U.S. DEPARTMENT OF ENERGY'S
CYBERFORCE® PROGRAM

CyberForce® 101

Encryption and Ciphers

October 2023

cyberforcecompetition@anl.gov

Encryption and Ciphers 101

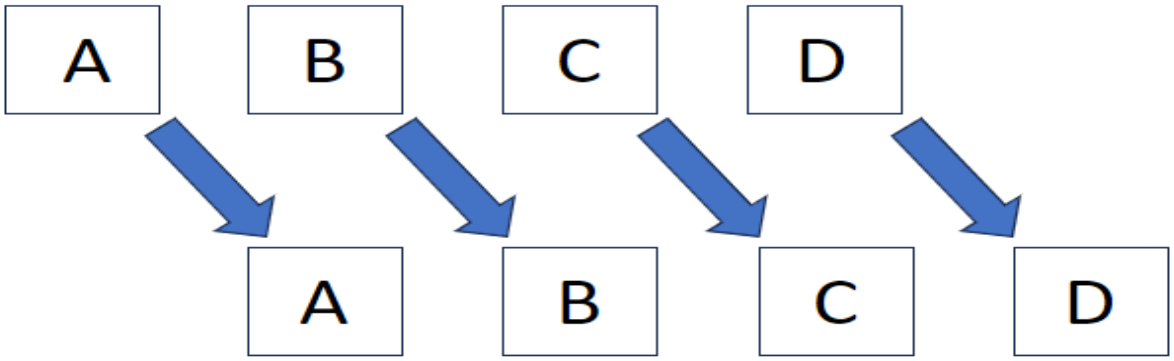
Encryption

Encryption is the process of taking a plaintext message, converting it to ciphertext and then back to plaintext. Plaintext is the readable message and ciphertext is the unreadable byproduct of encryption algorithms. For an encryption algorithm to be secure, the ciphertext should not reveal anything about the plaintext.

The process of encryption requires at least one key. Modern encryption can be divided into two types: Symmetric and Asymmetric. Symmetric means that the keys used to encrypt and decrypt a message are the same. Asymmetric means that they are different. The two keys are called public and private. As the names suggest, the public key is released to a person or group of people while the private key remains secret.

Caesar Shift Cipher

The Caesar Shift Cipher, named after Julius Caesar, shifts the letters in the alphabet. The person encoding the message first writes out their plaintext message. Second, they select a number between 1 and 25 to represent the number of letters the message will be shifted. After that, the letters in the message are shifted the amount that the encoder chose in step two. So, if the original message is “Hello World” and the shift is 5, the ciphertext is “Mjqqt Btwqi”.



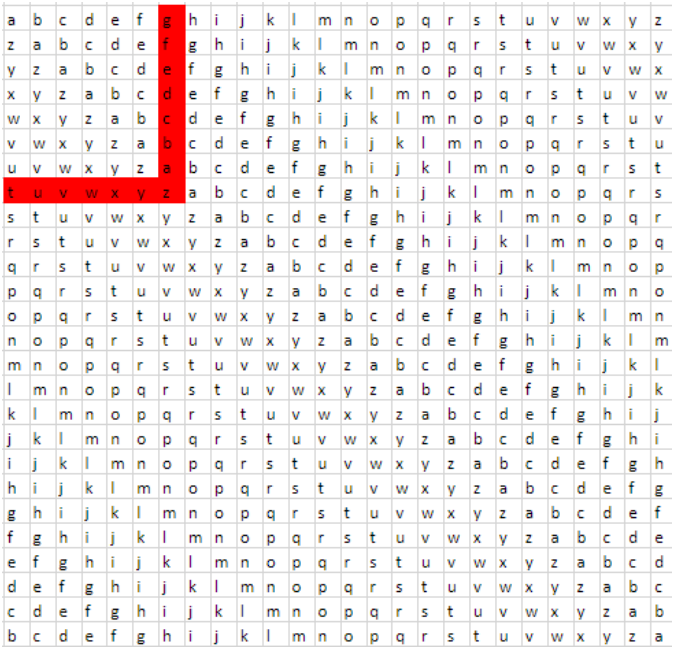
Substitution Cipher

The Substitution Cipher is a way of encoding messages by replacing one letter for another image or character. It is similar to the Caesar Shift Cipher, but the main difference is that this cipher does not use a shift to assign the substitutions. The letter correlations can be arbitrary or follow a pattern. This can be done with letters, numbers and symbols.

Vigenère Cipher

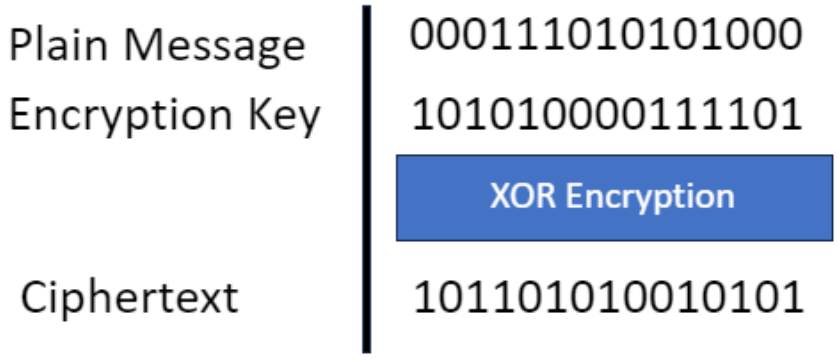
The Vigenère Cipher is a substitution cipher that uses a key word to calculate the shift of letters. It takes 2 parameters: the plaintext message and the key. The key is repeated until it is the size of the original message. Then each letter in the plaintext is matched with the corresponding letter in the key. After, a Vigenère Square is used to create the ciphertext.

