# A Novel Approach For Information Security With Automatic Variable Key Using Fibonacci Q-Matrix

[1]SHALIGRAM PRAJAPAT, [2]AMBER JAIN & [3]RAMJEEVAN SINGH THAKUR

International Institute of Professional Studies, D. A. University, Indore (MP), India
Computer Applications Department MANIT, Bhopal (MP), India
E-mail : shaligram.prajapat@gmail.com, i.amber.jain@gmail.com, ramthakur2000@yahoo.com

**Abstract** - **I**nformation security is essential nowadays. Large number of cipher generation and decryption algorithms exists and are being evolved due to increasing demand of users and e-commerce services. In this paper we propose a new approach for secure information transmission over communication channel with key variability concept in symmetric key algorithms using Fibonacci Q-matrix. Proposed approach will not only enhance the security of information but also saves computation time and reduces power requirements that will find it's suitability for future hand held devices and online transaction processing.

***Keywords****-cipher; key; encryption; decryption; fibonacci; Q- matrix;, symmetric key algorithm, automatic variable key*.

## I. INTRODUCTION

Information security plays a pivotal role nowadays. The requirement of information security is increasing because of widespread use of distributed systems, network and communication facilities for carrying information between terminal user and computer and between computer and computer [1]. Hence to provide confidentiality authentication, integrity and non-repudiation, information security has evolved.

Large number of algorithms and techniques are designed for secure transmission of data. Cryptographic algorithms play a central role in information security systems. There are two general types of key-based algorithms: Symmetric and Asymmetric algorithms. *Symmetric algorithms* (also called secret-key algorithms) are algorithms where the encryption key can be calculated from the decryption key and vice versa. In most symmetric algorithms, the encryption and decryption key are the same. Both the sender and receiver agree on a key before they can communicate securely. On the other hand, in *Asymmetric algorithms* (also called public-key algorithms) the decryption key cannot be calculated from the encryption key. So, keys play an important role in the security of any cryptographic algorithm. If weak key is used in algorithm, then any intruder may decrypt the data. One of the central factors contributing to the strength of symmetric key algorithms is the size of key used. In practice, most state-of-art cryptographic algorithms rely on increasing the key size to strengthen the security of algorithm [2]. In this paper, we instead focus for power efficient and fast algorithm based on varying the key to increase the security of algorithm.

## II. RELATED WORK

Symmetric algorithms can be divided into two types: Block ciphers and Stream ciphers. *Block cipher* processes the input one block of element at a time, producing an output block for each input block. *Stream ciphers* process the input element continuously, producing output one element at a time, as it goes along. In [1, 2, 3, 6], various cryptographic algorithms [see fig. 1] and their applications have been defined and discussed.

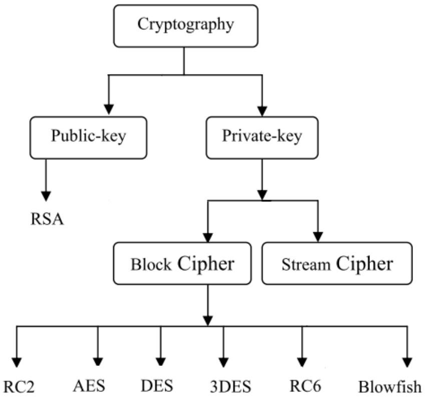

**Figure 1: Overview of field of cryptography**

Some symmetric block cipher algorithms are summarized in the Table 1. Literature survey reveals that cryptographic algorithms are improving with time. Asymmetric algorithms are almost 1000 times slower than symmetric algorithms, because they require more computational processing power [4].

Table 1: Summary of some symmetric block cipher algorithms

| S. No. | Algorithm | Block size | Key length |
|---|---|---|---|
| 1 | DES | 64 bits | 56 bits |
| 2 | 3DES | 64 bits | 168, 112 or 56 bits |
| 3 | RC2 | 64 bits | 8-128 bits (variable length key) |
| 4 | Blowfish | 64 bits | 32-448 bits (variable length key) |
| 5 | AES | 128 bits | 128, 192 or 256 bits |
| 6 | RC6 | 128 bits | 128, 192 or 256 bits |
| 7 | RSA | - | 1024-2048 bits (variable key length) |

A study was performed for analyzing the performance of security algorithms by varying the key size. The effect of changing the key size on power consumption in shown in Fig. 2 and Fig. 3 [5].

