Exercises #9 **Cryptography** **Math 201-SH4-AB**

1. Working with $\mathrm{mod}(26)$ calculations:

   (a) Explain why 7 is considered to be the multiplicative inverse of 15 in the context of $\mathrm{mod}(26)$ calculations.

   (b) Use matrix multiplication to determine which of the following matrices (B or C) is an inverse matrix $\mathrm{mod}(26)$ of the matrix $A = \begin{bmatrix} 5 & 9 \\ 1 & 4 \end{bmatrix}$. (In other words, which of the two matrices below would operate as a decryption matrix for the encoding matrix A?)

   $$B = \begin{bmatrix} 24 & 11 \\ 7 & 17 \end{bmatrix} \qquad C = \begin{bmatrix} 4 & 3 \\ 9 & 12 \end{bmatrix}$$

2. Why would the matrix $A = \begin{bmatrix} 5 & 3 \\ 7 & 12 \end{bmatrix}$ be a poor choice for a Hill 2-cipher encryption matrix?

3. Encode the word **JELLY** using a Hill 2-cipher with the encoding matrix $A = \begin{bmatrix} 2 & 7 \\ 3 & 10 \end{bmatrix}$.

4. Below are four encoding matrices. In each case, find the decryption matrix.

   (a) $A = \begin{bmatrix} 3 & 2 \\ 4 & 11 \end{bmatrix}$

   (b) $A = \begin{bmatrix} 8 & 5 \\ 5 & 5 \end{bmatrix}$

   (c) $A = \begin{bmatrix} 7 & 3 \\ 4 & 3 \end{bmatrix}$

   (d) $A = \begin{bmatrix} 9 & 2 \\ 5 & 3 \end{bmatrix}$

5. Using the encryption matrix $A = \begin{bmatrix} 3 & 2 \\ 1 & 3 \end{bmatrix}$, decode the ciphertext below to reveal a request:

   XSQXXRAJYPMC

6. Using the encryption matrix $A = \begin{bmatrix} 7 & 5 \\ 2 & 15 \end{bmatrix}$, decode the ciphertext below to answer the riddle, “What's the difference between 0 and 8?”

   QFQHFB

7. Using the encryption matrix $A = \begin{bmatrix} 1 & 3 \\ 2 & 5 \end{bmatrix}$, decode the ciphertext below to reveal the plea:

   WOHZBY

8. Using the encryption matrix $A = \begin{bmatrix} 1 & 1 \\ 4 & 1 \end{bmatrix}$, decode the ciphertext below to reveal the title of a great movie:

   REREHXDW

9. Using the encryption matrix $A = \begin{bmatrix} 1 & 3 \\ 5 & 6 \end{bmatrix}$, decode the ciphertext below to reveal a scientific feat:

   RRBSOIMJBLWRIUBW

10. Answers to the following trivia questions are provided in encrypted form, each time using one of the three following encryption matrices:

    $$A = \begin{bmatrix} 4 & 9 \\ 5 & 12 \end{bmatrix} \qquad B = \begin{bmatrix} 6 & 5 \\ 5 & 7 \end{bmatrix} \qquad C = \begin{bmatrix} 5 & 4 \\ 1 & 3 \end{bmatrix}$$

    Decrypt the answers to each of the questions below using the encryption matrices mentioned in each case.

    (a) What is the longest river in Europe?
    ODGNMQ, encrypted using A

    (b) Who wrote *The Catcher in the Rye*?
    NVUVRMTISG, encrypted using C

    (c) What word describes a dozen dozen?
    HQWQMK, encrypted using A

    (d) Who won the Nobel Prize in Litterature in 2016?
    IKFLBAXY, encrypted using B

    (e) In 2016, where was is the world’s tallest freestanding stucture located?
    YKQQUD, encrypted using B

    (f) Who painted *Luncheon of the Boating Party*?
    FGZGMK, encrypted using C

    (g) In physics, what is defined as the measure of a rotational force on an object?
    GTQHYI, encrypted using A

    (h) What is the average gestation period (in months) for an African elephant?
    AAVSKOAAIX, encrypted using B

11. A spy arrives in a foreign country and, in a train station locker, finds and opens a message that reads

Go to ***UXGHDZHKWY*** *and introduce yourself as* ***IDHKXEBL****.*
You contact will meet you there and identify himself by using the phrase ***QQZLWDUMQKGI*** *into his first sentence. He will give you further instructions.*

Before leaving your previous contact, you were asked to memorize the following three encoding matrices:

$A_1 = \begin{bmatrix} 2 & 9 \\ 1 & 8 \end{bmatrix}$ $\qquad A_2 = \begin{bmatrix} 10 & 1 \\ 11 & 3 \end{bmatrix}$ $\qquad A_3 = \begin{bmatrix} 4 & 1 \\ 7 & 7 \end{bmatrix}$

Use the encoding matrices, in order, to decode the message from the locker.

