Name: _____

UNI: _____

Instructor: Shrenik Shah

MATH UN3025 - Midterm 1

October 6, 2016 (75 minutes)

This examination booklet contains 6 problems. There are 10 sheets of paper including the front cover. This is a closed book exam. Do all of your work on the pages of this exam booklet. Show all your computations and justify/explain your answers. Cross out anything you do not want graded. Calculators are NOT allowed.

You have 75 minutes to complete the exam. Do not begin until instructed to do so. When time is up, stop working and close your test booklet. Cell phones, headphones, laptops and other electronic devices are not allowed.

Problem	Possible score	Your score
1	10	
2	15	
3	5	
4	10	
5	10	
6	10	
Extra Credit	6	
Total	60	

Grades will be posted on CourseWorks.

1. (10 pts.) Suppose you have a language with only 3 letters: A, B, and C, which occur with frequencies $0.7, 0.2$, and 0.1, respectively. The following ciphertext was encrypted by the Vigenère method:

$$BABABCBCAC.$$

Assume that the key length is either 1, 2, or 3. Find the most likely key length and determine the most likely key using the method from class.

2. Solve the following problems about modular arithmetic.

(a) (5 pts.) Use the Euclidean algorithm to find the greatest common divisor d of the numbers 123 and 270.

(b) (5 pts.) Use the extended Euclidean algorithm to write the number d from part (a) as

$$d = a \cdot 123 + b \cdot 270$$

for some integers a, b.

(c) (5 pts.) Find all solutions $x \pmod{270}$ to the linear equation

$$123x \equiv 6 \pmod{270}.$$

3. (5 pts.) What are the last two digits of the number 4321^{642}?

4. (10 pts.) Use the Chinese Remainder Theorem to find a number x modulo $5 \cdot 7 \cdot 8 = 280$ such that

$$\begin{aligned} x &\equiv 1 \pmod 5 \\ x &\equiv 2 \pmod 7 \\ x &\equiv 3 \pmod 8. \end{aligned}$$

Note: To receive any credit, you must use the Chinese Remainder Theorem method taught in class, rather than just trying different possible values of x.

5. Answer the following questions about the ElGamal cryptosystem.

(a) (2 pts.) State the ElGamal public key cryptosystem.

(b) (2 pts.) State the Computational Diffie Hellman Problem (CDHP).

(c) (6 pts.) Explain why breaking the ElGamal cryptosystem is equally hard as solving the CDHP. (Recall from class that to prove these are equally hard, you need to explain how to break ElGamal using a "box" that breaks the CDHP, and then explain how to break the CDHP using a "box" that breaks ElGamal.)

6. (10 pts.) Use the Pohlig-Hellman algorithm from class to find the discrete log $L_2(11)$ for the prime $p = 13$. You may assume that 2 is a primitive root modulo 13.

Note: You must correctly use the Pohlig-Hellman algorithm, rather than using a different method, in order to receive credit for your solution.

Hint: All the modular exponentials should be quick to calculate if you use the fact that

$$11 \equiv -2 \pmod{13}.$$

Extra credit. Suppose that Alice has encrypted and sent a message m to Bob using RSA, where the public key is (n, e). Assume that n is very large, but m is short, approximately around 10^{17}.

(a) (4 pts.) If Eve has intercepted the ciphertext c, explain how she can use the short plaintext attack from class to try to find m.

(b) (1 pt.) Explain why this attack is faster than encrypting all possible m's of size around 10^{17}.

(c) (1 pt.) Explain the conditions on m for this attack to be successful.