**VISVESVARAYA TECHNOLOGICAL UNIVERSITY**

**“JnanaSangama”, Belgaum -590014, Karnataka.**

****

**CRYPTOGRAPHY**

**AAT REPORT**

**on**

**IMAGE ENCRPTION AND DECRYPTION**

**USING TRIPE DES**

***Submitted by***

**C NEHA (1BM22CS074)**

**GANASHREE C M (1BM22CS097)**

**HEMA P (1BM22CS111)**

***Under the Guidance of***

|  |  |
| --- | --- |
| **Prof. Syed Akram**  **Assistant Professor, BMSCE** |  |

***in partial fulfillment for the award of the degree of***

**BACHELOR OF ENGINEERING**

***in***

**COMPUTER SCIENCE AND ENGINEERING**



**B.M.S. COLLEGE OF ENGINEERING**

**(Autonomous Institution under VTU)**

**BENGALURU-560019**

**April-2024 to August-2024**

**B. M. S. College of Engineering,**

**Bull Temple Road, Bangalore 560019**

(Affiliated To Visvesvaraya Technological University, Belgaum)

**Department of Computer Science and Engineering**



**CERTIFICATE**

This is to certify that the AAT work entitled “**IMAGE ENCRYPTION AND DECRYPTION USING TRIPLE DES**” is carried out by **C NEHA (1BM22CS074), GANASHREE C M (1BM22CS097) , HEMA P (1BM22CS111)** who are bonafide students of **B.M.S. College of Engineering.** It is in partial fulfillment for the award of **Bachelor of Engineering in Computer Science and Engineering** of the Visveswaraya Technological University, Belgaum during the year 2023-2024. The AAT report has been approved as it satisfies the academic requirements in respect of **Cryptography (23CS4ESCRP)** work prescribed for the said degree.

Signature of the Guide                 Signature of the HOD

Prof. Syed Akram Dr. Jyothi S Nayak

Assistant Professor Prof.& Head, Dept. of CSE

BMSCE, Bengaluru BMSCE, Bengaluru

**B.M.S. College of EngineerinG**

**DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING**

****

**DECLARATION**

We, C NEHA (1BM22CS074), GANASHREE C M (1BM22CS097), HEMA P (1BM22CS111) students of 4th Semester, B.E, Department of Computer Science and Engineering, B. M. S. College of Engineering, Bangalore, hereby declare that, this AAT entitled "IMAGE ENCRYPTION AND DECRYPTION USING TRIPLE DES" has been carried out by us under the guidance of Prof. Syed Akram, Assistant Professor, Department of CSE, B. M. S. College of Engineering, Bangalore during the academic semester April 2024-August 2024

We also declare that to the best of our knowledge and belief, the development reported here is not from part of any other report by any other students.

Signature

C NEHA (1BM22CS074)

GANASHREE C M (1BM22CS097)

HEMA P (1BM22CS111)

**TABLE OF CONTENTS**

1.ABSTRACT1

2.INTRODUCTION2

1.1.PROBLEM STATEMENT3

1.2.MOTIVATION3

3.ALGORITHM**4**

4.METHODOLOGY**4**

5RESULT**4**

6.CRYPTANANLYSIS**4**

7.CRYPTOOL**4**

8.CONCLUSION**4**

**ABSTRACT**

In the era of digital communication, the security of sensitive information, particularly in the form of images, is of paramount importance. This project focuses on the development of a robust web application designed to encrypt and decrypt images using the Triple Data Encryption Standard (Triple DES) algorithm. Triple DES is a symmetric key encryption method that applies the DES algorithm three times to each data block, significantly enhancing the security compared to the original DES algorithm. The application offers a seamless interface for users to securely upload and encrypt their images, ensuring that these images remain confidential during transmission and storage. Additionally, it allows for the decryption of these images, reverting them to their original state for authorized users. By leveraging the strength of Triple DES, this project aims to demonstrate a practical solution for safeguarding digital images against unauthorized access and cyber threats, thereby reinforcing the importance of cryptographic techniques in modern data security practices.

**INTRODUCTION**

**PROBLEM STATEMENT**:

The transmission and storage of images over the internet are common practices. However, these images often contain sensitive information that can be vulnerable to unauthorized access and cyber threats. Traditional encryption methods may not provide sufficient security to protect this data, leading to potential breaches of privacy and data theft. There is a pressing need for a more secure and efficient encryption technique to safeguard digital images.

This project addresses this challenge by developing a web application that uses the Triple DES algorithm to encrypt and decrypt images. Triple DES, an enhancement of the original Data Encryption Standard (DES), applies the DES cipher algorithm three times to each data block, significantly increasing its resistance to cryptographic attacks.

**MOTIVATION:**

The primary motivation for this project stems from the increasing need to secure sensitive information in an era where digital communication is ubiquitous. Images often contain personal, confidential, or proprietary information that, if compromised, can lead to significant privacy breaches, financial losses, and reputational damage.

