15110 Summer 2018
Problem Set 11

Name: ____

Andrew ID: ____

Instructions

1. Type or neatly write the answers to the following problems.
2. Save or scan this file as a pdf and submit to Gradescope

Exercises

1. (1 pt) Encryption.
    a. Caesar ciphers are substitution ciphers using a uniform rule for substitutions: every symbol is shifted by the same amount. A more general way to build a substitution cipher is to use a substitution rule that cannot be described by a uniform shift. Any symbol can be substituted for any other symbol, as long as the mapping is unique and hence invertible.

    For a 3 letter alphabet consisting of A, B, and C, the possible shifts are 0 (giving ABC), 1 (giving BCA), and 2 (giving CAB), but the other substitution possibilities, which are not shifts, are ACB, BAC, and CBA. So there are a total of 6 substitution rules. Generalizing from this example, how many distinct substitution rules are there for a 4 symbol alphabet?

    b. Suppose we have the 5-letter alphabet R, S, T, U, V (in that order). Show the ciphertext that results from applying the substitution rule **SVRUT** to the plaintext "TRUSTS".

2. (2 pts) Consider a public key encryption system using RSA encryption that starts with two prime numbers p = 181 and q = 227.
    a. Compute the public key pair (e, n) and the private key pair (d, n) for this system. Use Python to select the **smallest value for e that will work**, and then select the smallest value for d that will work given your value for e. Show your work, that is, show why e and d are proper values. (Hint: d must be at least $(\phi+1)/e$)

    b. Consider the numerical messages 2015 and 15110 that are to be transmitted. What are the encrypted forms of these messages? You should use Python to find the answer, but show your work, that is, show what arithmetic operations were used as in the lecture notes.

    c. Verify that the receiver can decode the messages from part (b) using the private key pair. Show your work, that is, show the arithmetic as in the lecture notes.

3. (2 pts) Suppose Mr. and Ms. J **share the same bank account** which has a net balance of $0. On the day they get their paychecks of, respectively, $2000 and $3000 they walk up to two different ATMs at exactly the same time and attempt to deposit their newly received checks into their account. The bank's computer executes the following program for each ATM user:

```
Program for a user X
1. Read X's balance from the user's account
2. If it is a deposit request increase the read value by the requested
   amount to obtain the new balance for X,
   Otherwise, if it is a withdrawal request decrease the read value by the
   requested amount to obtain the new balance for X
 3. Write X's new balance to user's account
```

   a. Give an execution (a sequence of steps) that would lead to a new balance of $2000 to be recorded in the database as opposed to the expected $5000. Hint: The three steps above are executed in the given order for a user, however, different users' steps may be interleaved. Your answer should be instantiating X with Mr. J or Mrs. J.

   b. How could you ensure that the balance is always written to the database as $5000 as expected?

4.(3 pts) At Sandwich Shop A, it takes 4 steps to serve a customer: (1) 30 seconds to put a sandwich together, (2) 3 minutes to run it through the oven, (3) 2 minutes to apply the toppings, and (4) 1 minute to deliver the sandwich and collect payment from the customer. The shop has three workers, and each has their own sandwich station, oven, topping station, and cash register so they can all work in parallel.

c. If three customers arrive at the Sandwich Shop A at the same time, how long will it take for all of them to be served?

d. Sandwich Shop B's owner does not want to invest much in equipment. He makes his bussiness work using just one sandwich station, one oven, one topping station, one cash register, and one worker. How long would it take her to serve three customers?

e. Sandwich Shop B can speed up the service by expanding the workforce to four people such that each step is handled by a different person, and using the technique of pipelining. Now, when three customers arrive at Sandwich Shop B shop, they can get faster service, although not as fast as Shop A. How long does it take all three to be served in this case? Show your calculation.

5. (2 pts) This question is based on your reading of Chapter 4 of Blown to Bits. It gives a description of how a typical search engine takes a query and delivers results to the user.
    a. Does a search engine search the entire web in real-time in response to a query?

    b. Name at least 3 aspects of the search operation that can be considered as trade secret of a search engine company.

    c. What did BMW do to increase their page rank on Google? What did Google to discourage BMW from these tactics?