
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

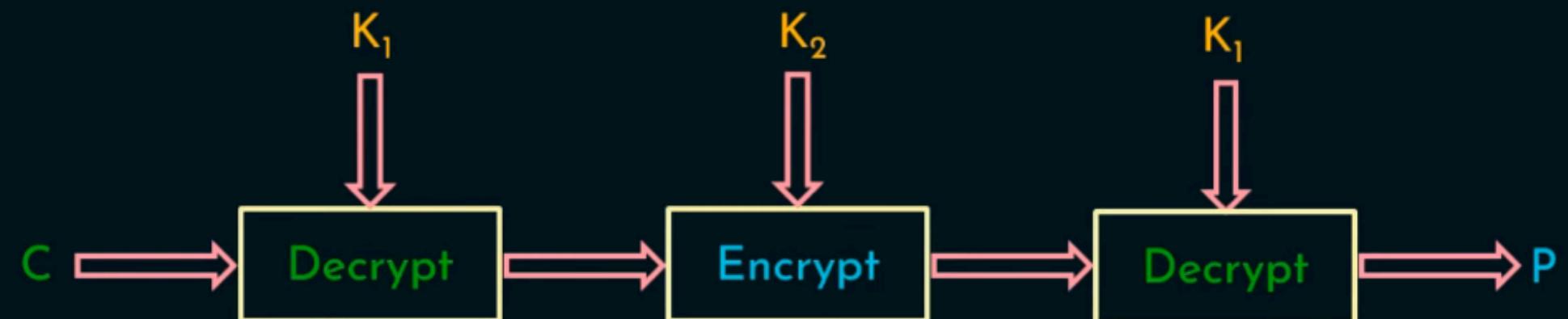
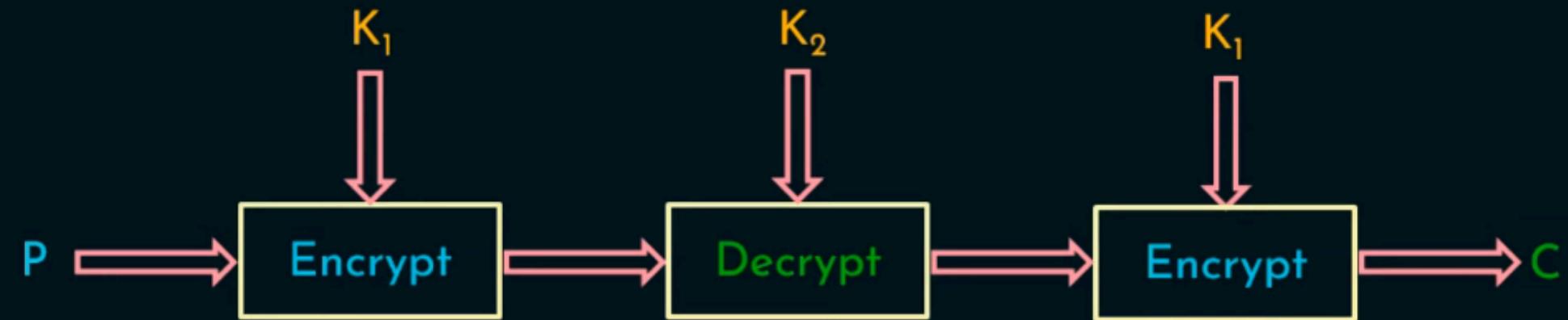
- Effectiveness of the Triple DES algorithm in encrypting image data, addressing the need for enhanced security while ensuring backward compatibility with the DES standard.
- The motivation for using Triple DES for image encryption includes its increased security through triple encryption, backward compatibility 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. 01 02
- 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



Methodology

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

01

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

02

- Triple DES Encryption Process:

Encrypt the binary data of the image with the first key (Key1) using the DES algorithm.

