Fall 2020 CIS 3362 Quiz #1 Part B: Hill, Enigma, Transposition, Navajo Code Solution

Date: 9/25/2020

1) (10 pts) In the cryptanalysis of Hill cipher, you've determined that two values of the key matrix satisfy the following equations:

$$19a + 4b \equiv 13 \pmod{26}$$
$$18a + 19b \equiv 14 \pmod{26}$$

Determine the values of a and b. Please express both as integers in between 0 and 25, inclusive.

Solution

Multiply the top equation by 19 and the bottom by 4 to prepare for elimination:

$19^2a + 19(4)b \equiv 19(13) \pmod{26}$ **Grading: 2 pts mult eqn to eliminate**
$4(18)a + 4(19)b \equiv 4(14) \pmod{26}$

Subtracting the bottom from the top, we get:

$(19^2 - 72)a \equiv 19(13) - 56 \pmod{26}$ **Grading: 2 pts subtract to isolate 1 var**

Since $19 \equiv -7 \pmod{26}$, we can simplify the arithmetic above a bit:

$((-7)^2 - 72)a \equiv (-7)(13) - 56 \pmod{26}$
$(49 - 72)a \equiv -91 - 56 \pmod{26}$
$-23a \equiv -147 \pmod{26}$
$3a \equiv 9 \pmod{26}$ **Grading: 1 pt simplify to get here.**

Multiply through by $3^{-1} \pmod{26}$, which equals 9 (look up from reference sheet):

$9(3a) \equiv 9(9) \pmod{26}$
$27a \equiv 81 \pmod{26}$
$a \equiv 3 \pmod{26}$ **Grading: 2 pts get here, can divide btw.**

Substitute a = 3 into the original second equation:

$18(3) + 19b \equiv 14 \pmod{26}$
$19b \equiv 14 - 54 \pmod{26}$
$19b \equiv -40 \pmod{26}$
$19b \equiv 12 \pmod{26}$ **Grading: 2 pts to substitute**

Using the look up chart on the reference sheet, $19^{-1} \pmod{26}$ is 11 so we have:

$11(19b) \equiv 11(12) \pmod{26}$
$b \equiv 132 \equiv 2 \pmod{26}$ **Grading: 1 pt to get here. Note if they give 2 answers, just -1.**

Thus, the values that satisfy the pair of equations are **a = 3 and b = 2.**

2) (6 pts) Consider an Enigma for an alternative language with 10 symbols in its alphabet and four slots for rotors instead of three. Also, imagine that to fill the slots for the rotors, there were a total of 6 potential rotors to be placed. Assume that similar look up charts could be constructed (to the ones that Rejewski had constructed), one for each possible rotor placement and rotation of each of the rotors. How many different charts would need to be calculated?

Solution

We can multiply the number of each rotor rotation to get 10^4 different settings for when the rotors are on different rotations with respect to one another. Then, for each of these, we have 6 choices for the rotor in slot 1, five choices for the rotor in slot 2, 4 choices for the rotor in slot 3 and 3 choices for the rotor in slot 4. The total number of look up charts would be:

$10^4 \times 6 \times 5 \times 4 \times 3 = 10{,}000 \times 30 \times 12 =$ **3,600,000**

Grading: 2 pts for 10^4, 3 pts for enumerating the number of choices for each of the rotors, 1 pt for multiplying it all.

3) (8 pts) The following ciphertext has been encrypted via column transposition, using the keyword "TENNESSEE". What is the decrypted plaintext?

```
EFCEV DMGEM VENTD RENDE IIALO HMOIL RMELL EEABE AATNE MRTIA RNN
```

Solution

Write a grid with the columns labeled by TENNESEE and then number them accordingly, and write the text above in column order, according to the column labels. Next, recognize that there are 53 characters. So since $53 \equiv 8 \bmod 9$, all columns except for the last one will have plaintext in them, so block off the right most column. Also, make sure there are 6 rows total, since ceiling(53/9) = 6. Plaintext will be copied in, in blue.

T	E	N	N	E	S	S	E	E
9	1	5	6	2	7	8	3	4
T	E	L	L	M	E	A	N	D
I	F	O	R	G	E	T	T	E
A	C	H	M	E	A	N	D	I
R	E	M	E	M	B	E	R	I
N	V	O	L	V	E	M	E	A
N	D	I	L	E	A	R	N	NOCH

Decrypting and spacing, we have:

TELL ME AND I FORGET. TEACH ME AND I REMEMBER. INVOLVE ME AND I LEARN.

Grading Criteria: 3 pts for column labels, 2 pts for showing which squares will not be written in, on the last row, 3 pts for copying the message by columns so it's readable in the grid.

4) (1 pt) Which company created Google Maps? **Google (Give to all)**