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

Date: 9/19/2025

1) (10 pts) Encrypt the plaintext "CUTTINGTHEGRASSNOW" using the Playfair cipher with the following key: "LAWNMOWER". Please use the padding character 'X'. What is the ciphertext? Please carefully fill in the empty Playfair square given below.

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

CU → OZ TI → ZT TH → SI (or SJ) RA → EW SN → YB
TX → QZ NG→ WH EG → RF SX → QY OW → RL

OZQZZTWHSIRFEWQYYBRL

Grading: If the third pair to encrypt isn't "TI", automatic -4.
If there's any error on the box, automatic -5
If neither of the items mentioned above are wrong, then -1 per pair

2) (5 pts) Answer these questions about the Enigma, as told in class (and in the course notes).

(a) (1 pt) From what country is the mathematician who initially broke the Enigma in the mid 1930s?

Poland (1 pt all or nothing)

(b) (1 pt) A spy from which country initially obtained the Engima blueprint from Hans Thilo Schmidt?

France (1 pt all or nothing)

(c) (3 pts) Initially, the Enigma machine had 3 scramblers, which could be placed in the machine in 6 possible orders. In 1939, the Germans added 2 scramblers, meaning that the number of possible orderings of the scramblers multiplied by 10, to 60. Let's suppose that the Germans then added 5 more scramblers, keeping the number of slots to place scramblers at 3. By what multiplicative factor would this have increased the number of possible orderings for the scramblers compared to the 1939 arrangement?

Number of orderings with 10 scramblers = 10 x 9 x 8. As given, number of orderings with 5 scramblers = 60. The desired multiplicative factor is $\frac{10\times9\times8}{60} = \frac{72}{6} = \mathbf{12.}$

Grading: All or nothing mostly, but can give 1 point if you see 720 somewhere.

3) (15 pts) The ciphertext "CYPZXRJX" was produced via the Hill cipher using the **encryption key** $\begin{pmatrix} 3 & 9 \\ 2 & 7 \end{pmatrix}$. What is the corresponding decryption key? What is the matching plaintext? (Note: To speed up computation, reduce values under mod appropriately, so use negatives as needed.)

First we must obtain the decryption key. The determinant of the encryption key is 3 x 7 – 2 x 9 = 3. It follows that the desired inverse is $(3^{-1} mod 26)\begin{pmatrix} 7 & -9 \\ -2 & 3 \end{pmatrix} = 9\begin{pmatrix} 7 & -9 \\ -2 & 3 \end{pmatrix} = \begin{pmatrix} 63 & -81 \\ -18 & 27 \end{pmatrix}$. Since we don't need to formally state this inverse and instead are using it for arithmetic by hand, this matrix reduces to the following form mod 26: $\begin{pmatrix} \mathbf{11} & \mathbf{-3} \\ \mathbf{8} & \mathbf{1} \end{pmatrix}$**.** Now we can recover the encrypted message:

$\begin{pmatrix} 11 & -3 \\ 8 & 1 \end{pmatrix}\begin{pmatrix} 2 \\ -2 \end{pmatrix} \equiv \begin{pmatrix} 11(2) - 3(-2) \\ 8(2) + 1(-2) \end{pmatrix} \equiv \begin{pmatrix} 28 \\ 14 \end{pmatrix} \equiv \begin{pmatrix} 2 \\ 14 \end{pmatrix}$, thus CY decrypts to CO, (notice that we substituted $Y \equiv 24 \equiv -2\ (mod\ 26)$, to make computation easier.)

$\begin{pmatrix} 11 & -3 \\ 8 & 1 \end{pmatrix}\begin{pmatrix} 15 \\ -1 \end{pmatrix} \equiv \begin{pmatrix} 11(15) - 3(-1) \\ 8(15) + 1(-1) \end{pmatrix} \equiv \begin{pmatrix} 168 \\ 119 \end{pmatrix} \equiv \begin{pmatrix} 12 \\ 15 \end{pmatrix}$, thus PZ decrypts to MP. (Again, we used a negative equivalent for Z to make computation easier.)

