www.ijsrnsc.org

Available online at www.ijsrnsc.org

IJSRNSC

Volume-6, Issue-1, February 2018
Research Paper

Int. J. Sc. Res. in Network Security and Communication

ISSN: 2321-3256

Modular Encryption Algorithm for Secure Data Transmission

P.Sri Ram Chandra[1*], G. Venkateswara Rao[2], G.V. Swamy[3]

[1*] Dept. of CSE, GITAM-Deemed to be University, Visakhapatnam, INDIA and
Faculty member in CSE, GIET (A), Rajahmundry, Andhra Pradesh, INDIA.
[2]Information Technology Department, GITAM-Deemed to be University, Visakhapatnam, INDIA
[3]Electronics and Physics Department, GITAM-Deemed to be University, Visakhapatnam, INDIA

[*]*Corresponding Author: psrgietcse@gmail.com*

Received: 09/Jan/2018, Revised: 21/Jan/2018, Accepted: 19/Feb/2018, Published: 28/Feb/2018

Abstract— Information is a strategic resource. Information technology and business transactions are becoming inextricably interwoven, where security for the data and concealed data transmission are made mandatory. Cryptography can be considered as the principle means of providing the data security. In this paper authors have proposed a new symmetric block cipher named Modular Encryption Algorithm with an acronym MEA which uses tri-modular matrix for its key generation, a set of operations on a matrix, Permutations and Substitutions for its encryption and decryption. As part of operations required in MEA authors have proposed M-Box, the functionality is described in this paper. The multilevel cipher rounds used in this algorithm can enhance the security such that even an intruder intercepts the message, it could be difficult to decipher the message. The strength of this algorithm has been analyzed over differential cryptanalysis. This algorithm undoubtedly follows the Strict Plaintext Avalanche Criterion (SPAC) and Strict Key Avalanche Criterion (SKAC) - the Shannon's property of "Confusion" and "Diffusion", the results are tabulated in this paper.

Keywords— Cryptanalysis, Cryptography, Deciphering, Enciphering, Intruder, Tri-modular matrix

I. INTRODUCTION

The outright developed digitalization is playing a fundamental role in handling the financial, business, personal and public sector related data. In transferring such significant data across the network may sometimes get into the hands of the intruder who can tamper the contents of the data [1]. In this regard, providing a high-end security system is a crucial issue. A cryptographic technique is the principle means of protecting the data and ensures the secure data transmission. Cryptography is the art of codifying the original messages so that they become unreadable and are intended only for the authorized people, further facilitates the secure data transmission. They can make it readable with the help of using proper set of keys [3]. In cryptography, cryptosystem is a suite of three necessary procedures involved viz., key generation, encryption, and decryption processes [1].

The cryptographic algorithms developed need to maintain few principles of security like confidentiality, integrity, authentication, non-repudiation [3]. Considering the data transmission between two entities A and B, 'if A ensures that none expect B gets the data' is termed to be as confidentiality, integrity states that both A and B will undergo an agreement such that, none of them would tamper the data further. 'B assures that the data was sent by A only' designated as authentication, non-repudiation does not allow the sender of a message to refuse the claim of not sending the message [3].

The key research contribution to this article is that the authors have proposed authors have proposed a new symmetric block cipher named Modular Encryption Algorithm with an acronym MEA which uses tri-modular matrix for its key generation, a set of operations on a matrix, Permutations and Substitutions for its encryption and decryption. As part of operations required in MEA authors have contributed M-Box, the functionality is described in the section 3.2.1. The content of this research contribution is organized as depicted here; section 2 briefly describes the preliminaries of cryptography, section 3 is organized to brief the MEA cryptosystem viz., key generation, encryption and decryption. Strength and Complexity analysis of this cryptosystem is depicted in the sections 4 and 5 respectively. Section 6 describes the conclusions and future scope of this research contribution.

II. PRELIMINARIES

Cryptography is one of the principle means of secure data transmission where the data encryption and decryption processes are involved with or without a secret key. Mathematical calculations along with substitutions and permutations are needed to accompany the steps of cryptography [4]. Encryption is the process where the original message is mutated into coded text so that an intruder cannot detect the original message and only the authorized users can access it [3]. In contrast to the encryption, decryption is the process of altering the coded text to original message [3]. Key holds the secret information in the cryptographic operation [4]. Here encoded message can be called as cipher text whereas the original message is called the plain text. Precisely speaking enciphering and deciphering are most common synonyms of encryption and decryption respectively [1].

2.1 Classification of Cryptography algorithms

From the point of view of using keys in the cryptographic algorithms, they primarily classified as symmetric and asymmetric key cryptography. The keys in practice can be represented as a shared secret between sender and receiver in order to maintain the private information link. The symmetric key cryptography uses two identical keys for the process of enciphering and deciphering [5]. On the other side asymmetric key cryptography uses two un-identical keys i.e., one for enciphering and the other for deciphering process respectively [1].

2.2 Classification of Ciphers

Encryption or decryption in symmetric key cryptography can be done through the use of symmetric key ciphers. These ciphers can be classified into two groups as stream and block ciphers.

2.2.1 Stream cipher

The sequence generated by the key-generating function of the cryptosystem is conventionally known as the key stream [6]. Stream cipher is a symmetric key cipher, where the plaintext bits are combined with a key stream. Precisely speaking plaintext bit is encrypted one at a time with the corresponding digit of the pseudorandom cipher stream (key stream) to generate the cipher-text bit.

2.2.2 Block cipher

Block cipher is an enciphering method that applies a deterministic function of the cryptosystem along with symmetric key to encrypt the block of text rather than bits in stream ciphers. Precisely speaking the plaintext is encrypted block-by-block with the corresponding key to generate the cipher text block.

