HW 4 CMSC 456. Morally DUE Oct 12
NOTE- THE HW IS FIVE PAGES LONG

1. (10 points)

   (a) What is the day and time of the midterm?

   (b) What is the day and time of the final?

   (c) What is the dead-cat policy?

GOTO NEXT PAGE FOR NEXT PROBLEM

2. (30 points. BASED ON SLIDES on Other Ciphers.) Alice and Bob are using the Rail Fence Cipher with 4 rows.

   (a) (10 points) Show how Alice encodes

   The rail fence cipher.

   Show all steps. Give the answer in blocks of 5 all caps for readability. (The last block will be smaller than 5.)

   (b) (10 points) State the rail fence cipher (with 4 rows) in MOD terminology (as I did on the slides).

   (c) (10 points) Give the modern view of the 5-row rail cipher, in terms of mods.

For next problem

GOTO NEXT PAGE

3. (30 points. BASED ON SLIDES: One Time Pad and Linear Cong. Gen) Alice is using a Linear Congruential Generator to generate random bytes. She has some numbers A, B, M, r_0 and is generating a sequence $r_1, r_2, \ldots$ using the recurrence

$$r_{n+1} = Ar_n + B \pmod{M}$$

Alice is then using the result of this rng for a one-time pad. Given a plaintext in the form of a sequence of integers $p_1, p_2, \ldots,$ she will encipher it into a ciphertext $c_1, c_2, \ldots$ by xoring it with her LCG:

$$c_n = p_n \oplus r_n$$

You have intercepted an encrypted message from Alice. You also know the start of the plaintext, based on analysis of her previous messages.

Your job is to write a program that figures out and prints the plaintext.

You will read from stdin a bunch of nonnegative integers separated by newlines. Each integer is on its own line. They will be, in order:

- A number n
- A number m, where $m < n$
- n numbers $c_1, \ldots, c_n$, representing your ciphertext
- m numbers $p_1, \ldots, p_m$, representing the start of the plaintext that you already know

Therefore, you will read $2 + n + m$ lines in total. You will print to stdout $4 + n$ integers:

- 4 numbers A, B, M, r_0, the coefficients of your LCG
- n numbers $p_1, \ldots, p_n$, the entire plaintext

For more information about the mechanics and logistics of this assignment

GOTO NEXT PAGE

We have added a few more languages by request. Java, Python 3, OCaml, Ruby, C, C++, and Scala are permitted. Use the file extensions .java, .py, .ml, .rb, .c, .cpp, .scala for each of those respectively.

Your numbers can be separated by any ASCII whitespace. There should be no text in your output besides your numbers and whitespace.

The xor operation used here is a bitwise xor. It is a caret (ˆ) in most languages.

You can assume all numbers are nonnegative and less than 1000. These numbers are intentionally small so that you can factor M by brute force.

Your output should have $A, B, r_0 < M$, e.g. if you find $A = 123$ and $M = 100$, you should print $A \bmod M = 23$, not 123.

If you have any other questions about how to write your program, please ask on Piazza or email Zan, the TA responsible for this problem (zanxu@umd.edu).

For Next Problem Goto Next Page

4. (30 points. BASED ON SLIDES for Matrix Cipher.) This problem is MOD 13.

   (a) (10 points) Fill in the XXX in the following statement:

   The 2×2 matrix

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

   has an inverse mod 13 IFF XXX.

   (XXX can't be something like *the determinant is not a number of Shen-type*, it has to be about a, b, c, d.)

   (b) (10 points) Give an example of a 2×2 matrix that DOES have an inverse mod 13 and give the inverse.

   (c) (10 points) Does there exist a 2×2 matrix with all entries DIFFERENT and in $\{1, \ldots, 12\}$ that DOES NOT have an inverse mod 13? If YES then give such a matrix, if NO then explain why not.