CIS 3362 Quiz #2: Playfair, Hill, ADFGVX, Transposition, Enigma, Navajo Code
Solutions
Date: 9/24/2021

1) (5 pts) What is the Playfair box for the keyword: "MISSISSIPPITENNESSEE"? Fill in the grid given below.

M	I/J	S	P	T
E	N	A	B	C
D	F	G	H	K
L	O	Q	R	U
V	W	X	Y	Z

Grading: 1 pt for MIS, 1 pt P, 1 pt for TEN, 2 pts for rest (give 1 pt if missed one of the letters in alpha order or repeated one)

2) (3 pts) Why were the letters ADFGVX chosen for the ADFGVX cipher?

They were easily distinguishable in Morse code, so that if there was one error in transmission of a letter, generally it could be error corrected. **Grading: Full credit for anything that gets the gist of the reason. Decide partial as you see fit.**

3) (6 pts) Imagine an Engima for the Spanish alphabet back in the 1930s, when Spanish had 30 letters. Given 5 rotors to choose from (the version of the Engima used during WWII), how many settings (different configurations for encryption, so ultimately potentially different substitution ciphers) could the machine be in (ignoring the plugboard)? (In your answer, just consider which rotors can be placed in which of the spots as well as the possible rotations of the rotors.) Express your answer in scientific notation.

We are filling in 3 slots with the rotors. For the first slot we have 5 choices, for the second slot we have 4 choices and for the last slot we have 3 choices, so the rotors can be placed in 5 x 4 x 3 = 60 configurations. In addition, each of the three chosen rotors can be in any one of 30 positions. Each of these are independent of one another, so we multiply each of these values to get:

60 x 30 x 30 x 30 = 1620000 = **1.62×10^6,** in scientific notation.

Grading: 2 pts logic for 5 x 4 x 3, 1 pt knowing that we pick 3 rotors, 2 pts to multiply 30 choices for each rotor, 1 pt to convert answer to scientific notation.

4) (6 pts) There were two reasons why the Navajo language was chosen among several potential Native American languages as the basis for the American WWII code. What are those reasons?

1) According to American intelligence, no Japanese knew Navajo.
2) There were enough young, fit, literate (in English) men who could endure the demands of the military and translate between the two languages because they knew both languages.

Grading: 3 pts for each reason, decide partial as you see fit.

5) (12 pts) Using the Hill cipher with a 2 x 2 key, the plaintext "FORT" encrypts to the ciphertext "FMRB". What are the possible encryption keys? (Make sure to remove extraneous solutions.) Put a box around your answers.

This gives us the following two matrix equations, where the encryption key is an unknown 2 by 2 matrix with entries a, b, c and d:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 5 \\ 14 \end{pmatrix} = \begin{pmatrix} 5 \\ 12 \end{pmatrix}$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 17 \\ 19 \end{pmatrix} = \begin{pmatrix} 17 \\ 1 \end{pmatrix}$$

Unpacking this, we get the following 4 equations in a, b, c and d:

5a + 14b = 5 (mod 26) 5c + 14d = 12 (mod 26)
17a + 19b = 17 (mod 26) 17c + 19d = 1 (mod 26)

Since 19 = -7 (mod 26) substitute:

5a + 14b = 5 (mod 26) 5c + 14d = 12 (mod 26)
17a - 7b = 17 (mod 26) 17c -7d = 1 (mod 26)

Multiply the bottom equation by two:

5a + 14b = 5 (mod 26) 5c + 14d = 12 (mod 26)
34a -14b = 34 (mod 26) 34c -14d = 2 (mod 26)

Add the pairs of equations:

39a = 39 (mod 26) 39c = 14 (mod 26)
13a = 13 (mod 26) 13c = 14 (mod 26)

The second equation has no solution, since 13c must always be either 0 or 13 mod 26. If the second equation has no solutions, then the system as a whole has no possible solutions.

Editorial: I multiplied this out by hand to make the question (so I chose an encryption key and multiplied it by FORT), but must have made an error. So, for grading purposes, I'll just give everyone 12/12 on this question. (It's too hard for me to figure out what grades to give based on the work that people show.)

6) (15 pts) The permutation cipher shown in class works as follows:

(a) Use a keyword (of length k) to generate a permutation of 0, .., k-1.
(b) Separate the plaintext into blocks of k letters. (Pad the last block to have k letters.)
(c) Within each block, reorder the letter according to the permutation.

For example, if the permutation generated in step (b) is 3, 5, 0, 1, 4, 2, then the plaintext `"WEAREDIVING"` encrypts to `"RDWEEAIGDINV"`. Complete the function in C below which takes in a plaintext string, an integer array storing the permutation, and the length of that array and returns the ciphertext. (Since this task requires dynamic memory allocation, all of the parts of the code that require dynamic memory allocation have been completed for you. You may treat the character array `cipher` as a regular array. I've also null terminated the string for you!) Assume all necessary includes have been done. **(Note: I suspect it's easiest to do this task with a nested loop structure instead of a single loop.)**

```
// Pre-condition: perm is of length pLen, strlen(plain) is a
//    multiple of pLen, and perm stores the integers 0, 1, …
//    pLen-1 in some order.
// Post-condition: The encrypted version of plain using the
//    permutation cipher with key perm is returned.
char* permEncrypt(char* plain, int* perm, int pLen) {

    int msgLen = strlen(plain);
    char* cipher = malloc((msgLen+1)*sizeof(char));


    // i represents the starting index of the block.
    for (int i=0; i<msgLen; i+=pLen)

        // j is the index into the permutation array.
        for (int j=0; j<pLen; j++)
            cipher[i+j] = plain[i+perm[j]];

    cipher[msgLen] = '\0';
    return cipher;
}
```

Grading: Many ways to do this (doesn't always have to be double loop structure, but I think that's easier…)

Filling each index in cipher – 3 pts
Accessing each individual index in plain – 3 pts
Indexing correctly into plain – 5 pts
Indexing correctly into cipher – 4 pts

7) (3 pts) In which sea did the WWII Battle of the Coral Sea take place? Coral Sea
Grading: Give to All