2.3 Cryptographic attacks

A cryptographic attack is a method in which the security of a cryptosystem is bypassed by the intruder having knowledge either on encryption or decryption, cryptographic protocol used or key management scheme [4]. The first attack identified was cipher-text attack, which occurs when an attacker is well aware of only the cipher text. The attacker can deduce the plain text on analyzing the frequency of the occurrences of the characters [1]. The known plaintext problem occurs when the attacker is having some paired fragments of plaintext and the corresponding cipher text [1]. The chosen cipher text is the attack in which the cryptanalyst (attacker) captures the part of the information and deduce the decryption process under the unknown key [1].

The chosen plain text is quoted to be one of the most dangerous attacks where attacker chooses a plaintext to be encrypted further analyses the relation between chosen plaintext and obtained cipher text to procure the key used for encryption process [1]. Codebook attack is a kind of attack where the block of given plaintext is always encrypted to same block of cipher text as long as the same key is used [4]. A 'man-in-the-middle' attack is a kind of active attack where the attacker furtively relays and perhaps amends the conversation between the two entities who believe they are directly communicating with each other [3].

2.4 General characteristics of the Cryptosystem

Cryptography is the art and science of keeping the messages secure and it is practiced by cryptographers. On the other side the cryptanalysts are the practitioners of cryptanalysis, the art and science of breaking the cipher-text [9]. Norman D. Jorstad had proposed a series of characteristics of the cryptosystem, which are as follows [9].

a) Type of the algorithm based on key: The algorithms based on usage of the keys are generally of two kinds i.e., symmetric key and asymmetric key.
b) Function: The encryption function used for message secrecy must follow the principles of security.
c) Key length: The key length is the base function in providing security to the cryptosystem.
d) Attack steps: Formally defined as the number of steps required by the attacker to perform the best known attack.
e) Attack time: The time taken by the attacker to crack the key or cryptosystem.
f) Rounds: The increase in the number of rounds of encryption may lead to more confusion and diffusion, hence more security exists.

III. MODULAR ENCRYPTION ALGORITHM-MEA

In this paper authors have proposed a new symmetric block cipher named Modular Encryption Algorithm with an

acronym MEA. It uses tri-modular matrix for its key generation, a set of operations on a matrix, Permutations and Substitutions for its encryption and decryption. As part of operations required in MEA authors have proposed M-Box and the functionality is described in the section 3.2.5.
Defnition1: The matrix is said to be *tri-modular* if and only if its determinant value is always three. Figure1 depicts the generalized tri-modular matrix.

Properties of the Tri-Modular matrix:

- Product of two tri-modular matrices is n-modular matrix with n=9.
- Product of two n-modular matrices is n^2-modular matrix.
- Determinant of inverse of the tri-modular-matrix is 1/3.

The premier strength of the cryptosystem depends on the key or its generation process. So the key generated should be protected i.e., even full or part of the key would have been stolen by the intruder, it should be an insurmountable task to generate the series of keys used. This way of giving protection to the keys made us to move a step ahead in considering the tri-modular matrix for the generation of keys and the cryptanalysis is shown in the section 4.3.

The newly proposed MEA is especially meant for the secure data transmission across the network. It takes a block of 72 bit plaintext as input to generate the corresponding 72 bit cipher-text. The encryption process in this algorithm is compassed with the two phases, phase-I and phase-II with 16 and 3 rounds respectively. The detailed execution of key generation, encryption and decryption are described in the consequent sections.

3.1 MEA Key Generation

A single round of phase-I is encrypted using two tri-modular matrices of 3x3 order each. In fact the same phase undergoes 16 rounds so it needs 32 number of 3x3 matrices to form a full-fledged key i.e., fourth tri-modular matrix (n=4) through 35th tri-modular matrix (n=35) with respect to this phase. In phase II the single round of encryption uses one tri-modular matrix of order 3x3 and it undergoes three rounds i.e., first three tri-modular matrices of 3x3 order each are required. Precisely speaking a total of 35 tri-modular matrices of 144 bits each i.e., 5040 bit key is required for the whole encryption process. The following Figure1 gives the generalized tri-modular matrix.

$$\begin{vmatrix} 8n^2+28n+20 & 2n+5 & 4n+4 \\ 4n^2+14n+10 & n+3 & 2n+3 \\ 4n^2+14n+11 & n+2 & 2n+1 \end{vmatrix}$$

Figure 1: Generalized Tri-Modular matrix (n ≥ 1)

As the MEA uses 35 tri-modular matrices as keys, instead of representing all the keys, the table1 provides a set of 5 keys represented in a step of 3 columns.

Table 1: A few sample set of keys in MEA represented as step of 3 columns.

Tri-modular matrix with n=1			Tri-modular matrix with n=2			Tri-modular matrix with n=3			Tri-modular matrix with n=4			Tri-modular matrix with n=5		
K_1			K_2			K_3			K_4			K_5		
56	7	8	108	9	12	176	11	16	260	13	20	360	15	24
28	4	5	54	5	7	88	6	9	130	7	11	180	8	13
29	3	3	55	4	5	89	5	7	131	6	9	181	7	11

After the keys generated, the sender has to send the sequence of decryption keys saved in a file to the concerned receiver via a secured means of communication channels like Short Message Service (SMS) or e-mail or Flash message (more secured, even older) [1].

