I. J. Computer Network and Information Security, 2017, 9, 46-53
Published Online September 2017 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2017.09.06

New Design of Tiny-Block Hybridization in AES

Ritu Goyal
NorthCap University/CSE, Gurugram, 122001, India
E-mail: ritugoyal1104@gmail.com

Mehak Khurana
NorthCap University/CSE, Gurugram, 122001, India
E-mail: mehakkhurana@ncuindia.edu

Received: 20 February 2017; Accepted: 17 April 2017; Published: 08 September 2017

Abstract—The cryptographic algorithm designed to enhance security in real life which storage track and increase speed. This is kind of Feistel cipher which real use for the processes from assorted (mixed/orthogonal) algebraic collections. AES is combined with segmentation and validation algorithm to improve the performance of the security. Also, Key expansion is done to make the AES more secure. The processes are pipelined to increase the speed of AES. Our strategies that are hybrid method which work as change the original files (data) into encoded/encrypted type using AES and Tiny Encryption Process. The hybrid Procedure is considered for easiness and improved performance. The encryption pattern, data is encoded using tiny-AES-128 encryption process and authentication SHA that alterations it into an indecipherable cipher text. In process of encryption that encodes the information which consider a random text through the idea of cryptography and then data/text for the user. Our proposed approach get minimize computational time and memory utilization which simulated in MATLAB 2014Ra.

Index Terms—Encryption, Decryption AES Encryption, Cryptography, security and TINY encryption.

I. Introduction

Today, cryptology hugely used in commercial applications. Generally, encryption/decryption platform implement the unique key generation of the crypto system. If we want generate defensive trustworthy data, then cryptosystem is providing highly secure for both individuals and sets. On the other hand, the most significant aim of cryptography is gives privacy and it is also arranged for results for other difficulties such as: data integrity/reliability, verification, non-repudiation. Basically, method of Cryptography which gives the permission for secure data sending and receiving for user, when data sent to receivers from sender then only receiver can able to see the data not anyone other that's called a Confidential method. The Symmetric encryption systems considered for source controlled devices that only a restricted past. Tiny Encryption Algorithm is an instance of cipher considered especially for resource constrained devices. TEA is commonly known as Yuval's proposal [1,2]. Earlier cipher does not give efficient resistance to differential and linear cryptanalysis attacks. Block ciphers in recent days, similar the Rijndael (AES) concentrates on deciding a composition of information safety, hardware/software complexity, and overall efficiency. Subsequently, when required a novel encryption/decryption which bestows with appropriate explanation for source controlled schemes.

II. Cryptology

Cryptography has big ability to protect the data using converting it into a scribbled form. The encrypted data is called as cyphertext. At the receiver end, the permission of access deciphers the message into plain text for receiving the original data that have exact info about secret key. Sometimes encrypted messages can be broken down by cryptanalysis, which is known as code breaking. Cryptography can be classified into two type's symmetric-key schemes and Asymmetric-key schemes. In symmetric-key encryption systems source and destination of the message make usage of the identical key; this unique key is used for encryption as well as decryption of the message. In the second type, which is asymmetric cryptography, a pair of answers is used for encryption as well as decryption of the message to provide security.

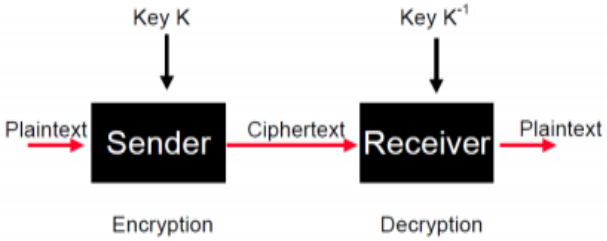

Fig.1. Cryptographic Technique.

In cryptography system encryption is the maximum active method for achieving records safety. To process an encrypted message must have proceeded to a secret password or key which makes decryption. Also, Decryption is the procedure of changing encrypted files back into the unique format, so that it can be implicit through the end user.

