CIS 3362 Quiz #2: Playfair, Hill, ADFGVX, Transposition, Enigma, Navajo Code Solutions

Date: 9/22/2023

1) (10 pts) The following ciphertext: "OPPLDIZCDIXPMEDNREDGXM" was encrypted via the Playfair cipher with the following key: “SUMMERTIMESADNESS". What is the plaintext?

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

OP → LO, PL → OK, DI →AT, ZC → WH, DI → AT, XP → YO, ME → UM, DN → AD
RE → EM, DG → ED, XM → OX

LOOK AT WHAT YOU MADE ME DO(X)

Grading: 5 pts for the square, 5 pts for the message (-1 per error, cap at 5)

2) (5 pts) Answer the following questions about the Enigma:

(a) (1 pt) From which country was the spy who initially obtained the blueprints to the Engima, which were then passed onto the Polish?

France (1 pt all or nothing)

(b) (2 pts) What piece of information was sent twice in every Enigma Message? How many characters long was (one copy of) this piece of information?

Message Code/Key, one copy of it was 3 letters long (1 pt for each part, 0 if word message isn't an adjective describing code or key)

(c) (2 pts) What role did Arthur Scherbius play with respect to the Engima?

He created the Enigma machine. (2 pts all or nothing.)

3) (12 pts) Find the inverse of the following matrix under mod 19: $\begin{pmatrix} 2 & 13 \\ 3 & 4 \end{pmatrix}$. After you get your answer, prove it's correct by multiplying your answer by the matrix above and show the result is the identity matrix.

The determinant of this matrix is 2 x 4 – 3 x 13 = 8 – 39 = -31 ≡ 7 (mod 19).

We must find 7^{-1} mod 19 to plug into the formula for the inverse of this matrix. Let's run the EEA to find this value:

19 = 2 x 7 + 5	5 – 2 x 2 = 1	3(19 – 2 x 7) – 2 x 7 = 1
7 = 1 x 5 + 2	5 – 2(7 – 5) = 1	3 x 19 – 8 x 7 = 1, thus
5 = 2 x 2 + 1	3 x 5 – 2 x7 = 1	-8 x 7 ≡ 1 (mod 19)

It follows that $7^{-1} \equiv -8 \equiv 11 \pmod{19}$.

Now we can solve for the desired inverse:

$$(7^{-1} mod 19)\begin{pmatrix} 4 & -13 \\ -3 & 2 \end{pmatrix} \equiv 11\begin{pmatrix} 4 & 6 \\ -3 & 2 \end{pmatrix} \equiv \begin{pmatrix} 44 & 66 \\ -33 & 22 \end{pmatrix} \equiv \begin{pmatrix} \mathbf{6} & \mathbf{9} \\ \mathbf{5} & \mathbf{3} \end{pmatrix} \boldsymbol{mod 19}$$

Let's prove our result is correct:

$$\begin{pmatrix} 6 & 9 \\ 5 & 3 \end{pmatrix}\begin{pmatrix} 2 & 13 \\ 3 & 4 \end{pmatrix} = \begin{pmatrix} 6(2)+9(3) & 6(13)+9(4) \\ 5(2)+3(3) & 5(13)+3(4) \end{pmatrix} = \begin{pmatrix} 39 & 114 \\ 19 & 77 \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} mod\ 19$$

Grading: 5 pts to find 7 inverse mod 19 via EEA
(automatic 0 out of 5 if they listed multiples of 7 or 19 or correctly guessed inverse)
2 pts to plug into formula
2 pts to reduce all 4 values in range [0,18]
3 pts for verification step with work

4) (5 pts) List several reasons why the United States chose Navajo as the language upon which to base a code.

1. The Navajo language was structured differently than most known modern Eastern and Western languages and here were no records of Japanese students being exposed to Navajo.
2. There were enough fit young men who knew both Navajo and English.

Grading: 3 pts for first reason given, 2 pts for second reason (these were the two key criteria laid out in language choice amongst the Native American languages.) Other reasons may be given partial credit.

5) (3 pts) What is the reason that the letters A, D, F, G, V, X were chosen as the only ciphertext letters in the ADFGVX cipher?

When transmitted in Morse code, the codes for these letters are "sufficiently different" so that even if there is a slight transmission error, it's likely that the operators could figure out which of the six letters was intended. **(Grading: mostly all or nothing)**

6) (14 pts) Consider the following alternative version of the transposition cipher:

1. The key is simply a permutation of 0, 1, 2, …, n-1. (This makes this question easier, so that no permutation has to be calculated.)

2. Just like regular transposition, copy the letters of the plaintext into a grid with n columns, going top to bottom. For example, with n = 5 and the plaintext "ITISALMOSTTHELASTQUESTION" and key {4, 2, 1, 3, 0} we have:

4	2	1	3	0
I	T	I	S	A
L	M	O	S	T
T	H	E	L	A
S	T	Q	U	E
S	T	I	O	N

3. Now, read the columns in order (column with label 0, followed by column with label 1, etc.) **but from the bottom to the top** to obtain the ciphertext. For this example it would be:

NEATA IQEOI TTHMT OULSS SSTLI (spaces for clarity).

Write a function (prototype given) **in C**, that takes in a plaintext, a permutation, and the length of that permutation and returns a pointer to the string storing the ciphertext. **YOU MAY ASSUME THAT THE MESSAGE LENGTH IS A MULTIPLE OF THE PERMUTATION LENGTH (to make the problem easier)**. (Note: all code for dynamically allocated memory is included.)

Solution #1

```
char* newtrans(char* plain, int* perm, int n) {

    int len = strlen(plain);
    int cols = len/n;

    int* invperm = malloc(sizeof(int)*n);

    for (int i=0; i<n; i++)

        invperm [ perm[i] ] = i ;        // 1 pt, 1 pt
                                         // give 0 if flipped

    char* cipher = malloc(sizeof(char)*(len+1));

    // Copy chars from plain into cipher.

    int j = 0;                           // 1 pt
    for (int i=0; i<n; i++)              // 1 pt
        for (int idx=(cols-1)*n+invperm[i]; idx>=0; idx-=n)//7pts
            cipher[j++] = plain[idx];    // 3 pts

    cipher[len] = '\0';
    free(invperm);
    return cipher;
}
```

Solution #2

```
char* newtransalt(char* plain, int* perm, int n) {
    int len = strlen(plain);
    int cols = len/n;
    char* cipher = malloc(sizeof(char)*(len+1));

    for (int i=0; i<n; i++) {                          // 1 pt
        int j = perm[i]*cols;                          // 3 pts
        for (int idx=(cols-1)*n+i; idx>=0; idx-=n)     // 7 pts
            cipher[j++] = plain[idx];                  // 3 pts
    }
    cipher[len] = '\0';
    return cipher;
}
```

7) (1 pt) What three dimensional shape is a Rubik's Cube? **Cube (Give to all)**