Name: ________________ **Period: _____**

Date: _______________ **MA2 Honors**

Mr. Mellina

Introduction into Cryptology

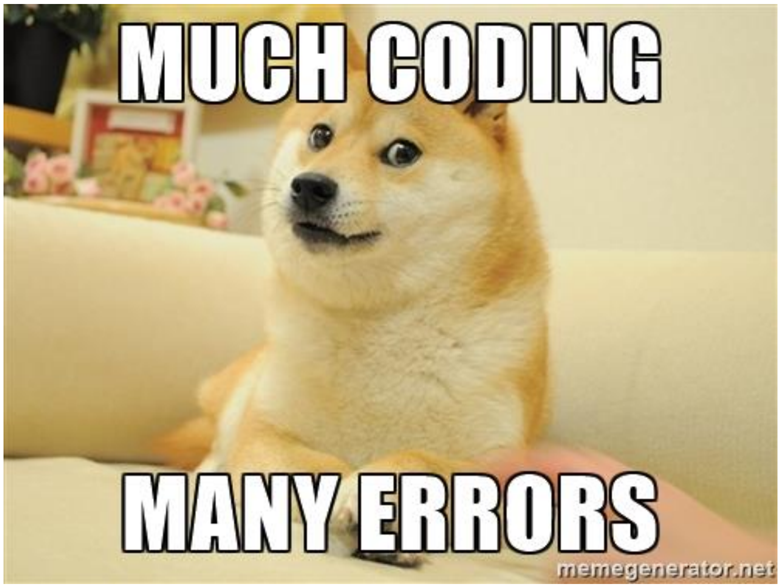
Warm Up!

Decode the following message

a. NBUI JT GVO

Cryptography, to most people, is concerned with keeping communications private. Indeed, the protection of sensitive communications has been the emphasis of cryptography throughout much of its history. Encryption is the transformation of data into some unreadable form. Its purpose is to ensure privacy by keeping the information hidden from anyone for whom it is not intended, even those who can see the encrypted data back into some intelligible form.

Encryption and decryption require the use of some secret information, usually referred to as a key. Depending on the encryption mechanism used, the same key might be used for both encryption and decryption, while for other mechanisms, the keys used for encryption and decryption are different.



Terminology

- ___________________*: defined as the science of making communication incomprehensible to all people except those who have a right to read and understand it.*

- __________________*: concerns itself with the secrecy system itself and its design.*

- __________________*: concerns itself with the breaking of the secrecy system above.*

- ___________*: a set of information that will allow words to be changed to other words or symbols.*

- ___________________*: the message that you wish to put into a secret form. (Usually written lowercase and with no spaces)*
    - *Ex:* "I will meet you at 5 PM in the mall" is written as: iwillmeetyouatfivepminthemall

- ____________*: the method for altering the plaintext.*

- _________________*: the secret version of the plaintext.*
    - *Ex:* iwillmeetyouatfivepminthemall may be changed to: **NBNQQRJJYDTZFYKNAJURNSYMJRFQQ**

- ________________*: changing from plaintext to ciphertext.*

- ________________*: changing from ciphertext to plaintext.*

- _________*: information that will allow someone to encipher the plaintext and also decipher the ciphertext.*

Most of us associate cryptography with the military, war, and secret agents. And, indeed, those areas have seen extensive use of cryptography. In World War II, for example, a great deal of effort was expended to create systems so that the high command could communicate with generals in the field over radio waves with the enemy not being able to decipher it. Even more time was spent in analyzing these messages and "breaking the code."

Today we need cryptology because of the everyday use of computers and the Internet. It is important for businesses to be able to protect the information in their computers. If you decide to buy a CD from Amazon.com using your credit card, it is important that no one but Amazon has the ability to read the file where your credit card number is stored. Electronic fund transfers have made privacy a great concern.

Cryptography Worksheet

(https://www.youtube.com/watch?v=sMOZf4GN3oc)

Encode the following messages.