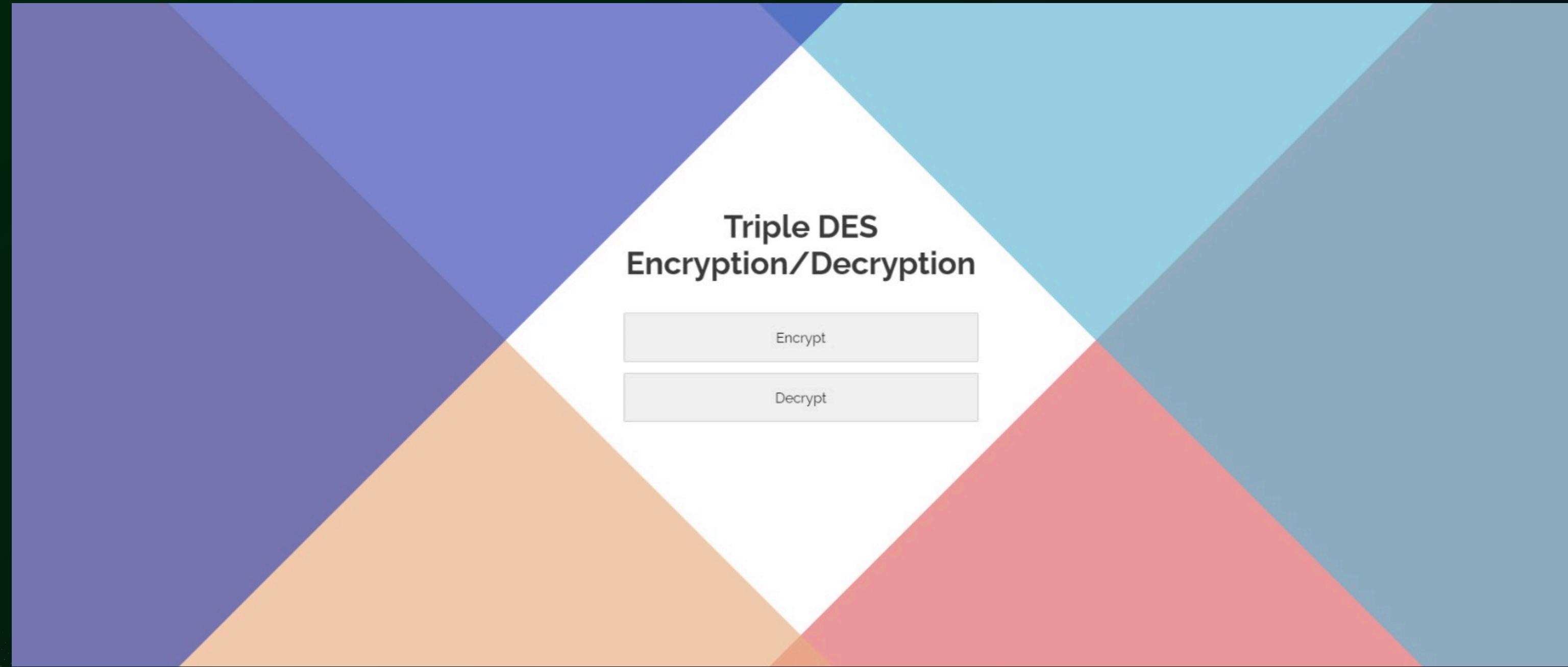
Decrypt the encrypted output from Stage 1 with the second key (Key2) using the DES

Encrypt the output from Stage 2 with the third key (Key3) using the DES algorithm.

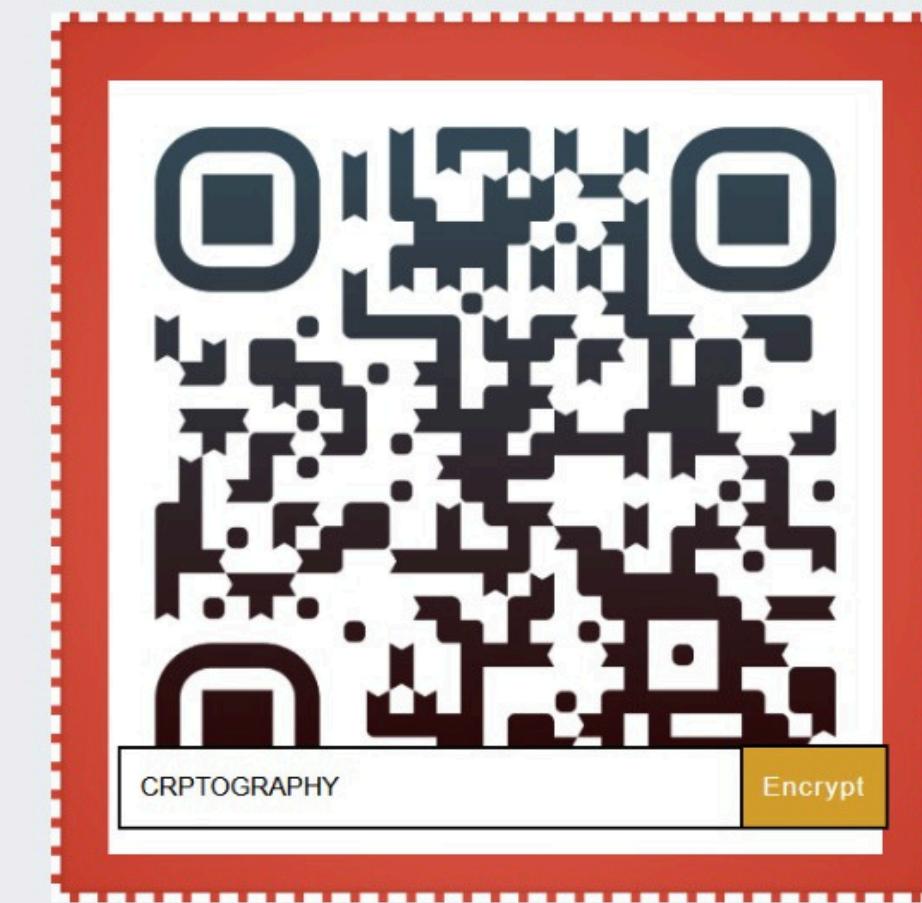
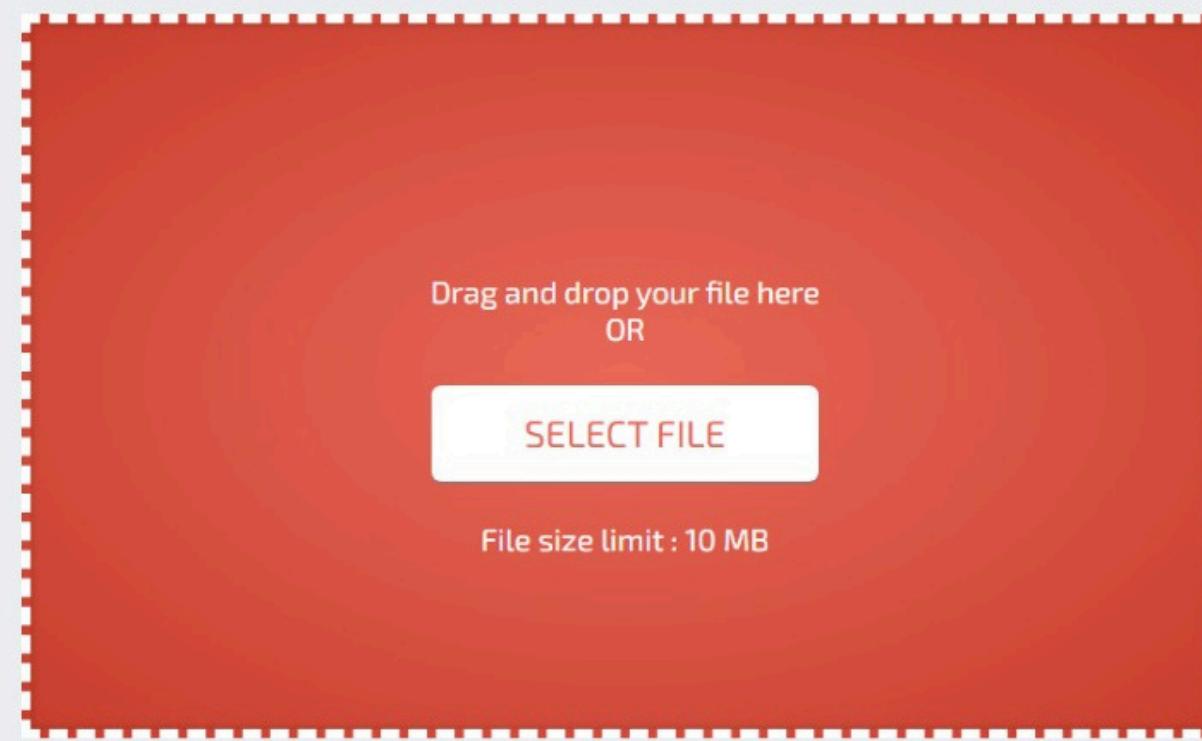
- Encryption Implementation: Apply the Triple DES encryption steps, and then save the encrypted data back into an image format.

