Journal of Mathematical Control Science and Applications (JMCSA)
ISSN: 0974-0570, Vol. 6, No. 1 (January-June, 2020)

Submitted: 19th August 2020 Revised: 22nd September 2020 Accepted: 30th September 2020

ALGORITHM FOR DATA ENCRYPTION & DECRYPTION USING FIBONACCI PRIMES

AKANSHA AGARWAL[1*], DR. SHUBHAM AGARWAL[2], DR. B.K. SINGH[3]

ABSTRACT. Today's world requires privacy and security of data and thus there is a need of study of algorithms for sending confidential messages without the worry of a leak by encryption and decryption methods. There are many algorithms already available to transmit data securely to a person by a person with close to no chance of insecurity. As all the transmission is computerized there are various theories going around and new theories coming up every other day. We will be introducing the application of Fibonacci primes as a method to secure any type of files / data for transmission and we propose the use of Fibonacci primes for data encryption and decryption.

1. Introduction

Everything is going online in today's internet world; therefore there is a need to secure data on the fly, so we use cryptography. There are several different approaches and algorithms for conducting knowledge exchange. Symmetric cryptography, public-key cryptography, and hash functions are three cryptographic techniques generally used to achieve the cryptographic transmission goals. Symmetric cryptography uses the same key for encryption as well as decryption of the data.

Cryptography means "hidden secret", it is the practice and the study in the presence of third parties of techniques for secure communication. Modern cryptography is heavily grounded in the practice of mathematical theory and computer science. Cryptography is a standard that provides secure information by controlling access to resources. As the data is controlled, the need to secure it comes before the transmission to the concerned person and that is a major concern which we are going to address.

Encryption is a way to encrypt any data such as words, numbers and images using mathematical formulas to make the data undecipherable to unauthorized viewers. Encryption has evolved over the past few decades and has adapted to meet the demands of emerging technology. Today the Advanced Encryption Standard (AES) is the highest standard. AES is a formal method of

[*]*Corresponding Author*
2020 Mathematics Subject Classification: *11T71; 68P25; 11B39*
Key words and phrases*: Encryption; Decryption; Fibonacci Primes; Security*

encryption employed by the National Institute of Standards and Technology (NIST). In the data encryption process, an encryption key is created which allows users to encrypt and decrypt the data when access is required. The techniques of encryption are very useful tools to protect the secret information. Encryption is also defined as converting the plain message into a cipher text that no one can read without decrypting the encrypted text.

Decryption is the reverse encryption process, which is the process of converting the encrypted text into plain text for reading.

2. Fibonacci numbers & Fibonacci primes

The Fibonacci sequences is,

1, 1, 2, 3, 5, 8, …….

Where each entry is formed by adding the two previous ones, starting with 1 and 1 as the first two terms, this sequence is called 'Fibonacci Sequence' and each term of this sequence is called Fibonacci number.

A Fibonacci prime, as you should easily guess, is a Fibonacci number that is prime. Recall that the Fibonacci numbers can be defined as follows:

$$F_1 = 0,\ F_2 = 1 \text{ and } F_{n+1} = F_n + F_{n-1}, \qquad (n>2)$$

3. Review of literature

Zhang X., et.al (2002) has presented various approaches for efficient hardware implementation of the Advanced Encryption Standard Algorithm. This optimization method can be divided into two classes Architectural Optimization and Algorithmic Optimization.

Rajalakshmi P., et.al (2010) has presented a compact hardware-software co-design of Advanced Encryption Standards (AES) on the Field Programmable Gate Arrays (FPGA) designed for low-cost embedded systems.

Sahu A., et.al (2012) proposed a new key generation algorithm based on palm print, which is used for encryption and decryption of an image. The scheme allows one party to send a secret image to another party over the open network, even if many eavesdroppers listen, this scheme gives reliable security.

Landge I., et.al (2012) described that both color and black & white images of any size saved in tagged image file format can be encrypted and decrypted using blowfish algorithm. Histogram of encrypted images is less dynamic and significantly different from the respective histogram of the original image.

Jamgekar R.S., et.al (2013) showed that the MREA algorithm is used to encrypt files and transmit encrypted files to other where it is decrypted. The

algorithm works efficiently for small size files while it consumes time for large size of files, at an instant only one files can be encrypted and transmitted.

Khadri, S.K.A., et.al (2014) highlighted the problem and provides some possible approach to solve the problem of secure data transmission using Fibonacci series. The Encryption of data is done by combining the original data with Fibonacci numbers to get a Cipher text which is non-understandable to any intruder. Only the receiver knows the logic to do so.