$\begin{pmatrix} 11 & -3 \\ 8 & 1 \end{pmatrix}\begin{pmatrix} -3 \\ 17 \end{pmatrix} \equiv \begin{pmatrix} 11(-3) - 3(17) \\ 8(-3) + 1(17) \end{pmatrix} \equiv \begin{pmatrix} -84 \\ -7 \end{pmatrix} \equiv \begin{pmatrix} 20 \\ 19 \end{pmatrix}$, thus XR decrypts to UT. (We used a negative equivalent for X to make computation easier.)

$\begin{pmatrix} 11 & -3 \\ 8 & 1 \end{pmatrix}\begin{pmatrix} 9 \\ -3 \end{pmatrix} \equiv \begin{pmatrix} 11(9) - 3(-3) \\ 8(9) + 1(-3) \end{pmatrix} \equiv \begin{pmatrix} 108 \\ 69 \end{pmatrix} \equiv \begin{pmatrix} 4 \\ 17 \end{pmatrix}$, thus JX decrypts to ER. (We used a negative equivalent for X to make computation easier.)

The corresponding plaintext is **COMPUTER.**

Decryption Key = $\begin{pmatrix} \mathbf{11} & \mathbf{-3} \\ \mathbf{8} & \mathbf{1} \end{pmatrix}$**.** Plaintext = **COMPUTER**

Grading: 1 pt for stating formula for inverse implicitly, 1 pt for determinant, 1 pt for determinant inverse, 4 pts to get to inverse matrix (so applying the formula and simplifying), then 2 pts per pair. Students can earn 8 points if their matrix multiplication is correct with the wrong inverse as long as everything is properly reduced under mod and converted correctly to letters.

4) (10 pts) The ciphertext below (of 54 characters) was encrypted via column transposition with the keyword "KLEENEX". Decrypt the message to recover the plaintext. Feel free to use the grid provided as you see fit. (Partial credit will be given if we can make sense of what you did with the grid but don't get the correct answer.)

ABIOINHLVE
GUHTTDCTET
VREIIETIRU
IHMHMNUOEE
DHNAHHSLHS
AEOF

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

Since there are 54 letters and 7 columns, we see that 54%7 = 5 columns, labeled 4, 5, 1, 2 and 6 will have more letters than the two columns labeled 3 and 7. Specifically, since 54/7 = 7, columns 4, 5, 1, 2 and 6 will have 7 + 1 = 8 letters and columns labeled 3 and 6 will have 7 letters. So, when reading the letters into columns, read 8 letters when reading columns 1 and 2, 7 letters when reading column 3, 8 letters when reading columns 4, 5 and 6, and finally the last seven letters iwll go in column 7.

The plaintext is: **I HAVE CLIMBED THE HIGHEST MOUNTAIN I HAVE RUN THROUOH THE FIELDS. (This is a U2 lyric with a single typo for THROUGH where the O should be replaced with a G.)**

Grading: 5 pts for the column labels, 5 pts for the message, give partial as needed.

5) (9 pts) Answer the following questions based on the lecture notes and in class lecture about the Navajo Code in World War II.

(a) (4 pts) What are the two main criteria that were used when searching for a Native American language to use as the basis for a secret code the United States was going to use during World War II?

1. **No known exposure of Japanese to the language.**

2. **A group/tribe that was large enough that it had enough young men who also knew English and could handle the physical rigors of war.**

(b) (2 pts) For each English letter, one or more Navajo words were assigned to that letter. In what situations were these words used in relaying an encoded message?

If there was a word that wasn't naturally in the Navajo language, it was either spelled out or there was a special codeword for it. Thus, if a word wasn't in Navajo AND there was no preset codeword for it, then in transmission, the Navajo would have to spell out the word, letter by letter. These assigned words were used for that purpose.

(c) (3 pts) As mentioned above, not each of the English letters had the same number of assigned Navajo words to it, why did some letters have more words assigned than others?

It was assumed that cryptanalysts would pick up on the fact that pieces of messages were spelled out, thus, frequency analysis could be done on those pieces. Byhaving more code words for the letter A than Z, the frequency analysis would be more difficult, since no single code word would actually represent the frequency of a single letter, necessarily.

Grading: Grader discretion completely!

6) (1 pt) Which Native American group previously lived in the same location (and many surrounding areas) as the current day Sioux City?

Sioux (Grading: Give to All)