Fall 2020 CIS 3362 Quiz #2 Part A: Playfair, ADFGVX Solutions

Date: 9/25/2020

1) (8 pts) Show the playfair box created with the keyword, "BLOODORANGELEMONADE".

Solution

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

Grading: 1 pt for having a 5 x 5 box
1 pt for BLO
1 pt for D
1 pt for R
1 pt for ANGE
1 pt for M
2 pts for rest

2) (9 pts) Using your playfair box from question #1, encrypt the following plaintext: "TAKINGAPHONECALL". Please us the padding character 'Z', if necessary.

Solution
TA → PE
KI → CK
NG → GE
AP → CV
HO → SG
NE → GM
CA → PC
LZ → RW
LZ → RW

Answer: PECKGECVSGGMPCRWRW

Grading: 1 pt per pair

3) (8 pts) Consider a plaintext message of 91 symbols (letters/digits) encrypted with the ADFGVX cipher and the keyword "HARRYPOTTER". The ciphertext has 182 symbols. The plaintext symbol in the **zero-index based** position of 19 is represented in the ciphertext with two letters (A, D, F, G, V, or X, not necessarily distinct). What are the index positions of those two letters in the **ciphertext**? **Please give your answers as two distinct integers in between 0 and 181, inclusive.** Note: most of the credit for this question will be based on your work and not the actual answers.

Solution

The zero based index 19 is represented by indexes 38 and 39 in the phase one encryption, where we substitute each letter with a digraph from ADFGVX.

Now, we must determine where these indexes end up in the grid. It's probably easiest to just visualize this with an empty grid with the keyword written on top. The row with … represents several rows. The last row is the 17th row, since 181 > 176 = 16 x 11.

The keyword numbering for the column transposition is indicated in blue.

Using 0 based indexing, the indexes in the leftmost column are multiples of 11, up to the row with index 33, then across this row, the indexes are written in until index 39, as we need. These are written in green.

X's are written in for places in the grid that don't have any letters in them. Since 176 letters fill the first 16 rows, the last row only has letters in the first six spots. These are in black.

H	A	R	R	Y	P	O	T	T	E	R
3	1	6	7	11	5	4	9	10	2	8
0										
11										
22										
33	34	35	36	37	38	39				
…										
						X	X	X	X	X

To get our final answer, we pretend reading the columns by number order and see how many characters precede being read off before the ones labeled 38 and 39. So we'll read all of column numbers 1, 2 and 3, which have 17, 16 and 17, characters, respectively. Then, we will read 3 more characters in the column number 4 before arriving at the number 39. Thus, index 39 from phase 1 is located in index 17 + 16 + 17 + 3 = 53 in the ciphertext. To get to the index originally labeled 38, we read the first four columns in full, plus three characters in column 5, so we get to index 17 + 16 + 17 + 16 + 3 = 69.

Thus, our final answers are **53** and **69.**

Grading: 1 pt for calculating indexes 38 and 39. 3 pts for showing the ordering of the columns, 2 pts for the calculation of the new index of the old location 39, 2 pts for the calculation of the new index of the old location 38.