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

RESULT



Encrypt your picture



ENCPYPTION KEY



picture

U2FsdGVkX1+
8/ybKO76C29IkqUt/pihFCHwqNe0HXRnEISyCGQYPhw/FZiZ02UhEB1yRN64f68X329MKR7tNG
X1Chx47AtxADAMoATYriVTElId+8v1
+T8EQF85fAzxuNpbVN/B/i3lw/IhknbeR9plFiyCsCZffSwZe5jDUARjgsfPCm3Oy8RcmxnvVE
ipZXjGW6
+XSPmITSb0N0F0M71WEtKHQoxCXsXEPWUOgmcB6Llh08GeXqggTpDWwwk63U/wJ7zmPqKNw8c9
2H6eOQ+wBya+EbFYRhoiJX75ce9lrPTOrjNIvwDz8hS+rTkHm020Nyck2ZRDSX6XY6RYqnZ
pq6H6N3thoFwG4NOIplMk0m4umMyDAxPCkpjQxtV5QzM6zKnCPvAqcE3Hds2JXS9ysAJNvZsf1
Sz0cHRejD0y0Anc2h2tanTNb8TvYRnY6NFA/1fMG4dQMCWUxmPZLm+j9gCkeQQJ+XCj+oilugc
CYvehhASd2HaSI+4Ri7API2GcYmN4K8VYP7
+xPC0r96Nkyw3oCZOZ46d24oR1NSEml/8EixoustsfpcabULgbUNKaC7tvR0U+bYqMcTr15w/P
X2/9KOLFVWSMacy28+zYr3A0t/t3vh6YZWQay7Q2NBSql8nwQWJw//9+5
+HKyOUKpGgMX3KVzeOHMDh3u6Ix+f+SbbARbnulxIS0L7Qk0wivPVhvTCLx9VQ/+
2nR6wImm5563rkkiP8gcKCIMfH4IMYqxpJXHp1z/pN2P4l2ZuCIS2DvyhdFjBsWQFEJ4p6nc1e
+KFiTswsSAqMTpQewWJDHV/Fnb8odHverHv64Gp/XcXx8ey4Tv5NRpcqloEXw30TQyBRs5YSEA
3twTtQaaGGQPXkHbnwIaaPp0fa7YVq1pBMxcw/44AcVNwxR8AFPzz+GRddVhbqA5qPA1e1rFH4
f0J6/YuJWv1Guh5DfhbiJ2MJk7ITyo4vA9UCDS9M5LvDiLGwTFgc+V1Qm9DKDPzsw5t6xhrT6o
ubDJ6e1ZbwDSe3UvPbwxi5X9VB80g5sKvNi8kX6rq29ZnClJryXV6nvKmMyi2yD+VwT0WmoSD
dex7yuDQb3WAMXKT7V91b52GHy7TGrnbJcGOeSvCT3Eu/OIlw4ac5tUrzb6dWwDr/dTuRoCgt
oolNcV77KOYVQysmts0BtEtfaFjqHpBx0ZKt5eocqyXvz0vikNM2BYrdupsK7iqQ7KaWam8wns
QW+
2ynoHCVDfcqUyP4/EGo6fz0BN2mYNG64mHUPpcseU50GtVbd435L4T7pPRuEFdu/ZswGnkMbJ2
KRV1nvvy8dyZcnNTAg3IscI0ZhpcxNKi9sdeMdbc/gYnWBvKxPUr/tVQxqWK27zt+D003wrQ19
YangG8IcETR1bQNN5yaBIPNaLaLkgey791z80dX91x5aPQvTJ2zNWXiP62NDmZ/DaFP+XbncSF
oFO0TAH1P0BmJsLB RGWhGfMs2/FccPo0Ha+UI3a6gGl873X2MYRS2Uhp xJL8aKUp58rLcMP1N
Y28TYag3SfaUk3ACPCgsWBiWpTQ8Z0sR6Xetp6pTI1/L5x10LV+eJdsqsX3y3ztZ8JR66X+

