ISSN: 2349-5197
Impact Factor: 2.715

INTERNATIONALJOURNALOFRESEARCH SCIENCE& MANAGEMENT

A NOVEL ENCRYPTION AND DECRYPTION SCHEME FOR DIGITAL SIGNALS USING BERNSTEIN POLYNOMIALS

Omar M. Barukab[*1] and S. H. Behiry[2]
[*1]Depratment of Information Technology, Faculty of Computing and Information Technology
[2]Department of Computer Science, Faculty of Computing and Information Technology

DOI: 10.5281/zenodo.546860

Keywords: Bernstein polynomial, encryption, decryption, nonsingular matrix, invertible matrix, Moore machine.

Abstract

The security of communications and electronic commerce in the digital era relies heavily on the modern incarnation of the ancient art of code and different forms of ciphers. Mathematics play the main rule in this realm. In this paper, a novel encryption scheme is proposed. It is mainly based on the usage of long key size and the incorporation of recurrence relations in conjunction with Moore finite state machine. In addition, the usage of Bernstein polynomial in accomplishing the encryption and decryption represents an additional layer of security to the proposed encryption scheme.

Introduction

Cryptography aims at hiding the meaning of the message from intruders except the intended receiver. Cryptanalysis aims at breaking the encrypted message to reveal its contents. The study of cryptography and cryptanalysis comes under cryptology. Due to the need of distance communication, cryptographic primitives were employed to realize message secrecy. Figure 1 depicts a generalized model of encryption and decryption process [1]. In this paper, we present a novel encryption and decryption scheme based on the utilization of Bernstein polynomials, recurrence relations and Moore finite state machine. It is similar to a work done in [2] which uses Moore machine in conjunction with recurrence relations. The only difference is the augmentation of using Bernstein polynomials to the techniques used in the former work accomplished in [2]. The aim is to accomplish both encryption and decryption of digital signals while in transient to their destination. The paper is organized as follows. Section 2, presents some notations adopted in this research work. Section 3, presents the literature review. Section 4 introduces Bernstein polynomials and Moore finite state machine. Section 5, presents a reproduced version of the first example presented in [2]. Section 6, presents an illustrative example of the new proposed encryption scheme. Section 7, deals with the performance issues of the new proposed scheme, while section 8 presents the conclusion and discusses future work.

