IMAGE ENCRYPTION AND DECRYPTION USING TRIPLE DES

ABSTRACT

- Triple DES (3DES) enhances security by applying the Data Encryption Standard (DES) algorithm three times to each data block, significantly improving security compared to standard DES.

- It employs a key length of 168 bits, utilizing three 56-bit keys, which provides substantial resistance to brute-force attacks. The encryption process involves three stages: encrypting the data with the first key, decrypting it with the second key, and re-encrypting it with the third key, known as the Encrypt-Decrypt-Encrypt (EDE) method.

- This design maintains backward compatibility with DES, allowing systems to upgrade their security measures without requiring a complete overhaul of the existing encryption infrastructure.

INTRODUCTION

01 02

- In the digital age, the protection of sensitive image data has become increasingly critical. As images are widely used across various domains, including healthcare, financial services, and social media, ensuring their confidentiality and integrity is paramount.
- Traditional encryption algorithms like DES (Data Encryption Standard) have been found to be inadequate due to their susceptibility to brute-force attacks.
- To address this issue, the Triple DES (3DES) algorithm was developed, offering a more secure alternative by applying the DES encryption process three times to each data block.
- This enhanced security mechanism makes Triple DES a viable choice for image encryption, providing a robust solution for protecting sensitive image data from unauthorized access and tampering.

PROBLEM STATEMENT AND MOTIVATION

01

02

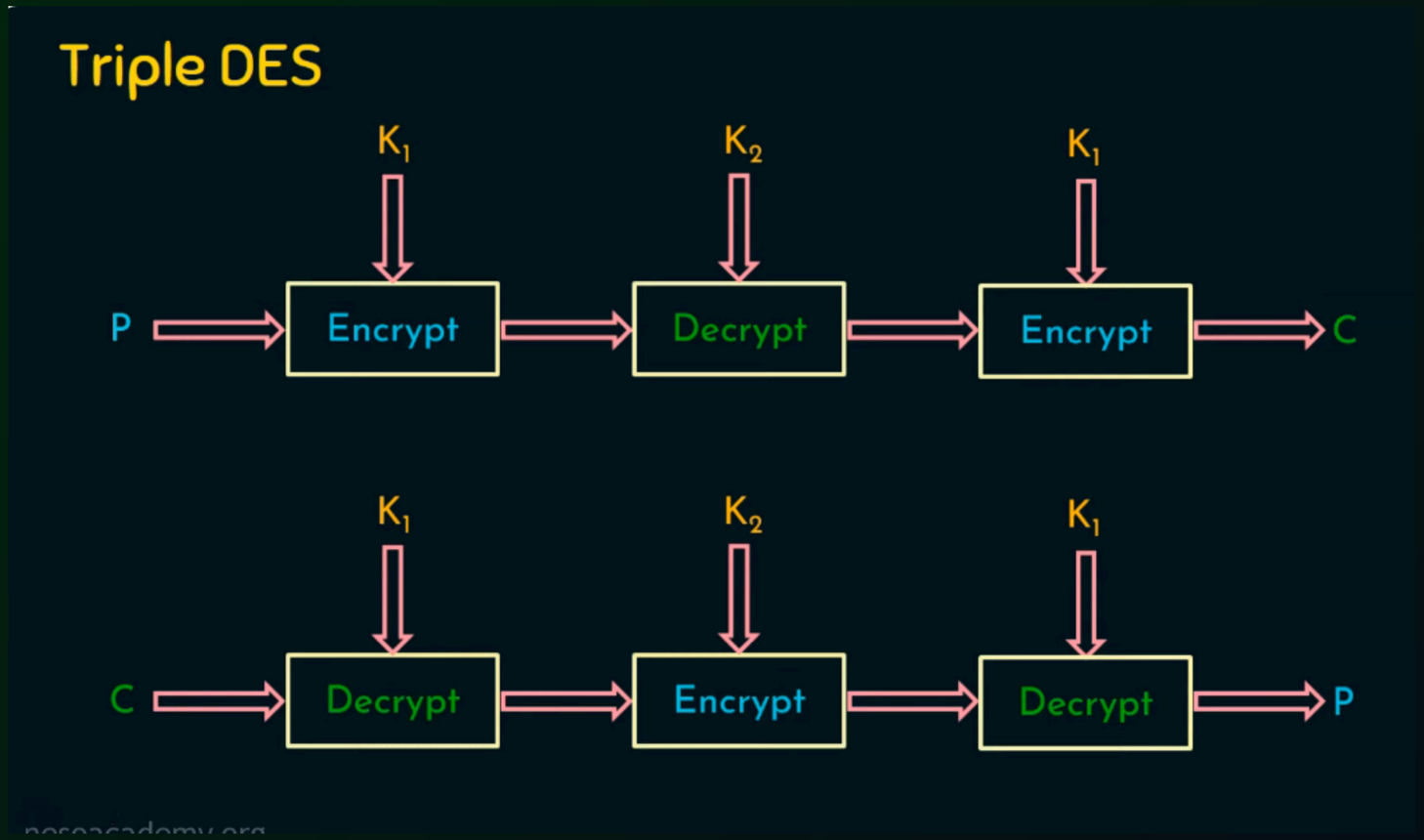
- Effectiveness of the Triple DES algorithm in encrypting image data, addressing the need for enhanced security while ensuring backward compatibility with the DES standard.