3.2 MEA Encryption process

The encryption process of MEA starts by considering the 72 bit block binary digits i.e., ASCII values of 9 plaintext characters, 8 bits each represented in hexadecimal. After the initial permutation the algorithm undergoes 16 and 3 rounds of encryption in phase-I and phase-II respectively. Here we have used Rijndael substitution-box(S-box), table of logarithms (L-table), table of exponentials (E-table) and newly proposed Compression permutation-box (M-box), the brief description of the encryption is discussed in the algorithm1.

Algorithm1:

Input: Plaintext string when divided into block of 9 characters (9*8 bits=72 bits).

1. Matrix $1_{ij}=\begin{bmatrix} a_{00} & a_{01} & a_{02} \\ a_{10} & a_{11} & a_{12} \\ a_{20} & a_{21} & a_{22} \end{bmatrix}$ such that a_{00} through a_{22} are the corresponding ASCII values of 9 characters represented in Hexadecimal format.
2. Apply Initial Permutation of the above 3x3 hexadecimal matrix.
   $2_{ij}=\begin{bmatrix} a_{21} & a_{22} & a_{01} \\ a_{02} & a_{00} & a_{10} \\ a_{11} & a_{20} & a_{12} \end{bmatrix} \leftarrow \begin{bmatrix} a_{00} & a_{01} & a_{02} \\ a_{10} & a_{11} & a_{12} \\ a_{20} & a_{21} & a_{22} \end{bmatrix}$

Phase-I:

For loop:=1 to 16 do

begin

3. $3_{ij}=\begin{bmatrix} a_{21} & a_{22} & a_{01} \\ a_{02} & a_{00} & a_{10} \\ a_{11} & a_{20} & a_{12} \end{bmatrix} \oplus K_i$ where $K_{i\ is}$ the Tri-Modular matrix such that $4 \le i \le 34$
4. 4_{ij}=Compression permutation (3_{ij}) through M-Box.
5. 5_{ij}=Table of logarithms (4_{ij}).
6. $6_{ij}=5_{ij} \oplus K_i$ where $K_{i\ is}$ the Tri-Modular matrix such that $5 \le k \le 35$
7. 7_{ij}=Compression permutation (6_{ij}) through M-Box.
8. 8_{ij}=Table of exponentials (7_{ij}).
   End;

Phase-II:

For loop:=1 to 3 do

begin

9. $9_{ij}=8_{ij} \oplus K_i$ where $K_{i\ is}$ the Tri-Modular matrix such that $1 \le k \le 3$.
10. 10_{ij}=Row Interchanges i.e., $R_i \leftarrow R_{(i+1)\ mod3}$ $0 \le i \le 2$.
11. 11_{ij}=Sub bytes (10_{ij})
    End;
12. 12_{ij}=Decimal values of 11_{ij}
13. 13_{ij}=Corresponding 9 ASCII values
    $\leftarrow\begin{bmatrix} a_{00} & a_{01} & a_{02} \\ a_{10} & a_{11} & a_{12} \\ a_{20} & a_{21} & a_{22} \end{bmatrix}\leftarrow\begin{bmatrix} a_{21} & a_{22} & a_{01} \\ a_{02} & a_{00} & a_{10} \\ a_{11} & a_{20} & a_{12} \end{bmatrix}$
14. **Output**: Cipher-text block of 72 bits.

Note: $\oplus$ represents Exclusive-OR Operation and $0 \le i,j \le 2$

In this algorithm authors have proposed an M-Box, the key component of encryption which converts four hexadecimal digits to two hexadecimal digits.

3.2.1 MEA M-box

Keeping in mind about the properties of "Confusion" and "Diffusion" and as part of compression permutation, we made compression permutation through M-box as one of the primary components of this algorithm which transforms *m* number of input bits to *n* number of output bits, where *m*=16 and *n*=8 i.e., 4 hexadecimal digits to 2 hexadecimal digits.

Algorithm2

Input: 4 hexadecimal digits.

1) Represent hexadecimal digits in 4 bit binary i.e., we count 16 bits here
2) Divide the above array of 16 bits in to two equal parts i.e., 8 bits each and write them as polynomial expression.
   Ex: Polynomial representation of hexadecimal digit 2A is $x^5+x^3+x^1$ and CF is $x^7+x^6+x^3+x^2+x^1+x^0$
3) Multiply the above obtained two polynomials using general multiplication procedure.
4) Consider the terms with odd coefficient only and divide the expression (without coefficients) with 11B (when represented as Polynomial expression)
   Ex: If the obtained expression is $x^{12}+x^{10}+3x^9+2x^8+5x^5+2x^2+x$, then the expression with odd coefficients is $x^{12}+x^{10}+3x^9+5x^5+x$, the same expression without coefficients is $x^{12}+x^{10}+x^9+x^5+x$ and divide with 11B i.e., $x^8+x^4+x^3+x+1$.
5) Convert the resultant polynomial expression in to binary, followed by hexadecimal format.

Output: 2 Hexadecimal digits.

Examples: M-Box (2ACF) = 2F

M-Box (021E) = 3C

M-Box (111F) = F4

The maximum values of step1 and 35th tri-modular matrix considered are FF and 10800 respectively. According to the XOR steps mentioned in the encryption algorithm, the maximum hexadecimal digit on which the M-box applied is FF XOR 10800 = 2ACF, where 2A and CF represents first half and second half of hexadecimal digits. In this regard we made 01 and 2A as lower and upper bounds for the first half of hexadecimal digits, 01 and CF as lower and upper bounds for the second half of hexadecimal digits. The values of the M-box are tabulated

in table2 as per the algorithm requirements, by creating a view from all the possibilities.

