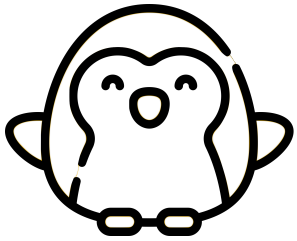


MCAMC

2022

# Team Round

Middlesex County Academy

April 30, 2022

This section of the competition is to be completed by **your team** within **1 hour**. This section consists of **20 questions**.

**No** calculators, notes, compasses, smartphones, smartwatches, or **any other aids** are allowed.

All answers must be written **legibly** on the answer sheet to receive credit.

Answers must be **exact** (do not approximate $\pi$) and in **simplest form**, with all fractions expressed as improper fractions.

Examples of **unacceptable answers** include: $\frac{4}{6}$, $1\frac{1}{3}$, $3+2$.

Examples of **acceptable answers** include: $\frac{2}{3}$, $\frac{4}{3}$, $5$.

There is **no need to include units** for any answer, and the units are always assumed to be the units in the question.

Either **exact decimal answers** or **improper fractions** will be accepted (i.e. $0.25$ and $\frac{1}{4}$ are both acceptable).

Some questions will require a brief explanation. Additionally, questions may have no answer. If so, the correct response is **"None"**.

**Best of luck!**

# 1 Answer Sheet

Name: _____

Team Name: _____

Team Number: _____ Please write your answers on this sheet legibly, and please follow the rules that were found on the first page.

1. _____
2. _____
3. _____
4. _____
5. _____
6. _____
7. _____

   _____
8. _____
9. _____
10. _____
11. _____
12. $\begin{bmatrix} \text{---} & \text{---} \\ \text{---} & \text{---} \end{bmatrix}$
13. $\begin{bmatrix} \text{---} & \text{---} & \text{---} \\ \text{---} & \text{---} & \text{---} \\ \text{---} & \text{---} & \text{---} \end{bmatrix}$
14. _____
15. _____
16. _____
17. _____
18. _____
19. _____

    _____
20. _____

    _____

## 2 Cryptography

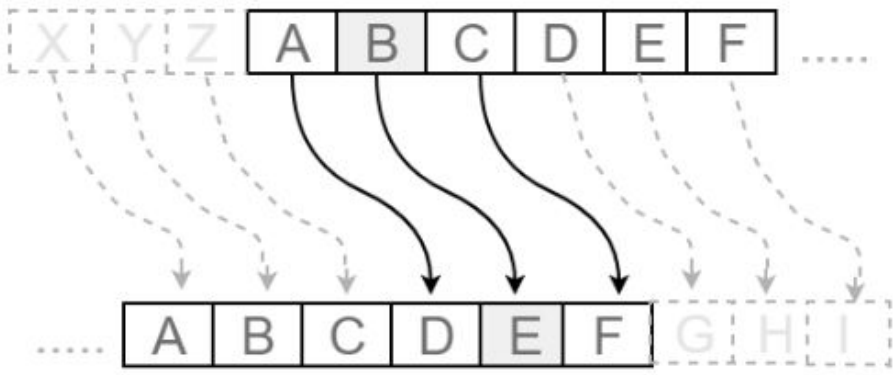
The word "cryptography" is derived from the Greek word *kryptos*, which translates to "hidden". This is fitting, as cryptography is the study of communication techniques that allow a user to send a message that can be read only by the person who they intend to do so.

Cryptography has a vast array of applications in the fields of computer science, mathematics, engineering, physics, and beyond. Skills with cryptography are also highly sought after by government organizations such as the FBI and CIA, dealing with matters of national security.

We should also note that there are two parts to cryptography: encrypting, or making the message into a code, and decoding/decrypting, or taking the code and finding the intended message.

With that said, let's get started.

Below is a very simple example of cryptography that utilizes a **Caesar Cipher**.




So how did this cipher work? As many of you may have figured out, the Caesar Cipher takes the letters of the original message and shifts them all a constant number. For example, in the diagram, A shifts to D, B shifts to E, and C shifts to F, with each letter shifting 3 times forward (if we cross 'Z' we "wrap around" the alphabet).

This cipher may seem extremely easy to understand, but its useful for examining the structure of how a message may be encrypted and decrypted.