Ln 1, Col 1 | 100% | Windows (CRLF) | UTF-8

CRYPTOGRAPHY Encrypt

Decrypt your picture

Drag and drop your file here
OR

SELECT FILE

File size limit : 10 MB

```
U2FsdGVkX1+8/ybK076C29IkqUt/pihFCHwqNe0HXRnEISyCGQ
YPhw/FZiZ02UhEB1yRN64f68X329MKR7tNGX1Chx47AtxAADAMO
aTYriVTElId+8v1+T8EQF85fAzxuNpbVN/B/i3lW/Ihknber9p
1FiyCsCZffSwZe5jDUARjgsfPCm30y8RcmxnvVEipZXjGW6+XS
PmITSb0N0F0M71WEtKHQoxCXsXEPWU0gmcB6Llh08GeXqggTpD
Wwwk63U/wJ7zmPqKNw8c92H6e0Q+w8ya+EbFYRhoiJX75ce91r
PT0rjNIvvVdIz8hS+rTkHm020Nyck2ZRDsx6XY6RYqnZpq6H6
N3thoFwG4NOIp1Mk0m4umMyDAxPCkpjQxtV5QzM6zKnCPvAqcE
3Hds2JXS9ysAJNvZSF1Sz0cHRejD0y0Anc2h2tanTNb8TvYRnY
6NFA/1fMG4dQMCWUxmPZLm+j9gCkEQQj+XCj+oilugcCYvehhA
Sd2HaSI+4Ri7API2GcYmN4K8VYP7+xPC0r96Nkyw3oCZ0246d2
4oR1NSem1/8EiXoUSTsfpcabULgbUNKaC7tvR0U+bYqMcTr15w
/PX2/9KOLFVWSMacy28+zYr3A0t/t3vh6YZWQay7Q2NBSqL8nw
QWJw//9+5+HKyOUKpGgMX3KVzEOHMdh3u6Ix+f+S8bARbnuLxIS
0L7Qk0wivPVhvTCLx9VQ/-2nR6wImm5563rkkip8gcKCIMfh4I
MYqxpJXHp1z/pN2P412ZuCIS2DvyhdFjBsWQFEJ4p6nc1e+KFi
TswsSAqMTpQewJDHV/Fnb8odHverHv64Gp/XcXx8ey4Tv5NrP
cqloExw30TQyBRs5YSEA3twTtQaaGGQPXkHbnwIaaPp0fa7YVq
1pBMxcw/44AcVNwxR8AFPzZ+GRddVHbqA5qPA1e1rFH4f0J6/Y
```

