Green University of Bangladesh

Department of Computer Science and Engineering (CSE)
Semester: (Fall, Year: 2023), B.Sc. in CSE (Day)

Multiple Encryption and Decryption of Cipher Techniques

Course Title: Computer and Cyber Security
Course Code: CSE 323
Section: 203 D2

Student Details

Name	ID
Mahabubur Rahman	203902008
Abdullah Al Noman	203902002
Omar Faruk Zidan	203902012

Submission Date : 01-09-2023
Course Teacher's Name : Md. Riad Hassan

[For Teachers use only: Don't Write Anything inside this box]

Project Report Status

Marks: ………………………………. **Signature: …………………**

Comments: ……………………………………… **Date: ………………………..**

Chapter 1

Introduction

1.1 Project Title

Multiple Encryption and Decryption of Cipher Techniques

1.2 Introduction:

Our platform, the "Multiple Encryption and Decryption of Cipher Techniques," provides a comprehensive service for encrypting and decrypting text. Users can effortlessly convert plain text to cipher text and vice versa using various encryption methods like left shift, right shift, and middle swap. Additionally, the platform incorporates advanced algorithms such as additive, multiplicative, affine, one-time pad, and Vigenere ciphers, allowing users to choose the most suitable method for their security needs. For heightened complexity and security, our site introduces a product cipher, combining mixed additive and swap techniques, ensuring a robust and intricate approach to encryption, making it more challenging for unauthorized parties to decipher sensitive information. Whether safeguarding confidential messages or decoding encrypted text, our Secure Text Transformation Hub provides a user-friendly and secure solution for all text encryption and decryption requirements.

1.3 Design Goals/Objective:

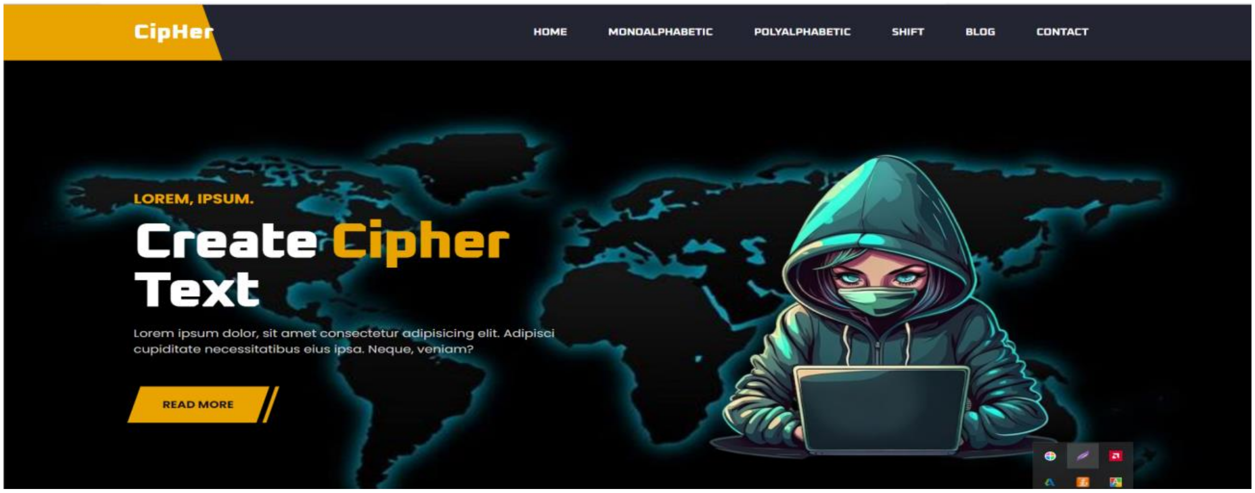
1. **Full-Spectrum Text Encryption/Decryption:** Our website is dedicated to providing a complete set of text encryption and decryption services. Users can effortlessly convert ordinary text into cipher text and back, utilizing a variety of cryptographic algorithms tailored to meet their individual requirements.
2. **Variety of Algorithms:**To fortify the security of encrypted messages, our platform integrates a broad selection of encryption algorithms. This encompasses additive, multiplicative, affine, one-time pad, and Vigenère ciphers, giving users a diverse range of choices to protect their information.
3. **Shifting Operations:**Our service accommodates left shift, right shift, and middle swap operations, empowering users to personalize their encryption techniques. This adaptability guarantees that users can adjust the encryption process according to the desired level of security for their text.

