Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 12 Issue 08, August-2023

Textual Fortification: A Multi-Layered Approach to Integrity with Cryptography, Steganography And Strong Passwords

B. Karunakar[1], B. Jaithra[2], Shruthi Jha[3], V. C. S. Abhishek[4], Reddyvari Venkateswara Reddy[5]
Karlapalem Sujitha[6]
[1,2,3,4] B. Tech Student, Department of CSE-Cybersecurity, CMRCET, Hyderabad, Telangana
[5]Associate Professor, Department of CSE-Cybersecurity, CMRCET, Hyderabad, Telangana
[6]Assistant Professor, Department of CSE-Cybersecurity, CMRCET, Hyderabad, Telangana

Abstract *- **The project aims to enhance information security and privacy through integration. Text steganography, password strength testing, and random strong password generators are tools for protecting sensitive data. Text encryption secures text for authorized users. The many different methods of text encryption include substitution ciphers, transposition ciphers, and public-key cryptography, to name just a few. Users can conceal information in other text or media files to avoid detection or interception, adding a layer of security. Users can use password security on the system. By examining their passwords' strength, users may make informed judgments.***

Keywords—text cryptography, text steganography, password strength checker, random strong password generator, information security.

1. INTRODUCTION

Protecting sensitive information is essential in today's digital world. To improve information security and safeguard textual data, the project incorporates text cryptography, steganography, password creation, and password security level testing. Text cryptography ensures secrecy and integrity by converting plaintext into ciphertext using encryption techniques. To effectively safeguard sensitive information, the project uses symmetric and asymmetric encryption methods. Steganography hides confidential text inside innocent carriers to prevent detection by unauthorized parties. Based on the suggested parameters, the password generator creates strong, secure passwords, reducing the possibility of unauthorized access. By assessing factors including length, character variation, and resistance to typical assaults, a password security level testing function aids users in determining the security level of their passwords. The concept is approachable.

2. LITERATURE REVIEW

S. Kumar and S. N. Srivastava's "Techniques and Challenges" (2020) This research article thoroughly analyzes text steganography methods with an emphasis on the concealment of plain text within plain text. The authors look at techniques that use the structure and semantics of natural language to hide information, including word-based, syntax-based, and linguistic steganography.

Stuart E. Schechter and Saranga Komondor's "Password Strength: An Empirical Analysis" (2010): The effectiveness of password strength meters and password composition guidelines are investigated in this research article. It assesses how different variables affect password security, including password length, character sets, and mnemonic devices. The results clarified the benefits and drawbacks of various techniques for evaluating the strength of passwords.

By Roger Needham, "Password Security: Case History" (1997): This influential research paper discusses the challenges and vulnerabilities associated with password security. It presents a historical perspective on password security, analyzing past practices and their weaknesses. The paper provides valuable insights into password security and highlights the need for stronger authentication mechanisms.

"Cryptography: Theory and Practice" by Douglas R. Stinson (1995): This book provides a comprehensive overview of cryptography, including various techniques and algorithms for text encryption and decryption. It covers both classical and modern cryptographic methods, such as substitution ciphers, block ciphers, and stream ciphers. The book also discusses topics like key management, data integrity, and authentication protocols.

3. METHODOLOGY

A webpage that allows users to encode and decode data is the system that is being proposed. The user will first arrive on the main page. The user will find different features on this page which can be used for their needs. It primarily consists of five features: cryptography, steganography, a password strength checker, a strong random password generator, and advice for users on how to use the features more effectively.

The information we collect usually possesses confidentiality, and non-repudiation provided by cryptography. It converts plaintext into cipher text and vice versa using mathematical algorithms and cryptographic keys. This website employs a number of different algorithms, including the Caesar cypher, Rot13, Base64, Reverse Cypher, and One-Time Pad Cypher.

Caesar ciphers are substitution ciphers that shift every letter in the text to the thirteenth position and replace it with

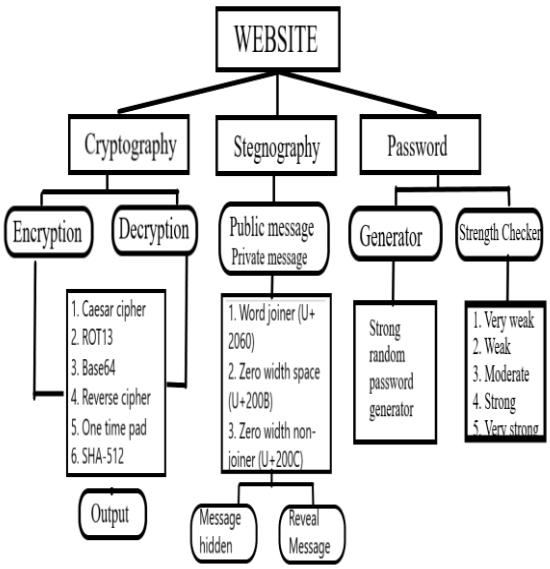
International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 12 Issue 08, August-2023

a different letter from the alphabet. As a result, "A" and "B" become, respectively, "N" and "O." Having a shift value of 13, ROT13 is a genuine Caesar cipher form.

