# PERFORMANCE ANALYSIS OF SECURED COMMUNICATION WITH CRYPTOGRAPHY USING FIBONACCI SERIES

MS. NAMITA GEORGE GONSALVES
Department of Information Science & Engineering, KLS's Gogte Institute of Technology, Belagavi-590008.

MS. NOOTANA G BHAT
Department of Information Science & Engineering, KLS's Gogte Institute of Technology, Belagavi-590008.

PROF.KIRAN K TANGOD
Asst. Prof., Department of Information Science & Engineering, KLS's Gogte Institute of Technology, Belagavi-590008.

## ABSTRACT

Data security has been a major concern in the today's information technology era. Especially it becomes serious in the cloud environment because the data is located in different places all over the world. Encryption has come up as a solution and different encryption algorithms play an important role in data security on cloud. Encryption algorithms are used to ensure the security of data in cloud. The purpose of securing data is that only concerned and authorized users can access it. In this paper we describes the basic characteristics (Key Length, File size) of symmetric Fibonacci Cryptography, Asymmetric RSA algorithms.

**KEYWORDS:** Encryption, Decryption, Symmetric key, Asymmetric key,Key length.

## INTRODUCTION

In today's world of the Internet, everything is going online, from grocery shops to clothing, to consumer electronics and real estate. There is a need of securing data on the fly, hence we use cryptography. There are numerous ways of cryptography, each having its own advantages and disadvantages. The cryptography implemented here will be using a unique technique called encryption-decryption with Fibonacci number series.

The proposed method will be more concerned with a technique of encoding the text in such a way that the recipient can only discover the original message. The original message usually called plain text is converted into cipher text by finding each character in the message and replacing it with another character based on the Fibonacci number generated. Further cipher text is converted into Unicode symbols, which avoid suspicion from the third party when sent through an unsecured communication channel.

## CRPTOGRAPHY ALGORITHMS

Cryptography means "secret writing" which is the science and art of transforming messages to make them secure and immune to attacks by unauthorized user. The original data/message, before being transformed is called cipher text. An encryption is a process to transform the plaintext into cipher text and decryption transforms the cipher text back into plaintext. The sender uses an encryption algorithm and the receiver uses a decryption algorithm. Thus, encryption and decryption help to secure transmission of the message and protect the message from unauthorized users [1][16].

There are three types of cryptography algorithm that are given below [2] [3]:

- Symmetric key cryptography algorithm
- Asymmetric key cryptography algorithm

## 1.1 SYMMETRIC (SECRET) KEY CRYPTOGRAPHY

This cryptographic method uses of two different algorithms for encryption and decryption respectively, and a same key is used both the sender and the receiver. The sender uses this key and an encryption algorithm to encrypt data, the receiver uses the same key and the corresponding decryption algorithm to decrypt that data [4] [5].

## FIBONACCI CRYPTOGRAPHY

Fibonacci Cryptography uses Fibonacci series to encrypt and decrypt messages. It uses same key to encrypt and decrypt the message. Key length doesn't affect the performance of algorithm.

## 1.2 ASYMMETRIC (PUBLIC) KEY CRYPTOGRAPHY

Asymmetric (public) Key Cryptography This cryptographic method makes use of two different algorithms for encryption and decryption respectively, a public key for encryption and a private key for decryption. The public key of the sender is used to encrypt the message by the sender. The receiver decrypts the cipher text with the help of a private key.

RSA

RSA (Rivest-Shamir-Adleman) is broadly used an asymmetric encryption /decryption algorithm which involves a public key and a private key. The public key can be informed to everyone and is used for encrypting messages. Messages encrypted with the public key can only be decrypted using the private key. It secured user data assimilate encryption before to storage, user authentication procedures prior to storage or retrieval, and making secure channels for data transmission [6] [7] [8] [9][16]. 4096 bit key size is used for execution of RSA algorithm.