ISSN: 2349-5197
Impact Factor: 2.715
INTERNATIONAL JOURNAL OF RESEARCH SCIENCE & MANAGEMENT

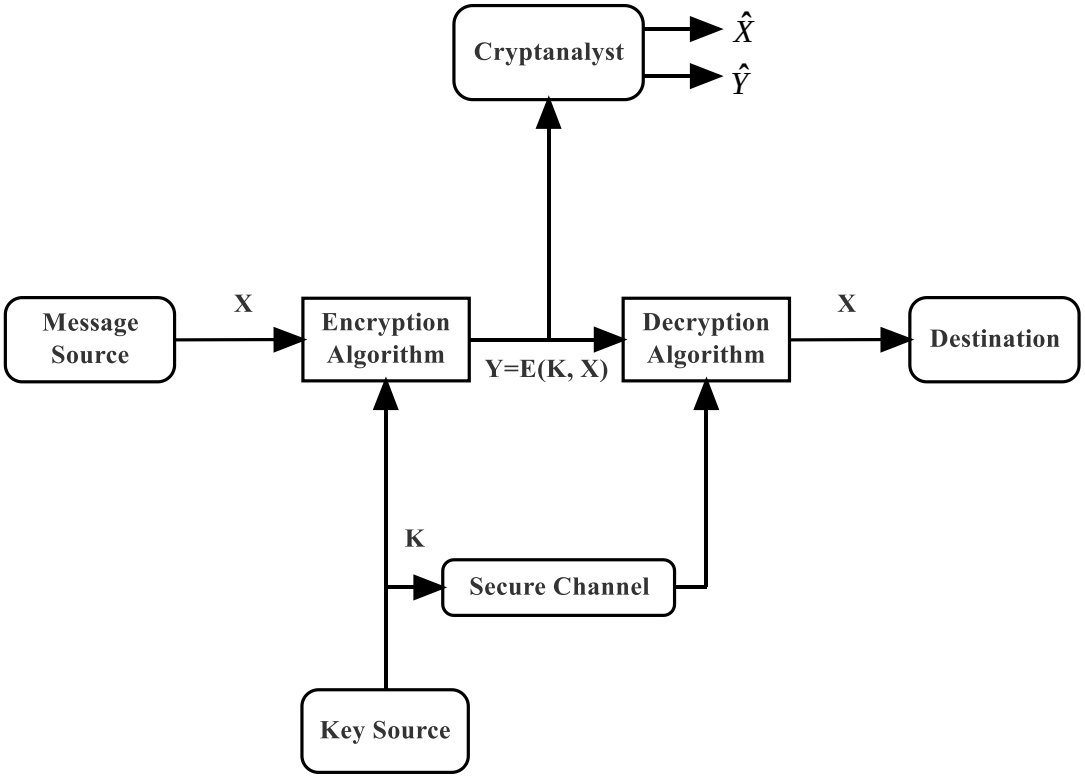

Fig. 1: Model of Symmetric Cryptography

Notations

The notations adopted in this paper will as follows:

p represents the pliantext message,
k_n n – bits key used for encryption,
⇒ secrure channel,
R_n recurrence relation.

With the adoption of the above notation, Fig. 1 can be modified accordingly by to reflect the notations used as shown in Fig. 2.