Mukherjee M., et.al (2014) proposed a novel technique that encrypted the message such a ways that the message encoded as well as hidden in an image. The proposed solution is to use image cryptography to hide textual message. The proposed technique use of an encryption technique that is based on Fibonacci series & image encryption and a secret key generated from the image.

Raghu M.E., et.al (2015) proposed a method using classical cryptography to protect the data in faster way in which encryption and decryption are done in parallel using threads with the help of underlying hardware and also analyzed the time taken by sequential and parallel method.

Bairola M., et.al (2018) defined some new definition of primes like Sam prime, Adherent prime, Extreme prime and Reverse prime and use them in cryptographic system for secure communication.

Bairola M., et.al (2019) formulated new primes & proposed an algorithm for encryption & decryption for more secure cryptographic system.

4. Proposed work

Advances in technology & increasing globalization have changed the scenario and all the information / data is now available online, therefore there is a need for securing the information. Cryptography has now turned into an industry standard for providing information security, confidentiality, non-repudiation, controlling access to resources, and electronic transactions. The use of cryptography is no longer limited to just securing the vulnerable information, it is applicable worldwide.

In the proposed method, the plain text (P) or the original message is first converted into intermediate text (I) using Fibonacci primes; further, the intermediate text (I) is converted into cipher text (C) using Unicode symbols.

In the reverse process, the cipher text (C) with Unicode symbols is converted into intermediate text (I) and then converted back to plain text (P) to retrieve the original message. Since the selection of the key depends on the Fibonacci primes, it provides additional security for the system, and any unauthorized person cannot interpret the message easily.

5. Encryption algorithm

Step-1: The original message / plain text (P) is converted into ASCII values.

Step-2: Find Intermediate text (I) by using a key and Fibonacci primes.

Step-3: The obtained Intermediate values are then converted into decimal values using ASCII codes.

Step-4: Add ASCII codes of plain text (P) & Intermediate text (I).

Step-5: Use second key & Unicode symbols to get the Cipher text (C) from the decimal numbers obtained in Step-4.

Fig. 1 shows the flowchart for encryption algorithm.

Let us consider a message (Plain text) to be encrypted is "**MATH**".
Each character is replaced with another character based on the Fibonacci prime and security key chosen. Any one character from English alphabet can be chosen as a first security key to generate Intermediate text.

Plaintext (P): **MATH**
Numbers corresponding to each character using ASCII code: **77 65 84 72**
First key chosen for encryption: **e**
Sequence of characters:

e **f g** h **i** j k l m n o p **q** r s t u v w x y z a b c d e f g ……

Since there are 4 alphabets in the plain text, consider 4 Fibonacci primes: **2 3 5 13**
Consider 2^{nd}, 3^{rd}, 5^{th} & 13^{th} alphabet from the sequence of characters to get Intermediate text (I): **f g i q**

In the second level of security, the ASCII code of each character obtained from the Intermediate text (I) is added with ASCII codes of original or plain text (P) and get the decimal numbers and find the equivalent Unicode symbols for these decimal numbers.
ASCII code for each character of Intermediate text (I):

102 103 105 113

Add ASCII codes of original or plain text (P) and Intermediate text (I), we get:

179 168 189 185

These decimal numbers obtained are now converted into equivalent Unicode symbols (U). The corresponding Unicode symbols (U) are:

31 37 39 31 36 38 31 38 39 31 38 35

Since all 4 Unicode symbols contains 3 numbers each, therefore the second key is **4x3**, which will help to separate the Unicode symbols.