Speaking of decryption, how would we go about doing this with a Caesar Cipher? In effect, it works just like encryption, but we reverse the shift (if we cross 'A' we "wrap around" the alphabet).In our previous example, decryption would involve a shift from D to A, E to B, and F to C, or a shift of 3 letters backward.

We won't spend too much time on this cipher, but it is critical that you understand the difference between encryption and decryption.

The next ciphers we cover will be much more difficult, involving modular arithmetic and matrices, so be prepared.

For now, try to solve some of these problems. Below is a chart to help you map letters to numbers.

| A | B | C | D | E | F | G | H | I | J | K | L | M |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ↕ | ↕ | ↕ | ↕ | ↕ | ↕ | ↕ | ↕ | ↕ | ↕ | ↕ | ↕ | ↕ |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |

| N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ↕ | ↕ | ↕ | ↕ | ↕ | ↕ | ↕ | ↕ | ↕ | ↕ | ↕ | ↕ | ↕ |
| 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |

**Problem 1.** In the image below, what is the forward shift used to encrypt the message using a Caesar Cipher?

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

**Problem 2.** Sid needs to urgently send Justin a message reading "QGLMZ", but does not want someone else to accidentally read the message (these letters are an acronym for a top secret project they are working on). He entrusts the 5 cipher brothers to help him.

When the first brother reads the message, he shifts each letter of the message x characters backwards.

The second brother then shifts each letter of the message $2x + 3$ forwards.

The third brother then shifts each letter of the message $4x - 1$ backwards.

The fourth brother shifts each letter of the message $7x + 2$ backwards.

The fifth brother is not paying attention, and instead of further shifting the message, he erases one of the letters, and sends it to Justin.

Justin reads that the message says **"EUZN"**. This encrypted message is missing a letter. Based on the encryption details, find the missing letter that should have appeared in the encrypted message at the right position.

**Problem 3.** Find x, which was the original shift performed by the first brother in **Problem 2**.

# 3 Affine Ciphers

Affine Ciphers are centered around modular arithmetic, so here is a quick review for those unfamiliar with it:

The expression $a$ mod $x$ refers to the remainder when a is divided by $x$. For example, 8 mod 3 is equal to 2 as when 8 is divided by 3, the remainder is 2. We can also say that $8 \equiv 2 \bmod 3$.

**Problem 4:** Find 47 mod 6.

Now, we will discuss the multiplicative inverses in modular arithmetic. Recall that a multiplicative inverse of any number in algebra is the number that generates a value of 1 when multiplied by the original number.

That is,

$$A^{-1} \cdot A = 1$$

In the above equation, $A^{-1}$ is the multiplicative inverse of the number A. For example, the multiplicative inverse of 8 is $\frac{1}{8}$, as $8 \cdot \frac{1}{8}$ is equal to 1.

In the same way, there is a multiplicative inverse in modular arithmetic as well. The multiplicative inverse of $a$ mod $b$ asks for the smallest integer $a^{-1}$ such that:

$$a * a^{-1} \bmod b \equiv 1$$

**Example 1:** Find $a^{-1}$ where $a = 7$ and $b = 12$ above.

The answer is $a^{-1} = 7$. This is because $7 \times 7 = 49$, and $49 \bmod 12 \equiv 1$ (48 is the greatest multiple less than 49). 7 is also the smallest positive integer which satisfies this.

Now try to solve the next three problems to solidify your understanding of modular arithmetic and the implementation of multiplicative inverses.

**Problem 5:** $a * a^{-1} \bmod 13 \equiv 1$ where $a = 19$. Find smallest such integer $a^{-1}$.

**Problem 6:** $a * a^{-1} \bmod 6 \equiv 1$. In this expression, assume that $a^{-1}$ is a positive integer. For which values of $a$ are there no suitable value of $a^{-1}$, i.e. no multiplicative modulo inverse for $a$ in mod 6?

Since we have gone over all the prerequisites needed, it is time to finally learn about Affine Ciphers, both encryption and decryption.

When encrypting a message using the Affine Cipher, we use the following formula:

$$(a \times x + b) \bmod m$$

We are supplied with the integer values of the variables $a$ and $b$, and $m$ is the number of values in the cipher, which in the case of the standard alphabet, is equal to 26.