1. Caesar cipher with shift +3: *hello tom*

2. Caesar cipher with shift +12: *klondike nuggets*

Decode the following messages

3. Caesar cipher with shift +5: *ltytufwnx*

4. Caesar cipher with shift +21 = –5: *adiyevhznwjiy*

5. Caesar cipher with shift +24 = –2: *ncwrmlkyllgle*

6. a. Caesar cipher with shift +23 = –3. *aliip*

   b. Caesar cipher with shift +4: *aliip*

7. Caesar cipher using frequency analysis. Shift is _______.

kbkxeutk

8. Caesar cipher using frequency analysis. Shift is _______.

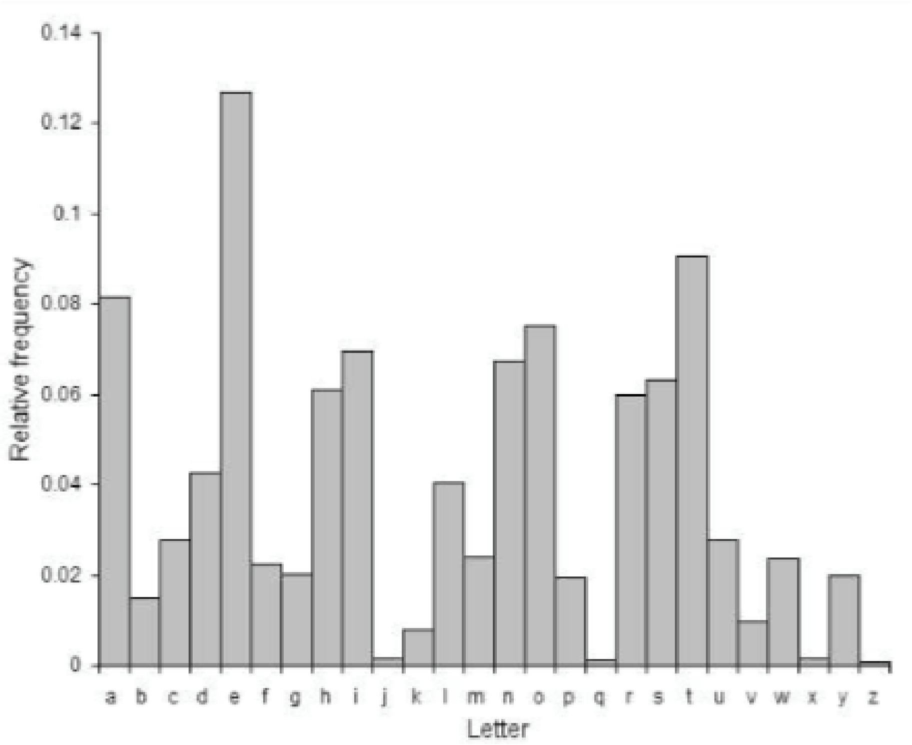
espntaspcsldmppymczvpy

9. Caesar cipher using frequency analysis. Shift is _______.

kgyezuhxkgq

10. Caesar cipher using frequency analysis. Shift is _______.

xskixxsxlisxlivwmhi



Today governments use sophisticated methods of coding and decoding messages. One type of code, which is extremely difficult to break, makes use of a large matrix to encode a message. The receiver of the message decodes it using the inverse of the matrix. This first matrix is called the ***encoding matrix*** *and its inverse is called the* ***decoding matrix****.*

Example*: Let the message be: "****PREPARE TO NEGOTIATE****". Encrypt the message with the encoding matrix below with a shift of +10.*

Let the encoding matrix be $E = \begin{bmatrix} -3 & -3 & -4 \\ 0 & 1 & 1 \\ 4 & 3 & 4 \end{bmatrix}$

Exercise 1

1. Shift the normal 26-letter alphabet 27 letters to the right in the next problem

55, 137, 340, 44, 114, 245, 61, 131, 292, 34, 106, 235, 30, 134, 348, 16, 106, 247, 44, 120, 320, 10, 118, 256, 20, 128, 284, 47, 119, 278, 27, 135, 330, 34, 142, 334, 39, 103, 231, 25, 133, 295, 41, 149, 365.

where the ***decoding*** *matrix is*

$$\begin{bmatrix} \frac{1}{3} & 1 & -\frac{1}{3} \\ -\frac{1}{2} & \frac{1}{2} & 0 \\ \frac{1}{6} & -\frac{1}{2} & \frac{1}{3} \end{bmatrix}$$

The Actual Message is : ____

____.

Exercise 2

1. *Shift the normal 26-letter alphabet five letters to the right in the next problem (it will look like the above row of letters that assigns the letter V to 1) to help you solve the following code:*

219, 134, -73, -152, 136, 77, -56, -91, 160, 0, -88, -32, 109, -3, -63, -20, 160, 40, -72, -64, 131, -25, -25, 0, 184, 124, 8, -130, 222, 168, -34, -176, 189, 34, -79, -66, 151, 89, -53, -103, 158, 18, -114, -50, 168, 124, -8, -130, 173, 37, -55, -61.

where the ***<u>encoding</u>*** *matrix was*

$$\begin{bmatrix} 2 & 3 & 3 & 1 \\ 0 & 4 & 3 & -3 \\ 2 & -1 & -1 & -3 \\ 0 & -4 & -3 & 2 \end{bmatrix}$$

The Actual Message is : ____

____.

Caesar Wheel

Directions:

1. Carefully cut around the two circles
2. Write the alphabet in BLACK around the SMALL circle
3. Write the alphabet in RED around the LARGE circle
4. Fix the small circle onto the big circle using a paper fastener through the center (marked with a dot)

You are ready to use your Caesar Wheel

REMEMBER the plaintext letters are written in BLACK, the ciphertext letters are written in RED

ENCIPHERING = BLACK → RED
DECIPHERING = RED → BLACK