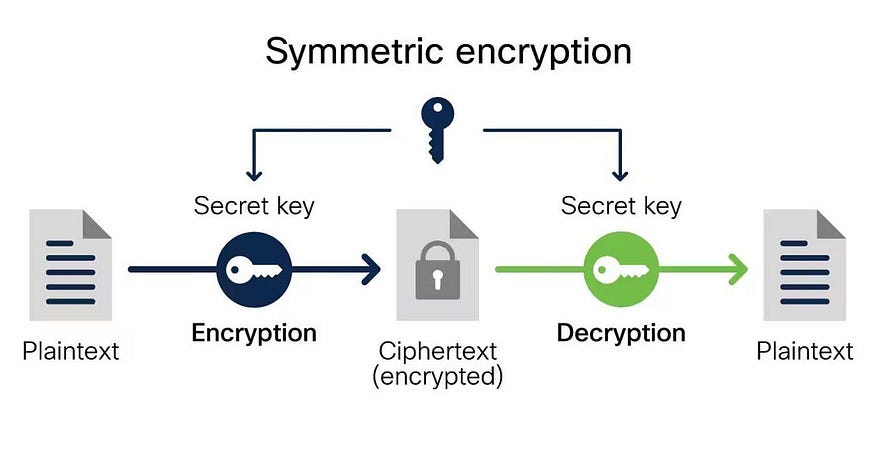
CRYPTOGRAPHY

Cryptography is a crucial aspect of cybersecurity that involves using algorithms and protocols to protect the confidentiality, integrity, authenticity of data and there are two distinct keys used in Cryptography; Symmetric and Asymmetric.

# ****Symmetric Key Encryption****

Symmetric key encryption is a method of encrypting data where the same key is used for both encryption and decryption. It’s a fundamental technique in cryptography used to secure data transmission and storage.

In symmetric key encryption, a single key is used to both encrypt and decrypt data. The sender and recipient must both have the same key and keep it secret.



Symmetric Key Encryption Process

****Encryption and Decryption Process in Symmetric Encryption****

* ****Encryption:**** The process of converting plaintext (readable data) into ciphertext (encrypted data) using the symmetric key.
* ****Decryption:**** The process of converting ciphertext back into plaintext using the same symmetric key.

****Algorithms:****

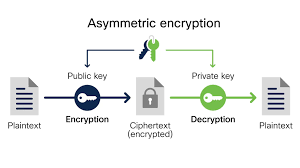
1. ****AES (Advanced Encryption Standard):**** Widely used symmetric encryption algorithm known for its security and efficiency. It supports key sizes of 128, 192, or 256 bits.
2. ****DES (Data Encryption Standard):**** An older symmetric encryption algorithm that uses a 56-bit key. It is now considered insecure due to advances in computing power and is largely replaced by AES.
3. ****3DES (Triple DES):**** An enhancement of DES that applies the DES algorithm three times to each data block, offering improved security over DES but is slower than AES.

# **Asymmetric Key Encryption**

Asymmetric key encryption, also known as public-key cryptography, is a method of encryption that uses a pair of keys: a public key and a private key. Unlike symmetric key encryption, where the same key is used for both encryption and decryption, asymmetric key encryption uses different keys for these operations.

****Public and Private Keys****

1. ****Public Key:**** This key is shared openly and can be distributed to anyone. It is used for encrypting data.
2. ****Private Key:**** This key is kept secret and is known only to the owner. It is used for decrypting data that was encrypted with the corresponding public key.