A. Basic Terms Used in Cryptography

(a) Encryption

A process of the original message into an unreadable from is known as Encryption.A process of converting Plain Text into Cipher Text is called as Encryption. Cryptography uses the encryption technique to send the confidential information over an channel. The process of encryption requires two things- an encryption algorithm and a key. An encryption algorithm means the technique that has been used in encryption. Encryption takes place at the sender side. Encryption Algorithm is used to make content unreadable by all but the intended receivers.

Encrypt(plaintext,key)=ciphertext
Decrypt(ciphertext,key) = plaintext

(b) Decryption

A reverse process of encryption is called as Decryption. It is a process of converting Cipher Text into Plain Text. Cryptography uses the decryption technique at the receiver side to obtain the original message from non-readable message (Cipher Text). The process of decryption requires two things- a Decryption algorithm and a key. A Decryption algorithm means the technique that has been used in Decryption. Generally, the encryption and decryption algorithm are same.

B. Types of cryptographic algorithms

There are several ways of classifying cryptographic algorithms. In this paper, they will be categorized based on the number of keys that are employed for encryption and decryption. The three types of algorithms are:

- Secret Key (Symmetric) Cryptography (SKC): Uses a single key for both encryption and decryption.
- Public Key (Asymmetric) Cryptography (PKC): Uses one key for encryption and another for decryption.
- Hash Functions: Uses a mathematical transformation to irreversibly "encrypt" information.

C. Security Functions of Cryptography

Cryptography is most often associated with the confidentiality of information that it provides. However, cryptography can offer the following four basic functions:

(a) Confidentiality

Assurance that only authorized users can read or use confidential information. For example, unauthorized users might be able to intercept information, but the information is transmitted and stored as cipher text and is useless without a decoding key that is known only to authorized users.

(b) Authentication

Verification of the identity of the entities that communicate over the network. For example, online entities can choose to trust communications with other online entities based on the other entities ownership of valid digital authentication credentials.

(c) Integrity

Verification that the original contents of information have not been altered or corrupted. Without integrity, someone might alter information or information might become corrupted, and the alteration could be undetected. For example, an intruder might covertly alter a file, but change the unique digital thumbprint for the file, causing other users to detect the tampering by comparing the changed digital thumbprint to the digital thumbprint for the original contents.

(d) Nonrepudiation

Assurance that a party in a communication cannot falsely deny that a part of the actual communication occurred. Without nonrepudiation, someone can communicate and then later either falsely deny the communications entirely or claim that it occurred at a different time. For example, without nonrepudiation, an originator of information might falsely deny being the originator of that information. Likewise, without nonrepudiation, the recipient of a communication might falsely deny having received the communication.

D. Basically, cryptography depend on Symmetric and asymmetric

Cryptographic techniques involve a general algorithm, made specific by the use of keys. There are two classes of algorithm:

Those that require both parties to use the same secret key. Algorithms that use a shared key are known as symmetric algorithms. Figure 1 illustrates symmetric key cryptography.

Those that use one key for encryption and a different key for decryption. One of these must be kept secret but the other can be public. Algorithms that use public and private key pairs are known as *asymmetric* algorithms. Fig2 illustrates asymmetric key cryptography, which is also known as *public key cryptography*.

The encryption and decryption algorithms used can be public but the shared secret key and the private key must be kept secret.

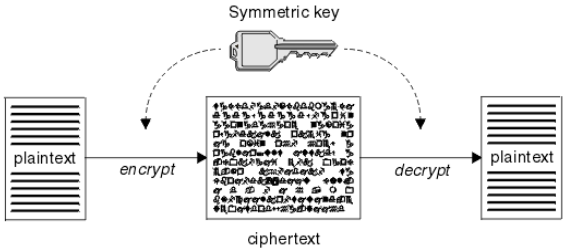

Fig.2. Symmetric Key Cryptography

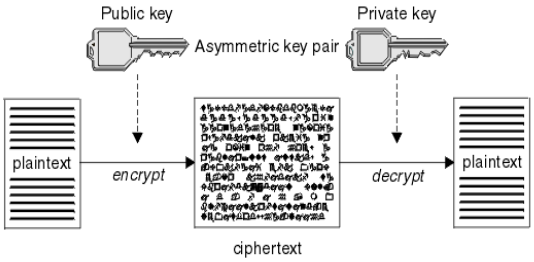

Fig.3. Asymmetric Key Cryptography

Fig.2 shows plaintext encrypted with the receiver's public key and decrypted with the receiver's private key. Only the intended receiver holds the private key for decrypting the ciphertext. Note that the sender can also encrypt messages with a private key, which allows anyone that holds the sender's public key to decrypt the message, with the assurance that the message must have come from the sender.