## ALGORITHM

### 3.1 ENCRYPTION

Step 1: Enter Plain text.
Step 2: Key generated automatically using random function.
Step 3: Digits in key are summed and kept in sum.
Step 4: If sum<=26 then it will take corresponding lower case alphabet else go to step 4.
Step 5: If sum >27 then sum=sum % 26 and take corresponding alphabet.
Step 6: Generate fibonacci series for number of characters present in plain text starting from 1,2....
Step 7: Take key as first letter in cipher.
Step 8: Consider fibonacci series and jump number of letters and add it in cipher.
Step 9: For each letter in cipher take acsii value of that letter and add ascii value previous and after that letter. To that sum add ascii value of respective character of plain text.
Step 10: Compare the sum obtained in step 8 with the decimal to unicode symbol table.
Step 11: Then put the unicode symbol in cipher text.
Step 12: Continue from step 9 for all the characters in plain text.
Step 13: Stop.

### 3.2 DECRYPTION

Step 1: Take cipher text.
Step 2: For each unicode symbol present in cipher text
find its decimal value from decimal to unicode symbol.
Step 3: Generate fibonacci series from 1,2,...
Step 4: Extract key from cipher text.
Step 5 : Take key as first letter in cipher.
Step 6:Consider fibonacci series and jump number of letters and add it in cipher.
Step 7: Take decimal value of each unicode symbol in the cipher text.
Step 8: The ascii value of the key and ascii value of letter previous and after the key are added and this sum is substracted from decimal value obtained in step 7.
Step 9: The result obtained is the ascii value of each character of plain text.
Step 10: Continue from step 8 for all unicode symbols in cipher text.
Step 11: Stop.

## EXPERIMENTAL METHODOLOGY & ENVIRONMENT

In this experimental performance analysis of the given algorithms on the basis of the following parameters on local system at different input size. In this section describes the experimental parameters and platforms.

## 1.3 EVALUATION PARAMETERS

Performance of encryption algorithm is evaluated considering the following parameters.

1. Encryption Time: The encryption time considered the time that an encryption algorithm takes to produces a cipher text from a plain text.
2. Decryption Time: The decryption time considered the time that a decryption algorithm takes to produces a plain text from a cipher text.

## 1.4 EVALUATION PLATFORMS

Performance of encryption algorithm is evaluated considering the following system configuration.

**1. Software Speciation:** Experimental evaluation on Visual Basic.Net with MySQL Server, Windows 7 64bit Operating System.

**2. Hardware Speciation**: 2 PC's with min 1 GB RAM and Windows Operating System, 50 MB of space on the Linux based cloud server.

## EXPERIMENTAL RESULTS AND ANALYSIS

Experimental results for encryption and decryption for Fibonacci cryptography and RSA is shown in table 4.1 and 4.2[14][15].The algorithms are compared for different file sizes(bytes,kb) and time taken. Time taken for different key lengths by Fibonacci cryptography are measured.

**TABLE 4.1- Performance comparison for Rsa and fibonacci cryptography of file seize in bytes.**

| File Size (bytes) | RSA (SEC) | FIBONACCI(SEC) |
|---|---|---|
| 10 | 8.997 | 0.004 |
| 15 | 12.504 | 0.006 |
| 20 | 14.566 | 0.007 |
| 30 | 19.601 | 0.008 |
| 60 | 31.353 | 0.038 |