Asymmetric Key Encryption Process

****Encryption and Decryption Process in Asymmetric Encryption****

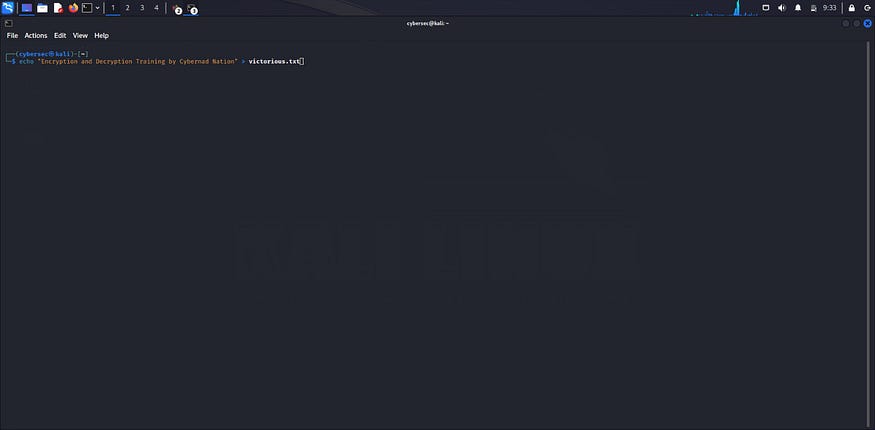
* ****Encryption:**** When data is encrypted with the public key, only the corresponding private key can decrypt it.
* ****Decryption:**** Data encrypted with the private key can be decrypted only with the corresponding public key.

****Algorithms:****

1. ****RSA (Rivest-Shamir-Adleman):**** One of the earliest and most widely used asymmetric encryption algorithms. It is based on the difficulty of factoring large integers.
2. ****ECC (Elliptic Curve Cryptography):**** A newer approach that offers similar security to RSA with smaller key sizes, making it more efficient.
3. ****DSA (Digital Signature Algorithm):**** Primarily used for digital signatures rather than encryption.

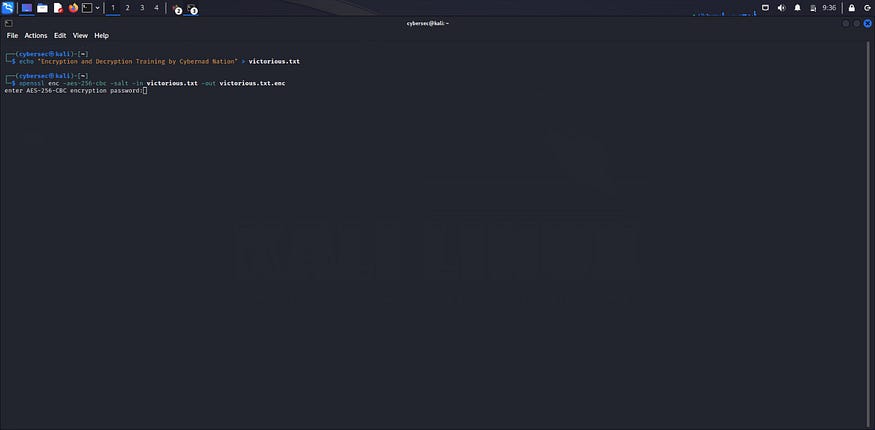
****STEPS IN ENCRYPTION AND DECRYPTION USING KALI LINUX****

1. Identify the Text you want to encrypt



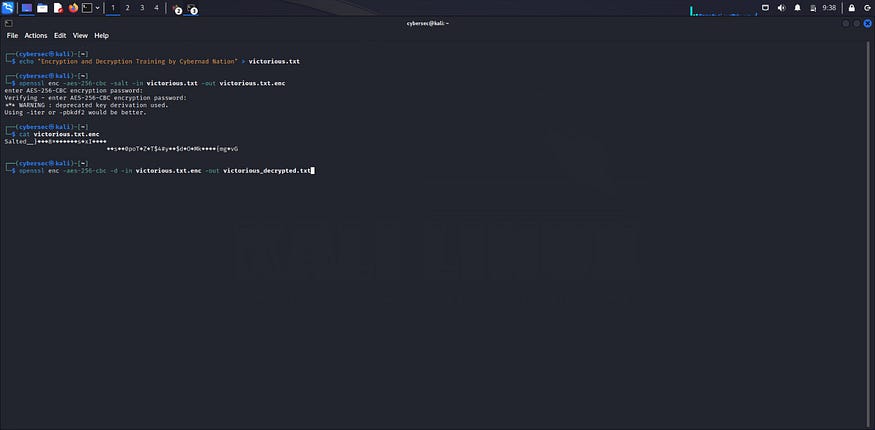
Identified the text using echo Function and saved it in a new directory with file name ‘filename.txt’ ..in above i use victorious.txt