The goal is to ensure that images remain confidential during transmission and storage, preventing unauthorized access and maintaining the privacy and integrity of the data. By providing a secure and user-friendly platform for image encryption and decryption, this project aims to enhance data security and protect sensitive information in the digital age.

**ALGORITHM**

Triple Data Encryption Standard (Triple DES or 3DES) is an encryption algorithm designed to provide a significantly enhanced level of security over its predecessor, the Data Encryption Standard (DES).

Triple DES increases the security of DES by applying the DES cipher algorithm three times to each data block. It uses either two or three unique keys for encryption, providing different levels of security:

1. **Triple DES with Two Keys (2TDEA)**:
   * Uses two keys: Key1 and Key2.
   * The data block is encrypted with Key1, decrypted with Key2, and then encrypted again with Key1.
2. **Triple DES with Three Keys (3TDEA)**:
   * Uses three unique keys: Key1, Key2, and Key3.
   * The data block is encrypted with Key1, decrypted with Key2, and encrypted again with Key3.

The process can be summarized in the following steps:

1. **Encryption**:
   * **Step 1**: Encrypt the plaintext using the first DES key (Key1).
   * **Step 2**: Decrypt the output of Step 1 using the second DES key (Key2).
   * **Step 3**: Encrypt the output of Step 2 using the third DES key (Key3) (in the case of 3TDEA) or the first key again (Key1) (in the case of 2TDEA).
2. **Decryption**:
   * **Step 1**: Decrypt the ciphertext using the third DES key (Key3) or the first key (Key1) in 2TDEA.
   * **Step 2**: Encrypt the output of Step 1 using the second DES key (Key2).
   * **Step 3**: Decrypt the output of Step 2 using the first DES key (Key1).

**METHODOLOGY**

The methodology of the project involves several key phases: requirement analysis, design, implementation, testing, and deployment. Each phase is crucial in ensuring the development of a secure and efficient web application for encrypting and decrypting images using the Triple DES algorithm.

**1. Requirement Analysis**

* **Objective Identification**: Define the primary goals of the project, such as providing secure image encryption and decryption through a user-friendly web interface.
* **Functional Requirements**: Identify the core functionalities required for the application, including image upload, encryption, decryption, and user authentication.
* **Non-Functional Requirements**: Determine the performance, security, and usability requirements, such as fast encryption/decryption processes, robust security measures, and an intuitive user interface.

**2. Design**

* **System Architecture**: Design the overall architecture of the web application, including the client-server model, database structure, and API endpoints.
* **User Interface Design**: Create wireframes and mockups for the user interface to ensure a seamless user experience.
* **Algorithm Integration**: Design the integration of the Triple DES algorithm for both encryption and decryption processes.

**3. Implementation**

* **Frontend Development**: Develop the client-side of the application using HTML, CSS, and JavaScript frameworks such as React or Angular to create an interactive and responsive user interface.
* **Backend Development**: Implement the server-side logic using a server-side language like Python, Node.js, or Java. Set up the web server, API endpoints, and database connections.
* **Triple DES Integration**: Implement the Triple DES encryption and decryption functions using a cryptographic library such as PyCrypto or CryptoJS. Ensure that the implementation adheres to best practices for security.
* **Image Handling**: Develop functionality for image upload, processing, and storage. Use libraries such as Pillow (Python) or Sharp (Node.js) for image manipulation.

**4. Testing**

* **Unit Testing**: Test individual components of the application, such as the encryption and decryption functions, to ensure they work correctly.
* **Integration Testing**: Test the interaction between different components of the application, including the frontend, backend, and database.
* **User Acceptance Testing (UAT)**: Conduct testing sessions with potential users to gather feedback on the usability and functionality of the application.
* **Security Testing**: Perform security assessments to identify and mitigate potential vulnerabilities, ensuring the application is resistant to common attacks such as SQL injection, XSS, and CSRF.

**5. Deployment**

* **Server Setup**: Configure the web server and deploy the application on a hosting platform such as AWS, Heroku, or a VPS.
* **Database Configuration**: Set up and configure the database for storing user data and encrypted images.
* **Domain and SSL**: Register a domain name and configure SSL certificates to ensure secure communication between users and the server.
* **Monitoring and Maintenance**: Implement monitoring tools to track the performance and security of the application. Plan for regular maintenance updates and security patches.