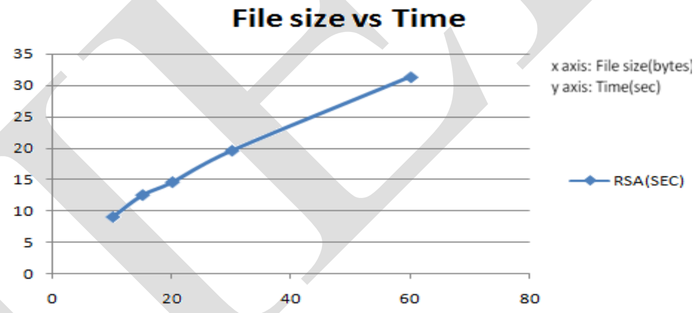

**Fig 4.1.1. Time taken by RSA algorithm for filesize in bytes.**

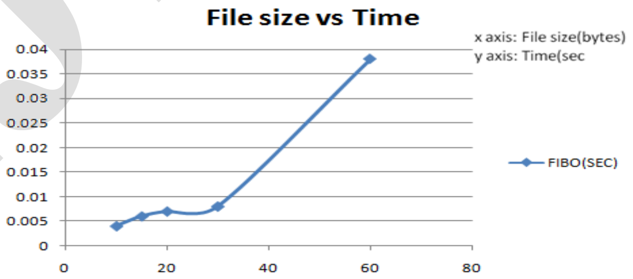

**Fig 4.1.2. Time taken by RSA algorithm for filesize in bytes**

**Table 4.2- performance comparison for rsa and fibonacci cryptography of filesize in kb.**

| File Size(kb) | RSA(SEC) | FIBONACCI(SEC) |
|---|---|---|
| 10 | 56 | 0.656 |
| 14 | 62 | 2.271 |
| 20 | 68 | 3.722 |
| 24 | 74 | 5.174 |
| 30 | 82 | 7.965 |

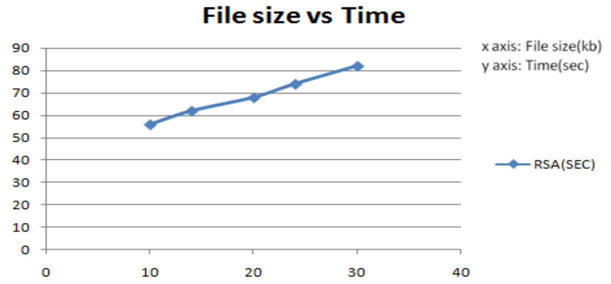

Fig 4.2.1. Time taken by RSA algorithm for filesize in kb.

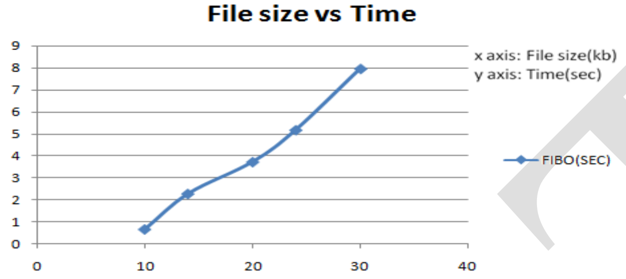

Fig 4.2.2. Time taken by RSA algorithm for filesize in kb.

Table 4.3- comparison of different key length for fibonacci cryptography

| KEY LENGTH(bits) | TIME(sec) |
|---|---|
| 16 | 0.002 |
| 32 | 0.002 |
| 64 | 0.002 |
| 128 | 0.002 |

## CONCLUSION

Cryptography has evolved from an ancient science to an important area of research to secure communications. It has evolved from simple substitution ciphers to quantum cryptography. This method provides the means and methods of hiding data, establishing its authenticity, and preventing its undetected modification or unauthorized use. In this algorithm key is generated automatically and also hidden in cipher text which provide confidentiality and reduces the large burden for user. From result analysis we conclude that time taken for Fibonacci cryptography is less than RSA algorithm.

