HW 3 CMSC 456. Morally DUE Oct 5
NOTE- THE HW IS FIVE PAGES LONG

1. (0 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. (20 points. Uses slides on Gen Sub and Random Looking Ciphers) Alice and Bob use the Keyword-shift cipher with keyword:

   The quick brown fox jumps over a lazy dog

   and the shift is 1.

   (a) (10 points) Write the encrypt table.

   (b) (10 points) Write the decrypt table.

   For the next problem

   GOTO NEXT PAGE

3. (30 points. BASED ON SLIDES for Vig Cipher)

   Like the previous homework where you cracked the Caesar cipher, here you will crack the Vig Cipher.

   (a) (10 points) The Vig Cipher slides on the class webpage has a section called "Step One - find Keylength".

       Write an algorithm *in pseudocode* based on the slides that finds a small set of possible key lengths. It should work given enough well-formed text, and it should be polynomial time. (This basically means "don't brute force the key".) This part is manually graded, write it down and include it with the rest of the homework.

   (b) (20 points) Write a program to break the Vig cipher, given the key length. Your program will take from stdin two lines.

       - On the first line is a number representing the key length.
       - On the second line is a string consisting entirely of lowercase letters a through z. This is a text that has been ciphered with the Vig cipher.

       Your program should guess the key and decrypt the ciphertext, and print two lines to stdout:

       - On the first line, you should print the key.
       - On the second line, print the plaintext.

       This program is autograded, upload it to gradescope.

For more information about the mechanics and logistics of this asignment

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 program will be run with on a vanilla Ubuntu 18 machine with with the default apt-gets for each language and no w

The grader is not case-sensitive.

You can assume the input will contain fewer than 25 000 000 characters, so you will not run out of memory.

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. (20 points. BASED ON SLIDES on One Time Pad.)

   Alice and Bob LIKE the One-Time-Pad but DISLIKE only having $\{0, 1\}$ in the alphabet.

   (a) (10 points) Alice and Bob use a one-time-pad with alphabet $\{0, \ldots, 9\}$. Fill in the following sentence:

   If the key is $(k_1, \ldots, k_N)$ *and the message is* $(m_1, \ldots, m_N)$ *then Alice sends Bob XXX.*

   (b) (10 points) Using your answer to part a, describe how you would encode

   990091393399332

   if the key was

   881119939103811?

   For the next problem

GOTO THE NEXT PAGE

5. (30 points) Josh has a brilliant idea! The VIG cipher did different SHIFT ciphers on different parts of the message. Lets instead do different AFFINE ciphers! We re-iterate how VIG works and then give Josh's idea which we call AFF-VIG

   - Shift-VIG: The key is a word like *dog* which is really (3,14,6). We then use shift:3 THEN shift:14, THEN shift:6, THEN shift:3, THEN shift:14, THEN shift:6, etc.
   - Shift-AFF: The key is two words like *dog pet* which is really (3,14,6),(15,4,19). We then use affine:$3x+15$, THEN affine:$14x+4$, THEN affine:$6x+19$.

   And now finally for the question which, in summary, will guide you through a proof that the Shift-AFF I have above DOES NOT WORK and asks you to fix it.

   NOTE that all of the math is mod 26.

   (a) (10 points) Do as much of this problem as you can and then describe what goes WRONG: Assume Alice and Bob are using AFF-Vig with keyword *dog pet*. Find the inverse functions for $3x + 15$, $14x + 4$, $6x + 19$ which are needed for decoding.

   (b) (10 points) State what is wrong with Shift-AFF.

   (c) (10 points) Give some way to fix Shift-AFF. Your method should work with key *dog pet*. What affine funtions do you use to encrypt if the key is *dog pet*