CMSC 456 Timed Midterm, Fall 2021

1. This is an open-book, open-slides, open-web exam. This test is 2h long.
2. There are 5 problems which add up to 50 points.
3. In order to be eligible for as much partial credit as possible, show all of your work for each problem, **write legibly**, and **clearly indicate** your answers. Credit **cannot** be given for illegible answers.
4. After the last page there is paper for scratch work.
5. Please write out the following statement: "*I pledge on my honor that I will not give or receive any unauthorized assistance on this examination.*"

6. Fill in the following:

NAME :
SIGNATURE :
UID :

THERE ARE FIVE PROBLEMS
MAKE SURE YOU DO ALL OF THEM

The following programs may be useful for some of the problems:
https://planetcalc.com/3311/
https://www.wolframalpha.com/

GOTO NEXT PAGE

1. (10 points) Daleks use an alphabet with 500 letters. Alice and Bob use the Affine Cipher. Explain why the function

$$f(x) = 200x + 36 \pmod{500}$$

SHOULD NOT be used by giving an EXAMPLE of what can go wrong. (It is NOT enough to say *because 36 is a Jordan Number* or something like that. I made up the term *Jordan Number*.)

PUT ANSWER HERE

GOTO NEXT PAGE

2. (10 points) Alice and Bob use Diffie Helman with prime $p = 47$ and $g = 7$. Alice picks $a = 2$ and Bob picks $b = 10$. What is the shared secret? Express as a number in $\{0, \ldots, 46\}$.

NO EXPLANATION NEEDED

PUT ANSWER HERE

GOTO NEXT PAGE

3. (10 points) Alice and Bob do Diffie Helman with $p = 47$ and $g = 10$. Eve of course knows that $p = 47$ and $g = 10$. You can and should use the tables on the next two pages to do this problem.

   Eve sees Alice send 27 and Bob send 38. What is the shared secret?

NO EXPLANATION NEEEDED

PUT ANSWER HERE

GOTO NEXT PAGE

a	$10^a \pmod{47}$
0	1
1	10
2	6
3	13
4	36
5	31
6	28
7	45
8	27
9	35
10	21
11	22
12	32
13	38
14	4
15	40
16	24
17	5
18	3
19	30
20	18
21	39
22	14
23	46

For the rest of the table

GOTO NEXT PAGE

a	$10^a \pmod{47}$
24	37
25	41
26	34
27	11
28	16
29	19
30	2
31	20
32	12
33	26
34	25
35	15
36	9
37	43
38	7
39	23
40	42
41	44
42	17
43	29
44	8
45	33
46	1

GOTO NEXT PAGE

4. (10 points) Alice and Bob are doing RSA. Alice broadcasts $N = 35$ and $e = 5$. Bob wants to send Alice the number 2. What number does he send? (It will be a number in $\{0, \ldots, 34\}$.)

NO EXPLANATION NEEDED.

PUT ANSWER HERE

GOTO NEXT PAGE

5. (10 points) Alice and Bob are doing RSA. Alice broadcases so $N = 65$ and $e = 5$. What is the value of d?

NO EXPLANATION NEEDED

PUT ANSWER HERE

GOTO NEXT PAGE