Homework 2

Due: October 20, 2021 **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 a and b are 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*) Consider the Otway-Rees protocol. Assume that each enciphered message is simply the bits corresponding to the components of the message concatenated together. So, for example, in the first message, one must know the names "Alice" and "Bob", and the length of the random numbers r_1 and n, to be able to parse the portion of the first message that is enciphered with k_{Alice}. The separate parts of the enciphered message have no indicators; the recipient is expected to determine them.
   (a) Consider Alice when all 4 steps of the protocol have been completed. How does Alice know that steps 2 and 3 have taken place?
   (b) Massicotte asks us to assume that an adversary Edgar is impersonating Bob, and has sufficient control over the exchange so that he receives the messages intended for Bob. Bob never sees them. What components of the protocol does Edgar know — that is, does he know r_1, r_2, n, or $k_{session}$, or the names of "Alice" and "Bob"? How?
   (c) Given this, in step 4 of the protocol, how might Edgar provide Alice with a session key that he knows?
   (d) How might someone fix this?

4. (*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?

5. (*20 points*) Consider Multics procedures p and q. Procedure p is executing and needs to invoke procedure q. Procedure q's access bracket is (5, 6) and its call bracket is (6, 9). Assume that q's access control list gives p full (read, write, append, and execute) rights to q. In which ring(s) must p execute for the following to happen?
   (a) p can invoke q, but a ring-crossing fault occurs.
   (b) p can invoke q provided that a valid gate is used as an entry point.
   (c) p cannot invoke q.
   (d) p can invoke q without any ring-crossing fault occurring, but not necessarily through a valid gate.

Extra credit

6. (*20 points*) The index of coincidence was defined as "the probability that two randomly chosen letters from the ciphertext will be the same." Derive the formula in Section 10.2.2.1 for the index of coincidence from this definition.