- The motivation for using Triple DES for image encryption includes its increased security through triple encryption, backward compatibility with DES, wide adoption in secure industries, and the need for a transitional step towards more advanced encryption algorithms like AES.

ALGORITHM-TRIPLE DES

- Triple DES (3DES) applies the Data Encryption Standard (DES) algorithm three times consecutively to each data block.
- It uses three different 56-bit keys (Key1, Key2, Key3), resulting in a 168-bit key length.
- The process involves encrypting the data with Key1, decrypting it with Key2, and then encrypting it again with Key3 (Encrypt-Decrypt-Encrypt).
- It mitigates vulnerabilities of DES, such as its susceptibility to brute-force attacks, by using multiple keys and a longer key length.
- Designed to be compatible with existing DES implementations, Triple DES allows systems to upgrade security without completely overhauling their encryption infrastructure.

TRIPLE DES


Triple DES
K1
K2
K1
P
Encrypt
Decrypt
Encrypt
C
K1
K2
K1
C
Decrypt
Encrypt
Decrypt
P

Methodology

- Key Generation: Generate three 56-bit keys (Key1, Key2, Key3).

01 02

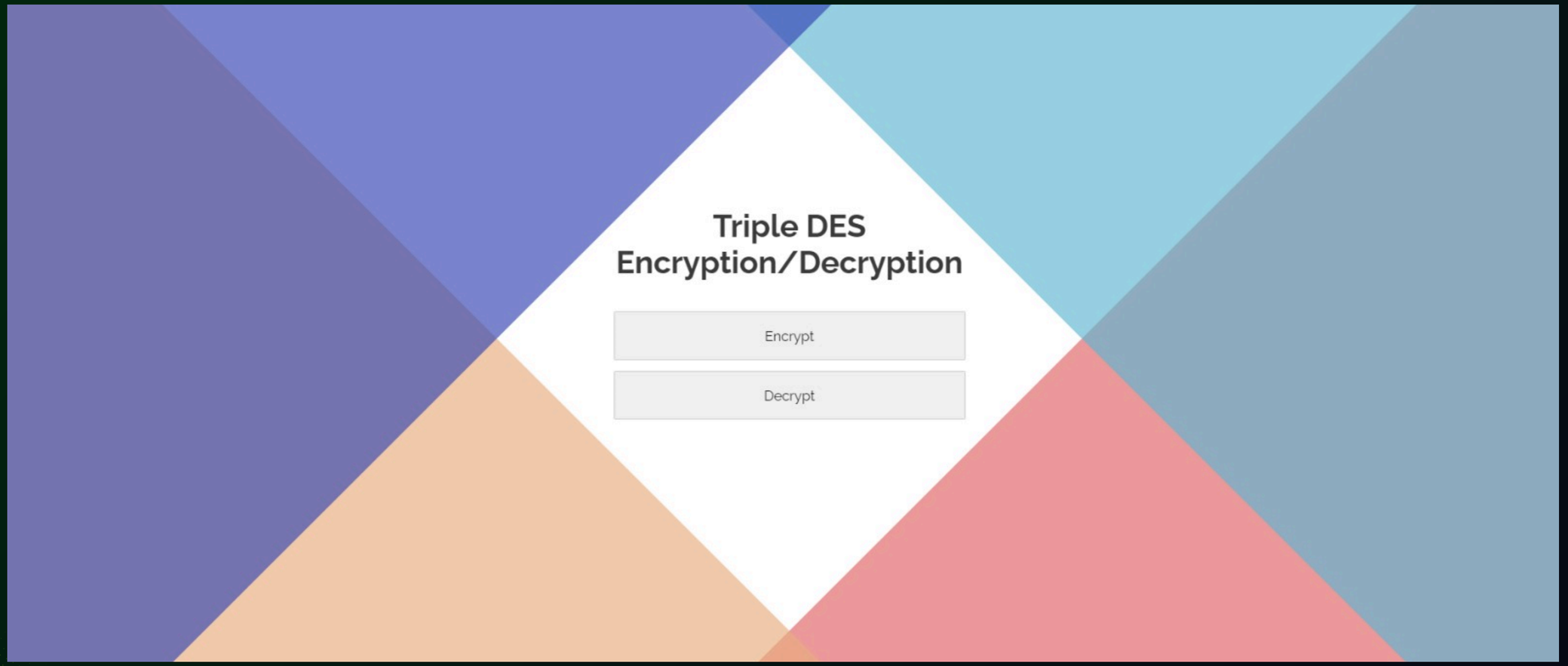
- Image Preprocessing: This involves reading the image file and representing its pixel data in a suitable format

- Triple DES Encryption Process:
  Encrypt the binary data of the image with the first key (Key1) using the DES algorithm.
  Decrypt the encrypted output from Stage 1 with the second key (Key2) using the DES
  Encrypt the output from Stage 2 with the third key (Key3) using the DES algorithm.

- Encryption Implementation: Apply the Triple DES encryption steps, and then save the encrypted data back into an image format.

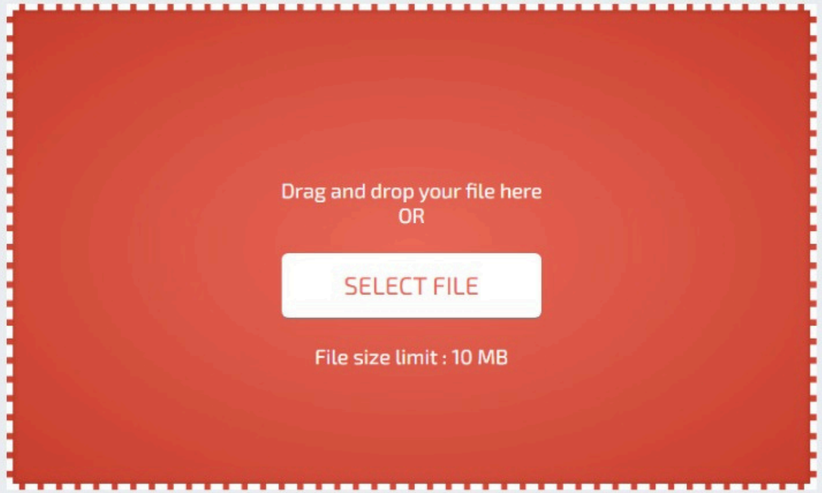
- Decryption Verification: Compare the decrypted image with the original to ensure that the encryption and decryption are accurately implemented a