CRYPTOGRAPHY **Decrypt**



decrypted_image (3).jpg
118 KB • Done

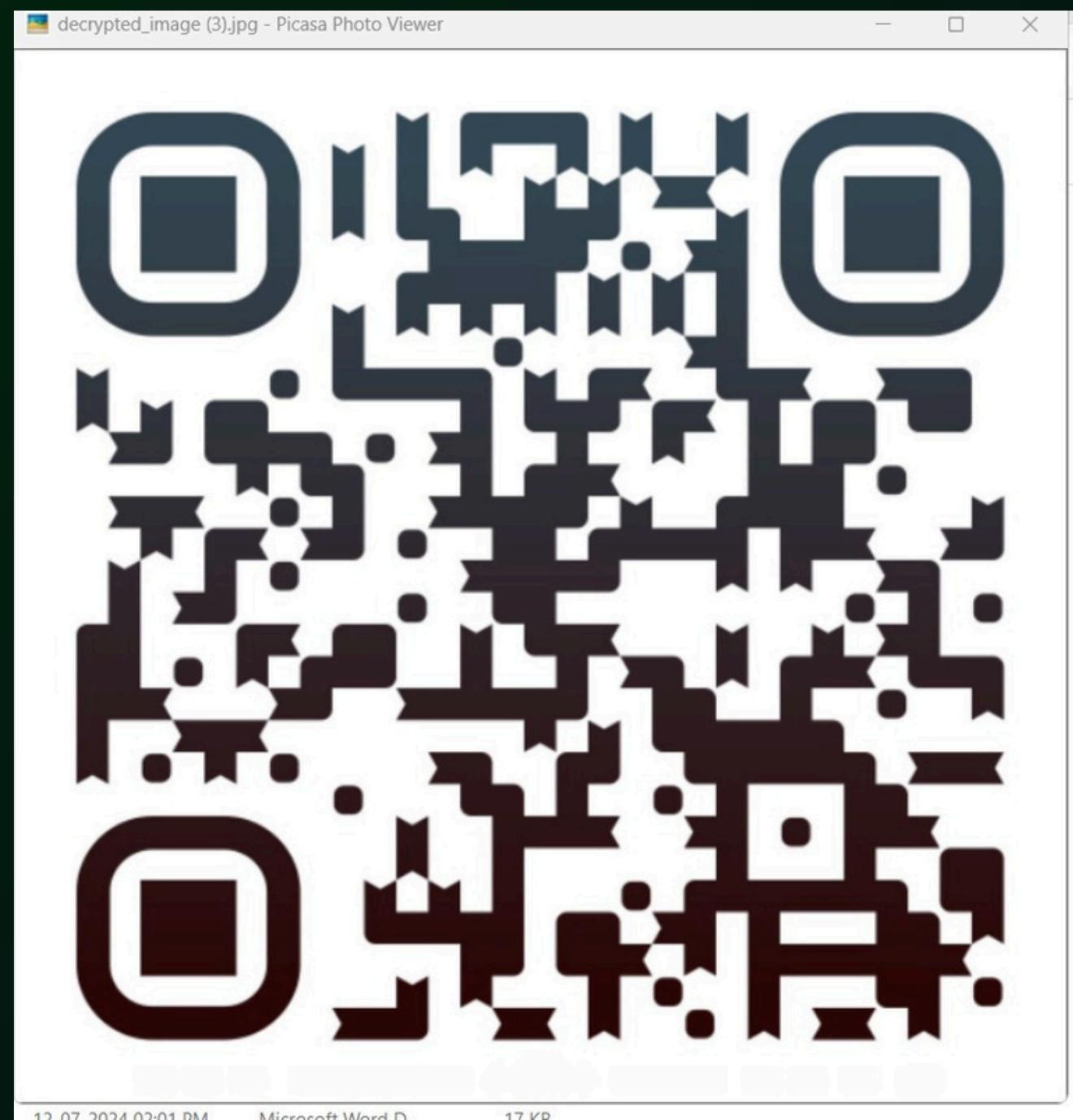
Encrypt your picture



```
U2FsdGVkX1+8/ybK076C29IkqUt/pihFCHwqNe0HXRnEISyCGQ
YPhw/FZiZ02UhEB1yRN64f68X329MKR7tNGX1Chx47AtxADAMO
aTYriVTElId+8v1+T8EQF85fAzxuNpbVN/B/i3lW/IhknbeR9p
1FiyCsCZffSwZe5jDUARjgsfPCm30y8RcmxnvVEipZXjGW6+XS
PmITSb0N0F0M71WEtKHQoxCXsXEPWUOgmcB6Llh08GeXqggTpD
Wwk63U/wJ7zmPqKNw8c92H6e0Q+wBya+EbFYRhoiJX75ce91r
PThOrjNIvwVdIz8hS+rTkHm020Nyck2ZRDSX6XY6RYqnZpq6H6
N3thoFwG4NOIp1Mk0m4umMyDAxPCkpjQxtV5QzM6zKnCPvAqcE
3Hds2JXS9ysAJNvZSf1Sz0cHRejD0y0Anc2h2tanTNb8TvYRnY
6NFA/1fMG4dQMCWUxmPZLm+j9gCkEQQJ+XCj+oilugcCYvehhA
Sd2HaSI+4Ri7API2GcYmN4K8VYP7+xPC0r96Nkyw3oCZ0Z46d2
4oR1NSem1/8EiXoUSTsfpcabUlgbUNKaC7tvR0U+bYqMcTr15w
/PX2/9KOLFVWSMacy28+zYr3A0t/t3vh6YZWQay7Q2NBSqL8nw
QWJw//9+5+HKyOUKpGgMX3KVzEOHMDh3u6Ix+f+SbbARbnuLxIS
0L7Qk0wivPVhvTCLx9VQ/+2nR6wImm5563rkkiP8gcKCIMfH4I
MYqxpxJXHp1z/pN2P4l2ZuCIS2DvyhdFjBsWQFEJ4p6nc1e+KFi
TsWsSAqMtpQewWJDHV/Fnb8odHverHv64Gp/XcXx8ey4Tv5NRp
cqloEXw30TQyBRs5YSEA3twTtQaaGGQPXkHbnwIaaPp0fa7YVq
1pBMxcw/44AcVNwxR8AFPzZ+GRddVHbqA5qPA1e1rFH4f0J6/Y
```

