International Journal of Advance Research in Science and Engineering
Vol. No.5, Issue No. 09 , September 2016
www.ijarse.com
IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

Security Analysis of data Method using MIPS Encryption Algorithm (MEA)

Sangeeta

sangeetaritu0@gmail.com

ABSTRACT

The MEA is an integral approach of block cipher and transposition cipher method. It takes 64 bit plain text input and produces 64 bit cipher text as in IDEA with modified key schedule to avoid possibilities of weak keys. It further makes transposition of the 64 bit cipher text to 128 bit end cipher text for disk storage. The increased length of end cipher text is a trade-off between the degree of increased security to SI and the nominal cost of storage media in the present state_of_the_art development.

Keywords: Encryption, Decryption, Block cipher, Transposition cipher, MEA

1. INTRODUCTION

Since PCs can be utilized to rapidly break credulous cryptosystems one should utilize encryption calculations that are free from and scientific shortcomings and that are computationally infeasible to break by making splitting additional tedious. In the meantime, the computational multifaceted nature of encryption and unscrambling ought to be inside sensible points of confinement since they speak to handling overheads too.

One calculation that is accepted to give a sensible trade off among these necessities depends on the Data Encryption Standards (DES) [4,5,10]. For as far back as 20 years, the best security the greater part of us have caught wind of has been given by DES. In spite of the fact that there has been a shortcoming of shrouded trapdoors through s-encloses DES [6,10], still it has been a decent and secure calculation against the mid seventies innovations. Presently with the appearance of rapid PCs it is confronting more feedback for not sufficiently giving security due to its 56 bit key size.

Some different calculations gave likewise been produced at the appointed time of time, for example, An Application of Chinese Remainder Theorem to Multiple-enter encryption in Database Systems[3] and A High Performance Encryption Algorithm [11] and so on.. These calculations likewise confront feedback for break because of existing break strategies like Brute power, Linear and Differential cryptanalytic techniques [14] and the advancement of high handling pace of PCs.

Keeping in mind the end goal to stay away from any cryptanalytic assault on figure content as a result of little key length in DES [6,10] another outstanding calculation IDEA (International Data Encryption Algorithm) [13], on 128 piece key with a square figure technique has been produced. It gives an intense encryption that opposes to a break plausibility emerging from fast of PCs of today and propelled break strategies [14]. This calculation deals with 64 bit

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

plain content information and produces 64 bit figure content. The outline theory behind this calculation is one of the blending activities from various arithmetical gatherings.

In contrast with DES, the calculation IDEA is by all accounts a more secure proposition in light of its 128 piece key approach yet to what extent it can remain to the difficulties postured by cryptanalytic strategies and expanding velocity of PCs is as yet an inquiry. The security of a figuring framework is such a testing field, to the point that it requests presentation of more up to date thoughts ordinary. The present encryption calculation named as MIPS1 Encryption Algorithm (MEA) is a stage forward toward this path and gives encourage protection from break than IDEA.

The Multilevel Information Protection System (MIPS) is an Information System which provides a relatively higher degree of security to a Sensitive Information (SI). The security to SI in MIPS is given by a MIPS Encryption Algorithm (MEA) and System Run Time Checker (SRTC): an Authentication module. The MEA works on user supplied 128 bit key whereas SRTC keeps monitoring of all unauthorized access on SI.

II MIPS Encryption Algorithm (MEA)

The MIPS Encryption Algorithm (MEA) chips away at symmetric key framework and is a change of IDEA [13] for more grounded encryption. It encodes SI in two passes. In the main pass it scrambles a contribution of 64 bit plain content (PT) in 64 bit figure content (CT2) utilizing square figure strategy with changed key timetable to take out frail keys of IDEA. The second pass changes over CT in end figure content (ECT) utilizing transposition figure strategy. The ECT at that point is utilized for capacity of encoded SI on circle. The expanded length of ECT can be viewed as an exchange off between the high security gave by this calculation and the ostensible cost of plate stockpiling media in current situation with the-workmanship advancement. The different strides of encryption/decoding of plain content in end figure content are appeared as takes after:

- Generation of encryption keys to encrypt PT in CT,
- Encryption of PT in CT,
- Encryption of CT in ECT,
- Decryption of ECT to CT,
- Generation of decryption keys to decrypt ECT to CT,
- Decryption of CT to PT

2.1 Generation of Encryption Keys to Encrypt PT in CT : The MIPS Encryption Algorithm is intended to encode SI in two passes. In the principal pass it scrambles a 64 bit plain content (PT) in 64 bit figure

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

content (CT). It requires a sum of 52 encryption keys with 16 bits each as in IDEA [13]. These 52 encryption keys are created from client inputted 128 piece enter by isolating it into 8 encryption keys with 16 bits each. The 96 bits out of 128 bits i.e. 6 encryption keys are utilized as a part of round1 of pass1. CT is utilized for transmission over Computer Networks.

The rest of the 32 bits are the initial two encryption keys for cycle 2. The 64 bits for four residual encryption keys of round2 are produced from coherent turn and Exclusive-OR task on encryption keys acquired from client provided 128 piece key. The third encryption key of round2 is produced from an Exclusive-OR task of 7 bits sensibly left pivoted first encryption key with legitimately 8 bits right turned second encryption key of round1. When all is said in done, the ith encryption key ($9 < I < 52$) is created from an Exclusive-OR activity of 7 bits legitimately left turned (I – 8)th encryption key with intelligently 8 bits right pivoted (I – 7)th encryption key.

2.2 Encryption of Plain Text in Cipher Text : Given a 64 bit plain text MEA converts it in a 64 bit cipher text as IDEA[3] with modified key schedule. It uses one logical and two algebraic operations for encryption as follows :

- Exclusive OR i.e. $x \otimes y = z$, $x \otimes z = y$, $y \otimes z = x$
- Addition Modulo 2^{16} (ignoring any overflow) i.e. Addition Modulo 2^{16} of x and y is (x+y) & 65535 (& stands for masking) ;
- Multiplication Modulo $2^{16}+1$ (ignoring any overflow) : We denote this operation as mul and show its result on two numbers x and y. This function is explained below :

```
unsigned mul(x,y)
unsigned x, y ;
```

[3] We have changed the notations of IDEA as per our convenience.

```
{
long int p ;
long unsigned q ;
if (x == 0) { p = 65537 – y} else if (y = = 0) { p = 65537 – x }
else { q = x * y ; p = (q & 65535) – (q >> 16) ; if (p <= 0) p = p + 65537 ; }
return (unsigned) ( p & 65535) } ;
```

The MEA divides 64 bit plain text data block in four sub-blocks as (pt1, pt2, pt3, pt4). It performs the operations as described above on these sub-blocks for eight rounds. After each round it produces four

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

intermediate output sub-blocks as ct11, ct12, ct13, ct14. The sequence of operations in each round is as follows :

(Notations :: ⊗ : Exclusive OR, ⊕ : multiplication modulo 2^{16} + 1 and & : masking)

ct1 = pt1⊕k1 ; ct2 = (pt2 + k2) & 65535 ; ct3 =)pt3 + k3) & 65535 ; ct4 = pt4 ⊕ k4 ;

ct5 = ct1 ⊗ ct3 ; ct6 = ct2 ⊗ ct4 ; ct7 = ct5 ⊕ k5 ; ct8 = (ct8 + ct7) & 65535 ; ct9 = ct8 ⊕ k6;

ct10 = (ct7 + ct9) & 65535 ; ct11 = ct1 ⊗ ct9 ; ct12 = ct3 ⊗ ct9 ; ct13 = ct2 ⊗ ct10 ;

ct14 = ct4 ⊗ ct10 ;

Here, the intermediate output after round1 is the four sub-blocks ct11, ct12, ct13 and ct14. The input data block for round2 is produced by swapping two inner sub-blocks i.e. ct12 and ct13. Thus the input data block for round2 is (pt1, pt2, pt3, pt4) such that :

pt1 = ct11 ; pt2 = ct13 ; pt3 = ct12 ; pt4 = ct14 ;