With asymmetric algorithms, messages are encrypted with either the public or the private key but can be decrypted only with the other key. Only the private key is secret, the public key can be known by anyone. With symmetric algorithms, the shared key must be known only to the two parties. This is called the key distribution problem. Asymmetric algorithms are slower but have the advantage that there is no key distribution problem.

E. Challenges of cryptography

We live in an era of inconceivably quickly progressing, remarkable machineries that allow prompt current of information – anytime, anywhere. The merging of computers and networks has been the key force last the growth of these respect stimulating skills. Collective use of schemes constructed using this Information Technologies (IT) is having a deep effect on our usual lives. These apparatuses are attractive all dominant and worldwide.

- The coding and decoding key controlling problems that rise reason behind dispersed countryside of IT properties, as fit the circulated environment of their controller, the last divided between numerous cloud performers. Moreover, the design of delivery differs through the kind of provision contribution - Organization as a Service (IaaS), Stage as a Service (PaaS) and Software as a Service (SaaS).
- The distinct experiments complex in organizing coding and decoding key organization purposes it can happen the safety necessities of the cloud Consumers, dependent upon the nature of the facility and the type of data produced/managed/stored through the service types.

F. Importance of the cryptography

Cryptology is receiving progressively significant in the evidence civilization; it is likewise suitable less and less visible. Cryptography combined into smart cards for commercial contacts, web browsers, working schemes, mobile phones and electric character cards. This achievement clarified through numerous issues: 1st, nearby it strong requirement for coding and decoding clarifications, 2nd acceptable procedures and procedures has industrialized and 3rd the declining cost of calculation types it low-cost to tool symmetric and uniform unequal cryptography.

- Low cost and/or low power: It can be attained via openhanded active high performance or high safety; this method is important to permit for addition of crypto in level the least strategies (e.g., ambient intellect). Project aims application of a rivulet code that suggestions a sensible safety level (say 80 bits) with usages less than 1000 gates.
- High performance: This is compulsory for extremely effectual explanations for requests such as bus encryption, hard disk encryption, and encryption in Terabit networks.
- High safety: particular use areas need coding and decoding procedures and procedures that can suggestion a developed self-assurance and assertion equal than the formal of the ability.

III. Tiny Encryption Algorithm - TEA

To the requirement for tiny encryption algorithm circumstances a 128-bit key separated into four 32-bit keywords & the block size of each encoded is 64 bits, of that is to be separated into two 32-bit. TEA uses a Feistel structure for encryption series in which 1 round of TEA comprises 2 Feistel processes and a sum of superfluities and bitwise XOR processes as presented in Fig. 2.

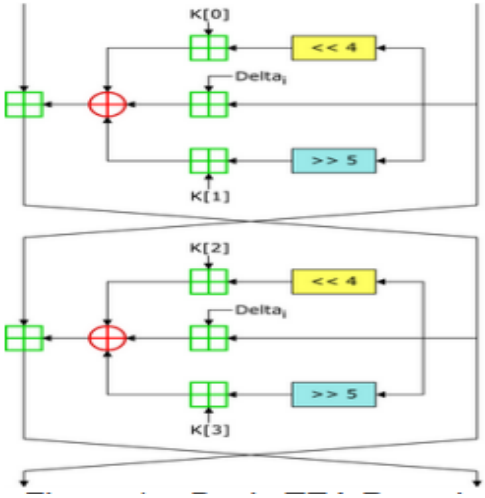

Fig.4. Simple Tiny Encryption Algorithm

The specification simply "suggests" that 32 TEA rounds be completed for each 64-bit block encrypted, all online resources appear to follow this suggestion.

