JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

File Encryption Using Fibonacci Series

Sahil Kumar Jain[1], Neetha S. S[2]
Student[1], Professor[2]
Department of BCA, School of Computer Science & IT,
JAIN Deemed -to-be University, Bengaluru, India

Abstract— Millions of people transmit information electronically every day thanks to the internet's accessibility and technical improvements, which exposes sensitive data to a variety of threats.. To mitigate these risks, cryptographic techniques are employed to protect sensitive information during transmission. Encryption plays a crucial role in safeguarding data, ensuring that the only allowed individuals to have access to given information. So in the given paper, we propose a novel approach to encryption by integrating the Fibonacci series into the Playfair encryption algorithm. The Fibonacci series is hashed to generate key sequences, enhancing the security of the encryption process. We chose the Fibonacci series for its nearly exponential growth and reduced predictability, making it resistant to brute force attacks and word association methods used in historical contexts. The integration of symbols in the extended 8x8 encryption matrix further strengthens the encryption scheme, making it harder to decipher. Additionally, we extend our encryption method to image encryption, demonstrating its effectiveness in protecting sensitive image data transmitted over the internet. Through experimentation and analysis, we show the efficacy of our modified encryption algorithm in ensuring privacy and confidentiality in electronic communications and image transmission.

Index Terms— Cryptography, Fibonacci sequences, Playfair Cipher, Encryption, Decryption, Hashing Function, Privacy, Keyword Matrices, Extended Matrix.

I. INTRODUCTION

Encryption stands as main core of cybersecurity, serving as a formidable barrier against unauthorized access to sensitive information. By transforming data into an indecipherable format, encryption ensures the confidentiality and integrity of data, safeguarding it from prying eyes and malicious actors. Conversely, decryption serves as the counterpart to encryption, enabling the retrieval of the original data from its encrypted form.

The evolution of encryption techniques spans centuries, with each era witnessing the development of innovative methods to fortify data protection. Among these techniques, the Playfair Matrix emerges as a seminal milestone, heralding the advent of practical digraph substitution ciphers. Its inception dates back to March 26, 1854, credited to Charles Whetstone, yet it gained widespread recognition under the name of his colleague and proponent, Lord Playfair.

The historical significance of the Playfair Matrix is profound, notably marked by its pivotal role during pivotal historical events such as the Second Boer War and both World Wars. Initially employed by the British military, its efficacy and reliability prompted its adoption by other nations, including Australia and Germany, further solidifying its status as a ubiquitous cryptographic tool on the global stage.

In this paper, we delve into the intricate workings of the Playfair Matrix, exploring its historical underpinnings, cryptographic principles, and practical applications. By examining its evolution and impact, we aim to unravel the enduring legacy of this iconic encryption technique and its enduring relevance in contemporary cybersecurity landscapes.

In this paper, we delve into expanding the utility of the Playfair Matrix beyond its conventional application in textual encryption to the realm of image encryption. By integrating the foundational principles of the Playfair Cipher and enriching them with the distinctive attributes of the Fibonacci series, we introduce an innovative approach to securing images. Our proposed hybrid encryption scheme is designed to fortify the security of sensitive image data transmitted over vulnerable channels, with the overarching goal of safeguarding confidentiality and preserving integrity in electronic communications.

II. LITRATURE REVIEW

Subhajit Bhattacharyya et al:[1] This study introduces a altered encryption technique by expanding the Playfair Cipher matrix to accommodate additional symbols and special characters, enhancing its ASCII completeness. The approach aims to augment the encryption capabilities of the Playfair Cipher, potentially improving its robustness against cryptographic attacks **Mohd Vasim Ahamad et al:[2]** The research explores an improved encryption technique that combines the Playfair Cipher with the Fibonacci series to generate a secret key. This novel approach seeks to enhance the security of encrypted data by leveraging the unique properties of both cryptographic methodologies.**Md. Atiullah Khan et al:[3]** The study proposes a hybrid encryption technique