4. **Product Cipher (Combined Additive and Swap):** Introducing a hybrid cipher that merges additive and swap operations elevates the intricacy of the encryption procedure. This inventive method augments the overall security of the encrypted text, bolstering its resilience against unauthorized access.
5. **5.Intuitive User Interface:** Our platform boasts an intuitive interface, ensuring straightforward navigation and usage of encryption and decryption services for individuals with diverse technical proficiencies. This user-friendly design enhances accessibility and promotes widespread usage.
6. **Emphasis on Privacy and Secrecy:** Privacy is a central focus of our design objectives. The platform prioritizes the confidentiality of user data, guaranteeing that both plain text and cipher text processed through the site stay protected and beyond the reach of unauthorized entities.
7. **Adaptability and Efficiency:** In response to the dynamic digital environment, our platform is constructed with adaptability as a key feature. It effortlessly adjusts to evolving encryption standards and technologies, assuring users of its continued reliability for secure text communication in the years to come.

Chapter 2

Design/Development/Implementation of the Project

2.1 Website Hero Section

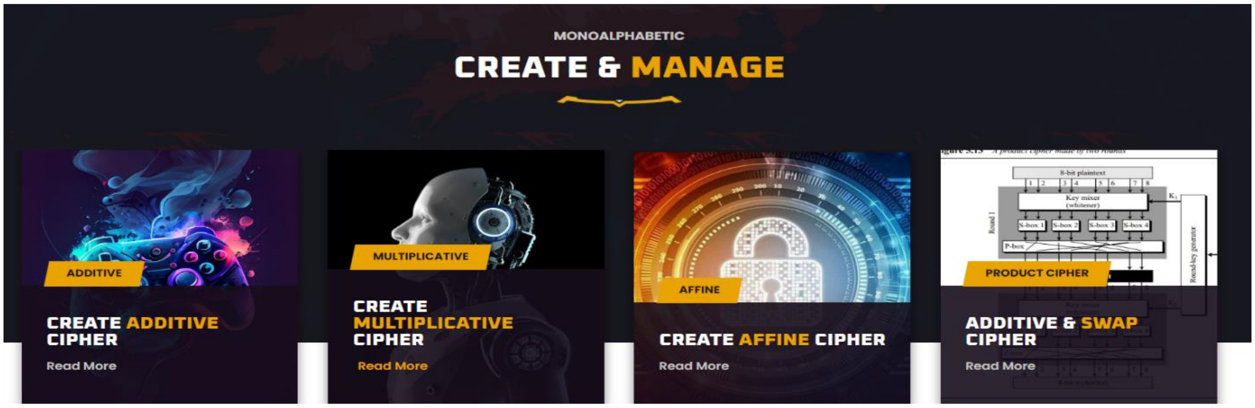


LOREM, IPSUM.

Create Cipher Text

Lorem ipsum dolor, sit amet consectetur adipisicing elit. Adipisci cupiditate necessitatibus eius ipsa. Neque, veniam?