This input (pt1, pt2, pt3, pt4) is encrypted by using the encryption keys of round2 with a similar set of operations as performed above in round1. This process of encryption should be repeated for 8 rounds. The final output after round8 will have following operations :

ct1 = pt1 ⊕ k1; ct2 = (pt2 + k2) & 65535 ; ct3 = (pt3 + k3) & 65535 ; ct4 = pt4 ⊕ k4 ;

Thus, MEA outputs 64 bit cipher text (ct1, ct2, ct3, ct4) from the plain text (pt1, pt2, pt3, pt4) at the end of pass 1.

2.3 Encryption of Cipher Text in End Cipher Text : The pass 2 of the MEA converts 64 bit cipher text in 128 bit end cipher text (figure 1). We apply transposition cipher method in this pass. The input for this pass is the end product of pass1 i.e. cipher text {(ct_1, ct_2, ct_3, ct_4)| where each ct_i is of 16 bits}. We apply 2^8 modulo operation on each 16 bit sub-block of cipher text to split it into two components. Likewise all four sub-blocks of cipher text are split as under :

ct1 = (ct_{11}, ct_{12}) ; ct_2 = (ct_{21}, ct_{22}) ; ct_3 = (ct_{31}, ct_{32}) ; ct_4 = (ct_{41}, ct_{42}),

Here $ct_{i1} = ct_i \bmod 2^8$ and $ct_{i2} = ct_{i1} \otimes ((ct_i - ct_{i1}) / 2^8)$, [⊗ : Exclusive – OR].

Thus the input block produced for transposition in pass2 is a 128 bit block (ct_{11}, ct_{12}, ct_{21}, ct_{22}, ct_{31}, ct_{32}, ct_{41}, ct_{42}). The positions of these sub-blocks are assigned values 1,2,3,,,,,,8 sequentially for reference in a transposition key. This data block is now transposed to increase intricacy of encryption using a 128 bit transposition key supplied by the user. As an example if a user inputs a transposition key as "1,4,5,8,3,2,7,6" then the end cipher text produced is (ct_{11}, ct_{22}, ct_{31}, ct_{42}, ct_{21}, ct_{12}, ct_{41}, ct_{32}).

International Journal of Advance Research in Science and Engineering
Vol. No.5, Issue No. 09 , September 2016
www.ijarse.com
IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

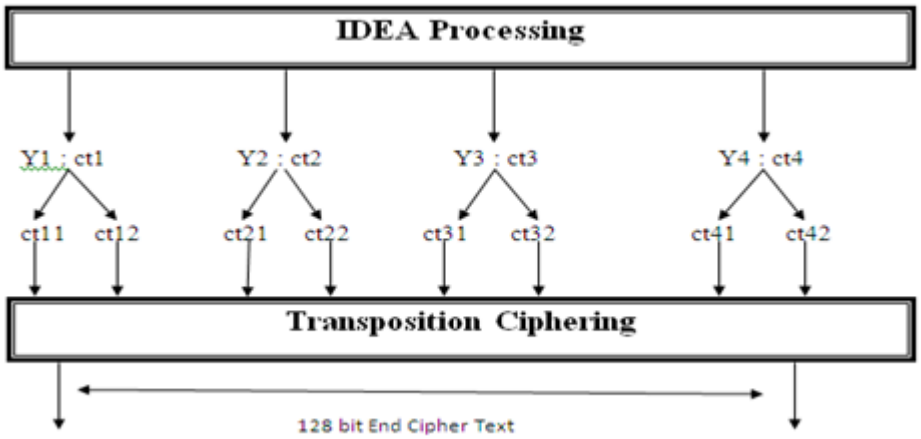

Figure 1: Application of Transposition Cipher Method

There are total 40320 transportation keys which can be used in pass2. Each transposition key k_i is a set of eight digits like $k_i = \{i_1, i_2, i_3, i_4, i_5, i_6, i_7, i_8 \mid i_j$ are distinct digits with $1 <= i_j <= 8\}$. Indeed, each i_j represents a sub-key from user inputted transposition key. However, a repetition of sub-keys may also be allowed with the condition that each transposition key has atleast six distinct sub-keys. The remaining two repeated sub-keys should then be replaced by the sub-keys s_i obtained from $S = \{s_1,s_2 \mid s_i \in \{1,2,,\ ,7,8\} - \{ i_1, i_2,\ldots, i_m \mid i_m$'s are distinct sub-keys in a transportation key$\}\ \}$ such that if $s_1 < s_2$ then s1 replaces at the first duplicating position from the left or vice-versa.

