CS 198 Codebreaking at Cal
Spring 2023 Homework

HW 7

Question 1

Explain why unhashed (AKA textbook, simple) RSA signatures are vulnerable to existential forgery attacks.

Question 2

Recall the Digital Signature Algorithm from lecture with private key x, public key $y = g^x \mod p$, where p, q are primes such that $p = aq + 1$ for some integer a. To sign, calculate (s_1, s_2) using a randomly chosen $k \mod q$, where

$$S_1 = (g^k \mod p) \mod q$$
$$S_2 = k^{-1}(H(M) + xS_1) \mod q$$

Define $V_1 \equiv H(M)S_2^{-1} \mod q$ and $V_2 \equiv S_1 S_2^{-1} \mod q$. Verification is as follows: check that $(g^{V_1} y^{V_2} \mod p) \mod q = S_1$.

1. Prove the correctness of DSA, i.e. prove that a valid signature will always pass verification.
2. Explain how an attacker is able to detect when two different signatures use the same ephermal signing key k, regardless of the message.

   HINT: Take a look at the equation for S_1
3. Show how an attacker can recover k given access to two different DSA signatures S, S' using the same k.

   HINT: Consider the expression $S_2 - S_2'$

Contributors:

- Ryan Cottone