CS 198 Codebreaking at Cal
Spring 2023 Makeup Assignment

Week 5

Question 1

Bob wants to create an RSA keypair. He uses the prime numbers $p = 5$ and $q = 7$.

1. What is the value of N here?
2. Why can't Bob choose the exponent $e = 2$?
3. Now suppose Bob chooses $e = 5$. Find his private key, d.

Question 2

Given that RSA exists, why is symmetric-key encryption still useful?

Question 3

One deseirable property of cryptosystems is *forward secrecy*, which means an adversary who observes all messages between two people and later compromises one of their machines should not be able to decrypt the messages they observed.

1. Does RSA provide forward secrecy? Why or why not?
2. Does Diffie-Hellman provide forward secrecy? Why or why not?

Contributors:
- Ryan Cottone, Will Giorza