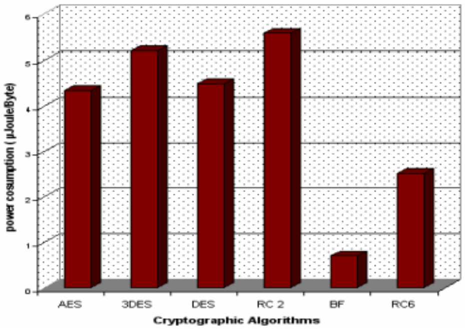

**Fig. 2: Power consumption to encrypt different text document file [5]**

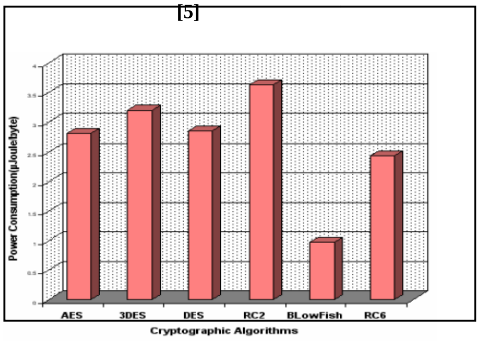

**Fig. 3: Power consumption to encrypt different text document files [5]**

The effect of changing the key size of AES (symmetric algorithm) on computation time in shown in Fig. 4.

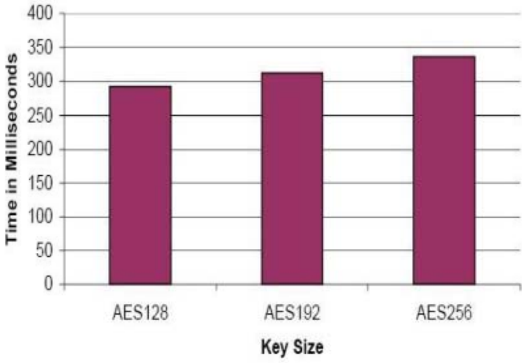

**Figure 4: Time consumption for different key size for AES [4] The effect of changing the key size of RC6 (symmetric algorithm) on computation time in shown in Fig. 5.**

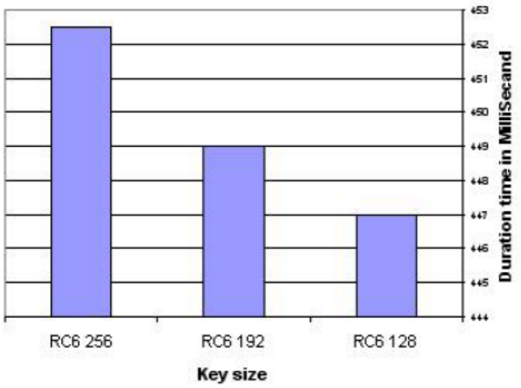

**Figure 5: Time consumption for different key size for RC6 [4]**

It was shown that larger key sizes lead to increase in computation time and battery power consumption.

*Reversible functions* are backbone of symmetric key algorithms. Many well known symmetric algorithm have been proposed using reversible *XOR* function. Stakhov proposed a coding/decoding system based on Fibonacci Q-matrix [8]. The Q-matrix is based on following concepts:

*A) Fibonacci-Number*

The Fibonacci numbers are obtained by following recursive function:

$$F_n = n \qquad \text{if } n = 0 \text{ or } n = 1$$

$$F_n = F_{n-1} + F_{n-2} \qquad \text{if } n > 1 \qquad (1)$$

*B). Fibonacci Q-Matrix*

$$Q = \begin{bmatrix} F_2 & F_1 \\ F_1 & F_0 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \qquad (2)$$

where Det(Q) = –1.

The nth power of this Q-Matrix can be computed as follows:

$$Q^n = \begin{bmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{bmatrix} \qquad (3)$$

where $F_{n-1}$, $F_n$ and $F_{n+1}$ are Fibonacci numbers.