RESULT



ENCPYPTION

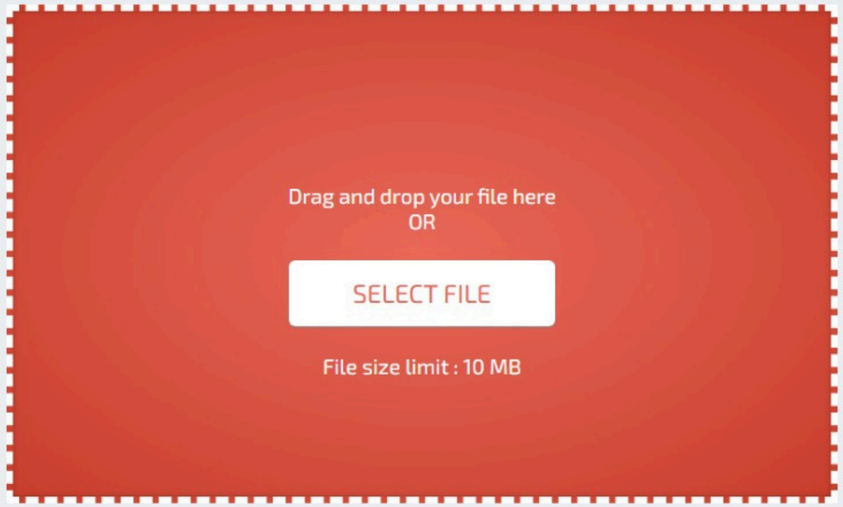
Encrypt your picture



ENCPYPTION KEY

DECRYPTION

Decrypt your picture



DECRYPTION KEY

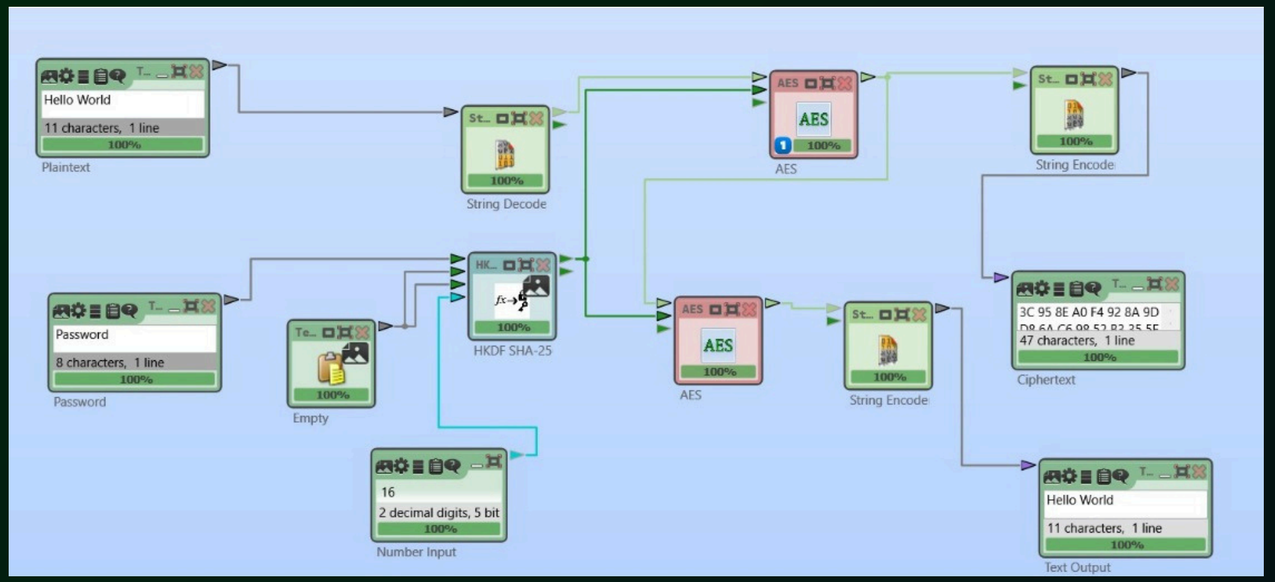
IMAGE DECRYPTED

CRYPTANALYSIS

- Meet-in-the-Middle Attack: This attack reduces the effective key strength of Triple DES from 168 bits (three 56-bit keys) to approximately 112 bits of security.
- Birthday Attack: The birthday attack exploits the probability of collisions in the encryption process due to the limited key length of DES.
- Differential Cryptanalysis: This method examines the differences in plaintexts and ciphertexts to infer information about the keys, potentially compromising the security of Triple DES under specific conditions.
- Sweet32 Attack: The Sweet32 attack exploits the birthday paradox to find collisions in the encryption process of Triple DES.