Table 2: Compression permutation through M-box

Input	Output	Input	Output
021E	3C	0915	BD
111F	F4	192E	93
965E	9A	2ACF	2F

3.2.2 Table of Logarithms and Exponentials

As same as S-box, the table of Logarithms (L-Table) and Exponentials (E-Table) also transforms *m* number of input bits to *n* number of output bits, where *m* is not necessarily equal to *n*. According to the criteria considered Strict Plaintext Avalanche Criterion (SPAC), a slight change in the plaintext should result significant changes in the cipher-text, this could be achieved by using L-Table and E-Table which are depicted in the following figures 2 and 3 respectively.

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0		00	19	01	32	02	1A	C6	4B	C7	1B	68	33	EE	DF	03
1	64	04	E0	0E	34	8D	81	EF	4C	71	08	C8	F8	69	1C	C1
2	7D	C2	1D	B5	F9	B9	27	6A	4D	E4	A6	72	9A	C9	09	78
3	65	2F	8A	05	21	0F	E1	24	12	F0	82	45	35	93	DA	8E
4	96	8F	DB	BD	36	D0	CE	94	13	5C	D2	F1	40	46	83	38
5	66	DD	FD	30	BF	06	8B	62	B3	25	E2	98	22	88	91	10
6	7E	6E	48	C3	A3	B6	1E	42	3A	6B	28	54	FA	85	3D	BA
7	2B	79	0A	15	9B	9F	5E	CA	4E	D4	AC	E5	F3	73	A7	57
8	AF	58	A8	50	F4	EA	D6	74	4F	AE	E9	D5	E7	E6	AD	E8
9	2C	D7	75	7A	EB	16	0B	F5	59	CB	5F	B0	9C	A9	51	A0
A	7F	0C	F6	6F	17	C4	49	EC	D8	43	1F	2D	A4	76	7B	B7
B	CC	BB	3E	5A	FB	60	B1	86	3B	52	A1	6C	AA	55	29	9D
C	97	B2	87	90	61	BE	DC	FC	BC	95	CF	CD	37	3F	5B	D1
D	53	39	84	3C	41	A2	6D	47	14	2A	9E	5D	56	F2	D3	AB
E	44	11	92	D9	23	20	2E	89	B4	7C	B8	26	77	99	E3	A5
F	67	4A	ED	DE	C5	31	FE	18	OD	63	8C	80	C0	F7	70	07

Figure 2: Table of Logarithms

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	01	03	05	0F	11	33	55	FF	1A	2E	72	96	A1	F8	13	35
1	5F	E1	38	48	D8	73	95	A4	F7	02	06	0A	1E	22	66	AA
2	E5	34	5C	E4	37	59	EB	26	6A	BE	D9	70	90	AB	E6	31
3	53	F5	04	0C	14	3C	44	CC	4F	D1	68	B8	D3	6E	B2	CD
4	4C	D4	67	A9	E0	3B	4D	D7	62	A6	F1	08	18	28	78	88
5	83	9E	B9	D0	6B	BD	DC	7F	81	98	B3	CE	49	DB	76	9A
6	B5	C4	57	F9	10	30	50	F0	0B	1D	27	69	BB	D6	61	A3
7	FE	19	2B	7D	87	92	AD	EC	2F	71	93	AE	E9	20	60	A0
8	FB	16	3A	4E	D2	6D	B7	C2	5D	E7	32	56	FA	15	3F	41
9	C3	5E	E2	3D	47	C9	40	C0	5B	ED	2C	74	9C	BF	DA	75
A	9F	BA	D5	64	AC	EF	2A	7E	82	9D	BC	DF	7A	8E	89	80
B	9B	B6	C1	58	E8	23	65	AF	EA	25	6F	B1	C8	43	C5	54
C	FC	1F	21	63	A5	F4	07	09	1B	2D	77	99	B0	CB	46	CA
D	45	CF	4A	DE	79	8B	86	91	A8	E3	3E	42	C6	51	F3	0E
E	12	36	5A	EE	29	7B	8D	8C	8F	8A	85	94	A7	F2	0D	17
F	39	4B	DD	7C	84	97	A2	FD	1C	24	6C	B4	C7	52	F6	01

Figure 3: Table of Exponentials

3.2.3 Substitution-box

In cryptography, an S-box (Substitution-box) is a basic component of symmetric key algorithms to perform substitution. In general, an S-box transforms *m* number of input bits to *n* number of output bits, where *m* is not necessarily equal to *n* [8]. According to the Shannon's property of Confusion, they are typically used to obscure the relationship between the key and the cipher-text [4]. Confusion is a mechanism where each binary digit (bit) of the cipher-text depend on several parts of the key, obscuring the connections between them. Diffusion states that the transition of a single bit of the plaintext, results a significant change in cipher-text i.e., half of the bits in the cipher-text should have been changed and vice-versa [4]. The following figure4 depicts the substitution box.

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

Figure 4: Substitution Box.

3.3 MEA Decryption process

The decryption process of MEA starts by considering the 72 bit block binary digits i.e., ASCII values of 9 cipher-text characters, 8 bits each represented in decimal number system. After the initial permutation the algorithm undergoes 3 and 16 rounds of decryption in phase-II and phase-I respectively. Here we have used Inverse Sub-bytes substitution box, table of logarithms (L-table), table of exponentials (E-table) and newly proposed Expansion permutation through Inverse M-Box, the brief description of the decryption is discussed in the algorithm3.

Algorithm3

Input: Cipher-text string when divided into block of 9 characters (9*8 bits=72 bits).

1. Matrix $1_{ij}=\begin{bmatrix} a_{00} & a_{01} & a_{02} \\ a_{10} & a_{11} & a_{12} \\ a_{20} & a_{21} & a_{22} \end{bmatrix}$ such that a_{00} through a_{22} are the corresponding ASCII values of 9 input characters represented in Decimal format.

