HW 3 CMSC 389. DUE Jan 8
WARNING- THE HW IS TWO PAGES LONG!!!!!!!!!!!!!
SOLUTIONS

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.

SOLUTION TO PROBLEM TWO

1) 1/13 = .076923076923...

For the key we put each digit into binary. We use spaces for readability

0 111 101 1001 10 11 (then repeat)

To encode 0110 I just need the first four bits. We do

$0110 \oplus 0111 = 0001$

2) $1/10 = 0.1000000000$ so the key is

1 0 0 0 0 0 0 ....

$11001 \oplus 10000 = 01001$

3) Take $n = 163$. Smaller numbers work also.

4)

PRO is that its easy and they key is short.

CON is that the sequence repeats. Hence it is not secure. For example Eve could use something similar to the way to crack Vig to find a key-length, and then the key.

END OF SOLUTION TO PROBLEM TWO

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.

SOLUTION TO PROBLEM THREE

Alice needs to give Bob a sequence of 2×2 matrices. Call them $M_0, M_1, \ldots, M_{L-1}$. She could just give the numbers directly or they could try some scheme where some phrase decomposes into sequence of 4 numbers (like WILLIAM GASARCH TEACHES DISCRETE MATH becomes WILL IAMG ASAR CHTE ACHE SDIS CRET ETEM and each four letter grouping codes a matrix. BUT this is awkward since you need to make sure the det is rel prime to 26. There are many ways around this but we skip this.

For $0 \le i \le L-1$ let T_i be the sequence of letters in positions $\equiv i \pmod{L}$. For $0 \le i \le L-1$ code T_i via matrix M_i. Note that to transmit L matrices Alice must give Bob a string of 4L elements of $\{0, \ldots, 25\}$.

Eve will try to get the key length the usual way (divisors of diff). After she has that she has a set of L sequence that has each been coded by a 2×2 matrix. Try all of them that are invertible and do IS-ENGLISH to the result. The IS-ENGLISH will have to operate with pairs-of-letters instead of letters.

END OF SOLUTION TO PROBLEM THREE
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?

SOLUTION TO PROBLEM FOUR

Alice and Bob share a long random sequence of digits $d_1 d_2 \cdots d_N$. To send a message $m_1 m_2 \ldots m_n$ (where $n \ll N$) Alice sends the following

$$(m_1 + d_1 \pmod{10}, m_2 + d_2 \pmod{10}, \ldots, m_n + d_n \pmod{10}).$$

END OF SOLUTION TO PROBLEM FOUR

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.)

SOLUTION TO PROBLEM FIVE

(a) General 2-cipher is better since it has a bigger search space so its harder to crack. The search space is the number of bijections from pairs of letters to pairs of letter which is $26^2!$. Matrix code is roughly 26^2 options.

(b) Matrix is easier for Alice and Bob since the matrix is much more compact and there is free software to do matrix mult.

END OF SOLUTION TO PROBLEM FIVE

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.

   SOLUTION TO PROBLEM SIX

   NOTE ON GRADING: many students did not have as an answer a matrix with 4 entries in $\{0, \ldots, 25\}$. They had things like

   1/3 times a matrix.

   This is not correct. You need to find, say, 1/3 mod 26, which is 9 and multiply that by the entries. ALSO- if you have, say, -10, thats really 26-10=16 and should be as such.

   We did not penalize too much for this error here but will in the future.