Taibah University

College of Computer Science and Engineering

Department of Computer Science

**Text Encryption and Decryption Tool**

**CS433 – Computer Security Class Project**

**Group(9) Names :**

Ali Saeed Alghamdi 4102809

Abdalrhman Hamad Alqroni 4104088

Osama Ali Naji 4108881

Abdulaziz Faisal Alharbi 4100569

**Supervised by**

Dr. Maher Alharby

**Contents**

[Introduction 4](#_Toc153141203)

[Getting Started 4](#_Toc153141204)

[How to Use 4](#_Toc153141205)

[Encryption Techniques 5](#_Toc153141206)

[Troubleshooting 8](#_Toc153141207)

[Additional Resources 8](#_Toc153141208)

[Conclusion 9](#_Toc153141209)

[**References** 10](#_Toc153141210)

# Introduction

The purpose of this project is to develop a tool for text encryption and decryption, not only as a practical utility but also as a means to educate and deepen the understanding of fundamental encryption methods and information security.

The aim of this project is to develop a user-friendly tool for text encryption and decryption. This tool is designed to provide an easy and effective way for users to secure their digital communications. The project focuses on creating a simple yet powerful tool that anyone can use for encrypting and decrypting text we ensure a high level of security for users, helping them protect their data from various security threats and breaches.

# Getting Started

1. Go to the link of GitHub and install the files and use it.

<https://github.com/azizener/Encryption-Decryption-app>

1. Or go to this link and use it.

<https://azizener.github.io/Encryption-Decryption-app/>

# How to Use

1. First, the user enters the tool.
2. The user selects either encryption or decryption.
3. They choose an algorithm from the four available options.
4. If the selected algorithm requires a key, the user enters the key.
5. The user inputs the text to be encrypted or decrypted.
6. Finally, the user clicks on the 'Process' button.

صورة تحتوي على نص, لقطة شاشة, الخط, رقم

تم إنشاء الوصف تلقائياً

# Encryption Techniques

* Caesar Cipher:

Description: This is a substitution cipher where each letter in the plaintext is shifted a certain number of places down or up the alphabet.

Example: If we use a right shift of 3, 'A' becomes 'D', 'B' becomes 'E', and so on. So, "HELLO" becomes "KHOOR".

صورة تحتوي على نص, لقطة شاشة, الخط, رقم

تم إنشاء الوصف تلقائياً

* Atbash Cipher:

Description: This is a monoalphabetic cipher where each letter of the alphabet is mapped to its reverse. So, 'A' is replaced with 'Z', 'B' with 'Y', and so on.

Example: In this system, "HELLO" would be encrypted as "SVOOL".

صورة تحتوي على نص, لقطة شاشة, الخط, رقم

تم إنشاء الوصف تلقائياً

* Rot13 Cipher:

Description: This is a specific case of the Caesar cipher with a shift of 13 places. It's a simple letter substitution cipher that replaces a letter with the 13th letter after it in the alphabet.

Example: Using Rot13, "HELLO" becomes "URYYB".

صورة تحتوي على نص, لقطة شاشة, الخط, رقم

تم إنشاء الوصف تلقائياً

* Vigenère Cipher:

Description: This method uses a keyword to encrypt a message. Each letter of the plaintext is shifted along the alphabet by a number of places defined by a corresponding letter in the keyword.

Example: If the keyword is "KEY" and the plaintext is "HELLO", then 'H' (the first letter) is shifted by 'K' (11 places), 'E' by 'E' (4 places), 'L' by 'Y' (24 places), and so on. Using this method, "HELLO" is encrypted to "RIJVS".

صورة تحتوي على نص, لقطة شاشة, الخط, رقم

تم إنشاء الوصف تلقائياً

# Troubleshooting

* issue: Key Mismanagement

Solution: When a key is required for encryption or decryption, it’s vital to keep it secure and accessible.

* The issue: The key does not appear.

Solution: It is necessary to select an algorithm when first entering the site in order for the key to appear.

# Additional Resources

1. "The Code Book" by Simon Singh: A fascinating read for beginners, this book offers a historical perspective on the evolution of cryptography [1].
2. "Cryptography I" by Stanford University on Coursera: A great starting point for learning the fundamental concepts of cryptography [2].
3. Crypto101.io: An introductory booklet available online for free, perfect for those just starting out [3].

# Conclusion

the Text Encryption and Decryption Tool not only provides an easy and secure way to manage digital communications but also stands as a testament to the importance of data privacy in the digital age. With its intuitive interface and robust encryption methods, it empowers users, from tech-savvy individuals to those new to digital security, to confidently safeguard their sensitive text data. By bridging the gap between complex encryption technologies and everyday users, the tool ensures that securing digital information becomes a seamless and accessible part of our daily digital interactions.

# **References**

|  |  |
| --- | --- |
| [1] | S. Singh, The Code Book. |
| [2] | D. Boneh, "Stanford University," [Online]. Available: https://www.coursera.org/learn/crypto. |
| [3] | "CRYPTO101," [Online]. Available: https://www.crypto101.io/. |
| [4] | N. K. Anjlee Verma, A Comparative Study of Classical Substitution, 2014. |
| [5] | J. F. Dooley, History of Cryptography and Cryptanalysis. |
| [6] | C. Swenson, Modern Cryptanalysis: Techniques for Advanced Code Breaking. |