2. Apply Initial Permutation of the above 3x3 Decimal matrix.

$$(2_{ij}) = \begin{bmatrix} a_{21} & a_{22} & a_{01} \\ a_{02} & a_{00} & a_{10} \\ a_{11} & a_{20} & a_{12} \end{bmatrix} \leftarrow \begin{bmatrix} a_{00} & a_{01} & a_{02} \\ a_{10} & a_{11} & a_{12} \\ a_{20} & a_{21} & a_{22} \end{bmatrix}$$

Phase-I

For loop:=1 to 3 do

begin

3. $3_{ij}=(2_{ij})_{16}\leftarrow(2_{ij})_1$ /* Decimal to hexadecimal Conversion */
4. 4_{ij}=Inverse sub bytes (3_{ij})
5. 5_{ij}=Row Interchanges i.e., $R_{(i+1)mod3} \leftarrow R_i$ $2\leq i\geq 0$.
6. $6_{ij}=5_{ij}\oplus K_i$ /*Where K_i is the Tri-Modular matrix such that $3 \leq k \geq 1$ */
   End;

Phase-II

For loop:=1 to 16 do

begin

7. 7_{ij}=Table of logarithms (6_{ij})
8. 8_{ij}=Expansion permutation (7_{ij}) through Inverse M-Box.
9. $9_{ij}=8_{ij}\oplus K_i$ ·····where K_i is the Tri-Modular matrix such that $35\leq k\geq 5$
10. 10_{ij}=Table of Exponentials(9_{ij})
11. 11_{ij}=Expansion permutation (10_{ij}) through Inverse M-Box.
12. $12_{ij}=11_{ij}\oplus K_i$ ·····where K_i is the Tri-Modular matrix such that $34\leq k\geq 4$
    End;
13. $13_{ij}=(12_{ij})_{10}\leftarrow(12_{ij})_{16}$····· Hexadecimal to Decimal Conversion
14. 14_{ij}= Corresponding 9 ASCII values $\leftarrow \begin{bmatrix} a_{00} & a_{01} & a_{02} \\ a_{10} & a_{11} & a_{12} \\ a_{20} & a_{21} & a_{22} \end{bmatrix} \leftarrow \begin{bmatrix} a_{21} & a_{22} & a_{01} \\ a_{02} & a_{00} & a_{10} \\ a_{11} & a_{20} & a_{12} \end{bmatrix}$

Output: Plaintext block of 72 bits.

3.3.1 Inverse Sub-bytes

As long as the decryption holds the inverse operations of the encryption, we need to use Inverse Sub-bytes in decryption to encompass Sub-bytes in encryption. The following figure5 depicts the Inverse Sub-bytes Substitution.

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	52	09	6A	D5	30	36	A5	38	BF	40	A3	9E	81	F3	D7	FB
1	7C	E3	39	82	9B	2F	FF	87	34	83	43	81	C4	DE	E9	CB
2	54	7B	94	32	A6	C2	23	3D	EE	4C	95	C4	42	FA	C3	4E
3	08	2E	A1	66	28	D9	24	B2	76	5B	A2	49	6D	8B	D1	25
4	72	F8	F6	64	86	68	98	16	D4	A4	5C	CC	5D	65	B6	92
5	6C	70	A8	50	FD	ED	B9	DA	5E	15	46	57	A7	8D	9D	84
6	90	D8	AB	00	8C	BC	D3	0A	F7	E4	58	05	B8	B3	45	06
7	D0	2C	1E	8F	CA	3F	0F	02	C1	AF	BD	03	01	13	8A	6B
8	3A	91	11	41	4F	67	DC	EA	97	F2	CF	CE	F0	B4	E6	73
9	96	AC	74	22	E7	AD	35	85	E2	F9	37	E8	1C	75	DF	6E
A	47	F1	1A	71	1D	29	C5	89	6F	B7	62	0E	AA	18	BE	1B
B	FC	56	3E	4B	C6	D2	79	20	9A	DB	C0	FE	78	CD	5A	F4
C	1F	DD	A8	33	88	07	C7	31	B1	12	10	59	27	80	EC	5F
D	60	51	7F	A9	19	B5	4A	0D	2D	E5	7A	9F	93	C9	9C	EF
E	A0	E0	3B	4D	AE	2A	F5	B0	C8	EB	BB	3C	83	53	99	61
F	17	2B	04	7E	BA	77	D6	26	E1	69	14	63	55	21	0C	7D

Figure 5: Inverse Sub-Bytes.

3.3.2 MEA Inverse M-box

As the section 3.2.1 discussed regarding compression permutation through M-box as one of the primary components of encryption algorithm which transforms *m* number of input bits to *n* number of output bits, where *m*=16 and *n*=8 i.e., 4 hexadecimal digits to 2 hexadecimal digits. In contrast to that we need to consider expansion permutation through Inverse M-box which has to transform *x* number of input bits to *y* number of output bits, where *x*=8 and *y*=16 i.e., 2 hexadecimal digits to 4 hexadecimal digits.

Table 3: Expansion permutation through Inverse M-box

Input	Output	Input	Output
3C	021E	BD	0915
F4	111F	93	192E
9A	965E	2F	2ACF

IV. MEA STRENGTH AND DIFFERENTIAL CRYPTANALYSIS

The increase in the security strength of the cryptosystem is based on the notion that deciphering must be a tough task to the intruder without having knowledge about the secret key and its design where the key size plays a fundamental role [1].