A Vigenère Square is a 26 by 26 grid where each row and column have all the letters of the alphabet. The plaintext message corelate to the columns and the key corelates to the rows. The ciphertext is then formed by taking the letter at which the key and plaintext intersect. This is repeated for each character.



XOR Cipher

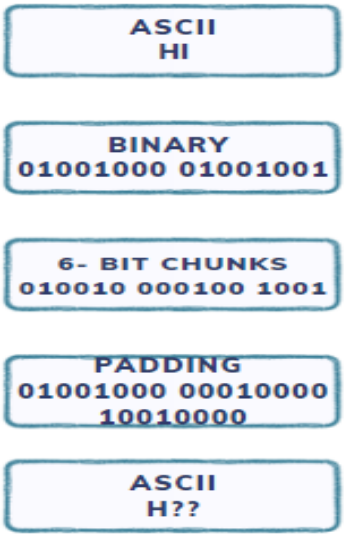
The XOR (exclusive or) cipher uses the XOR operator which only returns True when the inputs are different. The encryption works by taking a randomly generated key and performing the XOR operation. One parameter is the encryption key and the second is the plaintext message. This is because the XOR operation needs 2 parameters for this to work. Since this cipher is encoded and decoded with the same key, XOR Ciphers are a form of symmetric encryption.



Base64

Base64 was created to share files. Instead of the standard 8 bits to a byte, Base64 separates binary code into 6-bit chunks. It encrypts files (texts, images, videos, audio, ect.) through a series of steps:

1. Convert the file to binary
2. Separate the binary code into 6-bit chunks
3. Add padding to make the chunks bytes
4. Convert the binary to text (ciphertext)



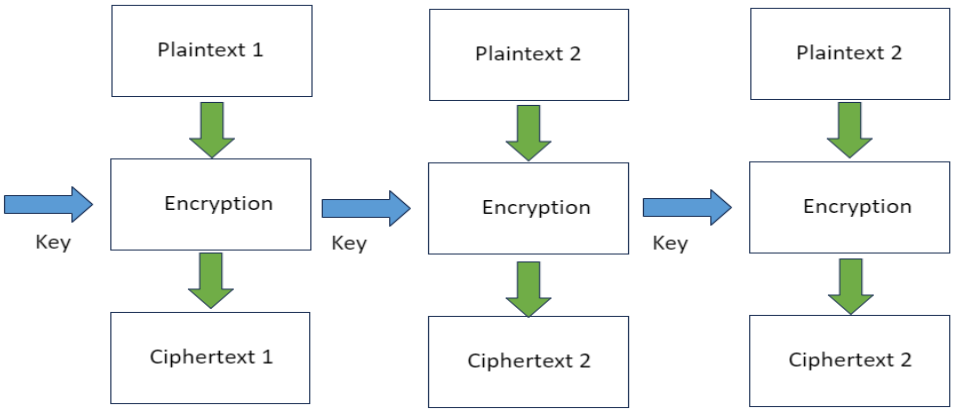
In Linux, the basic command to encode a text with Base64 is:

```
$ echo text | base64
```

To decode the text, all that needs to be added is –d.

TEA

Tiny Encryption Algorithm (TEA) is a block algorithm. It separates the plaintext message or file into blocks consisting of 64 bits (8 bytes) and uses 128 –bit keys. It then runs the blocks through the algorithm a minimum of 32 times (the recommended amount is 64).



AES

Advance Encryption Standard (AES) is best used on stagnant data, meaning that it is rarely, if ever, changed. It was created by NIST in 1997 to protect classified documents.

AES utilizes a machine's hardware and software and has 3 different key lengths (128, 192 and 256 bits). It uses those keys to put the data through 10-14 rounds of symmetric encryption.

RC4

Rivest Cipher 4 (RC4) is one of the most commonly used stream ciphers and is used in RSA encryption. It works by generating a random key that is either 64 or 128 bits. Then a Key Stream is calculated and the XOR operation is performed on each bit.

RC4 is lightweight, fast and easy to use. One of the biggest advantages is that it was designed to handle large streams of data and takes up minimal storage.

Sources:

- https://www.sciencedirect.com/topics/computer-science/substitution-cipher#:~:text=A%20substitution%20cipher%20merely%20substitutes,starting%20with%201%20for%20A.

- https://www.geeksforgeeks.org/vigenere-cipher/
- https://www.101computing.net/xor-encryption-algorithm/
- https://www.redhat.com/sysadmin/base64-encoding#:~:text=Fundamentally%2C%20Base64%20is%20used%20to,grouped%20into%2024%2Dbit%20sequences
- https://medium.com/@cafly/simple-and-efficient-encryption-algorithm-tea-7b6472a5a3fe
- https://www.techtarget.com/searchsecurity/definition/Advanced-Encryption-Standard?Offer=abt_pubpro_AI-Insider
- https://www.geeksforgeeks.org/what-is-rc4-encryption/