2.4 Decryption of End Cipher Text to Cipher Text : The unscrambling of end figure content to figure content is finished utilizing a similar transposition enter which was utilized as a part of encryption of end figure content from figure message because of our symmetric-key-framework encryption strategy. The sub-keys of transposition are masterminded in climbing request to hold places of information sub-squares of the end figure content like unique 128 piece information square created before transposition. The two 16 bits information sub-squares of along these lines got 128 piece information square are combined as (1,2), (3,4), (5,6) and (7,8) and afterward changed over into one piece of 16 bits utilizing the turnaround ventures of the activities. Hence, the yield delivered toward the finish of unscrambling of ECT to CT is a 64 bit figure content which for sure is same as final result of pass1.

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

2.5 Decryption of Cipher Text to Plain Text: The unscrambling rationale of figure content to plain content after decoding of ECT to CT is bit dubious and requires some doing. The use of decoding keys is position savvy [Table1-2] and depends on foundation of swapping of two inward sub-squares of info information obstruct from first to eight adjusts in pass1. The age of decoding keys depends on the backwards of capacities utilized for encryption, along these lines, the unscrambling keys are added substance and multiplicative reverse of encryption keys utilized as a part of pass1 and can be comprehended as takes after :

- **Decryption key produced from an additive inverse of an encryption key :** The decryption key corresponding to i^{th} encryption produced from an additive inverse is $2^{16} – i^{th}$ encryption key.
- **Decryption key produced from a multiplicative inverse of an encryption key :** The decryption key corresponding to an encryption key produced from a multiplicative inverse is based on Euclidean God Algorithm. The details of this algorithm to find a multiplicative inverse of an encryption key, say xin, can be understood as follows. It returns k as multiplicative inverse.

```
unsigned inv (xin)
usigned xin
if (xin == 0) b2 = 0
else {n1 = 65537 ; n2 = xin ; b2 = 1 ; b1 = 0
do {
r = 65537 mod xin ; q = (n1 – r) / n2 ;
if (r == 0) { if (b2 < 0) b2 = 65537 + b2 }
else n1 = n2 ; n2 = r ; t = b2 ; b2 = b1 – q * b2 ; b1 = t ;
} while (r! = 0) ;
K = (unsigned) b2 ;
return k ;
}
```

The decryption of 64 bit cipher text (CT) to 64 bit plain text (PT) follows the same logic as of encryption of CT from PT using decryption keys in place of encryption keys. The application of decryption keys (position wise) can be understood from Table 1-2.

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

Table 1 : Encryption keys (position wise)							Table 2 : Decryption Keys (position wise)						
Round 1	1	2	3	4	5	6	Round 1	49^{-1}	-50	-51	52^{-1}	47	48
Round 2	7	8	9	10	11	12	Round 2	43^{-1}	-44	-45	46^{-1}	41	42
Round 3	13	14	15	16	17	18	Round 3	37^{-1}	-38	-39	40^{-1}	35	36
Round 4	19	20	21	22	23	24	Round 4	31^{-1}	-32	-33	34^{-1}	29	30
Round 5	25	26	27	28	29	30	Round 5	25^{-1}	-26	-27	28^{-1}	23	24
Round 6	31	32	33	34	35	36	Round 6	19^{-1}	-20	-21	22^{-1}	17	18
Round 7	37	38	39	40	41	42	Round 7	13^{-1}	-14	-15	16^{-1}	11	12
Round 8	43	44	45	46	47	48	Round 8	7^{-1}	-8	-9	10^{-1}	5	6
Round 9	49	50	51	52			Round 9	1^{-1}	-2	-3	4^{-1}		

