CIS 3362 Quiz #2: Playfair, Hill, ADFGVX, Transposition, Enigma, Navajo Code
Date: 9/20/2024 Solution

1) (10 pts) The following ciphertext: "PGRXCTRGKCMRFUBSVOCU" was encrypted via the Playfair cipher with the following key: “SECONDHARVEST". What is the plaintext? (Note: it’s weird, but still recognizable, so to speak.)

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

PG → GR (col)
KC → MS (box)
VO → RN (box)
RX → AY (box)
MR → PA (box)
CU → SX (box)
CT → SF (box)
FU → TX (box)
RG → OR (col)
BS → TE (box)

Initial decryption: GRAYSFORMSPATXTERNSX. Removing the padding character X we get:

GRAYS FORMS PATTERNS

Note: I originally had “GRAY FORMS PATTERNS”, but the double letter didn’t match up, so I just added an S after GRAY. My goal in creating the phrase was to test all three rules: box, row and column.

Grading: 5 pts for the square, 5 pts total for the pairs (so 1/2 pt for each rounding down so that an integer score is recorded. If the box is wrong, give credit here according to their incorrect box.)

2) (5 pts) Answer these questions about the Navajo Code used during World War II.

(a) (1 pt) In what continent were the Navajo Code talkers used during combat during WWII?

Asia **(Grading: 1 pt all or nothing)**

(b) (2 pts) Of the 32 men in the first group of Navajo who developed the code, only 30 were subsequently sent to battle. What did the other 2 men do?

Train the next batch of Navajo Code Talkers **(Grading: 2 pts all or nothing)**

(c) (2 pts) What was the primary weakness of the code the US used for secure communications during WWII that the Navajo Code addressed?

It took a long time to encode and transmit. In a test between the Navajo code and the previously used code, the latter took 30 minutes to transmit the same message transmitted in 40 seconds via the Navajo code. **(Grading: 2 pts all or nothing)**

3) (15 pts) In attempting to find a Hill cipher key, you've arrived at the two following equations for 2 unknown variables, a and b:

$$17a + 9b \equiv 19 \ (mod\ 26)$$
$$7a + 23b \equiv 15 \ (mod\ 26)$$

Find both ordered pairs (a, b) with $0 \leq a, b \leq 25$ that satisfy these two equations simultaneously. (Note: To speed up computation, reduce values under mod appropriately, so use negatives!)

Multiply the equations through by 7 and 17 respectively, mapping the larger values to their corresponding equivalent values under mod 26:

$$(7)17a + (7)9b \equiv -7(7) \ (mod\ 26)$$
$$(17)7a - 3(17)b \equiv -11(17) \ (mod\ 26)$$

Subtracting the bottom from the top we get:

$$63b + 51b \equiv -49 + 187 \ (mod\ 26)$$
$$114b \equiv 138 \ (mod\ 26)$$
$$10b \equiv 8 \ (mod\ 26)$$

Since gcd(10, 26) = 2, we can't multiply through by the modular inverse of 10 mod 26. Instead, write out the corresponding equation for some integer n:

$$10b = 8 + 26n$$

Divide this equation through by 2: $5b = 4 + 13n \rightarrow 5b \equiv 4 \ (mod\ 13)$.

Find 5^{-1} mod 13:

13 = 2 x 5 + 3
5 = 1 x 3 + 2
3 = 1 x 2 + 1
3 – 1 x 2 = 1
3 – (5 – 3) = 1
2 x 3 – 1 x 5 = 1
2(13 – 2 x 5) – 1 x 5 = 1
2 x 13 – 5 x 5 = 1, take this equation mod 13
$-5 \times 5 \equiv 1 \ (mod\ 13)$, it follows that
$\mathbf{5^{-1} \equiv -5 \equiv 8 \ (mod\ 13)}$

Now, multiply the equation through:

$(8)5b \equiv (8)4 \ (mod\ 13)$.
$b \equiv 32 \equiv 6 \ (mod\ 13)$

Thus b = 6 or
b = 19 (since $19 \equiv 6 \ (mod\ 13)$)

If b = 6, $7a - 3(6) \equiv 15 \ (mod\ 26) \rightarrow 7a \equiv 33 \equiv 7 \ (mod\ 26)$. We can eyeball that the solution is a = 1 or multiply through by 7^{-1} mod 26 (15 on reference sheet) to get a = 1.

