

FILE ENCRYPTION USING FIBONACCI SERIES

ABSTRACT:

Nowadays, information security becomes complex and more important problem. Encryption/decryption can be an important tool to help in improving data security, to avoid hacking.

The aim is to provide features such as key for integrity and validation of user.

The proposed encryption/decryption algorithm is loss-less, key-dependent. The performance of the popular symmetric key algorithms including DES, 3DES, AES, Blowfish, are compared with Fibonacci Series encryption by encrypting input files of varying contents and sizes.

As data communication is becoming more pervasive, complex and the use of digital data is becoming much more widespread, data security has become a wider, complex and more important problem. Encryption can be an important tool to help in improving data security.

The critical concern in designing an encryption algorithm is the security of the algorithm against undesirable attacks.

In this project, the performance of the leading secret key algorithms has been compared on different platforms, using input data files of varying sizes and formats.

SCOPE:

The scope of using the substitution method for file encryption refers to the extent to which the method is applicable in securing and protecting digital files. The substitution method uses a substitution algorithm integrated with fibonacci series to replace plaintext characters with the corresponding encrypted characters.

The scope of this method can be considered to cover the following areas:

1. Data confidentiality
2. Data integrity
3. Data privacy

4. Secure communication

Encryption using substitution method can be used to avoid hacking of confidential data. Without knowledge of this software a third person cannot access data. The user should know the key used for encryption. This algorithm is most useful in e-commerce, banking, and online transaction processing applications, small or large scale industry, medical imaging, telemedicine, and military communication and Banking etc.

METHODOLOGY:

The Fibonacci method is an emerging field in data protection, basic statistical modeling, and several methods have been found to obtain the highest order terms of this method. The general idea of Fibonacci encryption is based on the Fibonacci functionality of the sequence of text data in the original message encryption. In the proposed Fibonacci and Random key technique, it is used to encrypt a solid key file. After successful key matching, the client will be able to translate text messages with this button to find the original text file.

In that original data, each distance or character is converted to digits by the encryption process to take a Fibonacci random key sequence key.

1. Let the first security key chosen be 'k'.

Plain Text: C O D E; Characters: k l m o p q r s t u v w x y z a b c d e f g h i j k l

Fibonacci : 1 2 3 5

Cipher Text: k l m o Cipher Text is converted into Unicode symbols and saved in a text file. The text file is transmitted over the transmission medium. It is the first level of security.

2. Cipher text to Unicode is another method. The ASCII code of each character from the cipher text plus the ASCII code of its previous character, and next character is added to the ASCII code of the equivalent character in the original message. Here, ASCII codes of four characters are used as a security key to further encode the characters available in the cipher text to Unicode symbols.

3. The Decryption process follows a reverse process of Encryption. Recipient extracted each symbol from the received text file and mapped to find its hexadecimal value. Obtained value is converted into a decimal value to find out the plain text using the key. Without knowledge of the key an unknown person cannot understand the existence of any secret message.
4. The Fibonacci numbers are Nature's numbering system. They appear everywhere in Nature, from the leaf arrangement in plants, to the pattern of the florets of a flower, the bracts of a pinecone, or the scales of a pineapple. The Fibonacci numbers are therefore applicable to the growth of every living thing, including a single cell, a grain of wheat, a hive of bees, and even all of mankind.

EXPECTED RESULTS AND OUTCOMES:

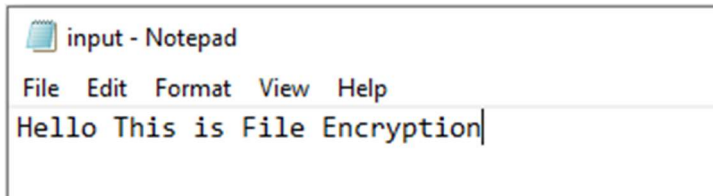
1. Providing an encryption program to encrypt files using Fibonacci series.
2. Decryption of the encrypted files back to original form.

The provided algorithm creates a good security for the content of the files which does not allow unauthorized people to read the contents. The contents are encrypted to provide security and they can be decrypted to get back the original content.

OUTPUT SCREENSHOTS:

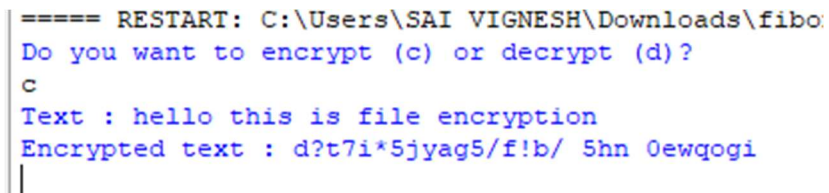
FOR ENCRYPTION:

INPUT FILE:



```
input - Notepad
File Edit Format View Help
Hello This is File Encryption
```

AFTER ENCRYPTION:



```
==== RESTART: C:\Users\SAI VIGNESH\Downloads\fibonacci
Do you want to encrypt (c) or decrypt (d)?
c
Text : hello this is file encryption
Encrypted text : d?t7i*5jyag5/f!b/ 5hn 0ewqogi
|
```


OUTPUT FILE CONTENTS:



```
output - Notepad
File Edit Format View Help
d?t7i*5jyag5/f!b/ 5hn 0ewqogi
```

FOR DECRYPTION:

INPUT FILE:

 input - Notepad

File Edit Format View Help

d?t7i*5jyag5/f!b/ 5hn 0ewqogi

AFTER DECRYPTION:

Do you want to encrypt (c) or decrypt (d)?


d

Text : d?t7i*5jyag5/f!b/ 5hn 0ewqogi

Decrypted text : hello this is file encryption

|

OUTPUT FILE CONTENTS:

 output - Notepad

File Edit Format View Help

hello this is file encryption

REFERENCES:

1. Khadri, Syed Khutubuddin Ahmed, Debabrata Samanta, and Mousumi Paul. "Approach of message communication using fibonacci series: in cryptology." Lecture Notes on Information Theory Vol 2.2 (2014).
2. Sinha, Sudipta. (2019). The Fibonacci Numbers and Its Amazing Applications. 6. 7-14.
3. Harikrishna Bommala, Dr. S. Kiran, T.Venkateswarlu, M. Asha Aruna Sheela. Fibonacci Technique for Privacy and Security to Sensitive Data on Cloud Environment. March – 7 2020
4. https://www.researchgate.net/publication/220902441_On_the_information_security_using_Fibonacci_series
5. [https://www.mukpublications.com/resources/jmcsa_v6-6-1-5_S_agarwal%20\(1\)%20\(1\).pdf](https://www.mukpublications.com/resources/jmcsa_v6-6-1-5_S_agarwal%20(1)%20(1).pdf)