$x$ then represents the integer value of a given letter, with the letter A equal to 0, the letter B equal to 1, the letter C equal to 2 . . . and finally, the letter Z equal to 25. Refer to the following image for all of the indices.

| Letter | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Number | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |

We then take the result of our equation and substitute the corresponding letter whose index is our answer using the formula.

This may seem complicated, so an example is the best form of explanation.

**Example 2:** Given that $a$ is equal to 36 and $b$ is equal to 14, encode the message $MCAMC$ using the Affine Cipher.

Let's break this problem down one step at a time. First, let us find the index of each of the letters used in the original message.

$$M : 12$$

$$C : 2$$

$$A : 0$$

$$M : 12$$

$$C : 2$$

Next we find the integer index of the letters in our encrypted message using our encryption formula.

First, let us do this for the letter $M$ from the original message.

$(36 \times 12 + 14)$ mod 26 is equal to 446 mod 26, or 4. The letter whose index is 4 is $E$, meaning that the $M$'s of the original message become $E$'s in the encoded message.

Now, let us repeat this process for the letter $C$ from the original message. $(36 \times 2 + 14)$ mod 26 is equal to 86 mod 26, or 8. The letter whose index is 8 is $I$, meaning that the $C$'s from the original message become $I$'s in the encoded message.

Finally, we need to do this once more with the letter $A$ from the original message. $(36 \times 0 + 14)$ mod 26 is equal to 14 mod 26 or 14. The letter whose index is 14 is $O$, meaning that the $A$'s from the original message become $O$'s in the encoded message.

Now, what is our encoded message? It is

$$EIOEI$$

From $MCAMC$ to $EIOEI$, this process may seem complicated, but it is extremely powerful nonetheless.

**Problem 7:** However, can you notice an important flaw in this cipher? While our encoding is correct, there is an issue for the person tasked with decoding this cipher. Find this issue, and give a brief explanation as to why this is the case. *Hint: It has something to do with the values of a and b.*

Now, try these two problems which involve encoding a message using the Affine cipher.

**Problem 8:** Given the values $a = 21$ and $b = 7$, encode the message $MARVEL$ using the Affine Cipher.

**Problem 9:** When we encode the message HAWKEYE using the Affine Cipher our result is the message KVFJLNL. Find $a$ and $b$.

Now that we have gone over encoding using the Affine Cipher, it is time to move on to decoding. While this is undoubtedly more difficult than encoding, it is still doable as long as we break it down into logical steps.

The decryption formula for an Affine Cipher is as follows

$$D(x) = a^{-1}(x - b) \bmod 26$$

This formula is clearly very difficult to understand, so let's break this down.

First, we want to find the smallest integer such that when its product with a is divided by 26, the remainder is 1. Let us call this integer k.

Here is a reference diagram to help you find the value of k quickly.

Note that if $a$ is even it is not possible for there to be a remainder of 1 no matter the integer it is multiplied by when divided by 26.

Note that if $a$ is greater than 26, use $a$ *mod* 26 instead.

| $a$ | 1 | 3 | 5 | 7 | 9 | 11 | 15 | 17 | 19 | 21 | 23 | 25 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $a^{-1}$ | 1 | 9 | 21 | 15 | 3 | 19 | 7 | 23 | 11 | 5 | 17 | 25 |

Now, let us evaluate $k \times (x - b)$, where $x$ is the index of a letter that made up the original message. We repeat this for all letters in the message.

Now we compute the mod 26 of this answer, and call this positive integer $t$. Now we find the letter whose corresponding index is $t$, and this is the decoded letter from the message. We now repeat this process for all letters in the message.

Once again, an example is critical to understand this concept.

**Example 3:** Using $a = 5$ and $b = 9$, decrypt the message $XQBW$ using the Affine cipher.

While this problem may seem scary, let's approach it logically. First, we can use the reference table to find that the multiplicative inverse of 5 is 21. Since $b$ is equal to 9, we now have the equation $21 \times (x - 9)$. Now let us find the indexes of each of the letters in the original message.

$$X : 23$$

$$Q : 16$$

$$B : 1$$

$$W : 22$$

Now we follow the process of substituting each of these integers into the expression above, and dividing the value by 26. We will then take the remainder and find which letter corresponds to that index.

$$21 \times (23 - 9) = 294 \bmod 26 = 8$$

The letter $I$ has an index of 8, meaning that the letter $X$ in the encrypted message was originally the letter $I$.

$$21 \times (16 - 9) = 147 \bmod 26 = 17$$

The letter $R$ has an index of 17, meaning that the letter $Q$ in the encrypted message was originally $R$.

$$21 \times (1 - 9) = -168 \bmod 26 = 14$$

Note that $26 \times -7 = -182$, and $-182 + 14 = -168$. The letter $O$ has an index of 14, meaning that the letter $B$ in the encrypted message was originally the letter $O$.

$$21 \times (22 - 9) = 273 \bmod 26 = 13$$

The letter $N$ has an index of 13, meaning that the letter $W$ in the encrypted message was originally $N$.