The Cipher text (C) is: **31 37 39 31 36 38 31 38 39 31 38 35**

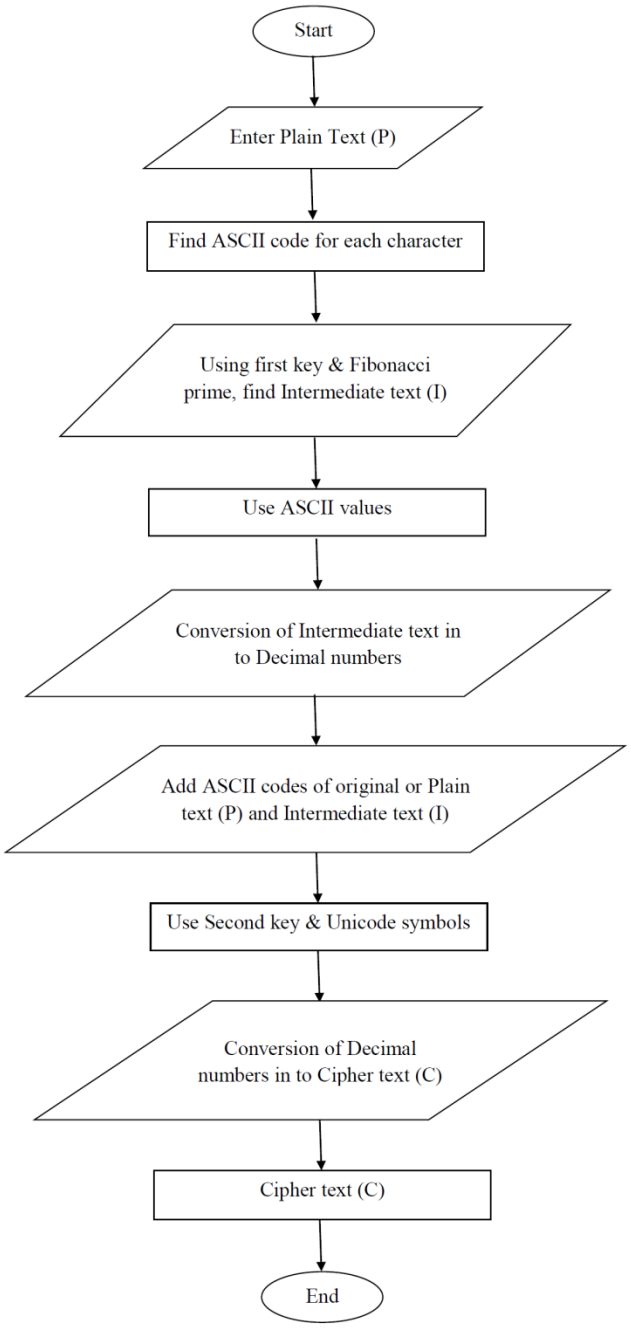

Fig. 1 Flowchart for encryption algorithm

6. Decryption algorithm

Decryption is the reverse method of encryption with the help of two keys.

Step-1: Firstly, transform the cipher text (C) into decimal values using second key & Unicode symbols.

Step-2: Obtain Intermediate text (I) using first key & Fibonacci primes.

Step-3: Find the decimal values for each character of Intermediate text (I) using ASCII code.

Step-4: Now subtract the decimal values obtained in Step-3 from the decimal values obtained in Step-1.

Step-5: Find the plain text (P) by converting values obtained in Step-4 using ASCII codes.

Fig. 2 shows the flowchart for decryption algorithm.

The Cipher text (C) is: **31 37 39 31 36 38 31 38 39 31 38 35**
Second key is: **4x3**

This key indicates that separate the whole Cipher text in 4 Unicode symbols contains 3 numbers each, for obtaining the Unicode symbols (U)

31 37 39 31 36 38 31 38 39 31 38 35

Decimal numbers (ASCII values) corresponding to these Unicode symbols as:

179 168 189 185

First key is: **e**
First 4 Fibonacci primes: **2 3 5 13**
Sequence of characters:

e **f g** h **i** j k l m n o p **q** r s t u v w x y z a b c d e f g ……

The Intermediate text (I) is: **f g i q**
ASCII code for each character of Intermediate text (I):

102 103 105 113

For obtaining plain text, subtract the ASCII values of Intermediate text (I) from ASCII values corresponding to Unicode symbols, we get