Since $\quad \mathrm{Det}(A^n) = (\mathrm{Det}\ A)^n$

Therefore, $\mathrm{Det}(Q^n) = (-1)^n$ where $n \in N$ (4)

Following identity connects three neighboring Fibonacci numbers:

$$F_{n-1} + F_n + F_{n+1} = (-1)^n \qquad (5)$$

Also, $\quad Q^n = Q^{n-1} + Q^{n-2}$ (6)

$\Rightarrow \quad Q^{n-2} = Q^n - Q^{n-1}$ (7)

where:

$$Q^{-n} = \begin{bmatrix} F_{n-1} & -F_n \\ -F_n & F_{n+1} \end{bmatrix} \qquad (8)$$

*C). Fibonacci encryption/decryption algorithm:*

The concept of Fibonacci Q-matrices allows us to develop a symmetric algorithm. This algorithms assumes an initial message in the form of square matrix M of size (p+1) x (p+1) where p = 0, 1, 2, 3,…. Now choose the Fibonacci $Q_p$-matrix, $Q_p^n$, of size (p+1) x (p+1) as a encryption (key) matrix and it's inverse matrix, $Q_p^{-n}$, of the same size as decryption (key) matrix. Therefore, the encryption and decryption are defined by parameters n and p.

*Encryption algorithm:*

```
Algorithm encrypt(M)
    1. Choose n
    2. Choose p
    3. Compute $Q_p^n$
    4. E ← M x $Q_p^n$        // Compute Cipher text
    5. End of algorithm
```

The working of above symmetric key encryption algorithm based on classical Q-matrix is beautifully illustrated in [8] and [9].

*Step 1:* Let plain text message is :

$$M = \begin{bmatrix} m_1 & m_2 \\ m_3 & m_4 \end{bmatrix}$$

Where $m_i > 0$; i = 1, 2, 3, 4.

*Step 2:* Choose n = 6 and p = 1 such that

$$Q^6 = \begin{bmatrix} 13 & 8 \\ 8 & 5 \end{bmatrix}$$

*Step 3:*

$$M \times Q^6 = \begin{bmatrix} m_1 & m_2 \\ m_3 & m_4 \end{bmatrix} \times \begin{bmatrix} 13 & 8 \\ 8 & 5 \end{bmatrix} = \begin{bmatrix} 13m_1 + 8m_2 & 8m_1 + 5m_2 \\ 13m_3 + 8m_4 & 8m_3 + 5m_4 \end{bmatrix}$$

This implies that,

$$e_1 = 13m_1 + 8m_2$$
$$e_2 = 8m_1 + 5m_2$$
$$e_3 = 13m_3 + 8m_4$$
$$e_4 = 8m_3 + 5m_4$$

*Decryption algorithm:*

```
Algorithm decrypt (n, p, E)
    1. Compute $Q_p^{-n}$
    2. M ← E x $Q_p^{-n}$     // Generate Plain text.
    3. End of algorithm
```

A. P. Stakhov et al [8, 9] explained the decryption process as follows:

*Step 1:* Received encoded message is represented in the matrix form

$$E = \begin{bmatrix} e_1 & e_2 \\ e_3 & e_4 \end{bmatrix}$$

*Step 2:* Compute the reversible decryption function:

$$Q^{-6} = \begin{bmatrix} 5 & -8 \\ -8 & 13 \end{bmatrix}$$

*Step 3:* Recover plain text

$$M = \begin{bmatrix} m_1 & m_2 \\ m_3 & m_4 \end{bmatrix} = \begin{bmatrix} e_1 & e_2 \\ e_3 & e_4 \end{bmatrix} \times \begin{bmatrix} 5 & -8 \\ -8 & 13 \end{bmatrix}$$

Above algorithm has been analyzed, implemented and tested [10] and they concluded that the algorithm works faster than symmetric algorithms (including DES, 3DES, AES and Blowfish).

In this paper, the idea of time varying key (using Fibonacci Q-matrix) has been suggested. Very little work has been done in this direction. P. Chakrabarti et al [7] proposed some approaches which are yet to be investigated experimentally.

