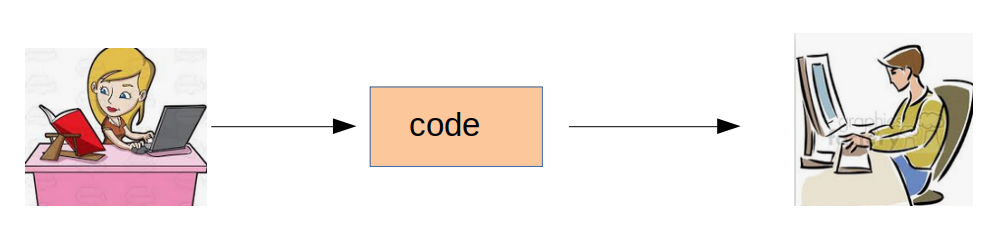
Name\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Secret Messages with coding and decoding**

**[Part 1]**



**Describe what is happening on the diagram above.**

**DECIMAL VALUE OF ASCII**

ASCII is an acronym for American Standard Code . These codes are used to communicate with computers since computers can only understand numbers.

Below is the ASCII character table and its values for capital letters and some characters.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O |
| 65 | 66 | 67 | 68 | 69 | 70 | 71 | 72 | 73 | 74 | 75 | 76 | 77 | 78 | 79 |
| P | Q | R | S | T | U | V | W | X | Y | Z | space | | . |  |
| 80 | 81 | 82 | 83 | 84 | 85 | 86 | 87 | 88 | 89 | 90 | 32 | | 46 |  |

Using the ASCII table, complete this activity with your group:

**Coding Activity**

1. Write a message - It should be a sentence.
2. Using the ASCII values that are shown on the table, convert each letter into decimal values - coding.
3. End each message with a period
4. Share that coded message to another group.

**Decoding ACTIVITY**

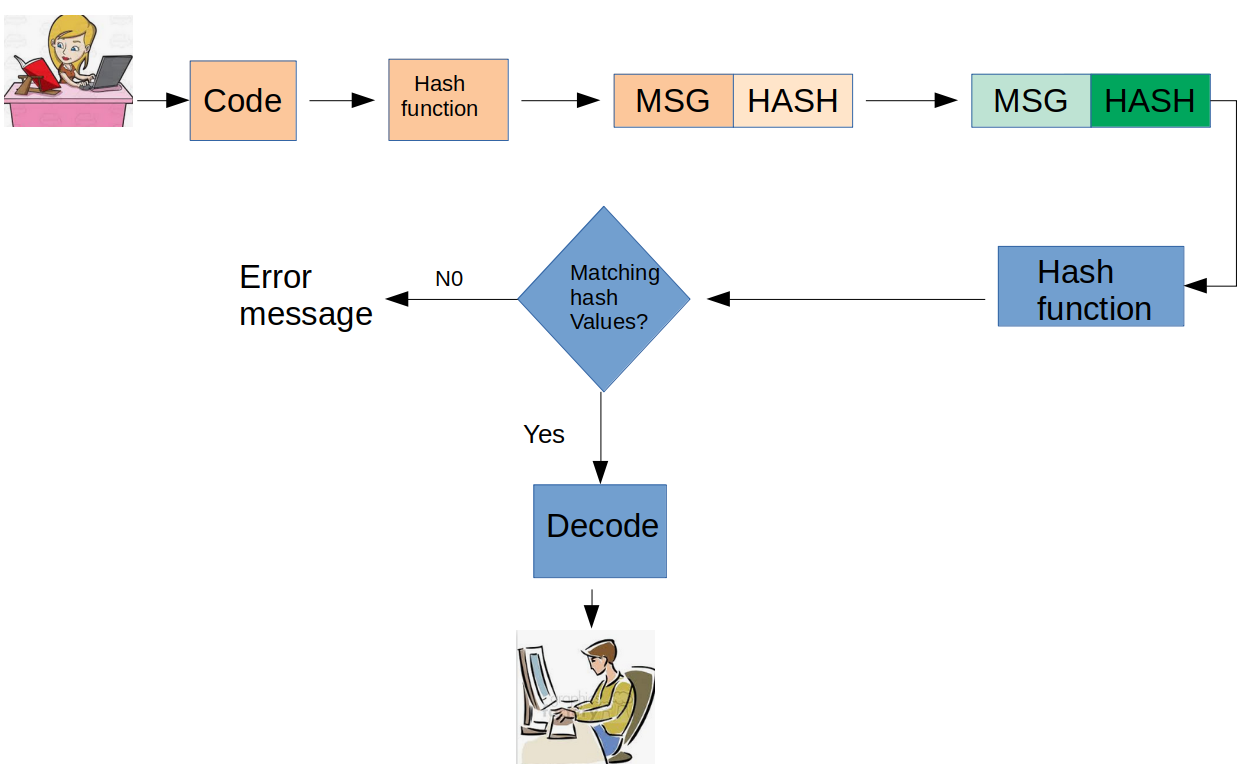
1. If you received the coded message from another group.
2. Decode the message using the ASCII table.
3. Send the decoded message back to the group to verify that it was decoded correctly.

