CS442: Introduction to Cryptography Instructor: Aarushi Goel

Homework 1

Due: February 7; 2026 (11:59 PM)

1 Probability

1. **(6 points)** Alice is taking an exam. For the first question, she is given four choices, exactly one of which is correct. The probability that Alice knows the correct answer is 0.7. If she does not know the answer, she guesses uniformly at random among the four choices.

   Let C denote the event that *Alice answers the question correctly*, and let K denote the event that *Alice knows the correct answer*. We use $\neg K$ to denote the event that *Alice does not know the correct answer.*

   Compute the following and briefly explain your reasoning:

   (a) $\Pr[C \mid K]$, the probability that Alice answers correctly given that she knows the answer.

   (b) $\Pr[C \mid \neg K]$, the probability that Alice answers correctly given that she does not know the answer.

   (c) $\Pr[C]$, the probability that Alice.

2. **(3 points)** Suppose there are $R > 1$ red balls and $G > 1$ green balls in a box. A ball is drawn uniformly at random from the box.

   - If the ball is red, it is returned to the box.
   - If the ball is green, it is discarded.

   After this, a second ball is drawn uniformly at random from the box.

   What is the probability that the first ball drawn was green, conditioned on the event that the second ball drawn is red? Explain your reasoning.

3. **(3 points)** A player rolls a fair six-sided die.

   - If an odd number is rolled, the player loses and has to give the host the roll number times 10 dollars. For example, if 3 is rolled, the player gives the host 30 dollars.
   - If an even number is rolled, the player wins, and the host gives the player the rolled number times 10 dollars. For example, if 4 is rolled, the player gets 40 dollars.

   What is the expected value that the player gets in this game? Explain your reasoning.

2 Groups and Fields

1. **(8 points) Determine whether each of the following algebraic structures forms a group.** If it is a group, explain why it satisfies all the properties of a group. If it is not a group, clearly indicate which property fails to hold.

(a) $(\mathbb{Z}_{10}, +)$, where $\mathbb{Z}_{10} = \{0, 1, 2, \ldots, 9\}$ denotes the set of integers modulo 10, and $+$ denotes addition modulo 10.

(b) $(\mathbb{Z}_{10}^*, \times)$, where $\mathbb{Z}_{10}^* = \{x \in \mathbb{Z}_{10} : \gcd(x, 10) = 1\}$ denotes the set of integers modulo 10 that are relatively prime to 10, and × denotes multiplication modulo 10.

2. **(8 points) Determine whether each of the following algebraic structures forms a field.** If it is a field, explain why it satisfies all the properties of a field. If it is not a field, clearly indicate which property fails to hold.

   (a) $(\mathbb{Z}_p^*, +, \times)$, where p is a prime number. Here $\mathbb{Z}_p^* = \{1, \ldots, p-1\}$, and $+$ and $\times$ denote addition and multiplication modulo p, respectively.

   (b) $(\mathbb{Z}_{12}, +, \times)$, where $\mathbb{Z}_{12} = \{0, 1, \ldots, 11\}$, and $+$ and $\times$ denote addition and multiplication modulo 12, respectively.

3 Perfect Secrecy

1. **(5 points)** Alice and Bob share a secret key $K =$ `0xFFEEDD` (written in hexadecimal). Alice wishes to privately send the message $M =$ `0x012345` to Bob, and she can only send ciphertexts written in hexadecimal.

   Explain how Alice can adapt the XOR-based encryption scheme from the previous question (defined over binary strings) to encrypt the message M using the key K and send the resulting ciphertext to Bob in hexadecimal form. Also specify the ciphertext that Alice sends.

2. **(10 points)** Let $\mathcal{M} = \{0,1\}^n$ and $\mathcal{K} = \{0,1\}^n$ denote the *message space* and the *key space*, respectively. Consider the following encryption scheme, where $\oplus$ denotes bitwise XOR:

   - $\mathsf{Enc}(k, m) := m \oplus k$.
   - $\mathsf{Dec}(k, c) := c \oplus k$.

   Prove that this scheme satisfies perfect secrecy *if and only if* the associated key generation algorithm KeyGen outputs keys that are uniformly distributed over $\mathcal{K}$.

   Hint: To prove an *if and only if* statement, you must establish both directions:

   (a) If the scheme satisfies perfect secrecy, *then* the key generation algorithm KeyGen outputs uniformly random keys from $\mathcal{K}$.

   (b) If the key generation algorithm KeyGen outputs uniformly random keys from $\mathcal{K}$, *then* the scheme satisfies perfect secrecy.

3. **(10 points) Determine whether the following scheme is perfectly secure or not. If it is a perfectly secure encryption, prove that it satisfies both correctness and perfect security. If not, explain which of these properties is violated.**

   The message space is $\mathcal{M} = \{0, 1, 2, 3, 4\}$.

   - $\mathsf{KeyGen} :=$ Selects a key k uniformly at random from the key space $\mathcal{K} = \{1, 3, 5, 7, 9\}$.
   - $\mathsf{Enc}(k, m) := (m + sk) \bmod 5$.
   - $\mathsf{Dec}(k, c) := (c - sk) \bmod 5$.