Math 259: Spring 2019
Quiz 1

NAME:

Are you taking this class for graduate credit?

Time: **30 minutes**

Problem	Value	Score
1	5	
2	5	
3	3	
4	4	
5	3	
Grad	4	
TOTAL	20	
Grad TOTAL	24	
Score		

Problem 1 : (5 points) Alice uses DLP to receive messages. Her public key is $(p, g, h) = (17, 3, 10)$ and her private exponent is $a = 3$. She receives from Bob the ciphertext pair $(c_1, c_2) = (13, 5)$. What is the message that Bob sent her?

As a hint, it might interest you to know that $13^{-1} \equiv 4 \pmod{17}$.

Problem 2 : (5 points) The ciphertext 75 was obtained using RSA with $N = 437$ and $e = 3$. You know that the plaintext is either 8 or 9. Determine which it is.

Problem 3 : (3 points) To receive full credit for this problem, it suffices that you factor $N = 2337 = pq$ where p and q are two primes. You may use brute force if you like, but this will probably take too much time to finish during this quiz.
Instead, you might be interested to know that

$$49^2 \equiv 8^2 \pmod{2337}.$$

Problem 4 : (4 points) It is a fact that 3 is a primitive root modulo 17. Please fill in the following table of discrete logarithms. Show your work.

a	$\log_3 a$	a	$\log_3 a$
1		9	
2	14	10	
3		11	7
4		12	
5		13	
6		14	9
7	11	15	6
8	10	16	8

Here are two facts which might interest you:

$$8 \times 7 \equiv 5 \pmod{17}, \quad 13^{-1} \equiv 4 \pmod{17}$$

Problem 5 : (3 points) Naive Nelson uses RSA to receive a single ciphertext c, corresponding to the message m. His public modulus is N and his public encryption exponent is e, as usual. Since he feels guilty that his system was only used once, he agrees to decrypt any ciphertext that someone sends him, as long as it is not c, and return the answer to that person. Evil Eve sends him the ciphertext $2^e c \pmod{N}$. In this problem we will show that this allows Eve to find m.

a) (2 points) Write an expression for what Nelson will send back to Eve. In other words, decrypt $2^e c$, or give the plaintext that goes with the ciphertext $2^e c$. Simplify your answer as much as possible!

b) (1 point) If you have simplified your answer enough in part a), you should now be able to explain how Eve can easily compute m. Please explain briefly.

Problem 6 : (4 points) This is an extra problem for graduate credit
Suppose that you are using RSA with modulus $N = pq$ and encrypting exponent e but you decide to restrict your messages to numbers m satisfying $m^{1000} \equiv 1 \pmod{N}$. Show that if d satisfies $de \equiv 1 \pmod{1000}$ then d works as a decryption exponent for these messages.