**Enrichment:**

This activity can be enriched by having students convert the decimal ASCII values into binary or hex representations of ASCII values.

**Secret Messages with Hashing**

**[Part 2]**

****

Above is a diagram of the data transfer with hashing value.

In your own words, describe what is happening to each step. Share your description with your group.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Hashing is a way for a computer to make sure the decrypted message wasn’t tampered. Hashing is a non reversible process. In mathematical terms, hashing is a function but not one to one function.**

**Can you write a math equation that is a function but not one to one? Justify your answer.**

When a user sends a secure message, a hash of the intended message is generated and encrypted, and is sent along with the message. When the message is received, the receiver decrypt the hash as well as the message. Then, the receiver creates another hash from the message. If the two hashes are identical when compared, then a secure transmission has occurred. This hashing process ensures that the message is not altered by an unauthorized end user.

Hashing is used to index and retrieve items in a database because it is easier to find the item using the shorter hashed key than using the original value.

<https://www.techopedia.com/definition/14316/hashing>

**MOD HASHING ALGORITHM**

Let’s look at an example of how hash value is determined:

One way of creating a hash value uses the “mod” function (the remainder from a division problem). We can calculate the hash values for a message by evaluating the mod for each decrypted number.

Ex: What is the remainder of 69 divided 5? We can write this as:

69 % 5 = 4

Let's look at this example trying to send the message: “EXTRA”

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ASCII Letters | E | X | T | R | A | . | *The message you want to send* | | |
| ASCII Numbers | 69 | 88 | 84 | 82 | 65 | 46 | *Using ASCII table to translate* | | |
| Hash Digit | 69%5 =  4 | 88%5 =  3 | 84%5 =  4 | 82%5 =  2 | 65%5 =  0 | 46%5 =  1 | *Using the (Ascii values % 5)* | | |

**Fully encrypted message: 698884826510122**

**HASHING ACTIVITY**

1. Write a word that has a minimum of 5 letters.
2. Using the ASCII values that are shown on the table, convert each letter into decimal values.
3. End each word with a period.
4. Determine the hash value using **\_\_%5**
5. Write the hash value to your to the coded message.
6. Share that coded message to another group.
7. If you received the coded message from another group, decode the message and verify that hashing value is authenticated. In other words, If your group is getting the same hash value, the message has not been altered.

**Enrichment:**

This activity can be enriched by having students explore other ASCII characters that would share the same hash values.

For example, all following mod function will evaluate the same remainder.

* 12%5 = 2
* 17%5 = 2
* 22%5 = 2

What other numbers can give you the same value of 2?

Questions:

1. Original message: XYZ

2. What would be the encrypted message if the key is f(x) = x - x + 4 using #%3 as mod function:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

