Problem 1: Optimizing Test Scores

Your friends Alice and Bob are both talented test-takers, but they can sometimes get distracted by their philosophies. Alice is an optimist, and she always wants to believe a statement is true. When given a true/false statement that is true, Alice gets the correct answer with probability 80%, but for false statements, Alice gets the correct answer only 35% of the time. On the other hand, Bob is a skeptic, and he tends to doubt the truth of statements. If a statement is true, he will get the correct answer with probability 15%, but if a statement is false, he will get the correct answer 85% of the time.

a. Your teacher receives a bonus if all of her students achieve at least 50%, so she wants to design a true/false test on which both Alice and Bob will expect to receive at least this score. What percentage of statements on the test would you set to true in order to achieve this?

b. Your teacher is now being forced by Alice’s parents to make her score as high as possible. However, she does not want Bob to fail the class. What percentage of statements should be true in order to maximize Alice’s expected score while keeping Bob’s expected score no less than 43%?

c. You are now taking a true/false test with Alice and Bob. You cannot read the language in which the test is written, but you can see both Alice’s and Bob’s answers for each question; Alice’s answers are independent of Bob’s. You also know that each statement on the test is true with probability 50%. How should you fill out your answer sheet to achieve the highest possible expected score? What will your expected score be?

Problem 2: Cryptography and P vs. NP

We know that if P = NP, there would be efficient ways to solve many hard problems. However, while making hard problems easy would be helpful in some areas, the field of cryptography depends on the existence of such hard problems. You want it to be hard for people to read your secret messages, but if all of NP suddenly became easy, then deciphering your messages might become easy as well.

In this problem, we will see how we can “break” encryption schemes if P = NP. A **public-key encryption** scheme is an encryption scheme where everyone has a pair of keys: a public key and a secret key. Anyone can encrypt a message for you with your public key (which is publicly known) but only you can decrypt it with your secret key. Such a scheme consists of three algorithms:

- The key generation algorithm $\text{KeyGen}$ is a polynomial-time probabilistic algorithm that, on input the security parameter $1^k$ outputs a key pair $(pk, s)$, where both $pk$ and $s$ are of length $k$.
- $\text{Enc}(m, pk; r)$ is a polynomial-time probabilistic algorithm that on input a message $m$, and a public key $pk$, outputs a ciphertext $c$. The value $r$ denotes the contents of its random tape.

---

1The security parameter is typically written in unary, i.e. it is a string of $k$ 1’s, so that the key generation algorithm is polynomial in $k$, which is the length of its input.
• $\text{Dec}(c, s)$ is a polynomial-time deterministic algorithm that on input the ciphertext $c$ and the secret key $s$, outputs a plaintext message $m$.

Let us consider a public key encryption scheme ($\text{KeyGen, Enc, Dec}$) that encrypts bits, i.e. $m \in \{0, 1\}$. Moreover, let us assume that $\text{Enc}$ only reads $k$ bits of its random tape ($k = |pk|$). So $r$, the contents of the random tape, is only $k$ bits long.

A public-key encryption scheme is correct if for any key pair $(pk, s)$ produced by $\text{KeyGen}$, for any valid $m$, and for any $r$, $\text{Dec}(\text{Enc}(m, pk; r), s) = m$. Consider the language

$$L_0 = \{\langle pk, c \rangle | \exists r \in \{0, 1\}^{|pk|} \text{ such that } c = \text{Enc}(0, pk; r)\}$$

Hence $L_0$ consists of the encryptions of 0 under the public key $pk$.

a. Prove that $L_0 \in \text{NP}$.

b. Show that if $P = \text{NP}$, a polynomial-time adversary can break any public-key encryption scheme.

(As part of answering this question, give a precise interpretation of the word “break.”)

Problem 3: Cryptography is the future

In Lecture 1, we got an overview of the field of cryptography. Please read this article Cryptography is the future available at https://cs.brown.edu/courses/csci1510/hw2016/future.pdf by Prof. Anna Lysyanskaya, published in Privacy in the Modern Age and identify real life scenarios mentioned in the article where cryptography can help. Also identify the concepts we would need to learn in class to understand the proposed cryptographic solutions.