Homework 2

Due: October 21, 2022 **Points:** 100

1. (*20 points*) An affine cipher has the form $c = (am + b) \bmod n$. Suppose m is an integer between 0 and 25, each integer representing a letter.

   (a) Let $n = 26$, $a = 3$, and $b = 123$. What is the ciphertext corresponding to the phrase `THIS IS A CIPHER MESSAGE`.

   (b) A requirement for a cipher is that every plaintext letter correspond to a different ciphertext letter. If either a and b is not relatively prime to n, does the affine cipher meet this property? Either prove it does or present a counterexample.

2. (*20 points*) Alice and Bob are creating RSA public keys. They select different moduli n_{Alice} and n_{Bob}. Unknown to both, n_{Alice} and n_{Bob} have a common factor.

   (a) How could Eve determine that n_{Alice} and n_{Bob} have a common factor without factoring those moduli?

   (b) Having determined that factor, show how Eve can now obtain the private keys of both Alice and Bob.

3. (*20 points*) Needham and Schroeder suggest the following variant of their protocol:

   1. Alice → Bob : Alice
   2. Bob → Alice : $\{\text{Alice}|rand_3\}k_{Bob}$
   3. Alice → Cathy : $\{\text{Alice}|\text{Bob}|rand_1|\{\text{Alice}|rand_3\}k_{Bob}\}$
   4. Cathy → Alice : $\{\text{Alice}|\text{Bob}|rand_1|k_{session}|\{\text{Alice}|rand_3|k_{session}\}k_{Bob}\}k_{Alice}$
   5. Alice → Bob : $\{\text{Alice}|rand_3|k_{session}\}k_{Bob}$
   6. Bob → Alice : $\{rand_2\}k_{session}$
   7. Alice → Bob : $\{rand_2 - 1\}k_{session}$

   Show that this protocol solves the problem of replay as a result of stolen session keys.
   Hint: Consider two cases, one in which the attacker does not send an initial message to Bob and one in which the attacker does.

4. (*20 points*) Does using passwords with salts make attacking a specific account more difficult than using passwords without salts? Explain why or why not.

5. (*20 points*) Suppose a user wishes to edit the file *xyzzy* in a capability-based system. How can he be sure that the editor cannot access any other file? Could this be done in an ACL-based system? If so, how? If not, why not?