III MEA SECURITY

MIPS Encryption Algorithm (MEA) is conceived in such a way in such a way, to the point that it will keep running from 16 bit machine onwards. The testing of MEA has been performed on the scope of machines including most recent Intel Core Processors and 64 bit RISC machines and has been fruitful. The previous information encryption calculation DES requires just 256 encryptions for break. A million chips equipped for testing a million keys every second can soften DES up 20 hours. In the event that one can plan a chip fit for testing a billion keys every second and uses a billion of them to tackle the issue then it will enjoy 1013 years to reprieve IDEA. Our calculations mirror that with a similar plan particulars of an arrangement of chips as to break encryption of IDEA, a period of 2x1013 years will be required to break MEA utilizing a strategy for beast compel however the inquiry is that would one be able to truly outline a machine with a variety of one billion chips with such required abilities. Yet at the same time MEA is new and is available to challenges.

This Privacy Policy depicts the routes together with its parent and auxiliary substances, "Security MEA", "we", "us", or "our" accumulates individual data, our data sharing practices, and how online clients, occasion registrants and endorsers may ask for changes to the way their own data is shared.

3.1 Individual Information We Collect

"Individual Information" implies any data got through your utilization of our sites which may sensibly be utilized to explicitly distinguish you and may incorporate your name, title, organization, address, email and telephone number. We gather individual data when you give it to us, for example, when you buy in to the Security MEA (either straightforwardly with us or through another organization, for example, a

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

membership office), agree to accept email bulletins, participate in a challenge, enlist for webpage enrollment or an online occasion, take an interest in overviews, go to eye to eye occasions, or generally speak with us. A few of the administrations that we offer, including however not restricted to record downloads, message sheets, webcasts and online public exhibitions, require enrollment as a state of utilization; when you enlist with, or sign into one of our destinations, you are not any more unknown. We may likewise get data about you from different sources and add it to the data you have given to us.

IV CONCLUSION

The author tried MEA utilizing various basic methodologies of an aggressor and watched that MEA gives moderately higher level of security. This calculation is by all accounts better secured because of the presentation of transportation figuring. It without a doubt intricates crafted by a cryptanalyst by including a look for a transportation key which was utilized to encode CT to ECT since we split 16 bits of figure content into two sections where one section is a modulo 28 of figure content sub-piece and other part is Exclusive-OR of the rest of remainder of CT with same activity. We additionally transpose along these lines delivered information sub-hinders by transposition. Subsequently while unscrambling, an expert may never make sure of finding a right code even in the wake of attempting all mixes of transposition since some false mixes may likewise be delivered because of the way that we have part each sub-square of figure content into two sections which can be spoken to in ASCII code.

Truth be told, part a CT in two sections is an endeavor to debilitate the use of technique for animal power which regularly guarantees arrangement. Moreover the utilization of differential cryptanalysis [14] may not be a simple assignment for aggressor. Indeed, even the techniques like known content may not be an effective assault on MEA as is the situation with the figure strategy.

In spite of the fact that the security of an Information System may request some progressing changes and changes in the present calculation to address up and coming difficulties, however at display the calculation MEA in MIPS looks secured for break. One may not deny the way that security locks are broken time to time rousing specialists for additionally work in this field. Who realizes what break may turn out tomorrow for MEA.

REFERENCES

[1]. D.E.Denning, Cryptography & Data Security, Addison Wesley Publication, 1982, Reading, M.A..

[2]. C.J.Holloway, “Controlling the Use of Cryptographic Keys”, Computer Security (UK), Vol 14, No.7, 1995, pp 587-598.

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

[3]. Modugu, R., Yong-Bin Kim, Minsu Choi, "Design and performance measurement of efficient IDEA (International Data Encryption Algorithm) crypto-hardware using novel modular arithmetic components ",Instrumentation and Measurement Technology Conference (I2MTC), 2010 IEEE

[4]. M.D.Abrams, H.J.Podell (eds.), "Computer and Network Security", IEEE Computer Society", 1987, Washington, DC.