TEA utilizes a value denoted as DELTA in the description which is defined as ($\lfloor 5 - 1 * 2^{31}$) which is "derived from the golden ratio" is used in multiply for every cycle to check as symmetry activities on the Feistel processes as presented in figure 1. The key program basically occurs as special OR'ing the keywords with a removed value of the previous state of every block words, this process "causes all bits of the key and data to be mixed repeatedly". For tiny encryption algorithm is alert a high-speed procedure as there is effectively set up or difficult key program for the cryptography procedure.

IV. Problem Statement

As the wireless and mobile devices use, has been increased, security has become the major concern. The issue is strong cipher algorithms are very expensive and not practical for lightweight applications. So, there is a need to create cryptographic primitives which are feasible for area restricted devices without any loss of its cryptographic strengths. The Advanced Encryption Standard (AES) block cipher is known for its great security. But, the e requirement for AES is very high for low resource devices. So, it's a need to create a lightweight algorithm which provide confidentiality with very less resource and power consumption.

We design a well-organized and real time feasible application for AES and TINY system which customs symmetric keys with encryption and decryption afterward project a procedure for its use in many user data-centric requests.

V. Method

The projected scheme considered into two parts: the sender's view and the receiver's view as presented in Fig. 3 and Fig. 4.

The secret txt is encoded through AES-128 encryption process using secret key from sender's side. After that the encrypted text is implanted into a 8*8 blocks by Tiny algorithm and it can produce the minimum response for sender's.

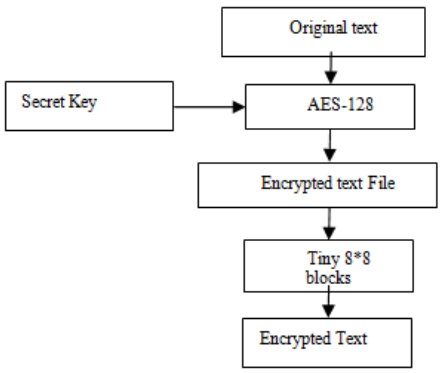

Fig.5. Block Diagram from the Sender'S View

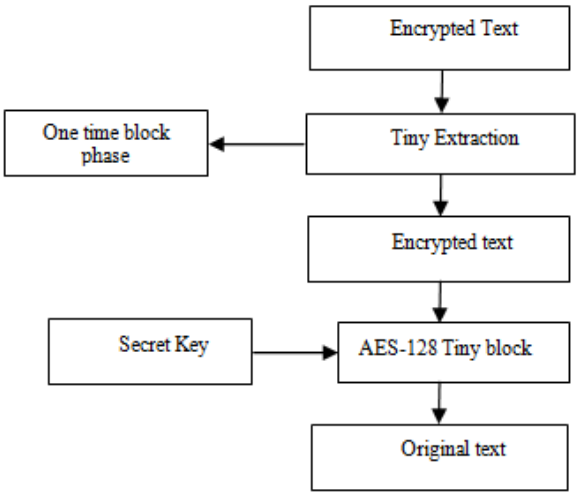

Fig.6. Block Diagram from the Receiver'S View

The encoded text is mined from the tiny blocks through using s-box mining system at the receiver's side. The mined secret text is decoded through the AES procedure with the mutual secret key and the unique message/packet is formerly created.

A. Proposed Line for Tiny-Block hybridization in AES-128

One of the most common implementation of encrypting the data that is converting the plain text in to cipher text and decrypting the data is by using the single core system Here only one core is used irrespective of the size of the file which has to be encrypted or decrypted. This method will work slowly if the data file is big in size. It may work well for data files which are small but it is sure that it takes much longer time to encrypt and decrypt the data for bigger files. So as to overcome the above-mentioned drawbacks and make improvements in the field of AES implementation, a parallel core processor is introduced in the paper. With this method, we made improvements in the conventional methods by reducing the run time process. AES is a symmetric key segment cryptography procedure. AES block cipher has 128, 192 or 256 bit keys to encrypt or decrypt data in blocks of 128-bits. AES has a discrete key development stage for the increase of 128, 192 or 256-bit keys so that these keys can be helped in numerous circles of cryptography process [11].