CRYPTOOL

AES(encryption and decryption)



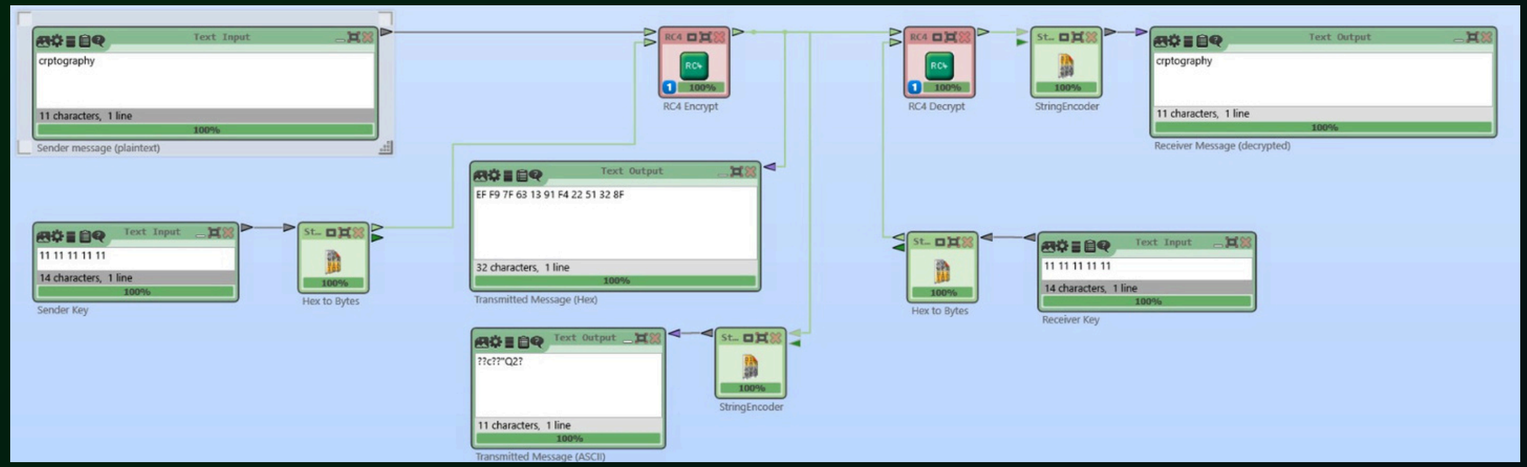
ALGORITHM:

- Symmetric encryption algorithm with variable key lengths (128, 192, or 256 bits).

- Operates on 128-bit blocks, using a series of substitution, permutation, and mixing operations (SubBytes, ShiftRows, MixColumns, AddRoundKey).

CRYPTOOL

RC4(encryption and decryption)