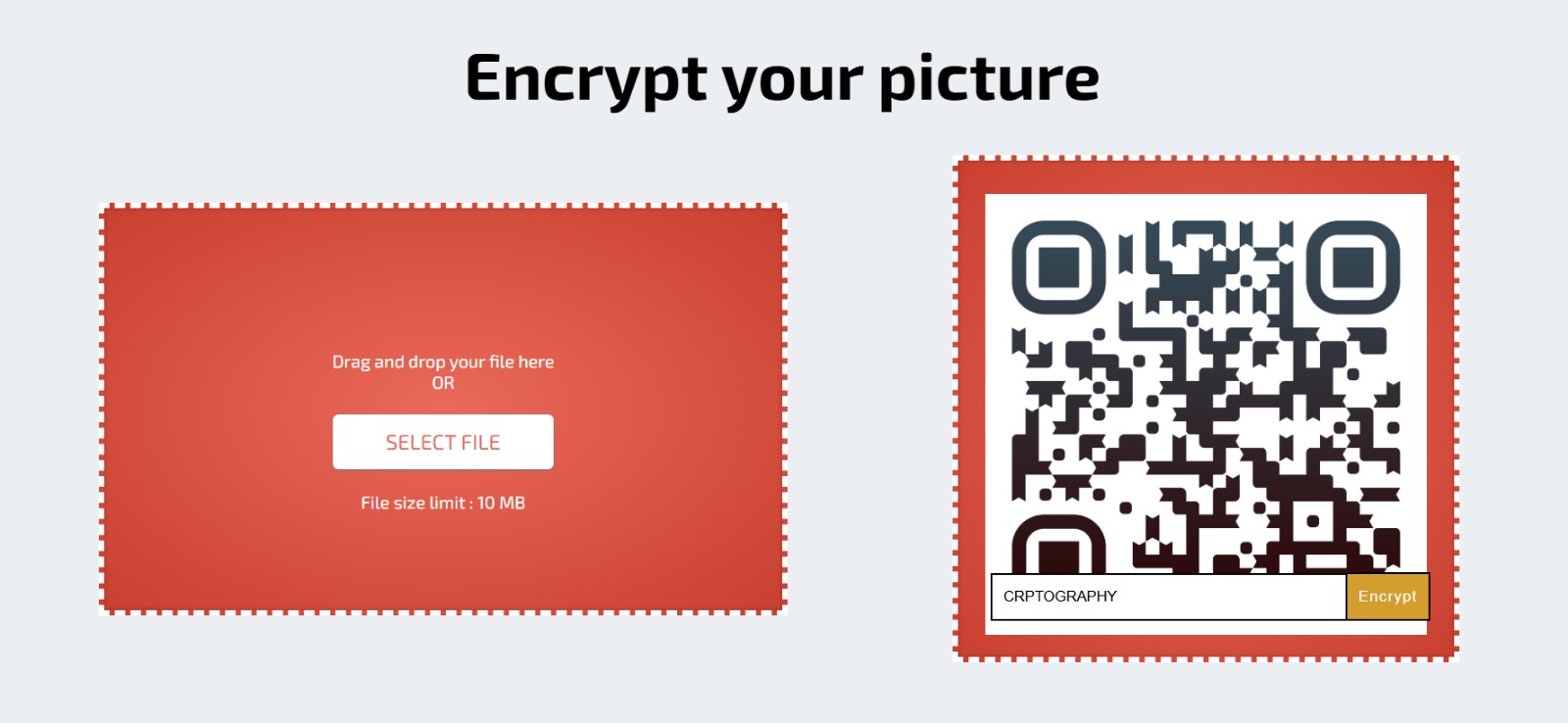
**6. Documentation**

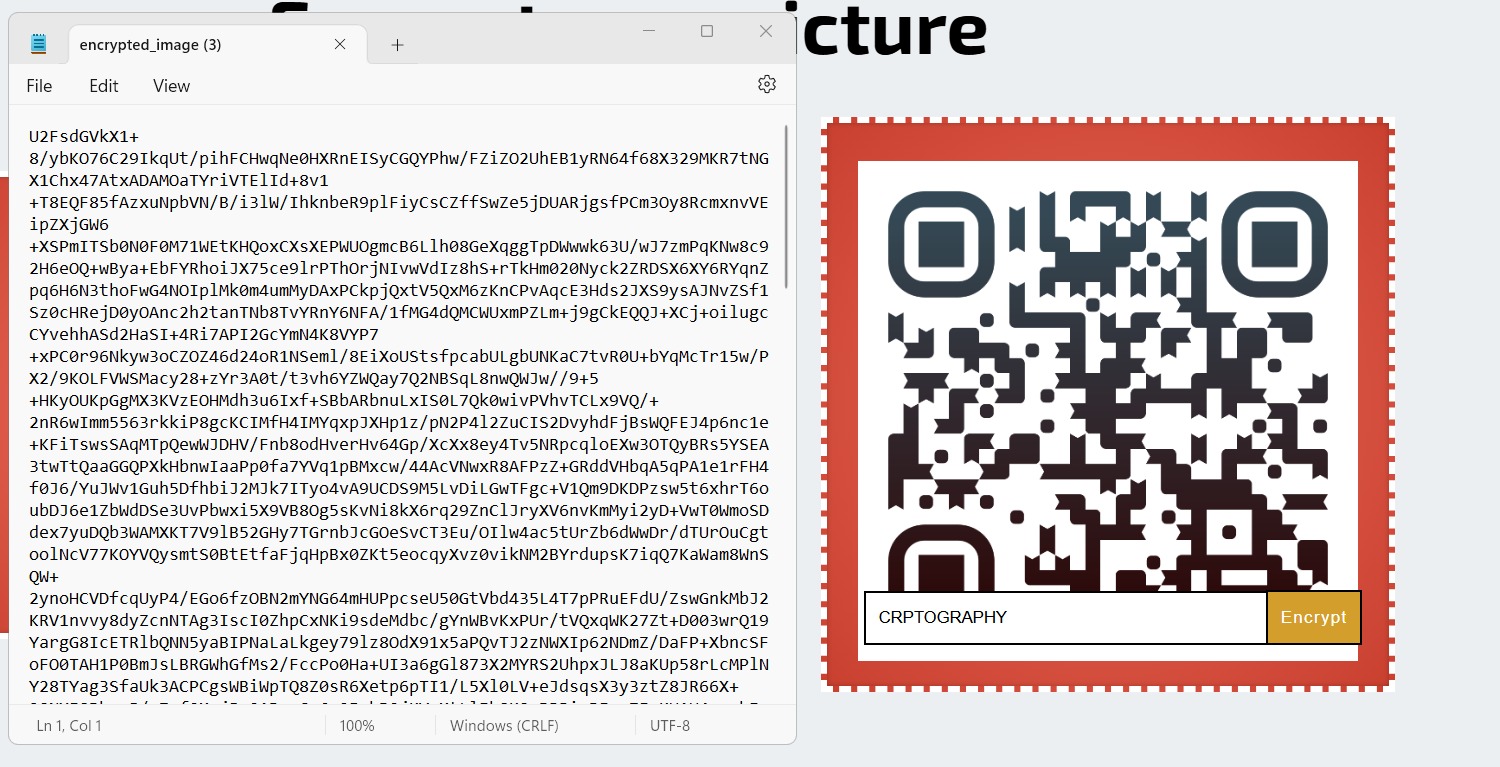
* **User Guide**: Create a user manual that explains how to use the application, including steps for uploading, encrypting, and decrypting images.
* **Technical Documentation**: Document the system architecture, API endpoints, database