## REFERENCES

1) Mudassar Aslam, Christian Gehrmann, Mats Bj¨orkman, *"Security and Trust Preserving VM Migrations in Public Clouds", Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference, Liverpool, 25-27 June 2012, pp 869 - 876, Print ISBN: 978-1-4673-2172-3, DOI: 10.1109 /TrustCom.2012.256.*

2) S C Rachana, Dr. H S Guruprasad, "*Emerging Security Issues and Challenges in Cloud Computing", International Journal of Engineering Science and Innovative Technology (IJESIT), Volume 3, Issue 2, March 2014, and ISSN: 2319-5967.*

3) Shakeeba S.Khan , Prof.R.R. Tuteja, "*Security in Cloud Computing using Cryptographic Algorithms", International Journal of Innovative Research in Compute and Communication Engineering, Vol. 3, Issue 1, January 2015.*

4) Omer K. Jasim, Safia Abbas, El-Sayed M. El-Horbaty and Abdel-Badeeh M. Salem, "*Efficiency of Modern Encryption Algorithms in Cloud Computing", International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), Volume 2, Issue 6, November – December 2013 ISSN 2278-6856.*

5) Rachna Arora, Anshu Parashar, “*Secure User Data in Cloud Computing Using Encryption Algorithms”, Rachna Arora, Anshu Parashar / International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 Vol. 3, Issue 4, Jul-Aug 2013, pp.1922-1926.*

6) Priyanka Arora, Arun Singh, Himanshu Tyagi *“ Evaluation and Comparison of Security Issues on Cloud Computing Environment” in World of Computer Science and Information Technology Journal (WCSIT) ISSN: 2221-0741 Vol. 2, No. 5, 179-183, 2012.*

7) Kalpana Parsi, Singaraju Sudha. *”Data Security in Cloud Computing using RSA Algorithm”. International Journal of Research in Computer and Communication technology, IJRCCT, ISSN 2278-5841, Vol 1, Issue 4, September 2012. pp. 145.*

8) Sunitha K, Prashanth K.S. “*Enhancing Privacy in Cloud Service Provider Using Cryptographic Algorithm”. IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 12, Issue 5 (Jul. - Aug. 2013). pp. 64.*

9) A. Dharini, R.M. Saranya Devi, and I. Chandrasekar, *“Data Security for Cloud Computing Using RSA with Magic Square Algorithm”, International Journal of Innovation and Scientific Research ISSN 2351-8014 Vol. 11 No. 2 Nov. 2014, pp. 439-444.*

10) Performance Analysis of Different Cryptography Algorithms, Md. Alam Hossain, Md. Biddut Hossain, Md. Shafin Uddin, Shariar Md. *Imtiaz Computer Science and Engineering Department, Jessore University of Science & Technology, Bangladesh.*

11) *Secured Communication through Fibonacci Numbers and Unicode Symbols, International Journal of Scientific & Engineering Research*, A . Joseph Raphael & Dr. V. Sundaram. Volume 3, Issue 4, April-2012 1 ISSN 2229-5518 4.

12) *Data Encryption through Fibonacci Sequence and Unicode Characters, MIT International Journal of Computer Science and Information Technology*, Prachi Agarwal, Navita Agarwal & Richa Saxena,Vol. 5, No. 2, August 2015, pp. 79-82 79 ISSN 2230-7621©MIT Publications.

13) *On The Information Security Using Fibonacci Series, International Conference and Workshop on Emerging Trends in Technology* (ICWET 2011) – TCET, Mumbai, IndiaB. S.Tarle& G. L. Prajapati

14) *A study and performance analysis of RSA Algorithm. M. Preetha, M. Nithya,Computer Science & Application & Periyar University, India* IJCSMC, Vol. 2, Issue. 6, June 2013, pg.126 – 139.

15) *Analysis of Cryptography Techniques* Prof Shivani Desai, Yamini Rathod Nirma University, INDIA, March-Sep 2014 pp.61-62 ISSN-0973-7391.

16) *Md. Alam Hossain, Md. Biddut Hossain, Md. Shafin Uddin, Shariar Md. Imtiaz, Performance Analysis of Different Cryptography Algorithms, International Journal of Advanced Research in Computer Science and Software Engineering, Computer Science and Engineering Department*, Jessore University of Science & Technology, Bangladesh, Volume 6, Issue 3, March 2016.