CS 198 Codebreaking at Cal
Spring 2023 Homework

HW 5

Question 1

Explain why public-key (asymmetric) encryption is necessary in a world with secure symmetric ciphers like AES.

Question 2

Instead of using Diffie-Hellman, Alice decides to share a symmetric key with Bob using RSA. She generates k and sends Bob `RSAEnc(`PK_{Bob}`, k)`, where PK_{Bob} is Bob's trusted public RSA key. Assume that there is an adversary Eve that can view all messages sent in this channel, but cannot modify or send any herself.

1. Argue why this scheme prevents Eve from reading k but lets Bob recover k.
2. There is, however, a large downside to using this scheme over Diffie-Hellman. Let's assume Alice and Bob frequently wish to establish a shared channel of communication, and use this RSA key sharing each time. **Explain why Eve would be able to detect when the same key is sent a second time, and why Diffie-Hellman avoids this problem.**

Contributors:

- Ryan Cottone