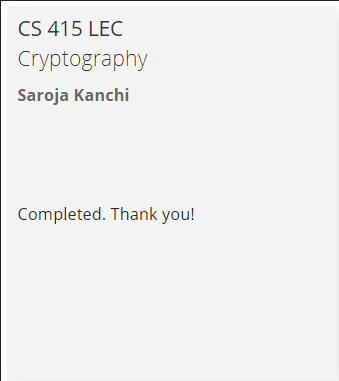
Kanchi, Summer 2020

CS 415 CRYPTOGRAPHY

FINAL EXAM

Your Name \_\_\_\_Colin Quinn\_\_\_\_\_\_\_\_\_

1. Make sure you write your name on the exam
2. You must turn in a single document (jpeg, pdf or word)
3. Show work for ANY credit
4. This is an open notes, open slides, open textbook exam
5. No other person can be consulted during exam
6. No internet look up is allowed
7. You may use scientific calculator on the internet
8. The answer to Question 7 can be replaced with copy of completion of teaching evaluation!

Here is the eval image.

1. (25 points )

1. How many elements does the set Z37\* have?
2. How many generators does the set Z37\* have? Explain
3. What are the possible element orders for elements of the group represented by Z37\* ?
4. Is 5 a generator for the group represented by Z37\*?Why or why not?

2. (10 points ) Compute the two public keys and the common key for the DHKE scheme with the parameters *p* = 29, = 2, *a* = 5, *b* = 12

3. (20 points) Consider an RSA set with parameters p= 5 and q=11.

1. Is 5 a valid public exponent for this RSA set up? Why or why not?
2. Assume the public exponent chosen is 7. Compute the private exponent using Extended Euclidean Algorithm. Show steps of the Euclidean algorithm
3. Decrypt the message y = 2 using the private exponent that you found in b) You must use square and multiply algorithm for this task.
4. (10 points) Does the following digital signature verify for the signed message (x=16,sig(x)=4) for RSA based signature scheme with parameters n = 31, e = 7
5. (15 points)
   1. How many elements have to be tried before hitting a collision with probability 80% on input size of 256 elements?
   2. A string is hashed to the sum of its ASCII values. Find a pair of strings of length 3 that contain collision. (that have the same hash value)

6) (15 points) Compute the output of first round of SHA-1 algorithm with the following inputs:

A = 0000 0000

B = 0000 0000

C= 0000 0000

D = 0000 0000

E = 0000 0001

The 512 bits of input to SHA-1 consists of all 0’s.

1. (5 points)

Show that order of the *p-1* in the group *Zp\** is 2.

Check one of the three options below.

**Option 1** : I have completed the student teaching evaluation. I would like to receive the 5 points for filling in my teaching evaluation instead of answering the question. (Attach an image of completion of teaching evaluation)

**Option 2**: I have completed the student teaching evaluation. I would like to answer the question and receive a grade for it AND receive 5 points extra credit on the exam for filling in the teaching evaluation. (Attach an image of completion of teaching evaluation)

**Option 3**: I am not providing a copy of the teaching evaluation. Here is the answer to the question.