ISSN: 2349-5197
Impact Factor: 2.715
INTERNATIONAL JOURNAL OF RESEARCH SCIENCE & MANAGEMENT

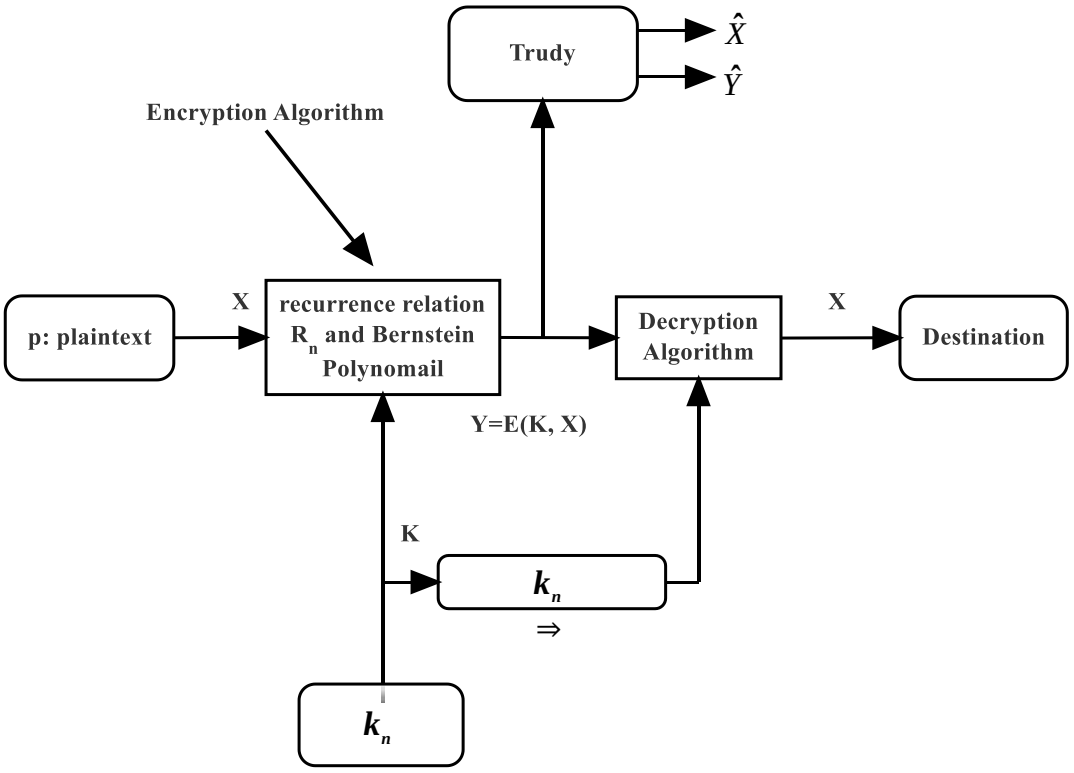

Fig. 2: Encryption algorithm using recurrence relations and Bernstein Polynomial.

Literature Review

An attempt to realize a public key cryptosystem using FPGA based on the usage of finite state machines was presented in [3]. Another attempt of using recurrence relations to cryptography by using finite state machine was shown in [4]. The work presented herein is an enhancement of the work accomplished in [2], where Bernstein polynomial is used in conjunction with the recurrence relations and Moore finite state machine. The inherent security of this novel scheme stemmed from the fact that the usage of Bernstein polynomial is adding an extra layer of security to the proposed encryption scheme. The science of cryptography is widely discussed in the available literature [5-12]. An abstract level of computer system security breaches and the quantification of the top event of interest can be found in [13-14]. Fault-tree analysis was used as an analytical tool for the quantification process.

Bernstein Polynomials and Moore Machine

This section presents both Bernstein polynomials and Moore machine briefly as follows.

Polynomials

The Bernstein polynomials [15] are some of the most important and very useful polynomials. Bernstein polynomials of n-th degree are defined on the closed interval [0, 1] as follows:

$$B_{i,n}(t) = \binom{n}{i} t^i (1-t)^{n-i}, \qquad \text{for} i = 0, 1, 2, \dots, \qquad n,$$

Where $\binom{n}{i} = \frac{n!}{i!(n-1)!}$

ISSN: 2349-5197
Impact Factor: 2.715

INTERNATIONAL JOURNAL OF RESEARCH SCIENCE & MANAGEMENT

We can easily rewrite Bernstein polynomials in terms of power basis $\{1, t, t^2, \dots, t^n\}$using the binomial theorem as follows:

$$B_{k,n}(t) = \binom{n}{k} t^k (1-t)^{n-k}$$

$$= \binom{n}{k} t^k \sum_{i=0}^{n-k} (-1)^i \binom{n-k}{i} t^i$$

$$= \sum_{i=0}^{n-k} (-1)^i \binom{n}{k} \binom{n-k}{i} t^{i+k}$$

$$= \sum_{i=k}^{n} (-1)^{i-k} \binom{n}{k} \binom{n-k}{i-k} t^i$$

$$= \sum_{i=k}^{n} (-1)^{i-k} \binom{n}{k} \binom{i}{k} t^i$$

In order to use matrix notation in what follows, we consider the following form for Bernstein polynomial,

$$B_{j-1,n}(t) = \sum_{i=j}^{n+1} (-1)^{j-i} \binom{n}{j-1} \binom{j-1}{i-1} t^{j-1}, \quad j = 1,2, \dots, n+1. \tag{1}$$

The $(n+1)\times 1$ column matrix function of $B_{j-1,n}(t)$, $1 \le j \le n+1$

$\varphi_n(t) = [B_{0,n}(t), B_{1,n}(t) \dots B_{n,n}(t)]^T$; (T: the transpose operation).

can be put in the following form [16]

$$.\varphi_n(t) = Q_n . [1 \;\; t \;\; t^2 \dots t^n]^T$$

The coefficient matrix Q_n is an upper triangular matrix, its elements can be deduced to take the following form, by utilizing relation (1)

$$q_{ij} = \begin{cases} (-1)^{j-i} \binom{n}{j-1} \binom{j-1}{i-1} & , j \ge i \\ 0 & , \; j < i \end{cases} ; i, j = 1,2,3, \dots, n+1 \tag{2}$$

Lemma 1.For $n \ge 1$, the matrix Q_n is an nonsingular matrix (i.e. **det**$(Q_n) \neq 0$) with the determinant value

$$\textbf{det}(Q_n) = \prod_{i=1}^{n+1} \binom{n}{i-1}. \tag{3}$$

Proof: The proof of this lemma is a straight forward, since Q_n is an upper triangular matrix, then

det$(Q_n) = \prod_{i=1}^{n+1} q_{ii}$ which gives (3).