4.1 General metrics of the cryptosystem

In prior to judge the strength of the cryptosystem, following are the primary metrics considered as part to support the criteria discussed in the section 4.2 [9].

a) Key Length Metric

The security of a symmetric cryptosystem is a function of the length

of the key. The longer the key, the more resistant the algorithm is to a successful brute force attack.

b) Attack Steps Metric

Attack Steps is defined as the number of steps required to perform the best known attack.

c) Attack Time Metric

Attack Time is defined as the time required in performing the fastest known attack on a specified processor.

d) Rounds Metric

Rounds Metric is defined as the number of Rounds used in the encryption or decryption processes.

4.2 Criteria to judge strength of the cryptosystem

Norman D. Jorstad had mentioned a list of key points as algorithm metrics to judge the strength of the cryptosystem [9]. In this regard the criteria and its respective justification for our algorithm are mentioned in the points 'a' through 'j'.

a) Criterion: The plaintext cannot be derived from the cipher text without knowing the key [9].

Justification: As the slight change in the plaintext or key results significant difference in the cipher text, deriving the plaintext without having knowledge about the key is impractical.

b) Criterion: No other attack over the cryptosystem should better than the brute-force attack [9]. The longer the key, the more resistant the algorithm is to a successful brute force attack.

Justification: As the MEA uses 35 tri-modular matrices of 144 bits each as key, there could be 2^{144} possibilities to crack each of the key, it seems that the brute-force attack is impractical and no other attack can pushover it. In-fact a total of 5040 bit key is being used to form the full-fledged key i.e., 2^{5040} possibilities are required to crack the key whole.

c) Criterion: Knowledge of the algorithm should not reduce the strength of the cipher.

Justification: As the Phase-I and Phase-II of individual rounds are associated with the keys, even the cryptographic algorithm is public the strength of the cipher could not be reduced.

d) Criterion: The algorithm should satisfy the Strict Plaintext Avalanche Criterion with an acronym SPAC i.e., with a fixed key and a minor change in the plaintext should result the significant changes in the cipher text [9].

Justification: We have analyzed this criterion and the results are tabulated in the table2.

e) Criterion: The algorithm should satisfy the Strict Key Avalanche Criterion with an acronym SKAC i.e., with a fixed plaintext and a minor change in the key should result the significant changes in the cipher text [9].

Justification: We have analyzed this criterion and the results are tabulated in the table2 and table3.

f) Criterion: The algorithm should contain non commutative set of permutations and substitutions as part of the encryption and decryption [9].

Justification: As we have used permutation of the 8 bit message and inverse permutation of the same in encryption and decryption.

Justification: Apart from this we are making use of table of Logarithms, table of Exponentials, Substitution-Box, and Inverse Substitution-Box, we can undoubtedly say that this algorithm is justified over this criteria.

g) Criterion: Redundant bit groups in the plaintext should be totally obscured in the cipher-text.

Justification: The corresponding values of SPAC in the table1 states the significant changes can be occurred in cipher-text with the minor change in plaintext, results that there would not be any redundant bit groups of the text.

h) Criterion: The generated cipher text and the considered plaintext or vice versa should be of same length [9].

Justification: The detailed execution of encryption and decryption described in Algorithms 1 and 3 regarding size of the input plaintext and output cipher-text, vice versa states that the length of the plaintext and cipher-text are same.

i) Criterion: Any possible key in the algorithm should produce the strong cipher [9].

Justification: As the developed algorithm is following the Strict Key Avalanche Criterion and the encryption has undergone multilevel cipher rounds, we can say that all the possible keys can generate the strong ciphers.

j) Criterion: The increase in the number of rounds can lead to greater "confusion" and "diffusion", which could enhance the security-Shannon's Property.

Justification: The Phase-I and Phase-II in this algorithm undergo 16 and 3 rounds of encryption respectively, which satisfies the mentioned criterion.

4.3 Cryptanalysis of the Keys used

Cryptanalysis is defined as the series of steps exercised by the intruder in cracking the cipher text/key/encryption/decryption procedures to obtain the plaintext. As encryption and decryption procedures are publicly revealed in symmetric key cryptosystem, the keys used are being considered as heart of the cryptosystem. It is mandatory to protect the key from intruders; even part of the key is revealed. In this section we further made a case study that how far an intruder can access the series of keys used if he/she is well aware in part of the whole key. In this regard we intentionally revealed a random and sequential set of keys to a suit of people considering them as intruders. The results are tabulated in the table6 says that accessing the key without the procedure involved in generating the key is an insurmountable task to the intruders.

Table 4: Effect of Cryptanalysis under SPAC and SKAC with respect to Phase-I Encryption

Phase-I							
Strict Plaintext Avalanche Criterion-SPAC				Strict Key Avalanche Criterion-SKAC			
Fixed key and change in plaintext				Fixed plaintext and change in key			
Round Number	No. of bits changed in Cipher-text	Round Number	No. of bits changed in Cipher-text	Round Number	No. of bits changed in Cipher-text	Round Number	No. of bits changed in Cipher-text
1	54	9	42	1	49	9	53
2	45	10	35	2	58	10	57
3	48	11	47	3	51	11	46
4	32	12	43	4	44	12	68
5	47	13	58	5	62	13	55
6	65	14	45	6	57	14	47
7	41	15	62	7	49	15	59
8	59	16	64	8	63	16	63

Table 5: Effect of Cryptanalysis under SPAC and SKAC with respect to Phase-II Encryption

Phase-II			
Strict Plaintext Avalanche Criterion-SPAC		Strict Key Avalanche Criterion-SKAC	
Fixed key and change in plaintext		Fixed plaintext and change in key	
Round Number	No. of bits changed in the Cipher-text	Round Number	No. of bits changed in the Cipher-text
1	54	1	51
2	59	2	57
3	65	3	66

Table 6: Cryptanalysis of the Keys used in MEA.