schema, and implementation details of the Triple DES algorithm for future reference and development.

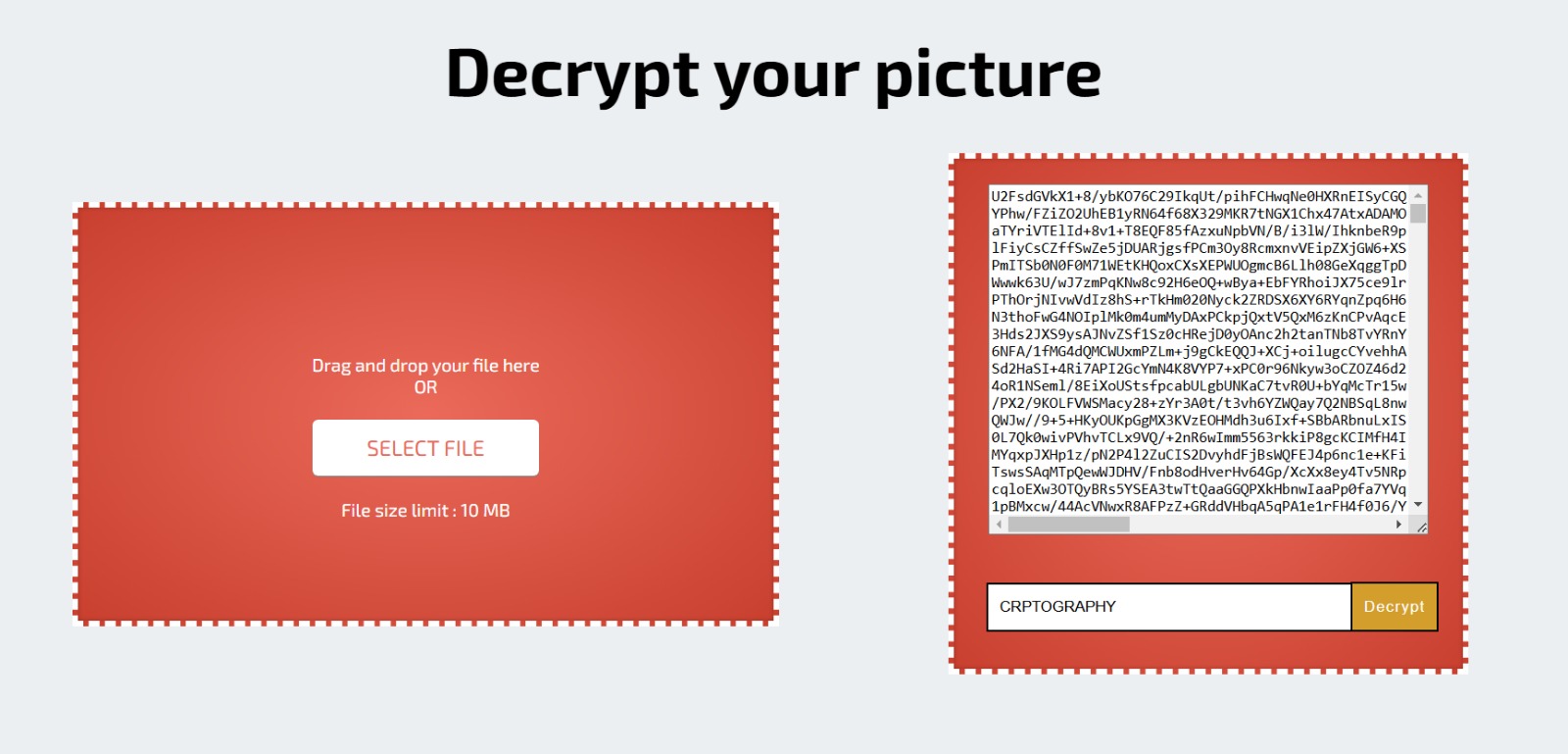
By following this methodology, the project ensures a structured approach to developing a secure and efficient web application for image encryption and decryption using the Triple DES algorithm.