integrating the Fibonacci series, XOR cipher, and PN cipher to encrypt various data segments within a file. By combining multiple encryption algorithms, the approach aims to enhance data security and resilience against unauthorized access.**Priyanka Goyal et al:[4]** This research focuses on implementing a altered version of the Playfair Cipher, utilizing an 8x8 matrix to accommodate a wider range of unique symbols. The adaptation aims to enhance the encryption capabilities of the Playfair Cipher, particularly for applications requiring the encryption of diverse data sets.**S.S. Dhenakaran et al:[5]** The study presents an extension of the Playfair Cipher using a larger 16x16 matrix, allowing for the encryption of null characters and introducing case sensitivity. The expanded matrix enhances the randomness and complexity of the cipher, potentially bolstering its resistance against cryptographic attacks.**Shiv Shakti Srivastava et al:[6]** This research proposes an extended version of the Playfair Cipher, utilizing an 8x8 matrix and implementing it in a Linear Feedback Shift Register (LSFR) manner for cryptanalysis. The approach aims to enhance the security of the Playfair Cipher against cryptographic attacks through improved randomness and complexity.**P Agarwal et al:[7]** The study explores data encryption through the combination of the Fibonacci sequence and Unicode characters. By leveraging these cryptographic elements, the approach aims to enhance data security and confidentiality in electronic communications.

III. EXISTING SYSTEM

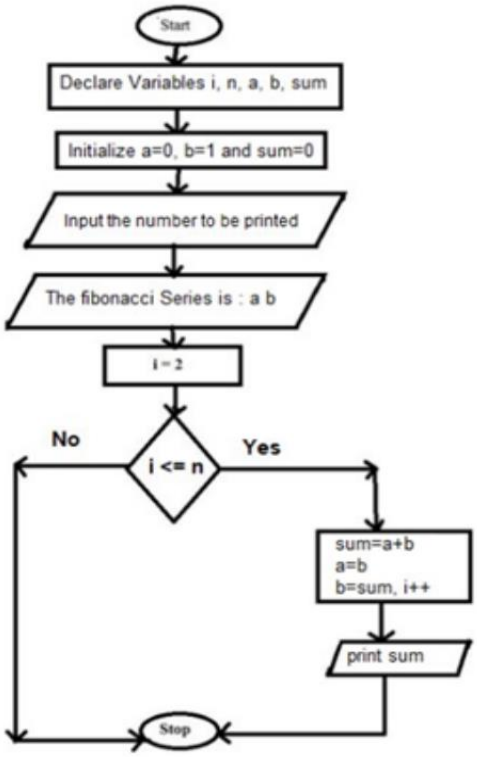
The existing systems utilizing the Playfair Encryption Matrix (PEM) predominantly rely on a simplistic 5x5 encryption matrix table containing only the Latin alphabet from A to Z. This system, originating in 1854 and primarily used for military purposes, has encountered vulnerabilities over time. During World War II, it was compromised through brute force attacks and word association techniques, leading to its susceptibility to exploitation. Another existing method involves the utilization of randomly generated keys, yet it still relies on human input for key generation and is restricted to alphabetic characters for creating ciphertext in bigraph pairs. This limitation has rendered the PEM ineffective and unsafe for modern encryption technologies, prompting its discontinuation.

In contrast, contemporary encryption algorithms such as AES, DES, and RSA have undergone rigorous testing and validation, offering robust security features. However, these algorithms typically involve multiple encryption rounds, resulting in longer encryption times and increased system resource utilization. While they provide superior security, the trade-off often involves higher execution times and performance demands.

It is evident that while the PEM has historical significance, its vulnerabilities and limitations have rendered it obsolete in the face of modern encryption requirements. Contemporary encryption algorithms offer a balance between security and performance, making them the preferred choice for safeguarding sensitive data in today's digital landscape.

