Week 1 Exercises (ECE 598 DA)

Exercise 0. If X is the number of Heads in 10 independent fair coin flips, $X \sim \text{Binomial}(10, 1/2)$. Then what is the expectation, variance, and standard deviation of X?

Exercise 1. Perfect secrecy intuition. Consider a simplified scenario: the message M is a single bit (either 0 or 1 with equal prior probability 1/2), the key K is a single random bit (0 or 1 with probability 1/2 each), and the ciphertext $C = M \oplus K$ is one bit. Enumerate the four equally likely combinations of (M, K) and the resulting C. Verify explicitly that $\mathbb{P}[M = 0 \mid C = 0] = \mathbb{P}[M = 0] = 1/2$ and $\mathbb{P}[M = 0 \mid C = 1] = \mathbb{P}[M = 0] = 1/2$, demonstrating perfect secrecy in this simple case.

Exercise 2. Consequence of key reuse. Suppose Alice sent two messages m_1, m_2 using the same one-time pad key. Show how an adversary given both ciphertexts can recover the XOR of the two plaintexts. Why is this a problem? What could an attacker do with $m_1 \oplus m_2$?

Exercise 3. Conditional probability in action. Two fair six-sided dice are rolled (independently). Let E be the event that the sum of the two dice is 8. Let F be the event that at least one die shows 6. Compute $\mathbb{P}[E]$ and $\mathbb{P}[E \mid F]$. Are E and F independent?

Exercise 4. Talking drums. Chapter 1 of Gleick's *The Information* highlights the talking drum as an early information technology: a medium that compresses, encodes, and transmits messages across distance. Through a modern cryptography and communications theory lens, can you describe the talking drum as a medium that achieves a form of secure communication?