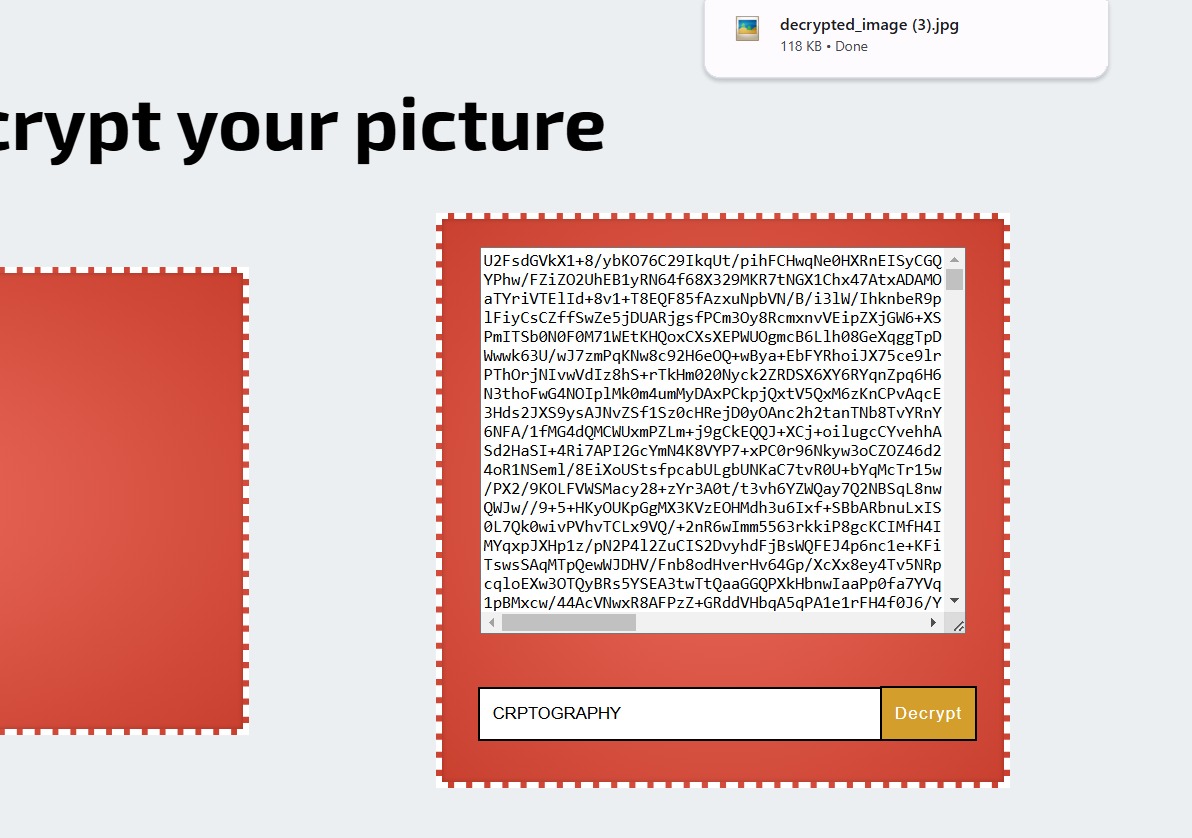
**RESULT**









****

****

**CRYPTANALYSIS**

Cryptanalysis is the study of analyzing information systems to understand the hidden aspects of the systems. When it comes to Triple DES (3DES), cryptanalysis involves evaluating the security and potential vulnerabilities of the algorithm. Here are some key aspects of Triple DES cryptanalysis:

1**. Brute Force Attack**

* Definition: A brute force attack involves trying all possible keys until the correct one is found.
* Triple DES Impact: Triple DES uses three 56-bit DES keys, effectively resulting in a key length of 168 bits. This makes a brute force attack extremely impractical with current computational capabilities. Even the simpler variant with two keys (112 bits effective) remains highly resistant to brute force attacks due to the enormous number of possible keys.

