Math 259: Spring 2019
Quiz 1

NAME: SOLUTIONS

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 $13^{-1} \equiv 4 \pmod{17}$.

To decrypt she does

$$c_1^{-a} c_2 \equiv 13^{-3} \cdot 5 \mod 17$$
$$\equiv (13^{-1})^3 \cdot 5 \mod 17$$
$$\equiv 4^3 \cdot 5 \mod 17$$
$$\equiv 16 \cdot 4 \cdot 5 \mod 17$$
$$\equiv (-4) \cdot 5 \mod 17$$
$$\equiv -20 \equiv -3 \equiv 14 \mod 17$$

$\boxed{m = 14}$

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.

Try both!

If $m = 8$: $c \equiv m^e \equiv 8^3 \equiv 64 \cdot 8 \equiv 512 \equiv 75 \mod 437$

It's $m = 8$

$$\begin{array}{r} \overset{3}{64} \\ \times\ 8 \\ \hline 512 \end{array} \qquad \begin{array}{r} \overset{4\,10}{\cancel{5}\cancel{1}2} \\ -\ 437 \\ \hline 75 \end{array}$$

It's not $m = 9$:

$c \equiv m^e \equiv 9^3 \equiv 81 \cdot 9 \equiv 729 \equiv 292 \not\equiv 75 \mod 437$

$$\begin{array}{r} 81 \\ \times\ 9 \\ \hline 729 \end{array} \qquad \begin{array}{r} \overset{6}{\cancel{7}}29 \\ -437 \\ \hline 292 \end{array}$$

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~~

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

Note: I meant to use $N = 2419 = 41 \cdot 59$ Then

$$50^2 \equiv 9^2 \pmod{2419}$$

would have worked, but I made a typo and started with $N = 41 \cdot 57 = 41 \cdot 3 \cdot 19$ which is not a product of 2 primes !! ⌢

We have that

$$49^2 - 8^2 \equiv 0 \pmod{2337}$$
$$(49-8)(49+8) \equiv 0 \pmod{2337}$$
$$41 \cdot 57 \equiv 0 \pmod{2337}$$

Eyeballing it, we check:

$$\begin{array}{r} \overset{2}{5}7 \\ 41 \\ \hline 57 \\ 2280 \\ \hline 2337 \end{array}$$

So $N = 57 \cdot 41$

Now 57 and 41 are way smaller and can either be shown to be prime, or not if the prof made a mistake. In any case N is factored.

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	0	9	2
2	14	10	3
3	1	11	7
4	12	12	13
5	5	13	4
6	15	14	9
7	11	15	6
8	10	16	8

then check that
$0,1,2,3 \ldots 15$
each appear
exactly once! ✓

Here are two facts which might interest you:

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

$\log_3 1 = 0$ always
$\log_3 3 = 1$ always
$\log_3 9 = 2$ because $3^2 = 9$

$\log_3 4 \equiv \log_3 2 + \log_3 2 \equiv 14 + 14 \equiv 28 \equiv 12 \mod 16$
since $2 \cdot 2 = 4$

$\log_3 5 \equiv \log_3 7 + \log_3 8 \equiv 11 + 10 \equiv 21 \equiv 5 \mod 16$
$\log_3 6 \equiv \log_3 2 + \log_3 3 \equiv 14 + 1 \equiv 15 \mod 16$
$\log_3 10 \equiv \log_3 2 + \log_3 5 \equiv {}_4 14 + 5 \equiv 19 \equiv 3 \mod 16$
$\log_3 12 \equiv \log_3 3 + \log_3 4 \equiv 1 + 12 \equiv 13 \mod 16$
$\log_3 13 \equiv -\log_3 4 \equiv -12 \equiv 4 \mod 16$

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!

$$m' \equiv (2^e c)^d \equiv (2^e c^e)^d \equiv 2^{ed} c^{ed} \equiv 2m \pmod{N}$$

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.

She divides by 2.

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.

Let d be such that $de \equiv 1 \pmod{1000}$, then there is $k \in \mathbb{Z}$ with $de = 1 + 1000k$

Then if $c \equiv m^e \bmod N$, we have

$$c^d \equiv (m^e)^d \equiv m^{ed} \equiv m^{1+1000k} \pmod{N}$$

$$\equiv m \cdot m^{1000k} \pmod{N}$$

$$\equiv m \cdot (m^{1000})^k \pmod{N}$$

$$\equiv m \cdot (1)^k \pmod{N}$$

$$\equiv m \pmod{N}$$

So d decrypts the message.