C	R	Y	P	T
O	A	B	D	E
F	G	H	I/J	K
L	M	N	Q	S
U	V	W	X	Z

IV. RESEARCH METHODOLOGY

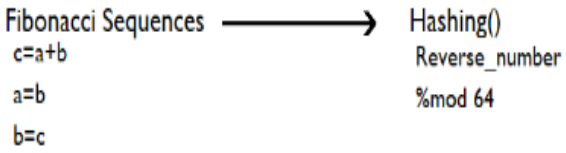


The Fibonacci Generation Algorithm:

The Fibonacci sequence is generated according to the recurrence relation Fn = Fn-1 + Fn-2, where n is greater than or equal to 1. This fundamental formula serves as the backbone for generating a sequence of Fibonacci numbers, a crucial component in our proposed encryption methodology.

To initiate the generation of a Playfair Encryption Matrix (PEM) with Fibonacci number sequences, it is imperative to establish a mechanism for generating the Fibonacci series. Utilizing the aforementioned formula, we can develop a modular algorithm capable of systematically generating the Fibonacci sequence.

HASHING

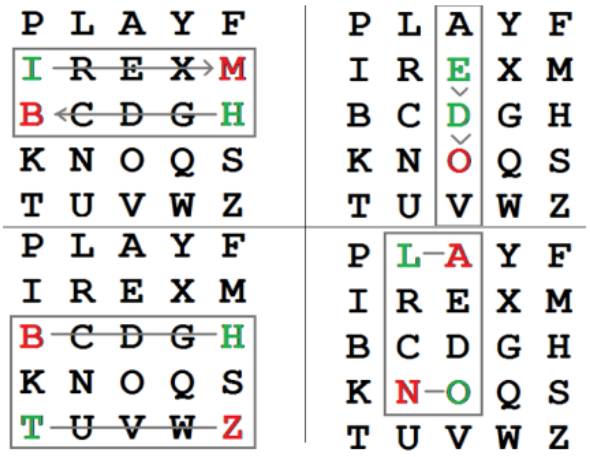


Following the generation of Fibonacci sequences, the next step involves passing them through a hashing function. A hashing function, in essence, is a mathematical operation that converts input data into a non-reversible output with minimal collision probabilities. For this project, we have implemented a simplistic hashing function that involves reversing the given input number.

Our hashing function, while straightforward, effectively minimizes collision occurrences. It operates by reversing the input number, thereby mitigating collision risks. Although collisions may arise in scenarios involving inputs such as 9, 90, or 900, the inherent properties of the Fibonacci series render such occurrences highly improbable.

To ensure optimal functionality within the dimensions of our 64-dimensional matrix, the hashing function employs modular division. This ensures that the resulting reversed number falls within the range of 0 to 63, preserving the reversibility of outputs. Consequently, it is advisable to initiate the generation of Fibonacci sequences with base numbers of at least three digits to maximize the cryptographic robustness of the encryption scheme.

V. *ENCRYPTION PROCESS*



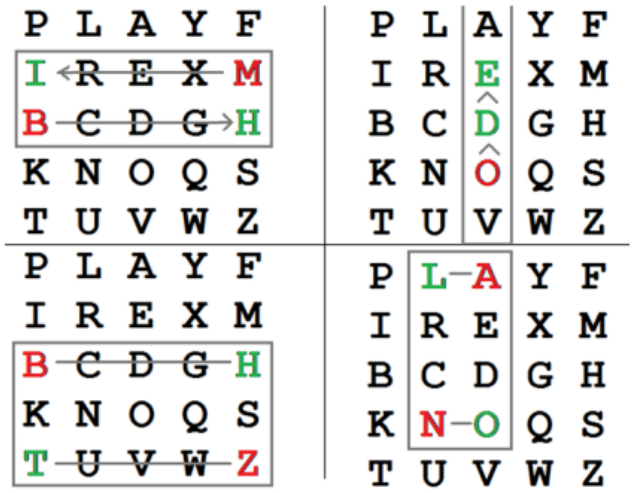
An encryption technique is required to convert plaintext into cipher text once we have the secret key and the plaintext message that has to be shared. The plaintext message is divided into digraphs in order to apply PEM. The Playfair cipher adheres to the following encryption rules:

• Create an 8x8 grid and insert the created key (a duplicate letter needs to be removed) into that matrix. Once the key is in place, use the remaining letters to fill in the remaining spaces in the grid.