This means that our decoded message is IRON. Decoding an Affine cipher can seem especially tricky due to the multiplicative inverse, but when the correct approach is utilized, they are rather straightforward. Now, try these two problems on your own.

**Problem 10:** If $a = 11$ and $b = 13$, decode the message $JSNRLA$ using the Affine cipher.

**Problem 11:** If $a = 7$ and $b = 8$ have been used to decode the message $QRBBREMRN$ using the Affine Cipher, what was the original message? For this problem, the alphabet set consists of letters A through S only rather than the usual A through Z.

# 4 Matrix Multiplication

A matrix is a rectangular array of numbers with rows and columns, and is used in many advanced areas of mathematics, especially in the field of Linear Algebra.

Matrix multiplication is an important concept in many ciphers, such as the Hill cipher, which will be mentioned later.

When we multiply a matrix by a number, this is called scalar matrix multiplication.

In this case, we simply multiply each element of the matrix by the quantity. Let us look at the example below.

$$4 \times \begin{bmatrix} 1 \\ 2 \\ 3 \end{bmatrix} = \begin{bmatrix} 1 \times 4 \\ 2 \times 4 \\ 3 \times 4 \end{bmatrix} = \begin{bmatrix} 4 \\ 8 \\ 12 \end{bmatrix}$$

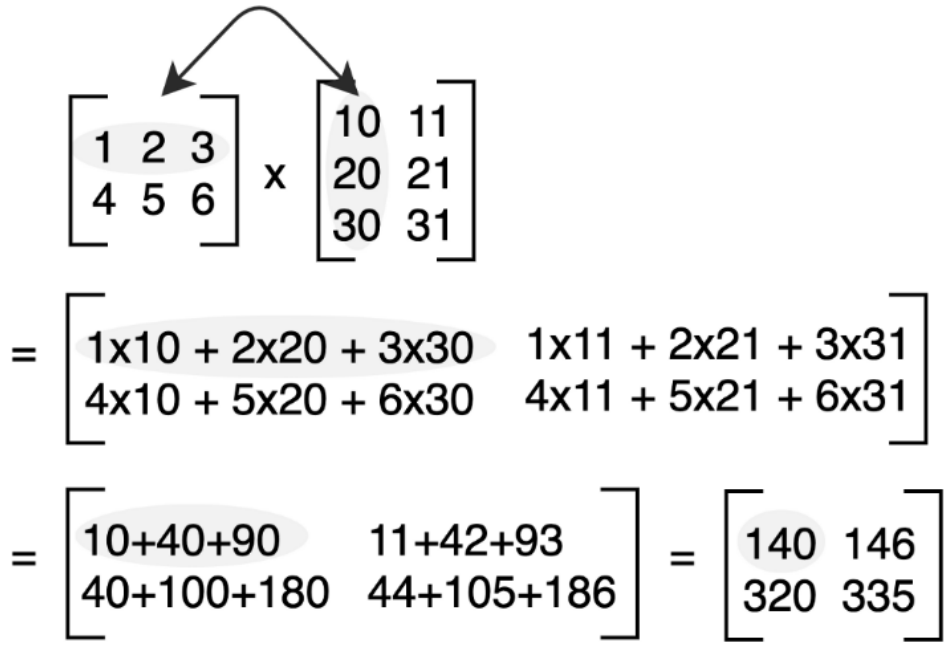
In this image, we can clearly see an example of multiplying a matrix with three rows and one column by the number 4. In fact, a matrix with only one column is actually referred to as a column vector.

We can then see that each element of the vector is multiplied by 4, giving us our final answer.

However, what if we want to multiply two matrices together? This is much more complicated than scalar multiplication, but let us break it down.