CRYPTOGRAPHY Decrypt

IMAGE DECRYPTED

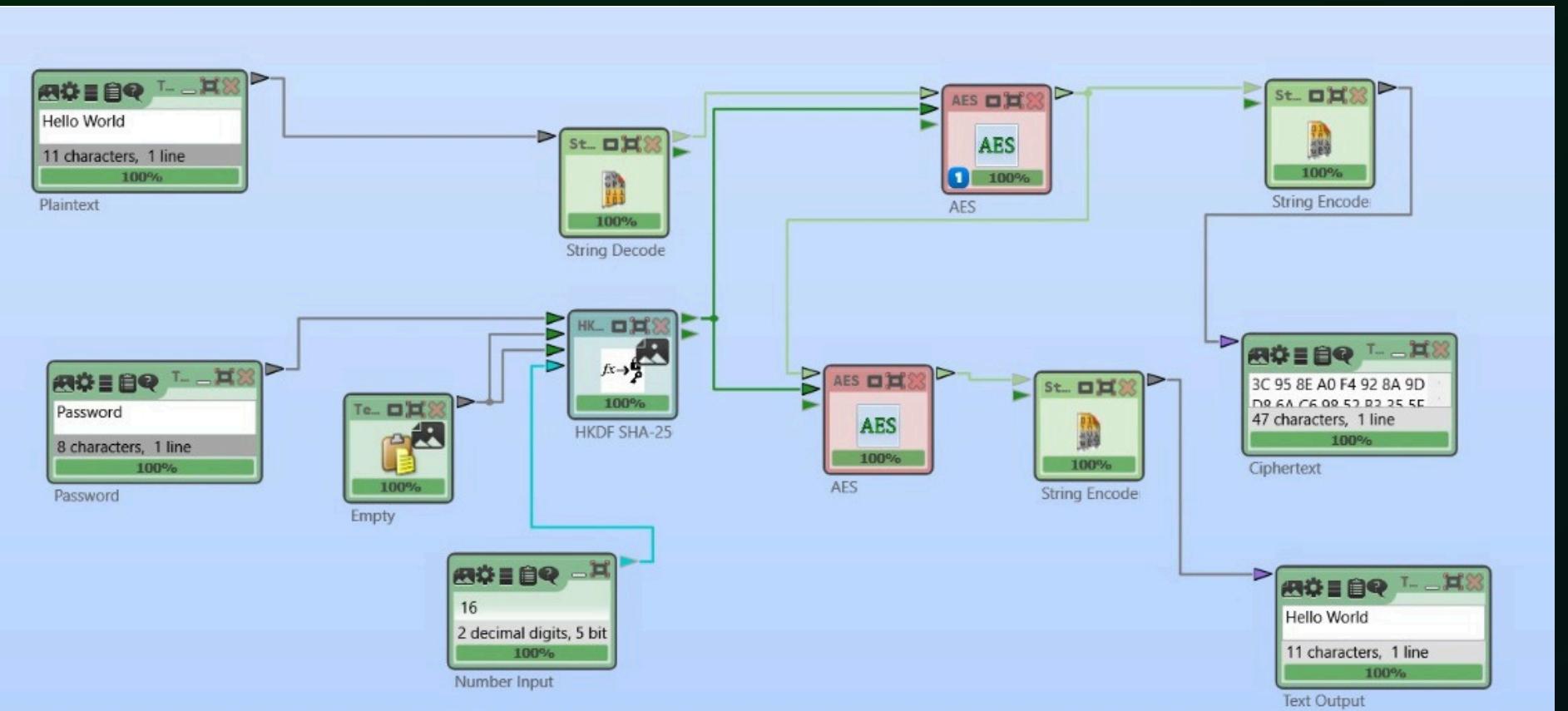


CRYPTANALYSIS

- Meet-in-the-Middle Attack: This ⁰¹attack reduces the effective ⁰²key 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

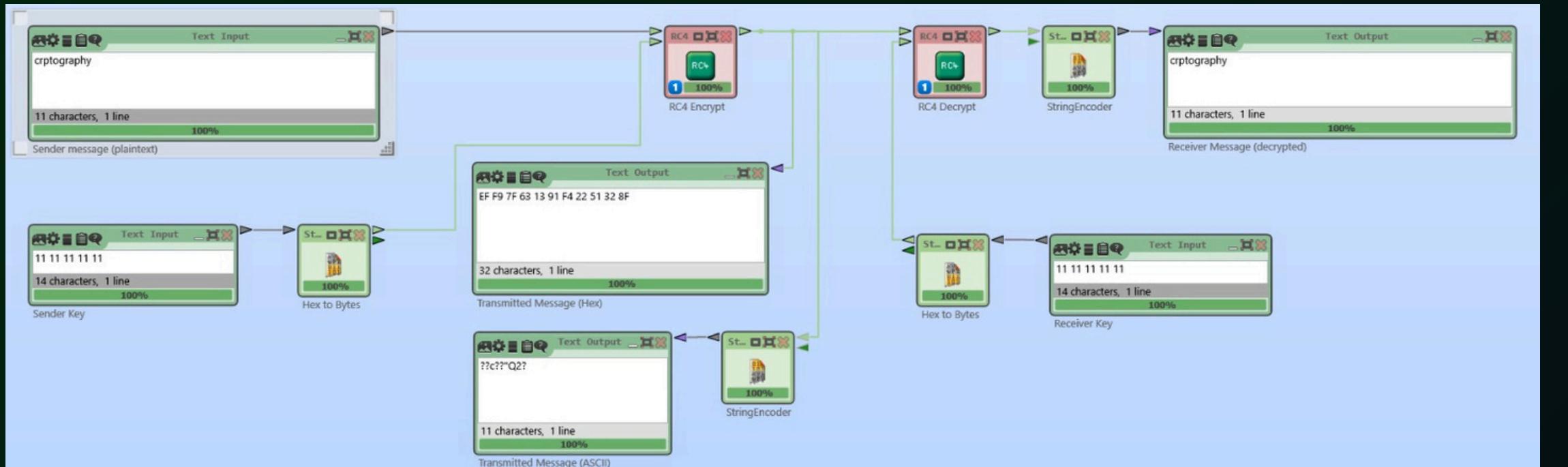
AES(encryption and decryption)



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).