• Choose the letter that appears below each digraph letter if the two plain text digraph letters are in the same column. Select the letter at the top of the grid if it is at the bottom.

• Replace the letters to the right of each digraph letter if both are in the same row. Select the leftmost letter in the same row if the digraph's rightmost letter is one of the letters.

VI. DECRYPTION PROCESS



The decryption procedure is likewise easy to understand. The key tables should be created in the same way as the encryption. Following that, the following guidelines can be applied to decrypt the encrypted text:

• Take the letter above each if both are in the same column (returning to the bottom if at the top).

• Take the letter to the left of each if both are in the same row (turning around if it is at the farthest left).

• If neither of the two rules above apply, arrange the two letters into a rectangle and place the letters on the diagonal corner of the rectangle.

VII. LIMITATION

Limited Key Space: The Fibonacci sequence generates a deterministic sequence of numbers, which may result in a limited key space compared to other encryption techniques. This limitation could make the encryption vulnerable to brute force attacks if the key space is relatively small.

Performance Overhead: Generating Fibonacci numbers computationally may introduce performance overhead, especially for large files or high-resolution images. This could impact the efficiency of the encryption and decryption processes, potentially leading to slower processing times.

Predictability: Although the Fibonacci sequence is mathematically deterministic, certain patterns may emerge over time, making the encryption predictable. Predictability could weaken the security of the encryption scheme and make it susceptible to cryptanalysis attacks.

Key Management: Managing the distribution, storage, and rotation of encryption keys generated from the Fibonacci sequence might provide difficulties. For encrypted files and images to remain secret and intact, secure key management procedures must be followed.

Adaptability to Various File Types and Image Formats: The encryption scheme based on the Fibonacci series may not be equally effective for encrypting different file types or image formats. Some file types or image formats may exhibit specific characteristics that affect the security and performance of the encryption process.

Limited Research and Validation: Compared to established encryption algorithms, such as AES or RSA, the use of the Fibonacci series for encryption may lack extensive research and validation in the field of cryptography. This limited research may raise concerns about the reliability and security of the encryption scheme.

VIII. REFERENCES

[1] S. Bhattacharyya, N. Chand, and S. Chakraborty, "A Modified Encryption Technique using Playfair Cipher 10 by 9 Matrix with Six Iteration Steps", International Journal of Advanced Research in Computer Engineering Technology, vol. 3, no. 2, pp. 307–312, 2014.
[2] Vasim Ahamad, Mohd Siddiqui, Misbah Masroor, Maria Fatima, Urooj. (2018). "An Improved Playfair Encryption Technique Using Fibonacci Series Generated Secret Key. International Journal of Engineering and Technology(UAE)". 7. 347-351. 10.14419/ijet.v7i4.5.20104.
[3] Md. Atiullah Khan, Kailash Kr.Mishra, N.Santhi, J.Jayakumari, "A New Hy-brid Technique for Data Encryption", Proceedings of 2015 Global Conference on Communication Technologies (GCCT 2015), 978 - 1 -4799 -8553 -1/15.
[4] Sharma, Gaurav Goyal, Priyanka Kushwah, Shivpratap. (2016). Implementation of Modified Playfair CBC Algorithm. International Journal of Engineering Research and. V5. 10.17577/IJERTV5IS060631.
[5] S.S.Dhenakaran, M. Ilayaraja, "Extension of Playfair Cipher using 16X16 Ma-trix", International Journal of Comuter Applications (0975 – 888) Volume 48 –No.7, June 2021.
[6] Shiv Shakti Srivastava, Nitin Gupta "A Novel Approach to Security using Extended Playfair Cipher", International Journal of Computer Applications (09758887) Volume 20 – No.6, April 2021 .
[7] P Agarwal, N Agarwal, R Saxena, "Data encryption through fibonacci sequence and unicode characters", MIT International Journal of Computer Science and Information
Journal of Computer Science and Information Technology, Vol. 5, No. 2, August 2015, pp. 79-82 ISSN 2230-7621