First, for two matrices to be multiplied, the number of columns in the first matrix and the number of rows in the second matrix have to be the same. Note that matrix multiplication is not commutative, switching the order of the two matrices will change our product.

Explaining matrix multiplication without an example is difficult, so let us examine one.



When we multiply two matrices together, the resulting matrix has the same number of rows as the first matrix and the same number of columns as the second matrix. For each element of this resulting matrix, we look at what row and column they are in. For example, in this image, we can see that in the resulting matrix, 140 is in the first row and first column, 146 is the first row and second column, 320 is in the second row and first column, and 335 is the second row and second column.

When solving for the first row and first column in our answer, we take the first row of the first matrix and the first column of the second matrix. We find the product of the first element of each row and column respectively, add this to the product of the second element of each row and column, and so on.

For example, this image illustrates that when we solve for the element in the first row and first column of the resulting matrix, we look at the first row of the first matrix, 1 2 3, and the first column of the second matrix, 10 20 30. We then take the product of 1 and 10, add this to the product of 2 and 20, and add this to the product of 3 and 30. This equates to 140, and this process is repeated for every element in our resulting matrix.

Here is another example to help solidify this concept.

**Example 4:**

$$\begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{bmatrix} \times \begin{bmatrix} 7 & 8 \\ 9 & 12 \\ 11 & 12 \end{bmatrix}$$

Let's break this down step by step. First, the number of rows in our first matrix is 2, and the number of columns in our second matrix is 2, meaning that our resulting matrix will be a $2 \times 2$ matrix.

Next, let us solve for the element in the first row and first column of our resulting matrix. This element will be equal to $1 \times 7 + 2 \times 9 + 3 \times 11$, or 58. The element in the second row and first column will be equal to $4 \times 7 + 5 \times 9 + 6 \times 11$, or 139. The element in the second row and second column will be $4 \times 8 + 5 \times 10 + 6 \times 12$, or 154. Finally, the element in the first row and second column will be $1 \times 8 + 2 \times 10 + 3 \times 12$, or 64.

As a result, our answer is:

$$\begin{bmatrix} 58 & 64 \\ 139 & 15 \end{bmatrix}$$

Now, try some of these problems:

**Problem 12:**

$$2 \times \begin{bmatrix} 10 & 6 \\ 4 & 3 \end{bmatrix}$$

**Problem 13:**

$$\begin{bmatrix} 1 & 7 & 3 \\ 2 & 4 & 3 \\ 8 & 5 & 9 \end{bmatrix} \times \begin{bmatrix} 3 & 3 & 9 \\ 5 & 2 & 1 \\ 1 & 5 & 4 \end{bmatrix}$$

**Problem 14:** The first row of a 2 by 2 matrix from left to right are an integer a and 3, and the second row from left to right are an integer 5 and b. The first row of the 2 by 2 matrix it is multiplied by from left to right are 7 and 8, and the second row from left to right are 12 and 13. If the first row of the resulting matrix from left to right are 99 and 111, and the second row of the resulting matrix from left to right are 239 and 261, find $a + b$.

Now that we know matrix multiplication, we are ready to learn a new cipher, the Hill Cipher.

# 5 Hill Cipher Encryption

While the Hill Cipher involves both encryption and decryption, we will only be covering encryption. Decryption requires the concepts of determinants and adjacent matrices, which is beyond the purview of what will be covered in this contest.

When encrypting using the Hill Cipher, we first have a matrix which serves as our key. This matrix can be a $2 \times 2$ or $3 \times 3$ matrix, and contains any of the letters A through Z.

Then, we are given a message to encrypt. If our key is a $2 \times 2$ matrix, we split the message in 2 letter parts, and if it is a $3 \times 3$ matrix, we split the message in 3 letter parts. Note that if the number of letters is not divisible by either 2 or 3, (depending on if a $2 \times 2$ matrix key or $3 \times 3$ matrix key is used) the letter Z is added onto the end of the matrix to make it so. However, this will not be necessary for the problems given.

Now, we take the matrix that is the key and substitute the letters for their corresponding number indexes (that is, A is 0, B is 1, C is 2, etc.). We then create a column matrix of length 2 or 3 (depending on if the key is a $2 \times 2$ or $3 \times 3$ matrix) of the first 2 or 3 letters of the message (depending on if the key is a $2 \times 2$ or $3 \times 3$ matrix). These letters are also converted to their number indexes.