(a) What three decryption matrices will you use?

(b) Where must you go?

(c) What name should you use to introduce yourself?

(d) What phrase will your contact use to identify himself?

12. You have a hard time memorizing dates and names and, during a test on 19^{th} century America, you can't seem to remember who was President of the Unites States in 1867. Luckily, you're quite good at math, and so is your best friend, who tosses you her answer in the following note, confident that your history teacher doesn't understand the Hill 2-cipher and would ignore it:

UTIBTODT $\qquad$ *Use* $\qquad A = \begin{bmatrix} 8 & 9 \\ 3 & 4 \end{bmatrix}$

Unfortunately, your best friend is also pretty bad at remembering names and dates, and she forgets that the correct answer is Andrew Johnson. What (incorrect) answer was in the note?

13. Sally and Steve have been married for ten years and love to leave each other notes written in the form of a Hill 2-cipher. This morning, Sally left the following note for Steve:

DCUHGORKKHWVXUBC

Encoding matrix $A = \begin{bmatrix} 3 & 7 \\ 3 & 12 \end{bmatrix}$

What was the message?

ANSWERS:

1. (a) 7 and 15 are multiplicative inverses $\mathrm{mod}(26)$ because $(7)(15) = 105 \equiv 1\,\mathrm{mod}(26)$.

(b) B is the inverse of A (and C is not) because

$$AB = \begin{bmatrix} 183 & 208 \\ 52 & 131 \end{bmatrix} \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \mathrm{mod}(26)$$

$$BA = \begin{bmatrix} 131 & 260 \\ 52 & 131 \end{bmatrix} \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \mathrm{mod}(26)$$

$$\text{but } AC = \begin{bmatrix} 121 & 123 \\ 40 & 51 \end{bmatrix} \equiv \begin{bmatrix} 17 & 19 \\ 14 & 25 \end{bmatrix} \mathrm{mod}(26)$$

2. A is not invertible $\pmod{26}$.

3. **CBDZQM**

4. (a) $A^{-1} = \begin{bmatrix} 15 & 2 \\ 4 & 23 \end{bmatrix}$

(b) $A^{-1} = \begin{bmatrix} 9 & 17 \\ 17 & 4 \end{bmatrix}$

(c) $A^{-1} = \begin{bmatrix} 9 & 17 \\ 14 & 21 \end{bmatrix}$

(d) $A^{-1} = \begin{bmatrix} 17 & 6 \\ 15 & 25 \end{bmatrix}$

5. PASS THE SUGAR

6. A BELT

7. HELP ME

8. MEMENTO

9. THEY SPLIT THE ATOM

10. Decryption matrices: $A^{-1} = \begin{bmatrix} 4 & 23 \\ 7 & 10 \end{bmatrix}$

$B^{-1} = \begin{bmatrix} 5 & 15 \\ 15 & 8 \end{bmatrix}$ $\qquad C^{-1} = \begin{bmatrix} 5 & 2 \\ 7 & 17 \end{bmatrix}$

(a) VOLGA

(b) J.D. SALINGER

(c) GROSS

(d) BOB DYLAN

(e) RENOIR

(f) DUBAI

(g) TORQUE

(h) TWENTY-TWO

11. (a) $A_1^{-1} = \begin{bmatrix} 16 & 21 \\ 11 & 4 \end{bmatrix}$ $\qquad A_2^{-1} = \begin{bmatrix} 7 & 15 \\ 9 & 6 \end{bmatrix}$

$A_3^{-1} = \begin{bmatrix} 9 & 21 \\ 17 & 20 \end{bmatrix}$

(b) HOTEL RUBIO

(c) SAM HILL

(d) PERFECT STORM

12. LINCOLN $\qquad$ (using $A^{-1} = \begin{bmatrix} 6 & 19 \\ 15 & 12 \end{bmatrix}$)

13. GET MILK. I LOVE YOU. $\qquad$ (using $A^{-1} = \begin{bmatrix} 6 & 3 \\ 5 & 21 \end{bmatrix}$)