Homework 2

Due: October 23, 2024 **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 is not relatively prime to n, does the affine cipher meet this property? If b is not relatively prime to n, does the affine cipher meet this property? In both cases, 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 following authentication protocol, which uses a symmetric cryptosystem. Alice generates a random message r, enciphers it with the key k she shares with Bob, and sends the enciphered message $\{r\}k$ to Bob. Bob deciphers it and sends $\{r+1\}k$ back to Alice. Alice deciphers the message and compares it with r. If the difference is 1, she knows that her correspondent shares the same key k and is therefore Bob. If not, she assumes that her correspondent does not share the key k and so is not Bob. Does this protocol authenticate Bob to Alice? Why or why not?

4. (*24 points*) The designers of the UNIX password algorithm used a 12-bit salt to perturb the first and third sets of 12 entries in the E-table of the UNIX hashing function (the DES). The maximum length of a UNIX password is 8 characters selected from a set of 96 characters, and the minimum length is 5 characters. Assume that each user is assigned a salt from a uniform random distribution and that anyone can read the password hashes and salts for the users. Also assume a password can be tested in time t.

   (a) What is the worst case time to find all passwords using a dictionary attack?

   (b) Assume that eight more characters were added to the password and that the DES algorithm was changed so as to use all 16 password characters — that is, the maximum length of a password was 16 characters and the minimum length is 5. What would be the worst case time to find all passwords using a dictionary attack?

   (c) Now assume that the passwords were between 5 and 8 characters long, as before, but that the salt length was increased to 24 bits. What would be the worst case time to find all passwords using a dictionary attack?

5. (*16 points*) A network consists of n hosts. Assuming that symmetric cryptographic keys are distributed on a per-host-pair basis, compute how many different keys are required.