Now, since $Q_n$is a nonsingular matrix, then it is invertible matrix. The elements of the inverse Q_n^{-1} of matrix Q_n are defined as in [17]

$$q_{ij} = \begin{cases} \frac{\binom{n-i+1}{j-1}}{\binom{n}{j-1}} & , j \ge i \\ 0 & , \; j < i \end{cases} ; i, j = 1,2,3, \dots, n+1 \tag{4}$$

ISSN: 2349-5197
Impact Factor: 2.715

INTERNATIONAL JOURNAL OF RESEARCH SCIENCE & MANAGEMENT

The following are examples for Q_n and Q_n^{-1} for n = 1, 2, 3

$$Q_1 = \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix}, \mathbf{det}(Q_1) = 1, \text{ and} Q_1^{-1} = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}.$$

$$Q_2 = \begin{bmatrix} 1 & -2 & 1 \\ 0 & 2 & -2 \\ 0 & 0 & 1 \end{bmatrix}, \mathbf{det}(Q_2) = 2, \text{ and} Q_2^{-1} = \begin{bmatrix} 1 & 1 & 1 \\ 0 & \frac{1}{2} & 1 \\ 0 & 0 & 1 \end{bmatrix}.$$

$$Q_3 = \begin{bmatrix} 1 & -3 & 3 & -1 \\ 0 & 3 & -6 & 3 \\ 0 & 0 & 3 & -3 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \quad \mathbf{det}(Q_3) = 9, \text{ and} Q_3^{-1} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & \frac{1}{3} & \frac{2}{3} & 1 \\ 0 & 0 & \frac{1}{3} & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

Moore Machine

In this section a brief overview of Moore machine is introduced. Moore machine is an Finite State Machine FSM whose output depends on the present state [18]. A Moore machine can be described by a 6-tuples of the form:

$\boldsymbol{M} = (Q, \Sigma, \Delta, \delta, \tau, q_0)$, where
Q: is a non empty finite set of states,
Δ: nonempty output alphabet,
Σ: nonempty finite set of input values,
δ: a transition function,
τ:is the output function $\tau : Q \to \Delta$,
q_0:is the initial state of Q.
Figure shows an example of Moore machine.

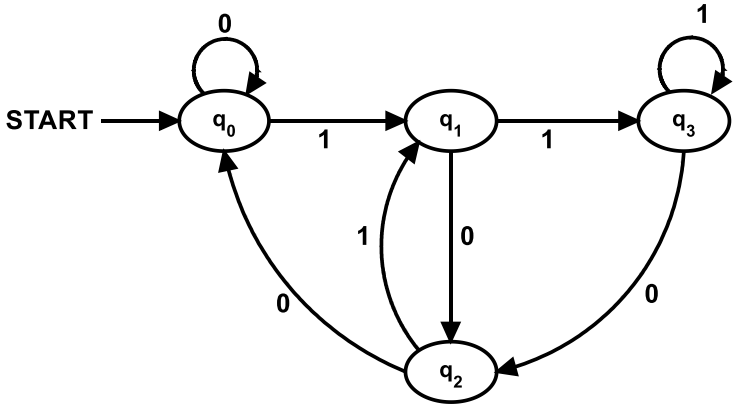

Figure 3: Moore machine with 4 states.