2. Encrypt the text using the command ‘openssl enc -aes-256-cbc -salt -in filename.txt -out filename.txt.enc’,(victorious.txt.enc) input password and press enter.



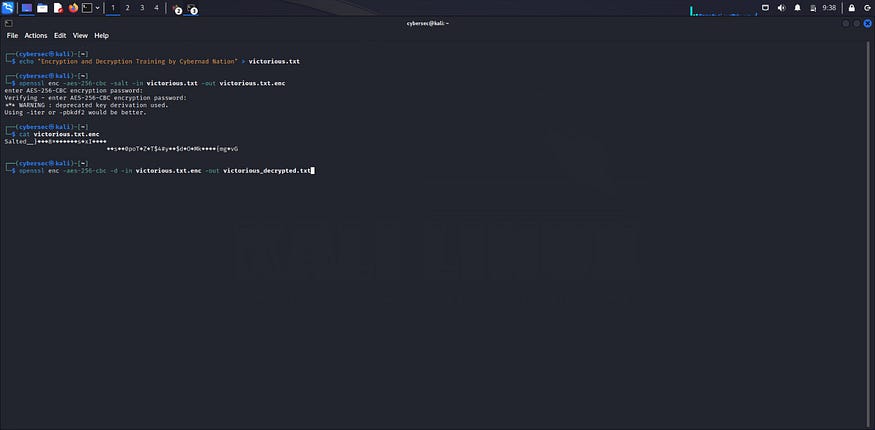
encrypting the victorious.txt file

3. Using the ‘cat’ function to check the encrypted files, then use the command ‘cat victorious.txt.enc to view encrypted the message.



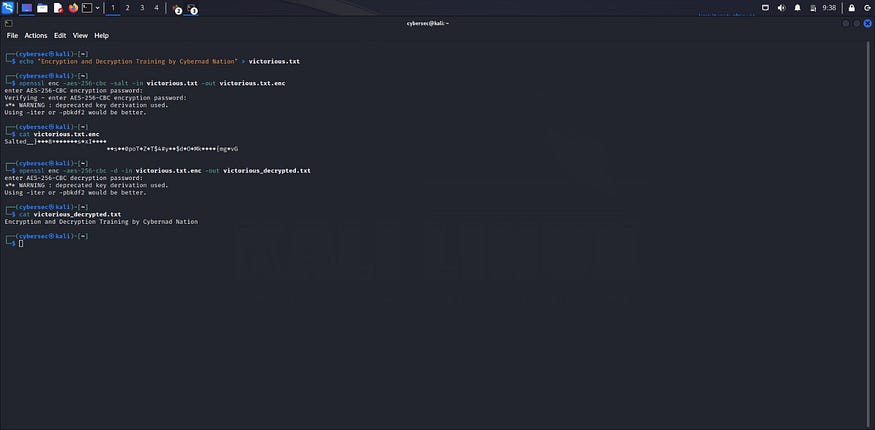
cat victorious.txt.enc

4. Using ‘open’ function openssl enc -aes-256-cbc -d -in filename.txt.enc -out filename\_decrypted.txt to decrypt the message



openssl enc -aes-256-cbc -d -in victorious.txt.enc -out victorious\_decrypted.txt

5. Using the ‘cat’ function to check the decrypted files, then use the command ‘cat victorious\_decrypted.txt to view decrypted the message.



cat victorious\_decrypted.txt