2.2 Monoalphabetic Section



MONOALPHABETIC

CREATE & MANAGE

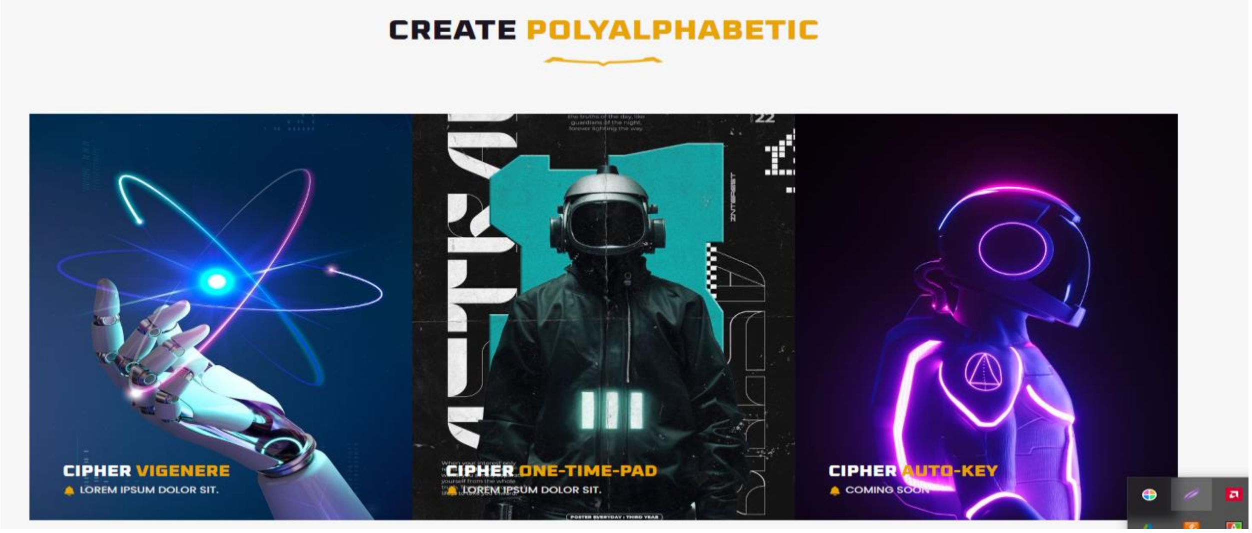
CREATE ADDITIVE CIPHER

CREATE MULTIPLICATIVE CIPHER

CREATE AFFINE CIPHER

ADDITIVE & SWAP CIPHER

2.3 Polyalphabetic Section



CREATE POLYALPHABETIC

CIPHER VIGENERE

LOREM IPSUM DOLOR SIT.

CIPHER ONE-TIME-PAD

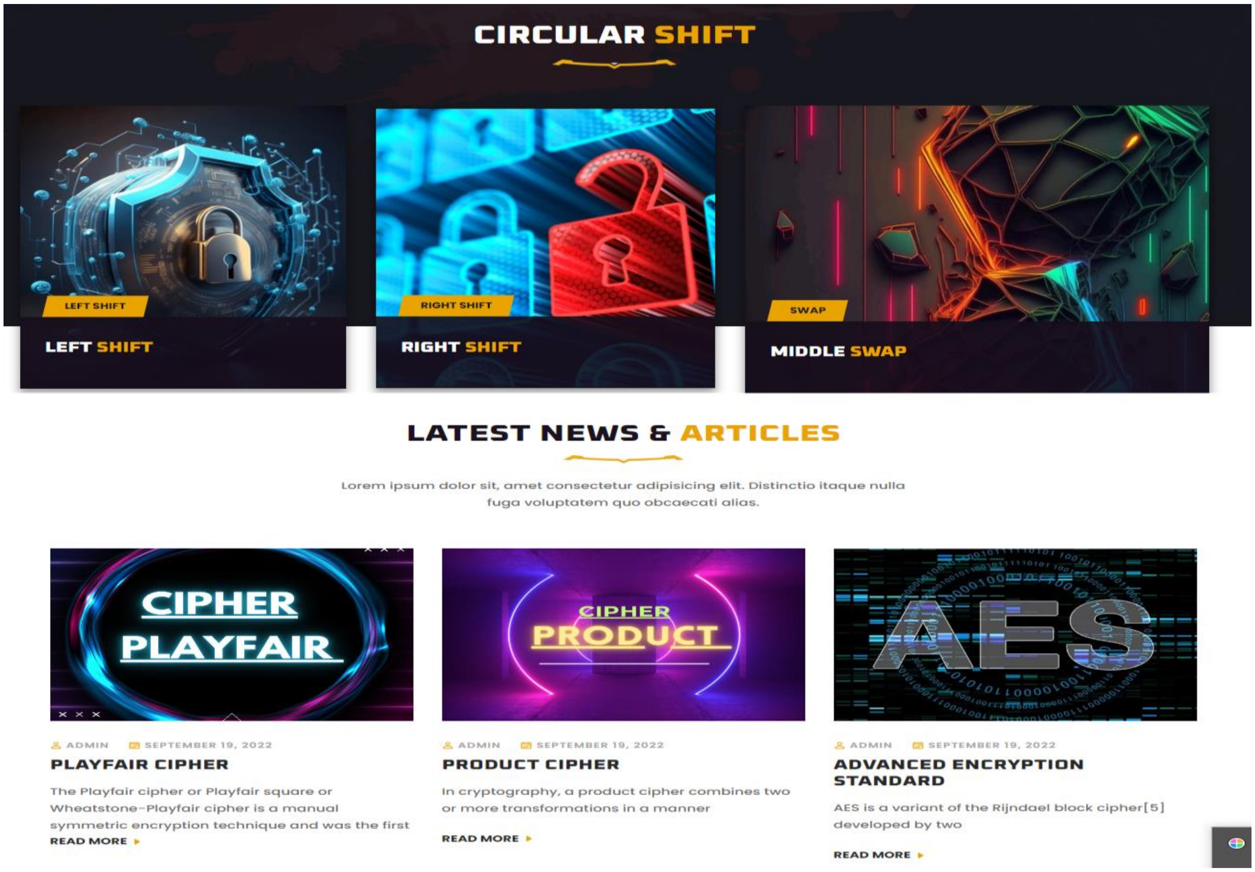
LOREM IPSUM DOLOR SIT.