ISSN: 2349-5197
Impact Factor: 2.715

INTERNATIONALJOURNALOFRESEARCH SCIENCE& MANAGEMENT

Example 1 Reproduced from Ref. [2]

Here is the first example as discussed in [2] is reproduced as a review with three corrections shown in table in bold in the last row of the table 3.

Let the plain text matrix used is $\boldsymbol{P} = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$

the recurrence relation of the Fibonacci sequence is $R(n) = \begin{pmatrix} f_{n+1} & f_n \\ f_n & f_{n-1} \end{pmatrix}$

input key in binary is = 10110

Recurrence matrix key $R[1] = \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix}$

Key matrices $R[1], R[2]$ and $R[3]$ are as follows:

$$R[1] = \begin{bmatrix} 2 & 1 \\ 1 & 0 \end{bmatrix}^1 = \begin{bmatrix} 2 & 1 \\ 1 & 0 \end{bmatrix}$$

$$R[2] = \begin{bmatrix} 2 & 1 \\ 1 & 0 \end{bmatrix}^2 = \begin{bmatrix} 5 & 2 \\ 2 & 1 \end{bmatrix}$$

$$R[3] = \begin{bmatrix} 2 & 1 \\ 1 & 0 \end{bmatrix}^3 = \begin{bmatrix} 12 & 5 \\ 5 & 2 \end{bmatrix}$$

It is also known that the cipher text at $q(i + 1) = q(i).R[n]$. where:

q_{i+1}: represents the output

q_i: represents the input

R_n:represents the output at state q_{i+1}

Now, table 1 for the present state can be obtained as follows:

Table1 .Previous and present states of the system.

Table1 .Previous and present states of the system.

Present State ={Previous State q_i } . $\boldsymbol{R[n]}$
$\boldsymbol{q_1}$= $q_0.R[1]$
$\boldsymbol{q_2}$= $q_1.R[2]$
= $q_2.R[1]\boldsymbol{q_1}$
= $q_1.R[3]\boldsymbol{q_3}$
= $q_3.R[2]\boldsymbol{q_2}$

ISSN: 2349-5197
Impact Factor: 2.715

INTERNATIONAL JOURNAL OF RESEARCH SCIENCE & MANAGEMENT

Now, the key matrices used in the ciphertext are obtained as shown in table 2 below.

Table 2. Key matrices obtained according to table 1 above.

Input	1	0	1	1	0	-
State	q_0	q_1	q_2	q_1	q_3	q_2
Output	R[1]	R[1]	R[1]	R[3]	R[2]	-
Key Matrix	$\begin{bmatrix}2 & 1\\1 & 0\end{bmatrix}$	$\begin{bmatrix}5 & 2\\2 & 1\end{bmatrix}$	$\begin{bmatrix}2 & 1\\1 & 0\end{bmatrix}$	$\begin{bmatrix}12 & 5\\5 & 2\end{bmatrix}$	$\begin{bmatrix}5 & 2\\2 & 1\end{bmatrix}$	-

It follows that the ciphertext for the given secret key is obtained as shown in table 3 below.

Table 3.Ciphertext for the given secret key.

No.	Input	Present State	Previous State	Output	Output	Cipher Text
1	*1*	q_1	q_0	$R[1]$	1	$q_0.R[1] = \begin{bmatrix}1 & 2\\3 & 4\end{bmatrix}\begin{bmatrix}2 & 1\\1 & 0\end{bmatrix} = \begin{bmatrix}4 & 1\\10 & 3\end{bmatrix}$
2	*0*	q_2	q_1	$R[2]$	2	$q_1.R[2] = \begin{bmatrix}4 & 1\\10 & 3\end{bmatrix}\begin{bmatrix}5 & 2\\2 & 1\end{bmatrix} = \begin{bmatrix}22 & 9\\56 & 23\end{bmatrix}$
3	*1*	q_1	q_2	$R[1]$	1	$q_2.R[1] = \begin{bmatrix}22 & 9\\56 & 23\end{bmatrix}\begin{bmatrix}2 & 1\\1 & 0\end{bmatrix} = \begin{bmatrix}53 & 22\\135 & 56\end{bmatrix}$
4	*1*	q_3	q_1	$R[3]$	3	$q_1.R[3] = \begin{bmatrix}53 & 22\\135 & 56\end{bmatrix}\begin{bmatrix}12 & 5\\5 & 2\end{bmatrix} = \begin{bmatrix}746 & 309\\1900 & 787\end{bmatrix}$
5	*0*	q_2	q_3	$R[2]$	**2**	$3.R[2] = \begin{bmatrix}746 & 309\\1900 & 787\end{bmatrix}\begin{bmatrix}5 & 2\\2 & 1\end{bmatrix} = \begin{bmatrix}\mathbf{4348} & 1801\\\mathbf{11074} & 9587\end{bmatrix}$