RC4(encryption and decryption)

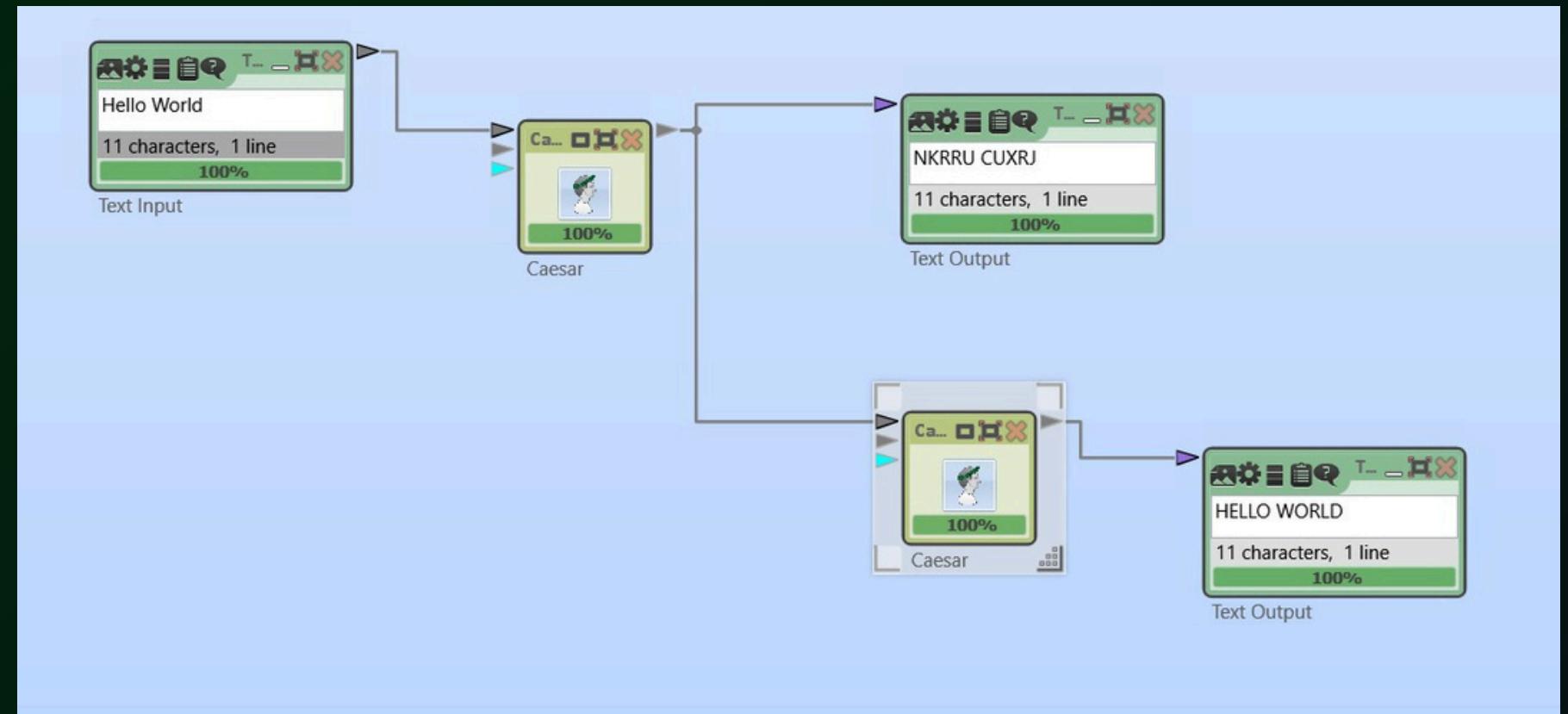


ALGORITHM:

- 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)