CIPHER AUTO-KEY

COMING SOON

Fig: Polyalphabetic Section

2.4 Shift Section



CIRCULAR SHIFT

LEFT SHIFT

RIGHT SHIFT

MIDDLE SWAP

LATEST NEWS & ARTICLES

Lorem ipsum dolor sit, amet consectetur adipisicing elit. Distinctio itaque nulla fuga voluptatem quo obcaecati alias.

ADMIN SEPTEMBER 19, 2022

PLAYFAIR CIPHER

The Playfair cipher or Playfair square or Wheatstone–Playfair cipher is a manual symmetric encryption technique and was the first

READ MORE ▸

ADMIN SEPTEMBER 19, 2022

PRODUCT CIPHER

In cryptography, a product cipher combines two or more transformations in a manner

READ MORE ▸

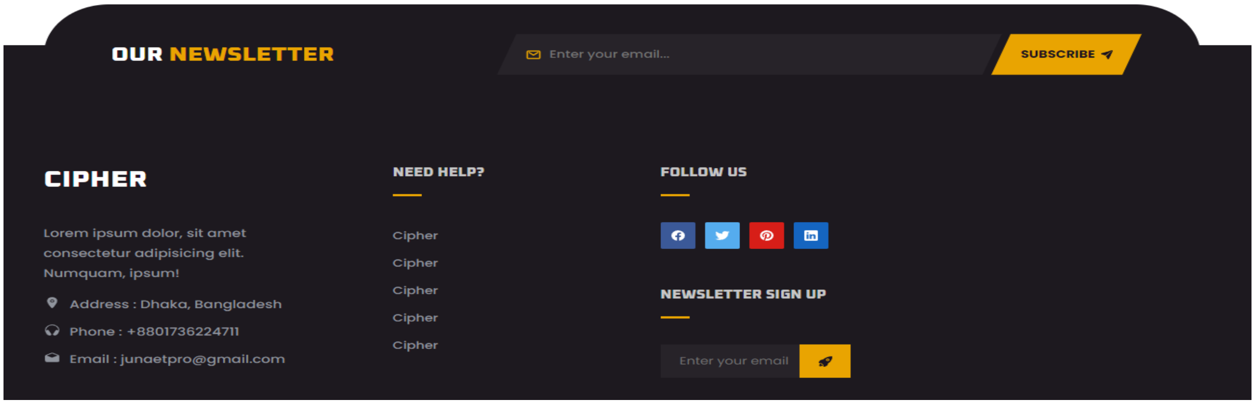
ADMIN SEPTEMBER 19, 2022

ADVANCED ENCRYPTION STANDARD

AES is a variant of the Rijndael block cipher[5] developed by two

READ MORE ▸

2.6-Footer



Lorem ipsum dolor, sit amet consectetur adipisicing elit. Numquam, ipsum!