as presented in [2], mod 41 operation is used. This implies that the ciphertext in the last raw of table 3 will be:

$\begin{pmatrix}2 & 38\\4 & 36\end{pmatrix}$.

ISSN: 2349-5197
Impact Factor: 2.715

INTERNATIONAL JOURNAL OF RESEARCH SCIENCE & MANAGEMENT

Illustrative Example based on Bernstein Polynomial

This example demonstrates the usage of the Bernstein polynomials in the encryption and decryption processes. The same data will be used as in the previous example which is:

Let the plain text matrix used is $\boldsymbol{P} = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$

the recurrence relation of the Fibonacci sequence is $R(n) = \begin{pmatrix} f_{n+1} & f_n \\ f_n & f_{n-1} \end{pmatrix}$

input key in binary is = 10110

Recurrence matrix key $R[1] = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$

Key matrices $R[1], R[2]$ and $R[3]$ are as follows:

$R[1] = \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix}$

$R[2] = \begin{bmatrix} 1 & -2 \\ 0 & 1 \end{bmatrix}$

$R[3] = \begin{bmatrix} 1 & -3 \\ 0 & 1 \end{bmatrix}$

it follows that the ciphertext will be generated as shown in table 4 below.

Table 4. Ciphertext for the given secret key.

No.	Input	Present State	Previous State	Output	Output	Cipher Text
1	1	q_1	q_0	$R[1]$	1	$q_0.R[1] = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}\begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 3 & 1 \end{bmatrix}$
2	0	q_2	q_1	$R[2]$	2	$q_1.R[2] = \begin{bmatrix} 1 & 1 \\ 3 & 1 \end{bmatrix}\begin{bmatrix} 1 & -2 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & -1 \\ 3 & 5 \end{bmatrix}$
3	1	q_1	q_2	$R[1]$	1	$q_2.R[1] = \begin{bmatrix} 1 & -1 \\ 3 & -5 \end{bmatrix}\begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & -2 \\ 3 & -8 \end{bmatrix}$
4	1	q_3	q_1	$R[3]$	3	$q_1.R[3] = \begin{bmatrix} 1 & -2 \\ 3 & -8 \end{bmatrix}\begin{bmatrix} 1 & -3 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & -5 \\ 3 & -17 \end{bmatrix}$
5	0	q_2	q_3	$R[2]$	2	$q_3.R[2] = \begin{bmatrix} 1 & -5 \\ 3 & -17 \end{bmatrix}\begin{bmatrix} 1 & -2 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & -7 \\ 3 & -23 \end{bmatrix}$

if we were to choose mod 41 arithmetic as in the previous example, we get the ciphertext of the value $\begin{bmatrix} 1 & -7 \\ 3 & -23 \end{bmatrix}$.