2. **Meet-in-the-Middle Attack**

* Definition: This attack attempts to reduce the complexity of breaking the encryption by simultaneously processing from both ends (plaintext and ciphertext) to find a common key.
* Triple DES Impact: Although 3DES is designed to thwart such attacks, the effective key length against a meet-in-the-middle attack is reduced to 112 bits instead of the full 168 bits. This still offers a robust level of security, but it demonstrates that the security of 3DES is not simply triple that of DES.

3. **Known-Plaintext and Chosen-Plaintext Attacks**

* Definition: In a known-plaintext attack, the attacker has access to both the plaintext and its corresponding ciphertext. In a chosen-plaintext attack, the attacker can encrypt plaintexts of their choosing and observe the ciphertexts.
* Triple DES Impact: Triple DES provides strong resistance to these attacks due to its multiple encryption and decryption processes, which obscure the relationship between the plaintext and ciphertext.

4. **Differential Cryptanalysis**

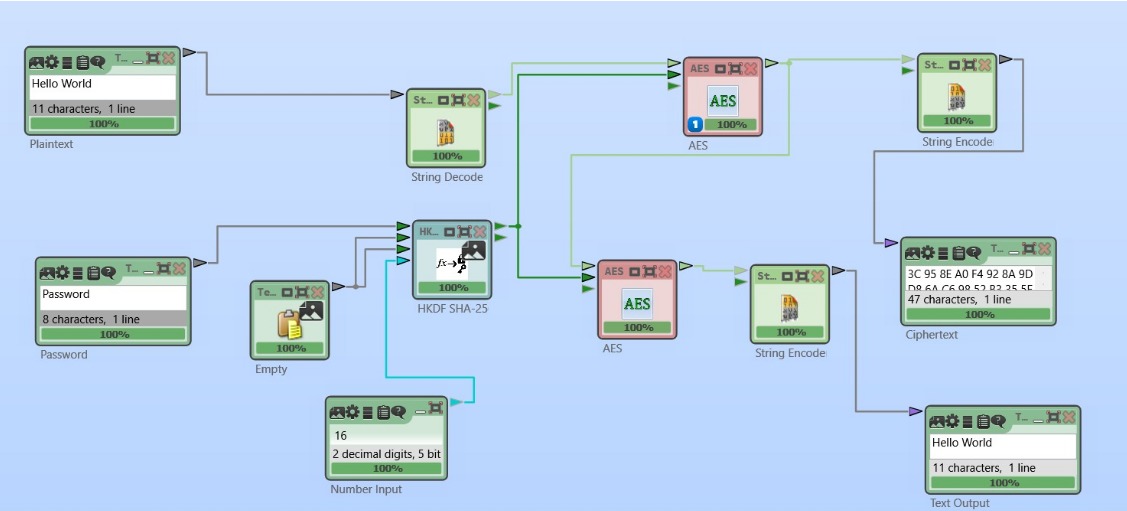
* Definition: This method involves analyzing the differences in ciphertexts resulting from specific differences in plaintexts to deduce information about the key.
* Triple DES Impact: DES was designed with some resistance to differential cryptanalysis, and Triple DES, by applying the DES process three times, inherits and enhances this resistance. The complexity and computational effort required to conduct a successful differential cryptanalysis attack on 3DES are impractical with current technology.