S.No	Keys revealed with missing values	key derived by the Intruder	Original key
1	56,7,8,_,_,5,29,_,_	56,7,8,15,3,5,29,1,5	56,7,8,28,4,5,29,3,3
2	_,15,24,_,_,13,181,_,11	252,15,24,124,17,13,181,1,11	360,15,24,180,8,13,181,7,11
3	1296,_,_,_,14,_,_,13,_	1296,1024,512,256,14,11,12,13,5	1296,27,48,648,14,25,649,13,23
4	920,_,_,460,_,_,_,11,_	920,847,471,460,236,85,45,11,12	920,23,40,460,12,21,461,11,19

V. PERFORMANCE ANALYSIS OF MEA

In general, the performance of the cryptosystem is being measured in terms of the time taken to generate the keys, time taken by the encryption or decryption processes. The following figure 6 and 7 describes it.

5.1 Key generation time

Apart from the strength of the cryptosystem, the performance parameters like key generation time, encryption and decryption times are also playing a vital role. In this regard we have implemented our cryptosystem on a machine having i3 processor with 2.30 GHz or $2.3X10^9$ cycles per second. The consequent section 5.1, 5.2 gives the details of the figures, which depicts the performance of MEA.

5.2 Times of Encryption and Decryption

The performance of the cryptosystem MEA is measured in terms of encryption and decryption times, the figure 7 depicts it.

No of Rounds	Key Generation time (Seconds)
2	0.5
4	0.6
6	0.8
8	0.9
10	1.0
12	1.2
14	1.4
16	1.5

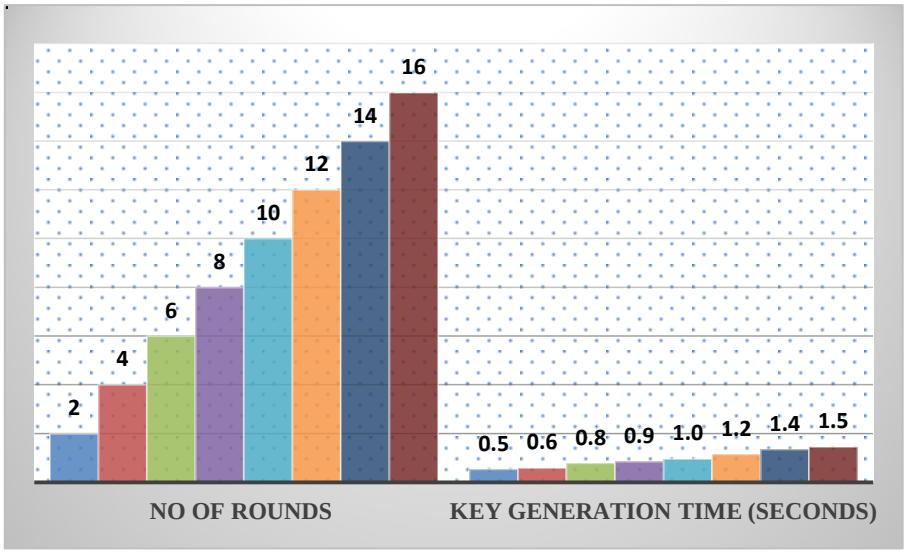

Figure 6: Graph showing No. of Rounds and their key Generation time

Encryption time in seconds	Decryption time in seconds	File size in MB
0.06	0.04	1
0.12	0.07	2
0.24	0.15	4
0.47	0.29	8
0.95	0.58	16
1.89	1.16	32
2.95	1.82	50
3.78	2.33	64
7.56	4.65	128
15.13	9.31	256
30.25	18.62	512
60.51	37.24	1024

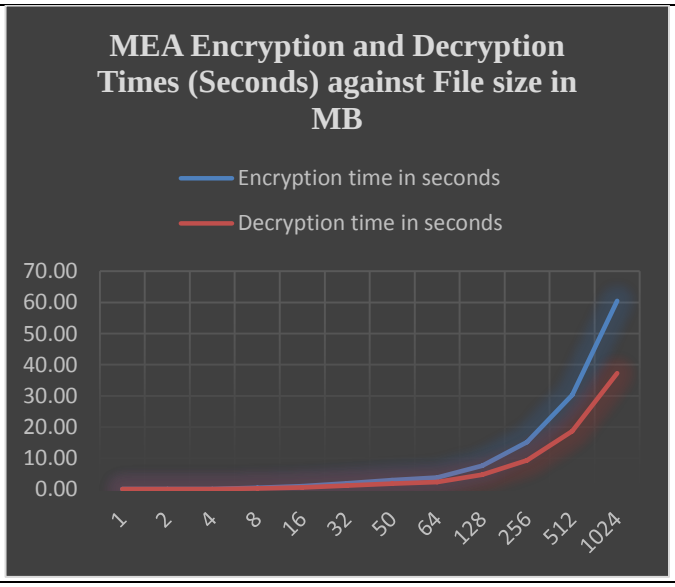

Figure 7: Performance of MEA in terms of Encryption and Decryption times (Seconds) Vs File size in MB

5.3 Complexity analysis

The time complexity of an algorithm signifies the total amount of time taken by it to run as a function considering the length of the input as *n*. Big Oh is the most commonly used asymptotic notation to represent the time complexity of an algorithm, which excludes the coefficients and lower order terms. For example if the time taken by the algorithm to all inputs of size *n* is at most $2n^3+3n^2+n+1$, the asymptotic time complexity is given as $O(n^3)$ [10].In another instance if the time complexity of the consecutive steps in an algorithm are $O(n^3),O(n^2),O(n)$, then the asymptotic time complexity is given as $O(n^3)$ which could be upper bound among all the three [1]. The complexity analysis of MEA is measured in three different categories called key generation, encryption and decryption. The theory of complexity analysis is briefly described in further Sections 5.3.1, 5.3.2, and 5.3.3 respectively.