B. For encryption, every round involves the Subsequent four steps:

Sub Bytes – a non-linear replacement stage where every byte is substituted with alternative allowing to a lookup counter (S-box). This stage is basically a stand lookup utilizing a 16×16 matrix of byte values termed as s-box. This matrix comprises of each probable arrangements of an 8-bit order (2*8 = 16 × 16 = 256) [10] [12]. It again, the s-box is not only a random variation of these capacities and there is an all-around measured method for formation the s-box tables [13]. Over the matrix that becomes functioned upon all over the encryption is identified as state. This alteration completed

of 2 phases: (i). Multiplicative inverses of every byte in the state. (ii). the outcome in this step is gained from phase (i) by altering y = f(x) Shift Rows – an inversion step where every row of the state is shifted regularly a positive number of times. Shift row convert the line of state which accumulative the offset of rotation moves left, first line unaffected. Another line loop left 1 byte, third line loop left 2 bytes, likewise fourth line loop 3 bytes [10][9]. The Inverse Shift Rows revolution achieves these circular shifts the further technique for every of the last three lines. Mix Columns – a mixing process which works on the columns of the state, merging the four bytes in every column. It creates complicate changes to columns in the state. Efficiently a matrix increase in GF (28) using prime poly m(x) =x8+x4+x3+x+1. Add Round Key – every byte of the state is joint with the round key; each round key is resulting from the cipher key using a key program. In this phase the 128 bits of state are bitwise XOR with the 128 bits of the round key. The process is perceived as a column wise procedure among the 4 bytes of a state column and single word of the round key. This conversion is as straightforward as would be sensible which supports in productivity though it also affects all of state. A small modification of this block based procedure can recover the entire text/data. Such modification of the block preparation of text is designated as S-Block retrieve. For instance, 4 × 4 non-overlying blocks for storage in matrix formation shifted from standard and size (N×M) box which gotten through M rows from the top and *N* columns from left. Let us signify the cropped image by $\hat{I}_{u;v}$ is (N-4) × (M-4).

Let's denote the round based block

$$\hat{I}_{u,v} \hat{I}_{u,v} = I - \hat{I}_{u,v}$$

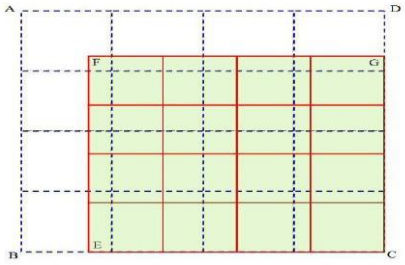

Fig.7. Tiny S-Block Based Reconstruction from S-Box

Another possible way of retrieve is to use a block size other than 4 × 4 i.e. using blocks of sizes $\boldsymbol{m} \times \boldsymbol{n}$ where $\boldsymbol{m} \neq \mathbf{4}$ and $\boldsymbol{n} \neq \mathbf{4}$. In such a case, the quantization matrix Q has to be changed accordingly to size $\boldsymbol{m} \times \boldsymbol{n}$ at the time of data extraction.

The TEA is a kind of Feistel type ciphers which usages operations from mixed (orthogonal) arithmetical groups XOR, ADD and SHIFT. A dual shift causes all bits of the data and key to be assorted commonly. The key program process is modest; the 128-bit key K is separated into four 32-bit blocks K = (K[0], K[1], K[2], K[3]). Tiny encryption algorithm aspects to be extremely resilient to difference cryptanalysis (Biham et al., 1992) and achieves whole dispersion (where a one bit alteration in the plaintext will cause about 32 bit differences in the cipher text). Time routine on a workstation is very stirring of this approach.

C. Steps involved in research

The Encoded file is in print on MATLAB platform and accepts a 32-bit word size. The 128 bit key is divided into four portions and is put in storage k [0] - k [3] and the Data is kept in v[0] and v[1].