Address : Dhaka, Bangladesh

Phone : +8801736224711

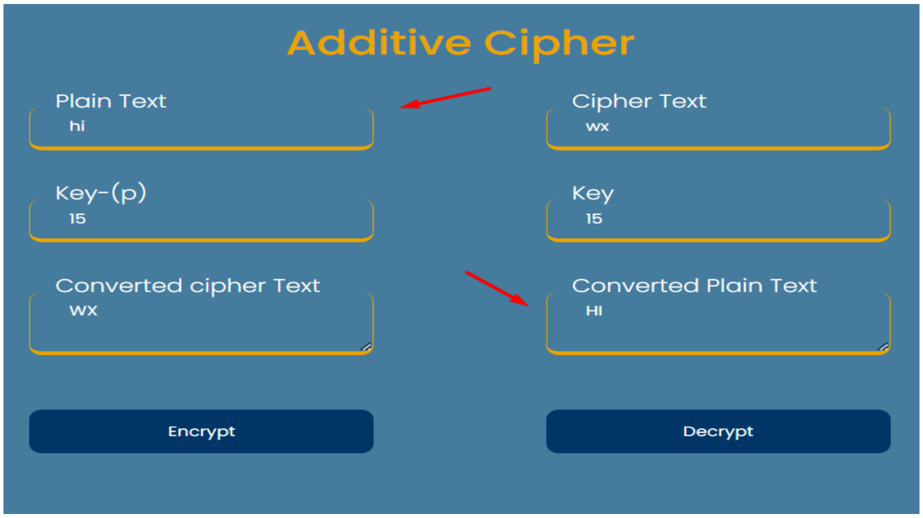
Email : junaetpro@gmail.com

Chapter 3

Performance Evaluation

3.1 Simulation Environment/ Simulation Procedure

1. Additive Cipher:



Additive Cipher

Plain Text
hi

Cipher Text
wx

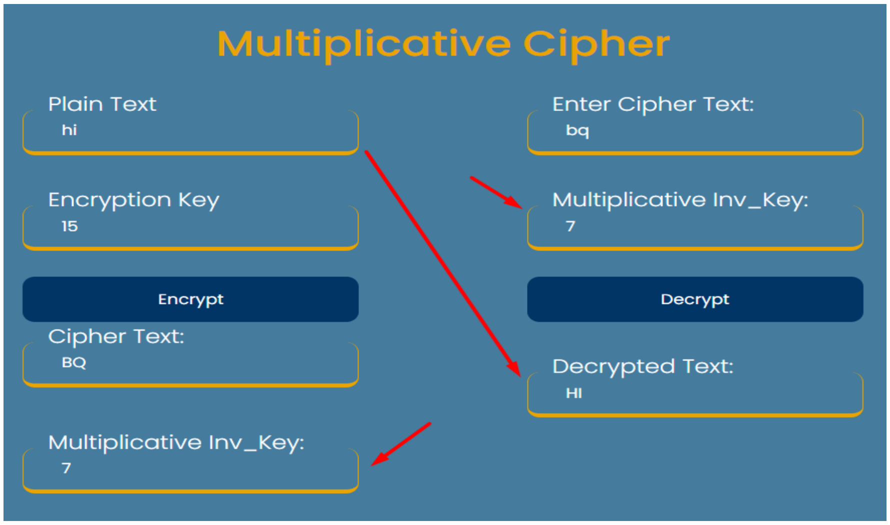
Key-(p)
15

Key
15

Converted cipher Text
WX

Converted Plain Text
HI

2. Multiplicative Cipher:



Multiplicative Cipher

Plain Text
hi

Enter Cipher Text:
bq

Encryption Key
15

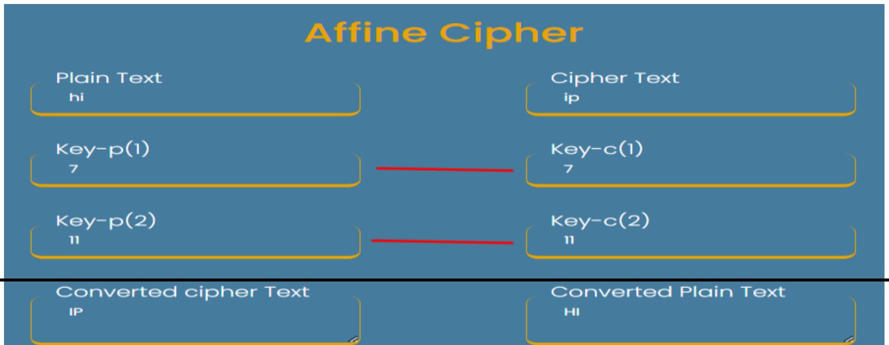
Multiplicative Inv_Key:
7

Cipher Text:
BQ

Decrypted Text:
HI

Multiplicative Inv_Key:
7

3. Affine Cipher:



Affine Cipher

Plain Text
hi

Cipher Text
ip

Key-p(1)
7

Key-c(1)
7

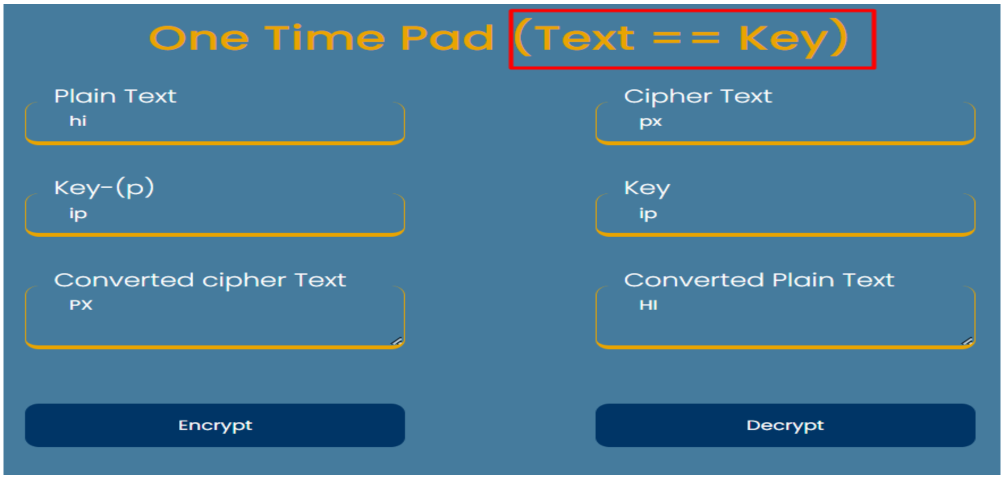
Key-p(2)
11

Key-c(2)
11

Converted cipher Text
IP

Converted Plain Text
HI

4. One Time Pad:



One Time Pad (Text == Key)

