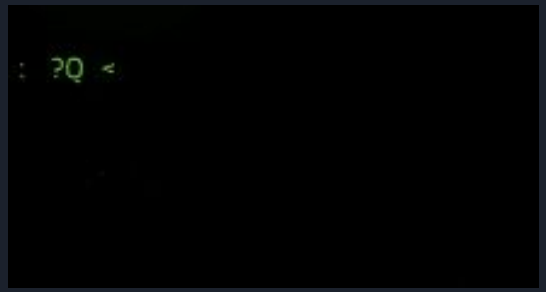

Welcome aboard!

Agenda

- Recap on Last week Ciphers
  - Caesar Cipher
  - Xor Cipher
  - linear congruential generator
- New Ciphers
  - Affine Cipher
  - Baconian Cipher
  - Base64 Cipher
  - Substitution Cipher
  - Vigenere Cipher
- Activity

RECAP



Caesar cipher

Definition: type of substitution cipher in which each letter in the plaintext is replaced by a letter some fixed number of positions down the alphabet.

Xor cipher

Definition: simple additive cipher technique that uses the XOR (exclusive OR) operation for encoding and decoding.

linear congruential generator (lcg)

Definition: A basic pseudo-random number generator (PRNG) that relies on a linear recurrence relation using a modular arithmetic approach to produce a sequence of pseudo-random numbers.

Substitution Cipher

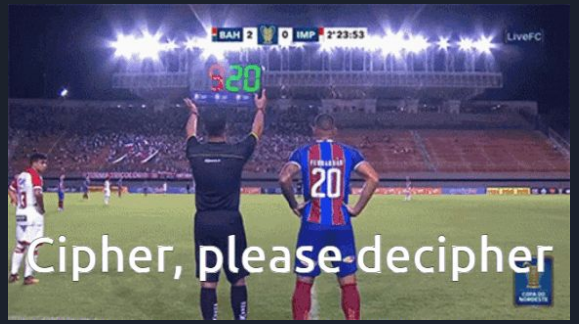
Definition: a type of cipher that replaces each letter in the plaintext with a different letter or symbol to create the ciphertext.

Advantages:

- Easy to grasp and implement.
- Customization: Users can create their own substitution keys, adding a layer of customization.
- Resistant to Frequency Analysis making decryption more challenging.

Disadvantages:

- Vulnerability to Letter Frequency Analysis
- Offers limited security against modern cryptographic attacks.
- Weak Against Known-Plaintext Attacks



Vigenere Cipher

Definition: polyalphabetic substitution cipher that uses a keyword to encrypt text by shifting letters based on their position in the keyword.

Advantages:

- Keyword-Based making it more secure than simple substitution ciphers.
- Different portions of the message are encrypted using different alphabets, adding complexity to the cipher.

Disadvantages:

- Vulnerable to Kasiski examination which reveals the length of the keyword.
- Key management can be complex, especially for long messages, and key distribution should be secure for effective use.

Affine Cipher

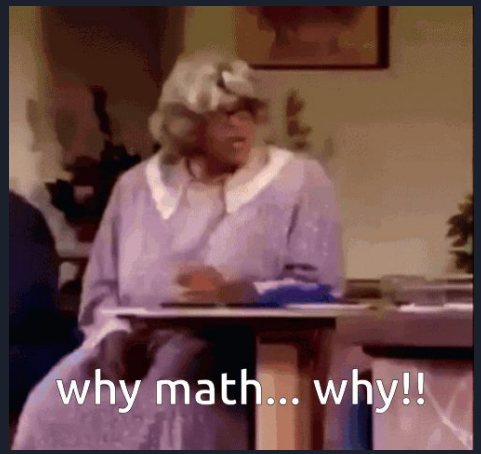
Definition: The Affine Cipher is a simple substitution cipher that combines modular arithmetic with linear transformations to encrypt and decrypt messages.

Advantages:

- Stronger than Caesar Cipher due to the use of two mathematical transformations, making it harder to crack.
- Preservation of Alphabetic Characters making it easy to decipher those with the correct key.

Disadvantages:

- Limited key space making it susceptible to brute-force attacks.
- Similar to other substitution ciphers, it is vulnerable to frequency analysis attacks.



Baconian Cipher

Definition: binary substitution cipher that encodes text by representing each letter with a unique sequence of five characters or binary digits.

Advantages:

- Baconian Cipher is less well-known, which can make it more challenging to decipher for those unfamiliar with it.
- Frequency analysis is less effective compared to other simple substitution ciphers.

Disadvantages:

- Complex Decoding: Decoding Baconian Cipher messages can be labor-intensive, especially without specialized tools.
- Fixed-Length Encoding: The fixed-length binary representation can reveal patterns, and it lacks flexibility.
- Not Secure for Modern Use: In the digital age, Baconian Cipher offers limited security against modern code-breaking methods.

Base64 Cipher

Definition: a binary to a text encoding scheme that represents binary data in an ASCII string format

Advantages:

- Simple and efficient way to represent binary data in a text format.
- Can be easily included in text documents, such as HTML, CSS, or JavaScript files.

Disadvantages:

- Increases the size of the data by about 33%, which can be inefficient for large data transfers.
- Base64 is **not a cipher** but an encoding method; it doesn't provide encryption or security on its own.

Activity

Caesar cipher:	nc chal.gopherhack.club 5020
Vigenere cipher:	nc chal.gopherhack.club 5021
Xor cipher:	nc chal.gopherhack.club 5022
LCG:	nc chal.gopherhack.club 5023
Base64:	nc chal.gopherhack.club 5024
Baconian Cipher:	nc chal.gopherhack.club 5025
Affine Cipher:	nc chal.gopherhack.club 5026
Substitution Cipher:	nc chal.gopherhack.club 5027