1. Make m×n non-overlapping block separating size of AES-128 matrix
2. Let designate this set of blocks by $P_{I\,u,\,v}^{(m\times n)}$
3. Select a set of blocks from $P_{\hat{I}\,u,\,v}^{(m\times n)}$ (using a key common through both ends) and achieve the cypher text in every nominated block by every standard SHA based authentication scheme. The quantization matrix *Q* which is a shared secret is used for finding the quantized coefficients.
4. Apply DE quantization and Inverse for same size of block matrix would be extracted for small size of message.

The sender sends A to the receiver B.
Then Decryption side
Receiver B essential does the subsequent:

1. Get the cipher text () from A.
2. Calculate (r) as follows:

$$r = y^{p-1-x} \bmod p$$

3. Improve the plaintext as follows:

$$m = (r * z) \bmod p$$

The TEA usages adding and calculation as the flexible operatives in its place of XOR. The TEA encryption routine depends on the alternative use of XOR and ADD to deliver nonlinearity. The procedure has 32 cycles (64 rounds). TEA is short sufficient to inscribe into virtually some sequencer on any computer.

The block based Tiny Encryption Algorithm (B-TEA) is a block cipher encryption procedure that is very modest to device has fast implementation time, and takings nominal storing space [2].

VI. RESULT

This work presents the hybrid cryptography of the Tiny Encryption and AES-128 Set of rules. In this investigation, we reviewed the best collective approaches in the cryptanalysis of a block cipher system.

The resultant of Public-Key Processes is symmetric, that is to approximately use to encode the text or given text by user is different from the key used to decrypt the message. The encryption key, identified as the Public key which used to encrypt a message, but the message can only be deciphered through the information that has the decryption key, recognized as the private key. This type

of encryption has a quantity of advantages over usual symmetric Ciphers. It means that the recipient can create their public key approximately available- someone deficient to send them a communication usages the procedure and the receiver's public key to do so. A viewer may have both the procedure and the public key, but will still not be capable to decrypt the message. Individual the receiver, with the private key can decrypt the message.

```
s_box : 63 7c 77 7b f2 6b 6f c5 30 01 67 2b fe d7 ab 76
        ca 82 c9 7d fa 59 47 f0 ad d4 a2 af 9c a4 72 c0
        b7 fd 93 26 36 3f f7 cc 34 a5 e5 f1 71 d8 31 15
        04 c7 23 c3 18 96 05 9a 07 12 80 e2 eb 27 b2 75
        09 83 2c 1a 1b 6e 5a a0 52 3b d6 b3 29 e3 2f 84
        53 d1 00 ed 20 fc b1 5b 6a cb be 39 4a 4c 58 cf
        d0 ef aa fb 43 4d 33 85 45 f9 02 7f 50 3c 9f a8
        51 a3 40 8f 92 9d 38 f5 bc b6 da 21 10 ff f3 d2
        cd 0c 13 ec 5f 97 44 17 c4 a7 7e 3d 64 5d 19 73
        60 81 4f dc 22 2a 90 88 46 ee b8 14 de 5e 0b db
        e0 32 3a 0a 49 06 24 5c c2 d3 ac 62 91 95 e4 79
        e7 c8 37 6d 8d d5 4e a9 6c 56 f4 ea 65 7a ae 08
        ba 78 25 2e 1c a6 b4 c6 e8 dd 74 1f 4b bd 8b 8a
        70 3e b5 66 48 03 f6 0e 61 35 57 b9 86 c1 1d 9e
        e1 f8 98 11 69 d9 8e 94 9b 1e 87 e9 ce 55 28 df
        8c a1 89 0d bf e6 42 68 41 99 2d 0f b0 54 bb 16
```

