HW 3 CMSC 456. Morally DUE Sep 23
NOTE- THE HW IS FOUR PAGES LONG

1. (0 points) READ the syllabus- Content and Policy. READ my NOTES on ciphers and on English. What is your name? What is the day and time of the first midterm?

2. (25 points) (This problem is based on material that you will see on Wed Sept 18.)

   (a) (5 points) Alice wants to compute $7^{81} \pmod{101}$. Do this using repeated squaring. Show all work. How many multiplications does it take?

   (b) (5 points) Alice notices that $81 = 3^4$. So instead of using repeated *squaring* she decides to use repeated *cubing*. Each cubing takes two multiplications but there are less iterations. Compute 7^{81} using this. Show all work. How many multiplications does it take?

   (c) (8 points) Give an algorithm that does the repeated cubing method for the problem: given a, n, p, find $a^n \pmod{p}$. Give a good upper bound on how many multiplications it takes as a function of n. You CANNOT use O-notation at all. You CAN upper bound something like $\lfloor BLAH \rfloor$ by BLAH.

   (d) (7 points) Recall that for repeated squaring the number of multiplications is

   $$\leq \lg(n) + (\text{ Number of 1's in binary rep of } n\ ) - 1.$$

   Give three examples of an $n \geq 99$ where the repeated-cubing algorithm takes less mults than the repeated-squaring algorithm.

   (e) (0 points) Why isn't repeated cubing used more often?

GO TO NEXT PAGE

3. (25 points) Alice and Bob are going to use the Affine Cipher. They get to choose their alphabet size! If the alphabet size is n then they will pick a number $a \in \{1, \ldots, n\}$ at *random* and then test if a will work to be the coefficient of x. If not, then try again. If so then they will use a as the coefficient for x. (We are not concerned with the picking of b.)

   (a) (10 points) Assume the alphabet size is 1000. What is the probability that the a they pick will work? Call this p_{1000}. (Think about but do not hand in: what is the expected number of times they will need to pick an a?)

   (b) (10 points) Assume the alphabet size is 1001. What is the probability that the a they pick will work? Call this p_{1001}. (Think about but do not hand in: what is the expected number of times they will need to pick an a?)

   (c) (5 points) Which of p_{1000} and p_{1001} is bigger? Based on this give some general advice on what alphabet size to use if a prime size is not available.

GO TO NEXT PAGE

4. (25 points) We describe the *Randomized Affine Cipher*. ALL arithmetic is mod 26.

   Let

   $$S = \{(a, b) \mid 0 \leq a, b \leq 25, a \text{ is rel prime to } 26\}$$

   The key is a function f from $\{0, \ldots, 25\} \times \{0, \ldots, 25\}$ to S. To send message $(m_1, \ldots, m_L)$ (each m_i a character) Alice does the following:

   - Pick random $r_1, \ldots, r_L \in \{0, \ldots, 25\} \times \{0, \ldots, 25\}$.
   - For $1 \leq i \leq L$ let compute $f(r_i) = (a_i, b_i)$.
   - Send $(r_1, a_1 m_1 + b_1), \ldots, (r_L, a_L m_L + b_L)$.

   (a) (15 points) Describe how Bob will, given

   $$(r_1, c_1), \ldots, (r_L, c_L),$$

   decode the message. (Note that Bob has the key f.)

   (b) (10 points) Alice and Bob are using the following key: $f(x, y) =$

   - The first coordinate is the first number AFTER x that is rel prime to 26 with the exception that $x = 25$ yields 1.
   - The second coordinate is $y + 1$ (all mod 26).

   Alice want to send the message *clyde*.

   Alice generates the following five random pairs to help her do this. They are

   (2,5), (3,6), (10,2), (15,7), (25,0).

   What does Alice send to Bob?

GO TO NEXT PAGE

5. (25 points) Alice and Bob are using the cipher on the Sept 9 slides, title *Awesome Vig or Psuedo One-Time Pad* EXCEPT that the mod is 2 digits long instead of 4 digits long.

   Eve is sure that the word ERIK will be in the plaintext.

   Eve looks at every 4-long sequence in the ciphertext and guesses that they decode to ERIK and sets up equations.

   Eve sees ABCD.

   (a) (7 points) Write down (but do not solve) the equations she will try to solve to find how the key is generated. Show all work.

   (b) (7 points) What are the bounds on M?

   (c) (11 points) Find the values of M that could possibly work, or show there aren't any.

   The following table will help you:

A	B	C	D	E	F	G	H	I	J	K	L	M
01	02	03	04	05	06	07	08	09	10	11	12	13

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25	26