5.3.1 Complexity analysis of Key generation

The key generation process of MEA holds the primary operation of selecting the tri-modular matrix and representing it in hexadecimal format (when required) with a complexity of *O(log n).*

5.3.2 Complexity analysis of Encryption

The encryption process of MEA holds the common complexity value $O(n^2)$ for the series of steps like 2,3,4,6,7,8,9,12. $O(n)$ for the steps 5,11 and $O(\log n)$ for the step 1, 13. Precisely speaking time complexity of this section could be $O(n^2)$, which is upper bound among all.

5.3.3 Complexity analysis of Decryption

As long as the sequence of steps used in decryption is in contrast to encryption, the series of time complexities may vary but the upper bound cannot be changed. The time complexity of the decryption process is given as $O(n^2)$.

VI. CONCLUSIONS AND FUTURE SCOPE

The concept of cryptography is playing a vital role in the present era where the secure data transmission is highly needed in the areas like banking, army and government. In this regard we proposed a new symmetric block cipher algorithm with a title “Modular Encryption Algorithm for Secure Data Transmission” which primarily focuses on handling sensitive data and providing secure data transmission. A series of permutations and substitutions are encouraged to be used in this algorithm to ensure the Shannon’s property of “Confusion” and “Diffusion”. The result tabulated in the tables 4 and 5 ensures that the Shannon’s property holds good. The strength of this algorithm is analyzed over differential cryptanalysis ensuring that SPAC and SKAC are satisfied.

The multilevel cipher rounds and the newly proposed M-box, Inverse M-box used in this algorithm enhances the security such that an intruder cannot intercepts the message and the results revealed that this algorithm withstand over any type of attack. The Primary advantage characteristics considered for this cryptosystem are extreme secure, energy efficient, more power and relatively fast. In contrast, sharing of keys is the disadvantage, but the cryptanalysis of the keys described in the section 4.3, table6 says that accessing the key without knowing the procedure involved in generating the key is an insurmountable task to the intruders. Further the cryptosystem can be enhanced by modifying the key size and using some tangled operations in the encryption and decryption.

REFERENCES

[1]. P. Sri Ram Chandra, G.Venkateswara Rao,G.V.Swamy,‘Ultramodern Encryption Standard Cryptosystem using Prolic Series for Secure Data Transmission’, International Journal of Latest Engineering Research and Applications (IJLERA) ISSN: 2455-7137 Volume – 02, Issue – 11, November – 2017, PP – 29-35.

[2]. Zirra Peter Buba & Gregory Maksha Wajiga.: Cryptographic Algorithms for Secure Data Communication. In: International Journal of Computer Science and Security (IJCSS), Volume (5): Issue (2): 2011.

[3]. A.Kahate, cryptography and network security (Third Edition). New Delhi: Tata McGraw Hill.2008.

[4]. Stallings, William, cryptography and network Security (6th edition.). Upper Saddle River, N.J.: Prentic Hall. pp. 67–68.

[5]. Delfs, Hans &Knebl, Helmut (2007). "Symmetric-key encryption". Introduction to cryptography: principles and applications. Springer. ISBN 9783540492436.

[6]. Matt J. B. Robshaw, Stream Ciphers Technical Report TR-701, version 2.0, RSA Laboratories, 1995

[7]. Solomon Kullback, Model Based Interface in the Life Sciences: A Primer on Evidence (New York: Springer 2008-01-01) 51-82.

[8]. Chandrasekaran J. et al. (2011): A Chaos Based Approach for Improving Non Linearity in the S-Box Design of Symmetric Key Cryptosystems in Meghanathan N. et al. Advances in Networks and Communications: First International Conference on Computer Science and Information Technology, CCSIT 2011, Bangalore, India, January2-4, 2011. Proceedings, Part 2. Springer. P.516.

[9]. Norman D. Jorstad.: Cryptographic Algorithm Metrics, January 1997.

[10]. Michael sipser, Introduction to the theory of Computation (Second Edition).

1*Authors Profile

Sri Ram Chandra. P has received his Bachelor's Degree in Computer science and Engineering from Andhra University, Master's Degree from GITAM University in the years 2010 and 2012 respectively. Currently he is a researcher in GITAM University with Mobile Computing and Cryptosystems Design & Cryptanalysis as research interests also he is a faculty member in CSE, Godavari Institute of Engineering and Technology (A), Rajahmundry, Andhra Pradesh, INDIA. He is a member of CSI. He has published 02 research papers in reputed International journals. He has 6 Years of Teaching Experience.

Dr.G.Venkateswara Rao has received his Master's Degree with Computer Science and Engineering as stream from Andhra University in 1999. He was awarded with Ph.D. from A.N.U. Guntur in 2010. He is serving the society with teaching as his profession past 20 years, of which the research experience is about 10 years. Currently he is working as Associate Professor in the department of Information Technology, GITAM-Deemed to be University, Andhra Pradesh, INDIA.

Dr.G.V.Swamy has received Masters and Doctoral Degrees from Andhra University. He is having more than 25 years of teaching experience of which research experience is about 10 years. Currently he is serving the GITAM-Deemed to be University as Professor and Head Electronics and Physics Department.