5. **Linear Cryptanalysis**

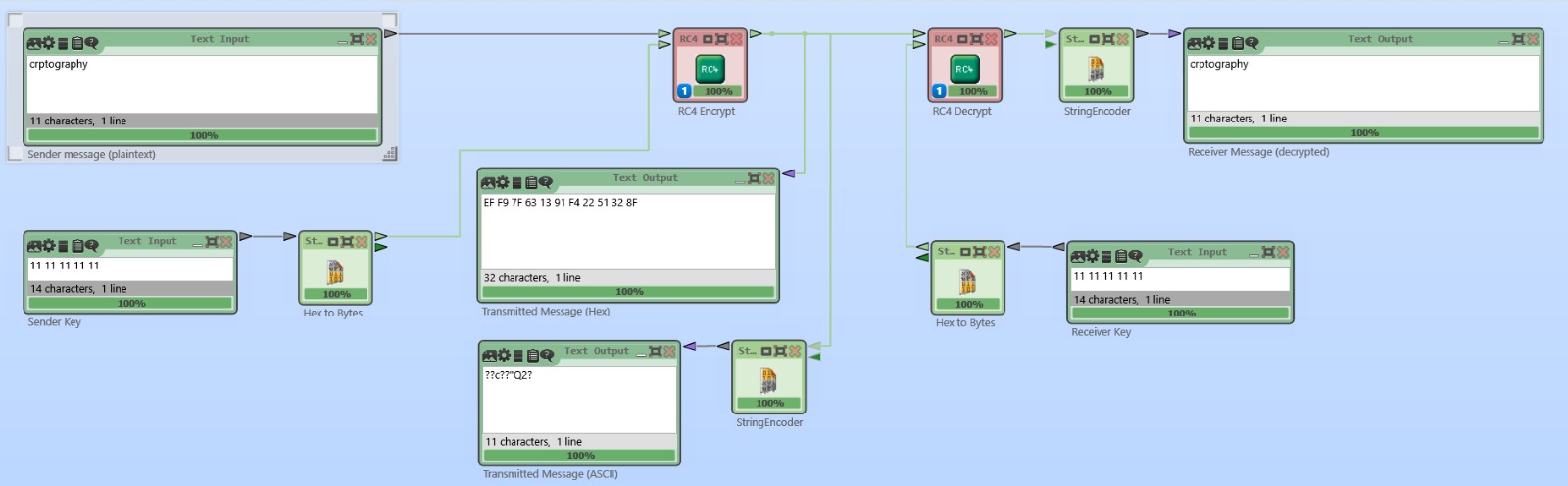
* Definition: Linear cryptanalysis uses linear approximations to describe the behavior of the block cipher and its components, gradually exposing information about the encryption key.
* Triple DES Impact: Similar to differential cryptanalysis, Triple DES's structure makes linear cryptanalysis highly impractical. The repeated encryption and decryption operations obscure linear relationships, significantly complicating such an attack.