The ROT13 cipher is not very safe because it can be cracked by simply moving the letters backward by 13 positions. It is occasionally used in internet forums to obfuscate text, such as spoilers or jokes. Binary data can be represented in ASCII using the Base64 encoding scheme. It is frequently used for operations like email attachments, internet data transfer, and storing binary data in text-based formats like JSON or XML. Base64 encoding (hence the name "Base64") transforms binary data into a string of characters using a set of 64 different characters.

The binary data is divided into groups of 3 bytes (24 bits) to start the encoding process. Then, each group is divided into four 6-bit portions. A character from the Base64 character set is assigned to each 6-bit chunk. The only characters in the resulting encoded string will be those found in the Base64 character set.

The reverse cipher also referred to as the mirror cipher or backward cipher, is a relatively easy encryption technique that involves flipping the characters in a message. At the other end of the message, every character is switched with



its corresponding counterpart.

One-time pad (OTP) cryptography utilizes a pre-shared key that is either larger or equal to the message size, ensuring uncrackable encryption. This method pairs plaintext with an arbitrary secret key and then adds each bit or character to create the encrypted version or character from the keypad.

The method of steganography known as zero-width based uses invisible, non-printable characters called zero-width characters to conceal information within text. When rendered, these characters are invisible to the human eye, but they can be encoded and decoded using programming. Zero-width-based steganography aims to covertly insert hidden messages into plain text.

An algorithm that produces random passwords with a high degree of security is known as a strong random password generator. An extra layer of security is added to user accounts and sensitive data by the fact that these passwords are made to be challenging for attackers to decipher or guess.

A password strength checker is a feature or algorithm that assesses a password's strength based on specific requirements. It is intended to evaluate a password's success in preventing unauthorized access to sensitive data.

Another feature is tips, which provide users with prewritten advice on how to create secure passwords, emphasize the value of cryptographic algorithms, and use steganography.

4. BENEFITS

1. Enhanced Information Security: The project ensures the confidentiality and integrity of sensitive textual data through encryption, steganography, and strong password practices.

2. Privacy Protection: The project helps maintain privacy and protects against unauthorized access by encrypting and hiding sensitive information.

3. Covert Communication: Steganography techniques enable covert communication, allowing users to exchange sensitive information discreetly.

4. Customizable Password Generation: The project provides a password generator that creates strong passwords based on customizable requirements, ensuring strong authentication.

5. Reduced Password Guessing Attacks: Strong password generation and security level checking mitigate the risk of password guessing attacks and unauthorized access.

6. Improved User Authentication: Strong passwords enhance user authentication and protect against unauthorized account access.

5. CONCLUSION

The project on text cryptography, steganography, password generator, and password security level checking encompasses a comprehensive set of tools and techniques to enhance information security, protect sensitive data, and promote strong password practices. The project offers several key advantages and benefits, including enhanced information security, privacy protection, and covert communication through steganography. The password generator facilitates the creation of strong and secure

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 12 Issue 08, August-2023

passwords, while the security level-checking feature empowers users to evaluate and improve their password strength. The project promotes user education, best practices, and user-friendly interfaces to ensure usability and widespread adoption. By combining these functionalities, the project addresses critical aspects of information security, encryption, data hiding, and password management. It enables individuals and organizations to actively participate in safeguarding their data, mitigating the risk of unauthorized access, and fostering a more robust security posture. With continuous improvement and adaptation to emerging security trends, the project holds great potential to contribute to the ongoing efforts of protecting sensitive information in today's digital landscape.

6. FUTURE SCOPE

As we move forward, we plan to enhance the security of our cryptographic algorithms and introduce new functionalities. These may include the ability to encrypt multiple files simultaneously, decrypt files that were encrypted by other programs, and generate passwords with varying lengths and complexity levels.

REFERENCES

[1] Stallings, W. (2017). Cryptography and Network Security: Principles and Practice. Pearson.

[2] Fridrich, J., Goljan, M., & Hogea, D. (2010). Steganography: Principles, and Applications. Cambridge University Press. https://doi.org/10.1017/CBO9781139192903

[3] S. Komondor, S. E. Schechter, and A. J. B. Brush (2010) Website authentication and the implications of role-playing on usability studies are covered in The Emperor's New Security Indicators. USENIX security conference.

[4] C. Harley and P. C. Van Oorschot (2012) The Reasonable Rejection of Security Advice by the Users: Goodbye and Thanks, but No Thanks for the Externalities.

[5] The authors are Bauer, Christin, Mazurek, M. L., Shay, R., Vedas, T., and Kelley (2012). Guess again—and again—by mimicking password-cracking methods to assess password strength.