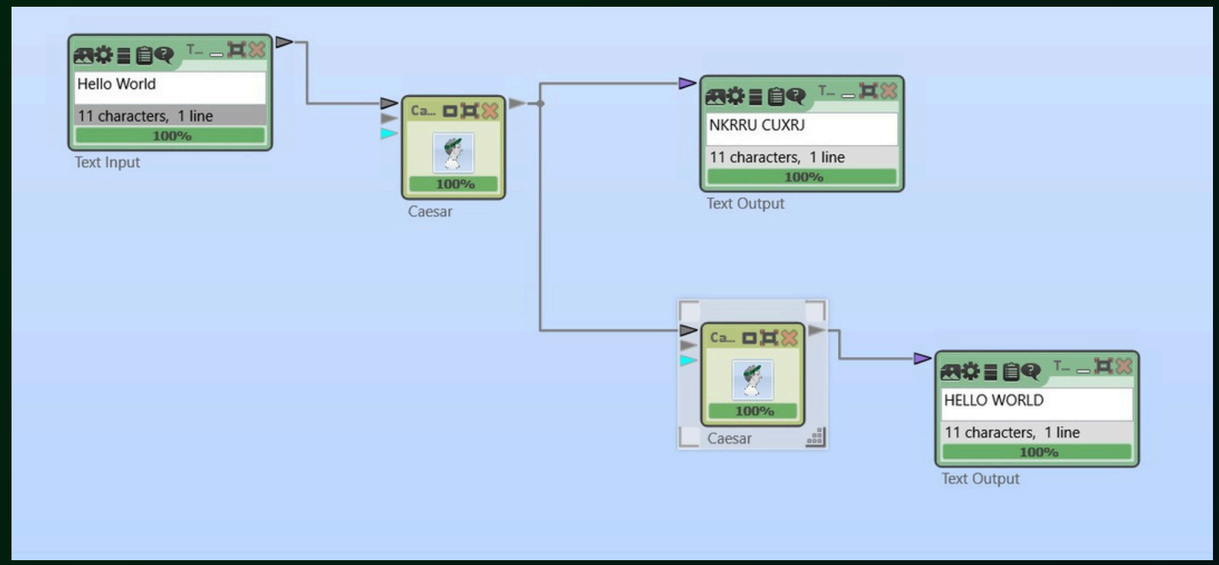


ALGORITHM:

- Stream cipher designed for efficient encryption of data streams.
- Operates with a variable length key (typically between 40 and 256 bits).
- Utilizes a pseudo-random key-scheduling algorithm to generate a keystream, which is XORed with plaintext to produce ciphertext.

CRYPTOOL

caesar(encryption and decryption)



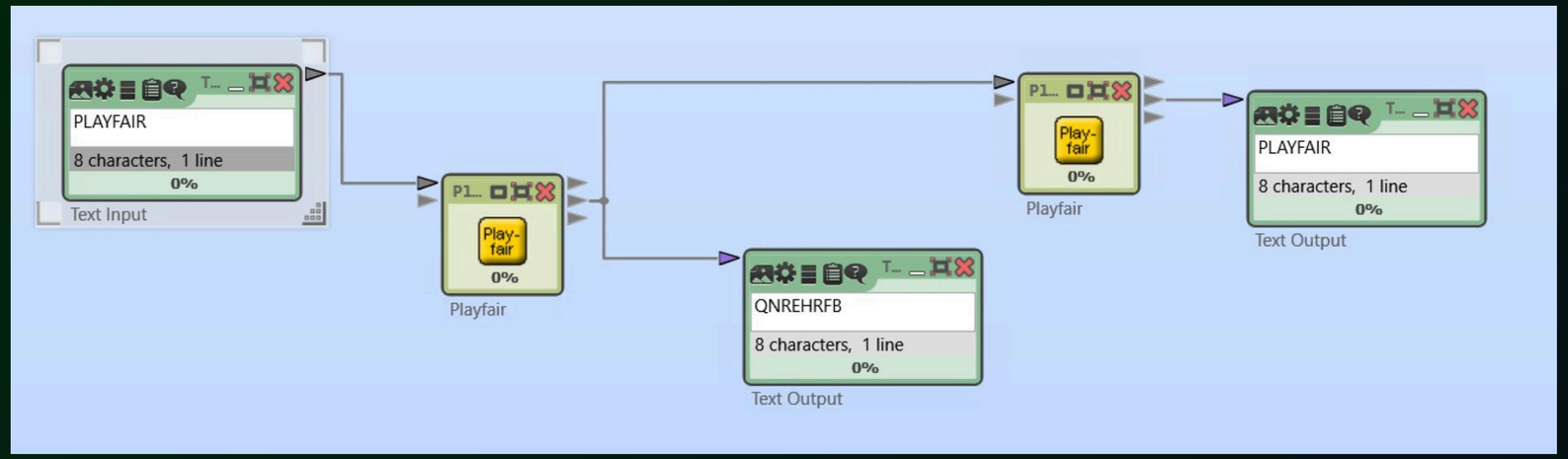
ALGORITHM:

- Simple substitution cipher where each letter in the plaintext is shifted a fixed number of places down or up the alphabet.