[5]. Biham Ali, "New Type of Cryptanalytic Attacks Using Related Keys", Jcryptol, Vol 7, No.4, Fall 1994, pp 229-242.

[6]. Rodeny H.Cooper, Willaim Hyslop and Wayne Patterson," An Application of the Chinese Remainder Theorem to Multiple-key Encryption in Data Base Systems", Proc IFIP/Sec84, Canada, Spet 84, pp 553-556.

[7]. "Data Encryption Standards", Federal Information Processing Standards Publication 46, National Bureau of Standards, 1977, Washington.

[8]. Bruce Schneier, "A IDEA Encryption Algorithm", Dr Dobbs Journal, Dec1993, pp 50-56.

[9]. Bruce Schneier, "Differential and Linear Cryptanalysis", Dr.Dobbs Journal (USA), Vol 21, No.1, Jan 1996, pp 42-48.

[10]. M.P. Leong, O.Y.H. Cheung, K.H. Tsoi and P.H.W. Leong, "A Bit-Serial Implementation of the International Data Encryption Algorithm IDEA," 2000 IEEE Symposium on Field-Programmable Custom Computing Machines, IEEE (2000), pp. 122-131.

[11]. E.B.Fernandez, R.C.Summer and C.Wood, Data Security & Integrity, Reprinted 1983, Addison Wesley Publishing Co..

[12]. M.E.Hellman, "DES Will be Totally Insecure Within Ten Years", IEEE of Software Spectrum, Vol.16 July 1978, pp 40-41.

[13]. Gerd E.Keiser, "Local Area Networks", 1989, MGH International Edition.

[14]. R. Gupta, A. Aggarwal & S. K. Pal, "Design and Analysis of New Shuffle Encryption Schemes for Multimedia", Defence Science Journal, Vol. 62, No. 3, May 2012, pp. 159-166.

[15]. Pankaj Rakheja, Amanpreet kaur, "A Unique Cryptographic Mechanism for Encoding Data Using DNA Structure", in International conference on Network Communication and Computers (ICNCC 2011) organized and sponsored by IACSIT, The Institute of Electrical and Electronics Engineers (IEEE), Singapore Institute of Electronics and other organizations.

[16]. W.Deffie, M.E. Hellman, "Exhaustive Cryptanalysis of NBS Data Encryption Standards", Computer, Vol.10, June 1977, pp 74-84.

[17]. Nabarun Bagchi, "Secure BMP Image Steganography Using Dual Security Model (I.D.E.A, image intensity and Bit Randomization)and Max-Bit Algorithm" *International Journal of Computer Applications* 1(21):18–22, February 2010.

[18]. Chong Fu, Zhen-chuan Zhang , Ying-yu Cao. " An improved image encryption algorithm based on chaotic maps" Third International Conference on Natural Computation. 2007, Vol. 13, pp.189-193.

[19]. Michalski, A., Buell, D., Gaj, K., "High-throughput reconfigurable computing: design and implementation of an IDEA encryption cryptosystem on the SRC-6E reconfigurable computer"Field Programmable Logic and Applications, 2005. Page(s): 681 - 686

[20]. J. Chen, "A DNA-based, biomolecular cryptography design," in IEEE International Symposium on Circuits and Systems (ISCAS), 2003, pp. 822–825

[21]. Sanchez-Avila, C. Sanchez-Reillol, "The Rijndael block cipher (AES proposal) : a comparison with DES" 2001 IEEE 35th International Carnahan Conference on Security Technology.

[22]. W.E.Madryga, A High Performance Encryption Algorithm", Proc IFIP/Sec84, Canada, Spet84, pp 557-570.

[23]. J.Reid, "Open Systems Security : Traps And Pitfalls", Computer Security (UK), Vol 14, No.6, 1995, pp 496-517.

[24]. Payal Maggo and Rajender Singh Chhillar., "Lightweight Image Encryption Scheme for Multimedia Security.", *International Journal of Computer Applications* 71(13):43-48, June 2013.