## III. PROPOSED METHOD

In this section we propose a technique where the key is made to vary from session to session. Hence even if the cryptanalyst gains the key of previous session, it would be theoretically impossible for extracting the original message in next session. We also enhance the security of algorithm based on the *automatic key variability* concept applied on the message based on Fibonacci function. Sender uses Fibonacci Q-matrix, with automatic variable key, to generate cipher text. Receiver can then apply inverse operation of this Fibonacci Q-Matrix to decipher to recover original message [8]. The scope and beauty of this Fibonacci function is that it is a reversible function (similar to XOR). Reversible functions are needed for successful operation of symmetric algorithms. So, the main focus is on the investigation of such reversible function.

*Automatic Variable symmetric Key using Fibonacci Q- matrix:*

From previous discussion it can be seen that Fibonacci Q-matrix is a powerful technique for securing input data and files of varying content and sizes. And as we have pointed out that state-of-art practices (for increasing the security of information transmission) rely on increasing the key size that consumes time and thus requiring more computation power as well as battery power. We claim here that Fibonacci Q-matrix can be used as reversible function and it can be used for automatic variability of key. The Q matrix at a particular session of given n and p values contains $F_{n-1}$, $F_n$ and $F_{n+1}$. Thus for one session the sender and receiver not only have the key of current session but also probable keys of previous and next session. Here key (n, p) is made to vary from session to session hence even if the intruder gets unwanted access to the key of session i, it would not be valid for original message extraction in session i+1 onwards. This enhances the security of algorithm and using the reversibility of Fibonacci Q-Matrix the receiver will receive the data correctly after the application of $Q_p^{-n}$. Further performance enhancement can be made in the symmetric key exchange over traditional ones that instead of exchanging entire key over communication channel, we pass the parameters only.

## IV. FUTURE WORK AND SCOPE.

In this paper we presented a model for investigation of cipher generation technique based on variability concept in Fibonacci Q-matrix. The design of alternative approaches for symmetric key algorithms based on variability of key instead of increasing key size is the biggest challenge, It's vulnerability from intruders point of view may be another direction in this regards.

## ACKNOWLEDGMENT

We would like to thank Dr. P. Chakrabarti for their valuable suggestions, support and guidance. This work is supported by research grant from MANIT, Bhopal, India under Grants in Aid Scheme 2010-11, No. Dean(R&C)/2010/63 dated 31/08/2010.

## REFERENCE:

[1] S. William and Stalling, Cryptography And Network Security, 4/E. Pearson Education India, 2006.

[2] B. Schneier, Applied cryptography: protocols, algorithms, and source code in C. Wiley, 1996.

[3] Maxime Fernández1, Gloria Diaz1, Alberto Cosme1,Irtalis Negrón1, Priscilla Negrón1, Alfredo "Cryptography: algorithms and security applications" The IEEE Computer Society's Student Fall 2000 Vol. 8 No. 2.

[4] D. S. A. Elminaam, H. M. A. Kader, and M. M. Hadhoud, "Performance Evaluation of Symmetric Encryption Algorithms," International Journal of Computer Science and Network Security, vol. 8, no. 12, pp. 280–286, 2008.

[5] D. S. A. Elminaam, H. M. A. Kader, and M. M. Hadhoud, "Performance Evaluation of Symmetric Encryption Algorithms on Power Consumption for Wireless Devices," International Journal of Computer Theory and Engineering, vol. 1, no. 4, pp. 1793–8201, 2009.

[6] M. Hellman, "An overview of public key cryptography," IEEE Communications Magazine, vol. 16, no. 6, pp. 24–32, 1978.

[7] P. Chakrabarti, B. Bhuyan, A. Chowdhuri, and C. Bhunia, "A novel approach towards realizing optimum data transfer and Automatic Variable Key (AVK) in cryptography," IJCSNS, vol. 8, no. 5, p. 241, 2008.

[8] Stakhov A.P., "Fibonacci matrices, a generalization of the 'Cassini formula', and a new coding theory," Chaos, Solitons & Fractals, vol. 30, no. 1, pp. 56–66, Oct. 2006.

[9] A. NALLI, "On the Hadamard Product of Fibonacci Qn matrix and Fibonacci Q- n matrix," Int. J. Contemp. Math. Sciences, vol. 1, no. 16, pp. 753–761, 2006.

[10] A. Nadeem and M. Y. Javed, "A performance comparison of data encryption algorithms," in Information and Communication Technologies, 2005. ICICT 2005. First International Conference on, 2005, pp. 84–89.

◈◈◈