- Limited security due to its predictable nature and vulnerability to frequency analysis.

CRYPTOOL

PLAYFAIR(encryption and decryption)

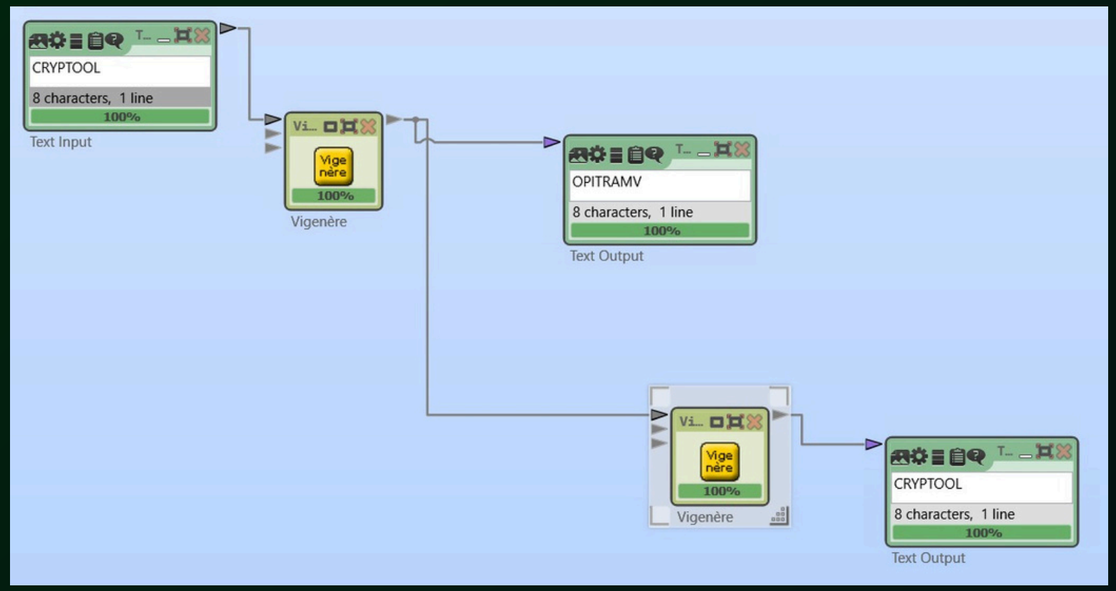


ALGORITHM:

- Polyalphabetic substitution cipher where plaintext letters are shifted using a keyword.
- Uses a keyword repeated to match the length of the plaintext, with each letter determining the shift amount (Caesar shift).
- Offers stronger security than simple substitution ciphers due to multiple alphabetic shifts.

CRYPTOOL

VIGENERE(encryption and decryption)



ALGORITHM:

- Polygraphic substitution cipher used for encrypting digraphs (pairs of letters) in plaintext.
- Uses a 5x5 matrix of letters derived from a keyword to generate the encryption table.
- Encrypts digraphs based on their positions in the matrix using specific rules for letter pairs.

CONCLUSION

- Implementing Triple DES for image encryption demonstrated effective protection against unauthorized access and tampering.
- While Triple DES provides enhanced security over DES, vulnerabilities highlighted the need for continuous evaluation and potential migration to more advanced encryption standards.
- Overcoming challenges such as key management and compatibility issues with legacy systems underscored the complexity of deploying robust encryption solutions.
- Future enhancements could focus on integrating more secure encryption algorithms like AES to address evolving security threats and improve overall data protection measures.

THANK YOU