Finally, we multiply the key matrix by the column vector, and take each element of the resulting matrix and find its remainder when divided by 26. We then convert each element to the letter which corresponds to that number index. This is repeated for all of the two letter segments, and we combine these new encoded segments to create our encoded message.

Like we have seen in our other ciphers, the Hill Cipher is nearly impossible to understand without an example.

**Example 5:** Encode the message "NICE" using the following $2 \times 2$ encryption matrix.

$$\begin{bmatrix} K & I \\ N & D \end{bmatrix}$$

Let's break this down step by step. First, we should find the number indexes of the letters k, i, n, and d. These numbers are 10, 8, 13, and 3. We will also break down "NICE" into the two letter segments "NI" and "CE". We can convert NI to the column vector with the elements 13 and 8, and CE to the column vector with the elements 2 and 4 (because of each letter's number index).

We now have to solve two matrix products, the first being the key multiplied by the column vector with the elements 13 and 8, and the second being the key multiplied by the column vector with the elements 2 and 4.

The first product yields a column vector with the two elements 194 and 193. After dividing each element by 26 and taking the remainder, we get 12 and 11, which corresponds to the letters M and L.

The second product gives us a column vector with the two elements 52 and 38. When dividing each element by 26 and taking the remainder, we get 0 and 12, which corresponds to the letters A and M.

Combining the two, our encoded message of "NICE" is "MLAM".

Now, try these next four ciphers on your own.

**Problem 15:** Using the 2x2 encryption matrix below, encode the message DOGS.

$$\begin{bmatrix} C & A \\ T & S \end{bmatrix}$$

**Problem 16:** Given the following encryption matrix, encode the message GOODNIGHT.

$$\begin{bmatrix} O & L & Y \\ M & P & I \\ A & D & S \end{bmatrix}$$

**Problem 17:** Using a 2x2 encryption matrix, we encrypt the message HI to become NS. What are the letters in the matrix?

# 6 Euler Totients

The Euler Totient function, invented by Leonhard Euler, counts the total number of positive integers less than the given number that are relatively prime to it. This function is widely used in mathematics and cryptography, most notably in the RSA cipher. However, we will not be discussing this cipher in the round. $\phi$ is the sign used to denote the Euler Totient Function. The formula used to solve for $\phi(n)$, where $n$ is a positive integer, can be expressed as the following:

$$n \times (1 - \frac{1}{p_1}) \times (1 - \frac{1}{p_2}) \times \cdots \times (1 - \frac{1}{p_m})$$

Here, the letter $p$ represents a prime factor of the number $n$, where $p_1$ is the first distinct prime factor of $n$, $p_2$ is the second distinct prime factor of $n$, all the way up to the final distinct prime factor of $n$, denoted by $p_m$. While this function may seem simple, it is extremely powerful in mathematics and cryptography.

**Example 6:** Find $\phi(78)$.

Let's break this problem down. We know the formula for the Euler Totient Function, which is what the symbol $\phi$ stands for. However, this formula involves finding all of the different prime factors of the number in question, which in this problem is 78.

We can break down 78 in the following manner:

$$78 = 2 \times 39$$
$$78 = 2 \times 3 \times 13$$

As 2, 3, and 13 are all prime, these are the values of $p_1$, $p_2$, and $p_3$. We substitute these values into the Totient Function.

$$\phi(78) = 78 \times (1 - \frac{1}{2}) \times (1 - \frac{1}{3}) \times (1 - \frac{1}{13})$$
$$\phi(78) = 78 \times (\frac{1}{2}) \times (\frac{2}{3}) \times (\frac{12}{13})$$
$$\phi(78) = 78 \times (\frac{24}{78})$$
$$\phi(78) = 24$$

This means that there are 24 numbers lower than 78 that are relatively prime to 78.

With this information, try the following problems.

**Problem 18:** What is $\phi(4312)$?

**Problem 19:** How many integers $n$ where $1 < n < 100$ satisfy that $\phi(n)$ is odd? (give a brief explanation and/or show your work)

**Problem 20:** $\phi(a) \cdot \phi(b)$ can be expressed as $\phi(k)$. Find $k$ in terms of $a$ and $b$, and give a brief proof/explanation as to why this is true.