**CRYPTOOL**

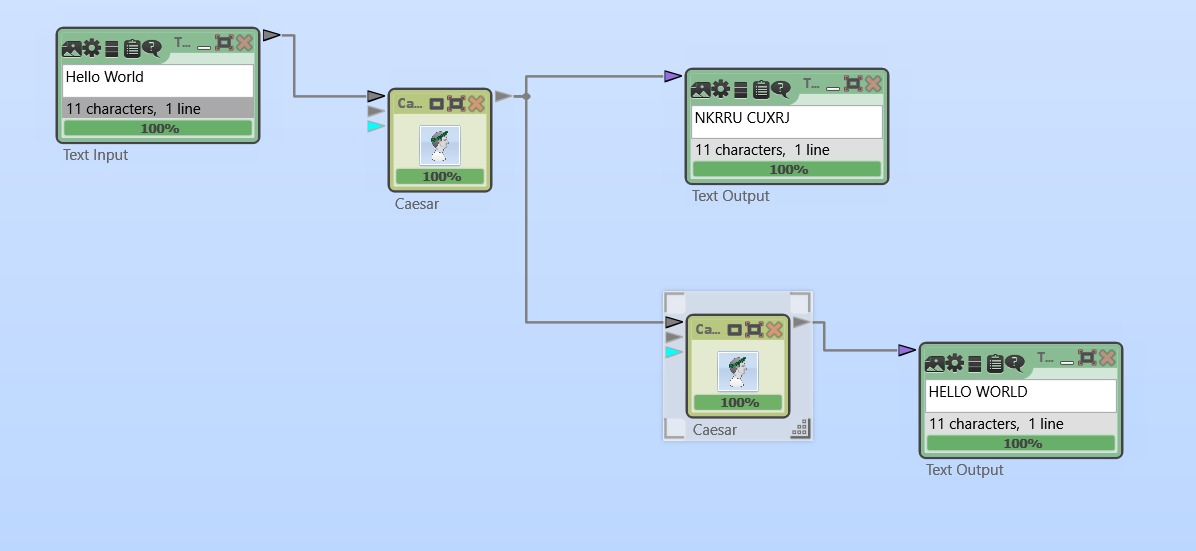
**AES(encryption and decryption)**

****

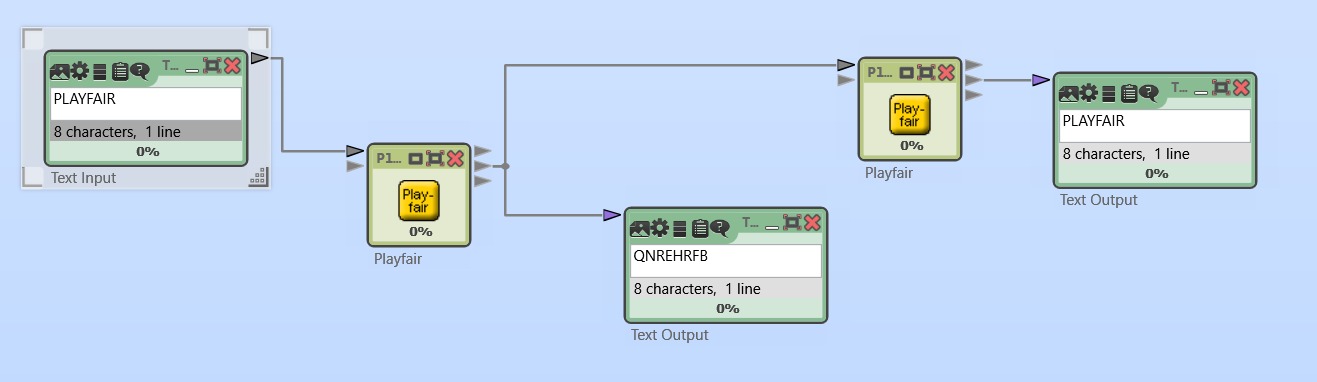
**RC4(encryption and decryption)**

****

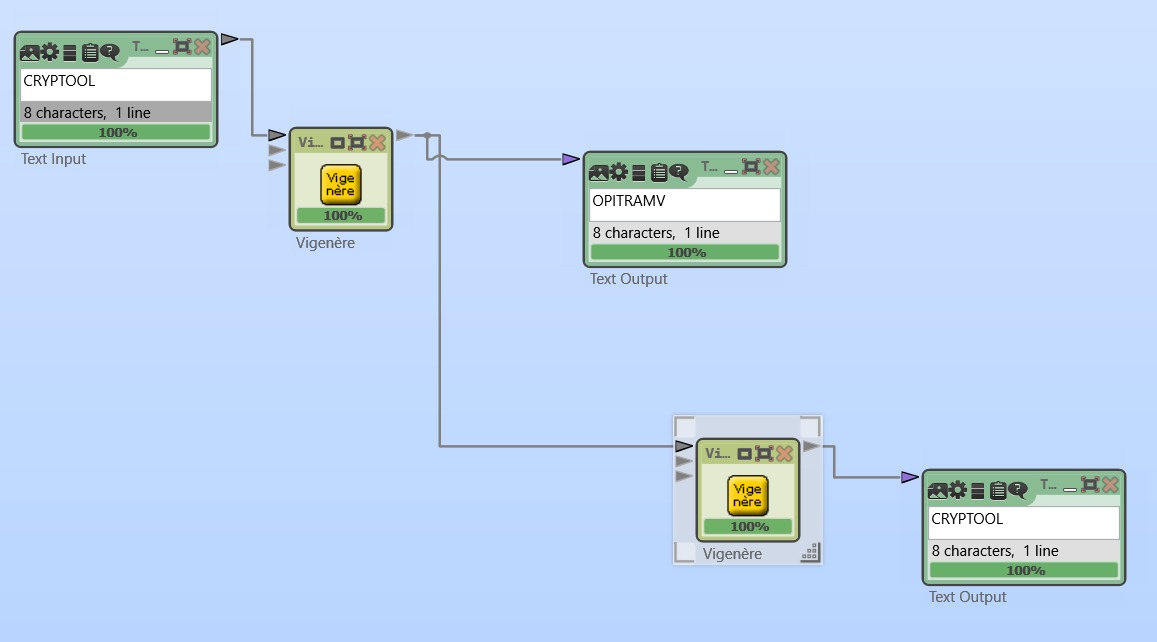
**CAESAR(encryption and decryption)**

****

**PLAYFAIR(encryption and decryption)**

****

**VIGENERE(encryption and decryption)**

****

**CONCLUSION**

The development of a web application for encrypting and decrypting images using the Triple Data Encryption Standard (Triple DES) algorithm addresses the critical need for enhanced data security in today's digital world. By leveraging the robust encryption capabilities of Triple DES, this project ensures the confidentiality and integrity of image data during transmission and storage, protecting it from unauthorized access and cyber threats.

Through a structured methodology encompassing requirement analysis, design, implementation, testing, and deployment, the project delivers a secure and user-friendly platform. The integration of Triple DES, despite its known vulnerabilities and performance drawbacks, provides a significantly higher level of security compared to the original DES algorithm. This project also highlights the importance of cryptographic techniques in safeguarding sensitive information and demonstrates a practical application of these principles in modern web development.

While Triple DES remains a reliable encryption method, it is essential to acknowledge its limitations and the ongoing evolution of cryptographic standards. As computational power continues to advance, more robust algorithms like AES are becoming the preferred choice for new systems. Nonetheless, this project exemplifies the practical implementation of Triple DES in enhancing data security, contributing to the broader goal of protecting sensitive information in an increasingly interconnected world.