HW 3 CMSC 389. DUE Jan 10
WARNING- THE HW IS TWO PAGES LONG!!!!!!!!!!!!

1. (0 points) Write your name! READ cipher and english.

2. (20 points) Alice and Bob want to use a 1-time pad but don't want to exchange 10^{100} bits. So they do the following:

   - Alice picks a number n between 1 and 1000 at random and sends it to Bob.
   - They both compute $1/n$ in base 10 and get a sequence of digits. They then take each digit and write it in base 2. This gives them both a shared infinite sequence of bits. (NOTE that in the case of a number that has a finite representation, pad infinitely with 0's.)

   Example: $n = 7$. $1/7 = 0.1428714287$. So use the key (which I write with spaces for your understanding)

   1 100 10 1000 111 1 100 10 1000 111 $\cdots$.

   Another Example: $n = 10$. $1/10 = .10000\cdots$ so use the key

   1 0 0 0 0 0 $\cdots$

   (a) (5 points) Alice picks $n = 13$. She then wants to send the message 0110. What does she send? (Show all of your work.)

   (b) (5 points) Alice picks $n = 10$. She then wants to send the message 11001. What does she send?

   (c) (5 points) Find a number n such that $1/n$ is of the form $0.YXXXX\cdots$ where X is at least 10 digits long (Y can be any length or even empty).

   (d) (5 points) Discuss the PROS and CONS of Bob and Alice's modification to the 1-time pad.

3. (20 points) Describe carefully how Alice and Bob can do a **VIG PLUS PLUS CIPHER** (the two PLUS's in a row are intentional) where they use a 2×2 matrix cipher instead of affine or shift. Also describe how Eve can crack it.

GO TO NEXT PAGE

4. (20 points) Alice and Bob want to use a 1-time pad, but they want to use sequences of digits instead of sequences of bits. How can they do this?

5. (20 points) Alice wants to use a general 2-char cipher. Bob wants to use a 2×2 matrix cipher (henceforth just *matrix cipher*).

   (a) Give reasons why the General 2-char cipher is better than the matrix cipher.

   (b) Give reasons why the matrix cipher is better than the General 2-char cipher.

   (NOTE- THE reason you can argue both is that I did not define 'better' carefully.)

6. (20 points)

   (a) (7 points) Give an example of a 2×2 matrix over mod 26 that IS invertible.

   (b) (7 points) Give the inverse of the matrix you just gave.

   (c) (6 points) Give an example of a 2×2 matrix over mod 26 that IS NOT invertible. No explanation needed.