ISSN: 2349-5197
Impact Factor: 2.715

INTERNATIONALJOURNALOFRESEARCH SCIENCE& MANAGEMENT

Performance Evaluation of the Proposed Scheme

As stated in [2], we end up with the same performance time. Let t_a be the time required to perform each addition operation, while t_m represents the time required to perform each multiplication operation. Then, the total time required to perform an n-key bits is $n[4t_a + 8t_m]$. There are four factors which contribute to the inherent security of this novel scheme. First, the length of the secret key. Second, the usage of the recurrence relation that will add an additional layer of security. Third, the inherent dependency of the output of each state in the Moore machine with . Finally, the adoption of the Bernstein polynomial to this novel scheme. This scheme also is a function of the key length in which case the difficulty of breaking the code will increase as the key length increases. The security analysis of this scheme follows the same rhythm as in [2].

Conclusion and Future Work

This novel encryption scheme employed Bernstein polynomial in the encryption process. It is built based on four pivotal components. First, the use of finite state Moore machine. Second, the usage of recurrence relations. Third, the usage of matrix multiplication. Finally, the employment of Bernstein polynomial in constructing the recurrence relation.

Acknowledgements

This article was funded by the Deanship of Scientific Research (DSR), King Abdulaziz University, Jeddah. The authors, therefore, acknowledge with thanks DSR technical and financial support.

References

[1] **W. Stallings**. Cryptography and Network Security: Principles and Practice. Seventh edition. Pearson. 2016.

[2] **B. K. Gandhi et al.** Cryptographic Scheme for Digital Signals using Finite State Machines. International Journal of Computer Application. (29)6, September 2011.

[3] **N. Nhan.** Implementation FPGA of Public Key Cryptosystems Based on Finite State Machine Reconfiguration. International Journal of Advanced Science and Technology. 67(2014), PP. 33-42.

[4] **P. Ray. et. al.** Application of Some Recurrence Relations to Cryptography using Finite State Machine. International Journal of Computer Science and Electronics Engineering (IJCSEE). 2(4): 2014. Pp. 220-223.

[5] **D. R. Stinson**. Cryptography: Theory and Practice. Second edition. (CRC Press, Boca Raton, Fl 2003).

[6] **P. Fred and S. Murphy**. Cryptography: A Very Short Introduction. (Oxford Univ. Press). Oxford, 2002.

[7] **G. H. Hardy and E. M. Wright**. An introduction to the theory of numbers. Sixth edition. Oxford Univ. Press, New York, 2008.

[8] **C. Paar and J. Pelzl.** Understanding Cryptography: A Textbook for Students and Practitioners.

[9] **J. Buchmann**. Introduction to Cryptography. Second edition. Sprinter, 2009.

[10] **N. P. Smart**. Cryptography Made Simple. First edition. Springer 2016.

[11] **J. Hoffstein** et.al. An Introduction to Mathematical Cryptography. Springer 2008.

[12] **B. Shneier**. Applied Cryptography: Protocols, Algorithms and Source Code in C. First edition. 2015.

[13] **A. Rushdi and O. Barukab**. Fault-Tree modeling of computer system security. International Journal of Computer Mathematics, 82(7)(2005): 805-819.

ISSN: 2349-5197
Impact Factor: 2.715

INTERNATIONALJOURNALOFRESEARCH SCIENCE& MANAGEMENT

[14] **A. Rushdi and O. Barukab**. A doubly-stochastic fault-tree assessment of the probabilities of security breaches in computer systems. In Proceedings of the 2nd Saudi Science Conference, vol. 4(2004), pp. 1-17.

[15] **G. Tachev**. Pointwise approximation by Bernstein Polynomials, Bull. Aust. Math. Soc. 85(3)(2012), pp. 353-358.

[16] **S. A. Yousefi and M. Behroozifar**. Operational matrices of Bernstein Polynomials and their applications. I.J. Sys. Sci. 41(2010), pp. 709-716.

[17] **K. Parand and S. A. Kaviani**. Application of the exact operational matrices based on the Bernstein polynomials, J. Math & Comp. Sci., 6(2013), **pp**. 36-59.

[18] **J. Shallit**. A Second Course in Formal languages and Automata Theory. Cambridge University Press, New York, 2009.