CS 198 Codebreaking at Cal
Spring 2023 Homework

HW 6

Question 1

Explain how the discrete-log problem provides security for the Diffie-Hellman Key Exchange.

Question 2

In this problem, we will construct a **zero-knowledge proof** system based on the discrete logarithm problem! A zero-knowledge proof system aims to have Alice (prover) convince Bob (verifier) that she *knows* a specific value, without Bob learning of the value himself.

In this case, Alice wants to prove to Bob she knows the **discrete log** of $y = g^x \mod p$, e.g. she knows x in this expression, whereas Bob only knows g, p, y.

First, Alice computes a random number r and sends Bob $C = g^r \mod p$. Bob then flips a coin and asks for either the value of r, or the value of $x + r \mod p-1$.

If Bob requests the value of r, he verifies that the published value of C is truly equal to $g^r \mod$ p. If he asked for $x + r \mod p-1$, he verifies that

$$\begin{aligned} g^{x+r \mod p-1} \mod p \\ &\equiv g^x \cdot g^r \mod p \\ &\equiv y \cdot C \mod p \end{aligned}$$

The $\mod p-1$ in the exponent preserves the confidentiality of x when added to a truly random r, much like a one-time pad.

1. Argue why Alice can satisfy either of Bob's requests if she truly knows x.
2. Show how Alice can **cheat** if she knows Bob will request the value of r. That is, show how Alice would construct a response to Bob that will be verified as correct, despite not knowing the value of x.
3. Show how Alice can **cheat** if she knows Bob will request the value of $x + r \mod (p-1)$.
4. Explain why Alice can only succeed in convincing Bob with probability $\frac{1}{2}$ + some negligible value if she does not know x.

   Why is this important? Since each round provides a 0.5 probability of cheating, we would chain together n rounds to get a probability of 2^{-n} *that Alice is cheating.*

Contributors:
- Ryan Cottone