal{K}$ and $\xrightarrow{M} \mathcal{M}$ be two random variables. Π is called **perfectly secure** if for all $m \in \mathcal{M}$ and $c \in \mathcal{C}$ we have

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

Prove or refute the following:

   (a) Assume $|\mathcal{K}| = |\mathcal{C}| = |\mathcal{M}|$. Π provides perfect secrecy if and only if every key is used with equal probability $\frac{1}{|\mathcal{K}|}$, and for every $m \in \mathcal{M}$ and every $c \in \mathcal{C}$, there is a unique key k such that $\text{Enc}(m, k) = c$.

   (b) Π provides perfect secrecy if and only if for every probability distribution $\mathbb{P}_M$ over $\mathcal{M}$, every $m_0, m_1 \in \mathcal{M}$, and every $c \in \mathcal{C}$, we have:

$$\mathbb{P}[C = c \mid M = m_0] = \mathbb{P}[C = c \mid M = m_1].$$

10 marks

2. Let $f : \mathbb{R} \to \mathbb{R}$ be a one-way function. Is $g(x) = f(f(x))$ necessarily a one-way function? What about $g(x) = (f(x), f(f(x)))$? Prove your answers.

10 marks

3. Let N be an odd composite integer. Suppose there exists an algorithm $\mathcal{A}$ that, given an integer x coprime to N, computes the order of x modulo N. Show that there exists an algorithm to find a non-trivial factor of N, using $\mathcal{A}$ as a subroutine, with only polynomial overhead. You may use the following theorems:

   (a) If $x^2 \equiv 1 \pmod{N}$ and $x \not\equiv \pm 1 \pmod{N}$, then at least one of $\gcd(x-1, N)$ or $\gcd(x+1, N)$ is a non-trivial factor of N.

   (b) If N has m distinct prime factors, the probability that a random x coprime to N has even order r and $x^{r/2} \not\equiv \pm 1 \pmod{N}$ is at least $1 - \frac{1}{2^m}$.

   Your solution should describe the algorithm, justify its correctness using the theorems above, and analyze its running time.

20 marks

2 Let's get it rolling.

4. Two standard dice have faces labeled 1 through 6. When rolled together, the possible sums range from 2 (if both show 1) to 12 (if both show 6), and every whole number in between is achievable. Now, imagine a twist: instead of regular dice, you have two blank cubes. You get to choose the numbers that go on each of the six faces of both dice. The two dice do not need to be identical, and you may use any positive integers you like (including repeats if necessary). Your task is to label these two dice such that, when rolled together, the sum of their faces yields all integers from 1 to 36.

   (a) Prove whether such a labeling is possible.

   (b) If yes, construct such a pair of dice and justify your design.

   (c) Explore whether other such dice exist that achieve the same 1–36 range. Can you generate a generalized formula or approach?

30 marks

3 To know, or not to know.

5. Design a zero-knowledge proof protocol for the 3-coloring of graphs. Specifically, given a graph $G = (V, E)$ that is claimed to be 3-colorable, describe an interactive protocol in which a prover can convince a verifier that G is 3-colorable *without revealing* the actual coloring. Show that your protocol satisfies completeness, soundness, and zero-knowledge.

30 marks