3. Can there be other encrypted messages that might have the same hash value?

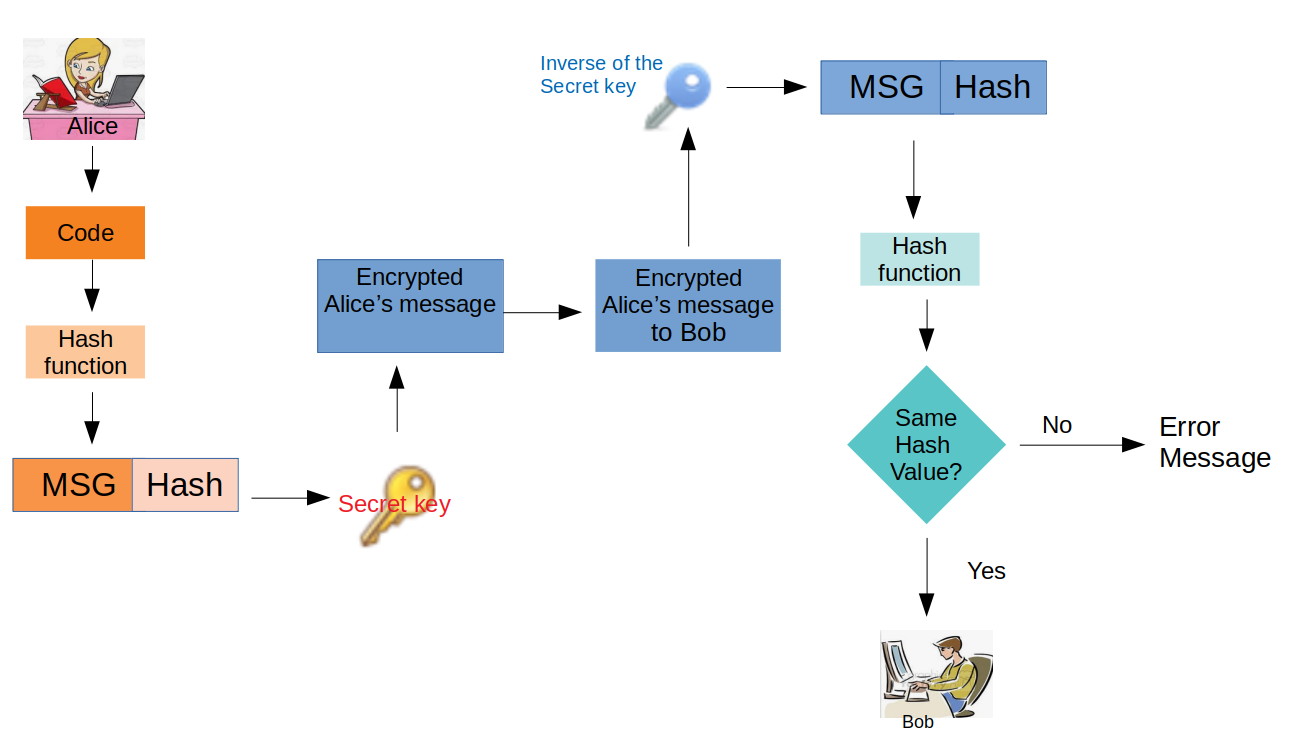
Justify and give examples.

4. What are some problems you can foresee ?????

**Secret Messages with Encryption & Decryption**

**using symmetric-key algorithm**

**[Part 3]**

****

Above is a diagram of the data transfer with encryption and decryption using the symmetric key algorithm.

In your own words, describe what this diagram is trying to illustrate. Share your description with your group.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Let's look at this example trying to send the message: “EXTRA.”

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ASCII Letters | E | X | T | R | A | . | *The message you want to send* | | |
| ASCII Numbers | 69 | 88 | 84 | 82 | 65 | 46 | *Using ASCII table to translate* | | |
| Hash digit: | 69%5 =  4 | 88%5 =  3 | 84%5 =  4 | 82%5 =  2 | 65%5 =  0 | 46%5 =  1 | *Using the (Ascii values % 5)* | | |
| Encryption: | 71 | 90 | 86 | 4 | 67 | 44 | ***Using secret key function***  ***f(x) = x + 2*** | | |

In this case, encrypted message using ***the secret key***: 7190868467434201

Hash value is determined before the encryption.

By encrypting, one can send messages with more security.

**Privately shared secret key Activity:**

1. Convert Message of letters to message of numbers (using ASCII)
2. Evaluate the hash value by using the mod function.
3. Convert the ASCII value ( from step 1) to new numbers using your secret key (use math functions). For example using the y = x+2 as a secret key. Do not convert the hash value.
4. Share your encrypt message with another group.
5. In order to decrypt the message, find the inverse function of the secret key. In this case it would be y = x-2
6. Convert the new numbers to letters (using ASCII)
7. Evaluate the hash value using the values you got from step 6.
8. Validate or check to see if you have the same hash value.
9. What does it mean if the hash value is different?
10. Read the message!
11. Can you confirm that message received is authenticated? Justify your answer.

**In your own words…….**.

What is the difference between sending encoded vs. encrypted messages?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Explain how math is applied to encrypt messages:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_