Plain Text
hi

Key-(p)
ip

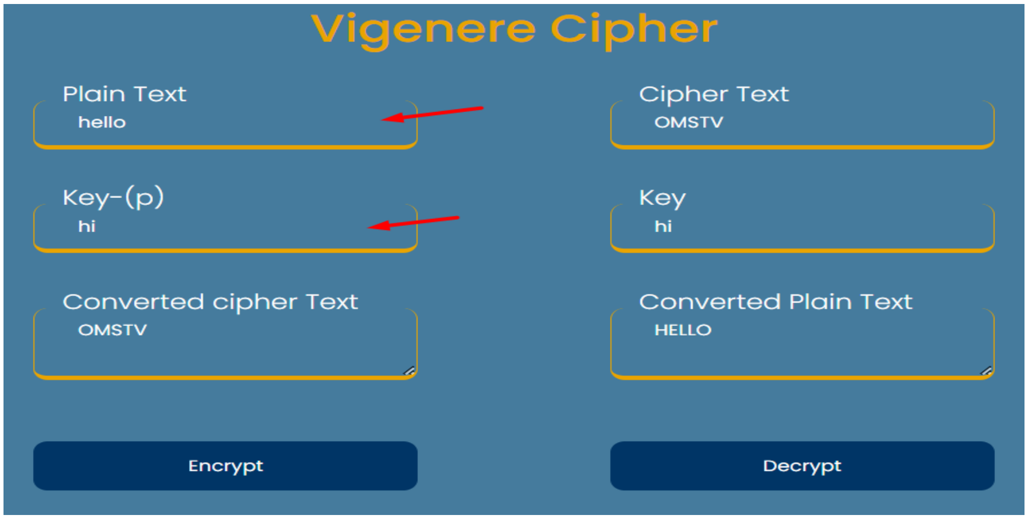
Converted cipher Text
PX

Cipher Text
px

Key
ip

Converted Plain Text
HI

5. Vigenere Cipher:



Vigenere Cipher

Plain Text
hello

Key-(p)
hi

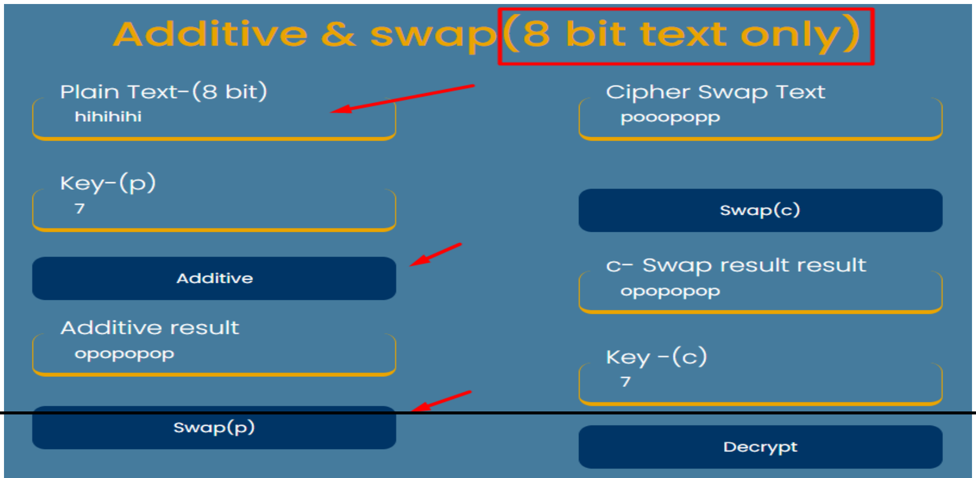
Converted cipher Text
OMSTV

Cipher Text
OMSTV

Key
hi

Converted Plain Text
HELLO

6. Product Cipher (Mixed Additive and Swap):



Additive & swap(8 bit text only)

Plain Text-(8 bit)
hihihihi

Key-(p)
7

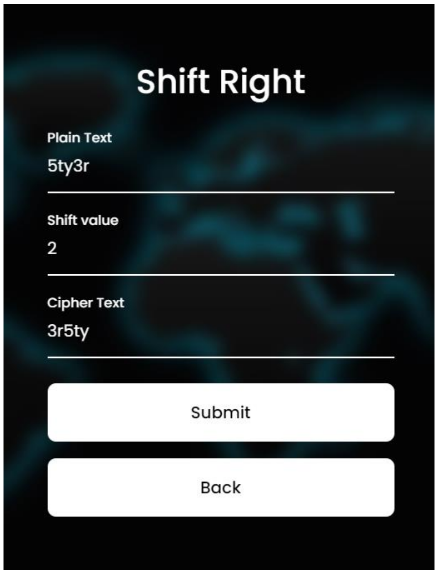
Additive result
opopopop

Cipher Swap Text
pooopopp

c- Swap result result
opopopop

Key -(c)
7

7. Left Shift, Right Shift, Middle Swap:

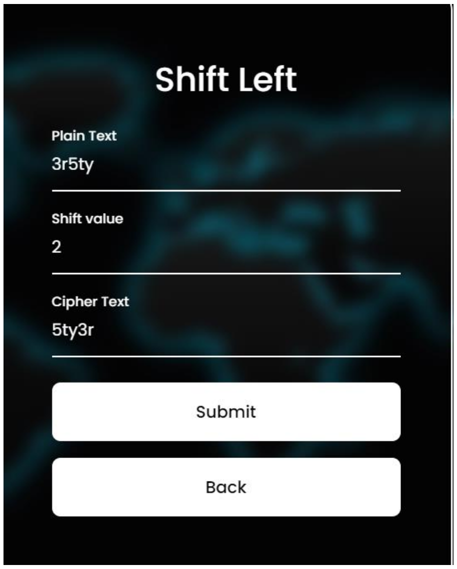


Shift Right

Plain Text
5ty3r

Shift value
2

Cipher Text
3r5ty

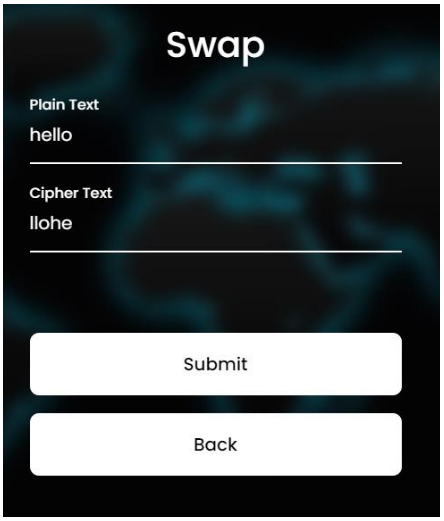


Shift Left

Plain Text
3r5ty

Shift value
2

Cipher Text
5ty3r



Swap

Plain Text
hello

Cipher Text
llohe

3.2 Results and Discussions

1. Additive Cipher: The additive cipher has proven effective in concealing plain text, yet it is vulnerable to frequency analysis and brute force attempts, diminishing its security for highly confidential information. Although the additive cipher offers a rapid and straightforward encryption approach, users must exercise caution when dealing with critical data, as it may not withstand sophisticated cryptographic attacks.

2. Multiplicative Cipher: The multiplicative cipher efficiently alters plain text, introducing an extra level of security. Nevertheless, akin to the additive cipher, it might fall short for highly sensitive data, susceptible to specific attacks. While the multiplicative cipher complements other encryption techniques, its use should be careful and combined with robust algorithms for heightened security.