If b = 19, $7a - 3(19) \equiv 15 \ (mod\ 26) \rightarrow 7a \equiv 72 \equiv 20 \ (mod\ 26)$. We can multiply this through by 15 to yield $a \equiv 15(20) \equiv 300 \equiv 14 \ (mod\ 26)$.

It follows that the two desired solutions are **(1, 6) and (14, 19).**

Here is an alternate solution that immediately changes the 23 to -3 and recognizes that it's better to multiply the second equation by 3 and add the two equations:

$$17a + 9b \equiv 19 \ (mod\ 26)$$
$$7a - 3b \equiv 15 \ (mod\ 26) \rightarrow$$
$$21a - 9b \equiv 45 \ (mod\ 26)$$

Adding the first and third equation above we get:

$$38a \equiv 64 \ (mod\ 26)$$
$$12a \equiv 12 \ (mod\ 26)$$

This latter equation can be written as 12a = 12 + 26n. Dividing through by 2 yields

$$6a = 6 + 13n$$

It follows that $6a \equiv 6 \ (mod\ 13)$, which has the solution $a \equiv 1 \ (mod\ 13)$. It follows that a = 1 or a = 14.

From there, we can back substitute a = 1: $7(1) - 3b \equiv 15 \ (mod\ 26) \rightarrow 3b \equiv 18 \ (mod\ 26)$. This clearly has the unique solution b = 6.

For the other option, we have: $7(14) - 3b \equiv 15 \ (mod\ 26) \rightarrow 3b \equiv 83 \equiv 5 \ (mod\ 26)$. Multiply through by 3^{-1} mod 26 (it's 9) to yield $b \equiv (9)5 \equiv 45 \equiv 19 \ (mod\ 26)$.

Thus, in this manner we arrive at the same two solutions **(1, 6) and (14, 19).**

Grading: 5 pts for eliminating one of the two variables correctly.
4 pts for getting 1 of the two solutions for the uneliminated variable
2 pts for getting the first matching solution for the uneliminated variable
2 pts for getting the second solution for the uneliminated variable
2 pts for getting the matching solution for the uneliminated variable

4) (14 pts) Encrypt the plaintext, “WELLPARTYLIKEITS1999” using the ADFGVX cipher with the box shown below as the first key and “SCREAM” as the second keyword.

	A	**D**	**F**	**G**	**V**	**X**
A	E	U	K	Y	two	one
D	Q	D	five	J	C	R
F	N	S	L	G	eight	H
G	F	T	A	P	three	zero
V	O	V	Z	nine	W	seven
X	B	I	six	X	four	M

Feel free to use this grid below to aid you.

S	C	R	E	A	M
6	2	5	3	1	4
V	V	A	A	F	F
F	F	G	G	G	F
D	X	G	D	A	G
F	F	X	D	A	F
A	A	X	D	G	D
F	D	A	X	V	G
V	G	V	G		

FGAAGV VFXFADG AGDDDXG FFGFDG AGGXXAV VFDFAFV

Grading: 10 pts for filling out grid, give partial credit proportionally. (So ½ a pt per pair round down to a whole number of points.)

4 pts for reading the columns in the right order. Give partial as you see fit.

5) (5 pts) When two scramblers were added to the Engima for potential use, it multiplied the number of configurations of the machine by 10. Imagine, if a similar augmentation was made and another two scramblers were added after the first modification. Let X equal the number of configurations after the first modification. Let Y equal the number of configurations after the second (fictitious) modification. Y = aX where a can be represented as a decimal number with exactly one digit after the decimal point. With proof, find the value of a.

If there are k scramblers ($k \geq 3$), they can be arranged in $k(k-1)(k-2)$ ways.

Thus, after the first augmentation (which went from 3 to 5 scramblers), there were 5 x 4 x 3 = 60 ways to arrange the scramblers.

If another two were added, k = 7 and there would be a total of 7 x 6 x 5 = 210 arrangements.

It follows that $a = \frac{210}{60} = \frac{7}{2} = \mathbf{3.5}$

Grading: 2 pts for count of # of configurations after the first augmentation.
2 pts for count of # of configurations after the second augmentation.
1 pt for the final answer
Not the value doesn't have to be multiplied out to get the 2 pts. We can Avoid the multiplication via canceling:

$$\boldsymbol{a = \frac{7 \times 6 \times 5}{5 \times 4 \times 3} = \frac{7}{4} \times 2 = \frac{7}{2} = 3.5}$$

6) (1 pt) What three-dimensional shape is The Great Pyramid of Giza? **Pyramid (Give to All)**