77 65 84 72

Original or Plain text (P): **MATH**

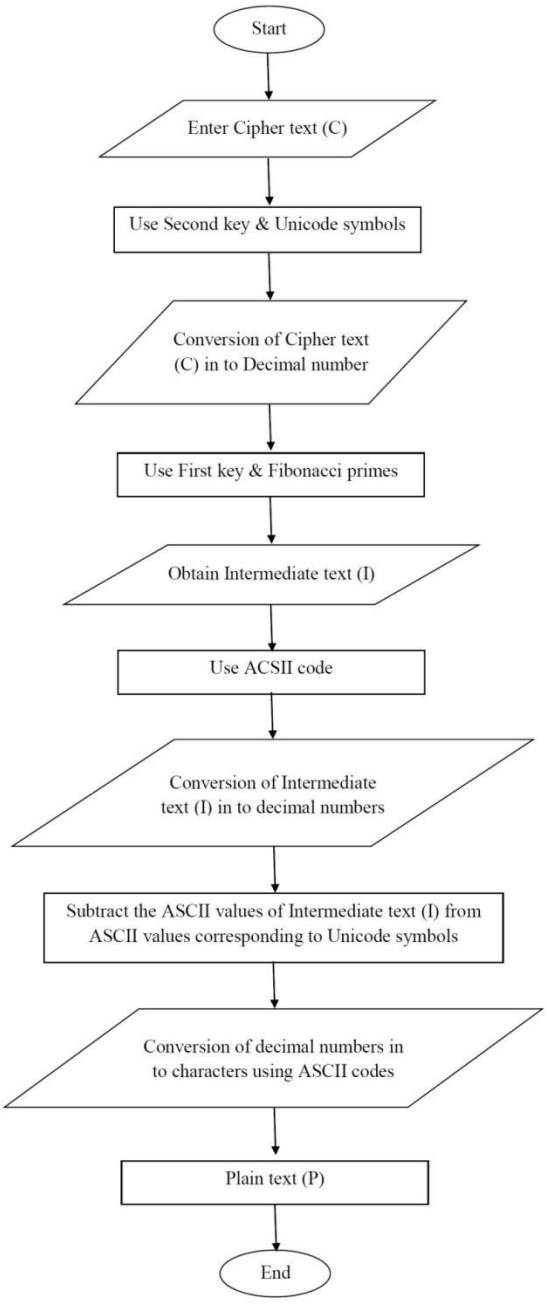

Fig. 2 Flowchart for decryption algorithm

7. Conclusion

This paper proposes a method to hide data, establish credibility and prevent unauthorized use. In addition, this paper presents a technique that can transfer enormous amounts of secret data with high level of security between two parties. Every text data form can be viewed as a hidden message and transmitted via the open channel. This suggested strategy is, in short, very safe and easy to implement. The encryption algorithm being used can produce a different output each time it is used, based on the key selected, which also increases the level of security of data. The advantage of this paper is to make information transmission secure in a mentioned criterion by encrypting it. The application instead of sending the message / file converts it into a file and transmits it and saves time encrypting all written strings on that file. In the next step at the receiver's end, the file is decrypted only if the person knows the decryption key and feeds it into the system giving him access to the file.

References

1. Zhang X. & Parhi K.K., "*Implementation of Approached for the Advanced Encryption Standard Algorithm*", IEEE (2002).
2. Rajalakshmi P., "*Hardware-software co-design of AES on FPGA*", International Conference of Advanced Study in Computing, Communications and Informatics, (2010), pp: 1118–1122.
3. Sahu A., Bahendwar Y., Verma S. & Verma P., "*Proposed Method of cryptographic Key Generation for Securing Digital Image*", International Journal of Advanced Research in Computer Science and Software Engineering, Vol.2, Issue 10, October (2012).
4. Landge I., Contractor B., Patel A. & Choudhary R., "*Image Encryption and Decryption using Blowfish Algorithm*", World Journal of Science and Technology (2012), 2(3), pp: 151-156.
5. Jamgekar R.S. & Joshi G.S., "*File Encryption and Decryption using Secure RSA*", International Journal of Emerging Science and Engineering (IJESE), Vol.1, Issue-4, February (2013), pp: 11-14.
6. Khadri, S.K.A., Samanta, D. & Paul, M., "*Approach of Message Communication Using Fibonacci series: In Cryptology*", Engineering and Technology Publications", Vol.2, No.2, (2014), pp: 168-171.
7. Mukherjee, M. & Samanta, D., "*Fibonacci Based Text Hiding Using Image Cryptography*", Lecture Notes on Information Theory, Vol.2, No.2, (2014), pp: 172-176.
8. Raghu M.E. & Ravishankar K.C., "*Application of Classical Encryption Techniques for Securing Data – A Threaded Approach*", International Journal on Cybernetics and Informatics (IJCI), Vol.4, No.2, April (2015), pp: 125-132.
9. Bairola, M. & Uniyal, A.S., "*Application of Advanced Cryptographic System*", International Journal of Mathematics Trends and Technology (IJMTT), ISSN: 2231-5373, Vol.55 (4), (2018), pp: 311-316.

10. Bairola, M., Agarwal, S. & Uniyal, A.S., "*Application of Prime Numbers in Cryptographic System*", Book Chapter in "Paradigm Shift in Management Practices for Fostering Excellence" New Delhi Publishers, New Delhi, ISBN: 978-93-86453-92-1, (2019), pp: 246-251.

[1]**AKANSHA AGARWAL**: RESEARCH SCHOLAR, DEPARTMENT OF MATHEMATICS, IFTM UNIVERSITY, MORADABAD, 244102, INDIA
Email Address: ***agw.akansha@gmail.com***

[2]**DR. SHUBHAM AGARWAL**: ASSOCIATE PROFESSOR, DEPARTMENT OF MATHEMATICS, NEW DELHI INSTITUTE OF MANAGEMENT, NEW DELHI, 110062, INDIA
Email Address: ***meshubhamagarwal@gmail.com***

[3]**DR. B.K. SINGH**: PROFESSOR, DEPARTMENT OF MATHEMATICS, IFTM UNIVERSITY, MORADABAD, 244102, INDIA
Email Address: ***drbksingh@iftmuniversity.ac.in***