3. Affine Cipher: By amalgamating the additive and multiplicative ciphers, the affine cipher enhances security, demonstrating greater resilience against attacks than either additive or multiplicative ciphers alone. The inclusion of the affine cipher proves beneficial in our encryption suite, especially in scenarios where striking a balance between simplicity and security is paramount.

4. One Time Pad: The one-time pad, theoretically impervious when applied accurately, ensures an elevated level of security. Nevertheless, its real-world application demands a genuinely random key matching the message length, leading to logistical hurdles. Despite offering unmatched security, the one-time pad faces practical constraints in actual scenarios due to strict key prerequisites and the necessity for secure key distribution.

5. Vigenere Cipher: Exhibiting adaptability across various text types, the Vigenère cipher offers a more resilient encryption technique. Yet, its vulnerability to specific attacks persists when the key is not carefully selected. While the Vigenère cipher proves practical for encrypting lengthy messages, users must implement effective key management practices to bolster its security.

6. Mixed Additive and Swap: Blending additive and swap operations in the product cipher resulted in a heightened complexity of the encryption procedure, augmenting overall security. The product cipher presents a favorable strategy, introducing an additional layer of intricacy to the encryption process. Nevertheless, prudent assessment of computational overhead and user experience remains crucial.

7. Left Shift, Right Shift, Middle Swap: These uncomplicated operations introduced added diversity to the encryption process, enriching the array of transformations. While these operations may not serve as standalone encryption techniques, their incorporation into the broader algorithm can enhance security and introduce greater unpredictability.

Chapter 4

Conclusion

4.1 Introduction.

The undertaking entails developing a website focused on text encryption and decryption, enabling users to convert plain text to cipher text and vice versa. The platform incorporates diverse encryption algorithms, including additive, multiplicative, affine, one-time pad, and Vigenere cipher. Additional features such as left shift, right shift, middle swap, and a product cipher (combining additive and swap) are available. Future objectives encompass fortifying security measures, implementing user authentication, broadening language support, creating a mobile application, introducing file encryption capabilities, optimizing performance, and fostering community engagement. The project's ultimate goal is to deliver a secure and user-friendly environment for cryptographic operations related to text.

4.2 Scope of Future Work.

Here are some potential areas for the future goals for your confidential text generating website:

1. Advanced Security Measures:
- Incorporate cutting-edge encryption algorithms to stay ahead of evolving threats.
- Explore post-quantum cryptography to safeguard encrypted data against potential quantum attacks.

2. User Authentication and Access Management:
- Integrate user authentication methods to control access to encryption and decryption services.
- Implement role-based access control for efficient user privilege management.

3. Multi-language Support:
- Broaden website language support to cater to a more diverse user base.
- Implement localization features for users to interact with the website in their preferred language.

4. Mobile Application Development:
- Create a mobile application version for convenient text encryption and decryption on the go.
- Ensure a responsive design suitable for both mobile and tablet devices.

5. File Encryption and Decryption:
- Expand functionality to enable secure file encryption and decryption.
- Support various file formats and sizes.

6. Secure Key Management:

- Enhance key management systems for secure key generation, storage, and distribution.
- Implement key rotation and revocation mechanisms for heightened security.

7. Performance Optimization:

- Optimize website performance for faster encryption and decryption.
- Explore parallel processing and distributed computing for efficient handling of large data volumes.

8. User-Friendly Interface:

- Gather user feedback to enhance the interface for a more intuitive experience.
- Implement tooltips, tutorials, or guides to assist users in utilizing encryption and decryption features.

9. Integration with Cloud Services:

- Integrate the website with cloud storage for seamless data encryption and decryption.
- Implement secure communication protocols for data transfer between the website and cloud services.

10. Collaboration and Sharing Features:

- Enable secure collaboration on encrypted documents.
- Implement sharing options with customizable access levels for shared encrypted content.

11. Compliance with Standards:

- Ensure adherence to data protection regulations such as GDPR or HIPAA.
- Maintain legal and ethical standards for user privacy.

12. Continuous Security Audits:

- Conduct regular security audits and vulnerability assessments.
- Stay informed about cybersecurity developments and update the system accordingly.

13. Community Engagement:

- Foster a user community, encouraging the exchange of encryption techniques and best practices.
- Establish forums for users to interact and share ideas.

14. Educational Resources:

- Develop educational content to help users understand encryption concepts effectively.

15. Cross-Browser Compatibility:

- Ensure seamless website functionality across various web browsers for enhanced accessibility.