**Computer Security Fall 2016 CS 436 Midterm (Group 1)**

Total marks: 50 points

**Instructions:**

**There are 5 questions. Each problem is worth 10 points. All questions are mandatory. Please type your answers. You are free to consult textbooks for answering the questions. However, you may not discuss the problems with anyone else. You also cannot copy-paste anything verbatim from any source – you must write your answers using your own words.**

**For any clarification to the questions, please send a message to the instructor directly through Canvas.**

1. (10 points) Customers in a large grocery store use point of sale (PoS) terminals to pay for purchases. (e.g., pay by swiping a credit card). Write a complete threat model for such a system. (Please include all sections of the threat model).
2. A. (3.5 points) Use substitution cipher with k=8 to encrypt the following string:

Four score and seven years ago our fathers brought forth on this continent a new nation conceived in Liberty and dedicated to the proposition that all men are created equal.

(For this problem, ignore the whitespaces (i.e., no need to encrypt the spaces, just encrypt the text of the above sentence)).

B. (3.5 points) Decrypt the following ciphertext which was encrypted with substitution cipher.

F xynyhm ns ynrj xfajx snsj.

Assume that the value of k can be between 0 and 10.

C. (3 points) Assume that you have the following one time pad:

kghnrtllhytkgvgxbxmlrykiyteirumgmbnbxjvd

Using this one time pad, encrypt the following message:

pleasecallatfiveoclock

(please show your calculations to get full credit.)

1. A. (3 points) Write your name below. Then compute the md5 hash of your name using openssl.

B. (7 points)

Alice wants to send a message to Bob. Alice and Bob shares a symmetric secret key K. To send the message, Alice encrypts it with K and Bob decrypts it with K upon receipt of a message. A malicious attacker Trudy can listen to the messages sent by Alice.

1. (3 points) Assuming Trudy does not have access to the key K and cannot break the encrypted messages, can Trudy insert a fake message purporting to be from Alice?
2. (4 points) Bob claimed that Alice sent the message (“I will pay $100”). Alice denies sending that. Using the current setup, can Bob prove that Alice sent the message? If yes, how? If no, why?
3. A. (6 points) Alice runs a web server. Alice notices that her web server is getting a lot of ping responses from random IP addresses.
4. (2 points) What kind of attack might be causing this?
5. (4 points) How can Alice prevent this attack? Explain how the solution works.

B. (4 points) Goofy runs a web based search engine where users enter search queries in the search form. Goofy notices that there is a sudden spike in search queries, with hundreds of users each sending 10+ queries per second using the search form.

i) (1 point) Is this an attack or are these queries from regular users?

ii) (3 point) How can Goofy slow down this attack?

1. A. (6 points) Acme Inc. decides to use the following biometrics based authentication system for its employees when they are entering their offices: each employee is asked to pull a cord as hard as possible. The system monitors how strong the employee is. Acme expects that each employee has a different strength level and they can be authenticated uniquely based on how hard they can pull the cord.

Is this a good biometric? Justify your answer considering the properties of good biometric systems.

B. (4 points) Charles needs to pick a password. What are the problems with each of the following passwords (1 point each):

Group 1:

1. abcd
2. abcd1234
3. HelloWorld1
4. Jksikgjdklxhgiuweguyrhsekldtnlkrwnstiwh4iu55we4q34u293434