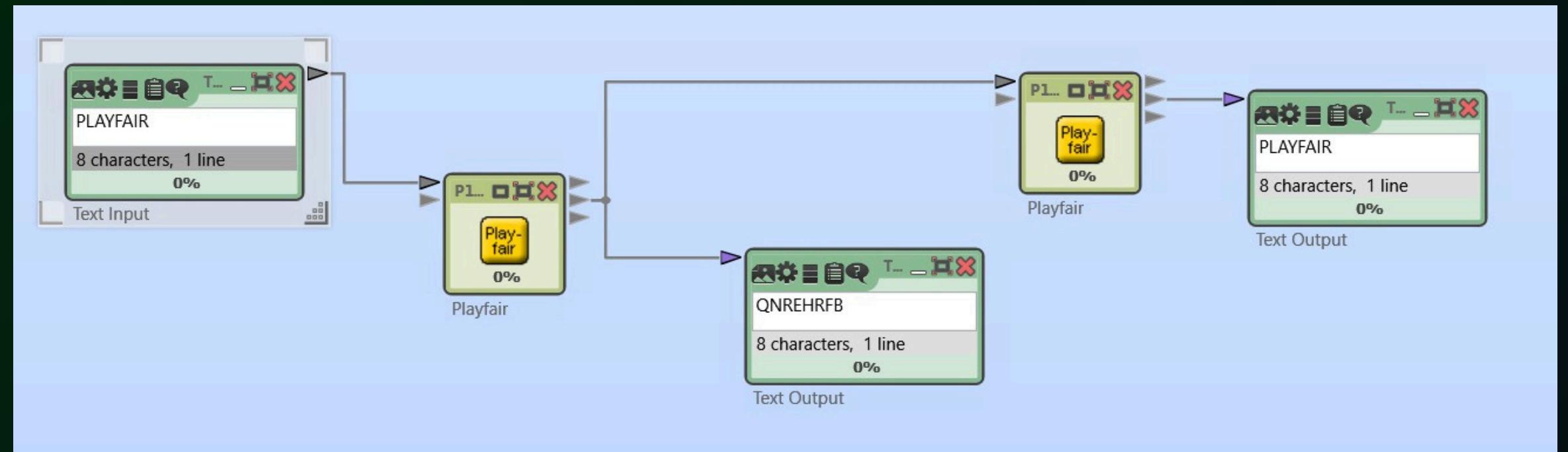


ALGORITHM:

- 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)



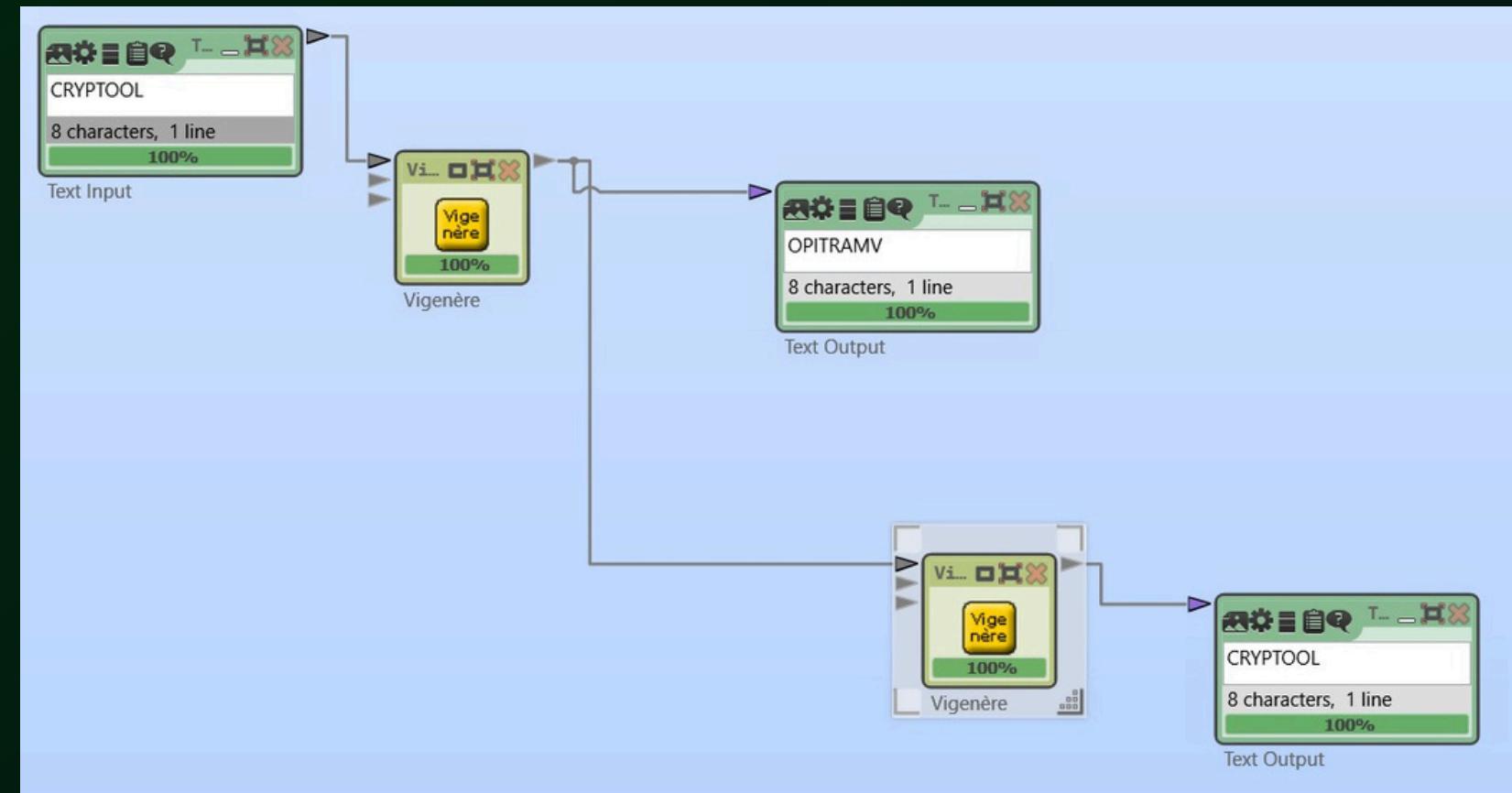
ALGORITHM:

03

- 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