Fig.8. S-box matrix

```
inv_s_box : 52 09 6a d5 30 36 a5 38 bf 40 a3 9e 81 f3 d7 fb
            7c e3 39 82 9b 2f ff 87 34 8e 43 44 c4 de e9 cb
            54 7b 94 32 a6 c2 23 3d ee 4c 95 0b 42 fa c3 4e
            08 2e a1 66 28 d9 24 b2 76 5b a2 49 6d 8b d1 25
            72 f8 f6 64 86 68 98 16 d4 a4 5c cc 5d 65 b6 92
            6c 70 48 50 fd ed b9 da 5e 15 46 57 a7 8d 9d 84
            90 d8 ab 00 8c bc d3 0a f7 e4 58 05 b8 b3 45 06
            d0 2c 1e 8f ca 3f 0f 02 c1 af bd 03 01 13 8a 6b
            3a 91 11 41 4f 67 dc ea 97 f2 cf ce f0 b4 e6 73
            96 ac 74 22 e7 ad 35 85 e2 f9 37 e8 1c 75 df 6e
            47 f1 1a 71 1d 29 c5 89 6f b7 62 0e aa 18 be 1b
            fc 56 3e 4b c6 d2 79 20 9a db c0 fe 78 cd 5a f4
            1f dd a8 33 88 07 c7 31 b1 12 10 59 27 80 ec 5f
            60 51 7f a9 19 b5 4a 0d 2d e5 7a 9f 93 c9 9c ef
            a0 e0 3b 4d ae 2a f5 b0 c8 eb bb 3c 83 53 99 61
            17 2b 04 7e ba 77 d6 26 e1 69 14 63 55 21 0c 7d
```

Fig.9. Inverse S-box matrix

The encrypted message is

25	0	5	0	11	15
0	0	1	23	13	0
0	23	0	0	0	27
0	0	27	0	0	0
7	23	0	0	23	9
0	7	0			

The decrypted mes in ASCII is

57	32	37	32	43	47
32	32	33	55	45	32
32	55	32	32	32	59
32	32	59	32	32	32
39	55	32	32	55	41
32	39	32			

The decrypted message(Theoritical) is: Columns 1 through 15

105 116 109 32 99 111 108 108 97 103 101 32 104 103 106

Columns 16 through 30

104 100 115 32 120 115 104 106 100 119 103 32 104 103 121

Columns 31 through 33

100 119 32

The decrypted message(Present) is: ‘work with full dedication’

Time Complexity for Existing Technique: 7.666132e-01

Original message: ‘work with full dedication’

Integer representation: 105 116 109 32 99 111 108 108 97 103 101 32 104 103 106 104 100 115 32 120 115 104 106 100 119 103 32 104 103 121 100 119 32

Key Pair using Tiny-

Modulus: 943

Ciphertext: 564 231 290 706 895 281 807 807 792 733 545 706 808 733 7 808 420 759 706 424 759 808 7 420 18 733 706 808 733 607 420 18 706

Decrypted Message: ‘work with full dedication’

Authentication:

Signature: 455 714 659 788 520 227 239 239 663 33 52 788 358 33 546 358 324 736 788 916 736 358 546 324 877 33 788 358 33 77 324 877 788

Is Verified: 1

Time Complexity for proposed Technique: 7.666132e-01

Decryption time

Elapsed time is 0.222523 seconds.

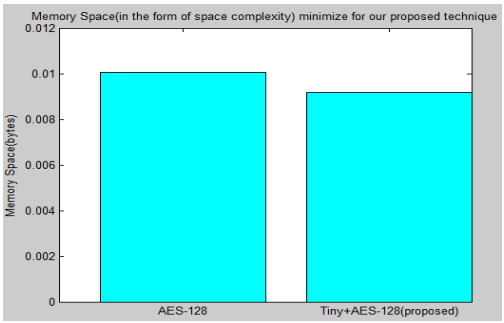

Fig.10. Memory Space (In the Form of Space Complexity) Minimize for Our Proposed Technique

As we seen in above result figure that the memory space of basic AES-128 is more than the Hybrid Tiny + AES

This planned scheme efforts on the secure approach of light weight cryptographic procedure. Tiny Encryption Algorithm to adjust with countless real time restraints

like memory space. The proposed scheme uses block based.

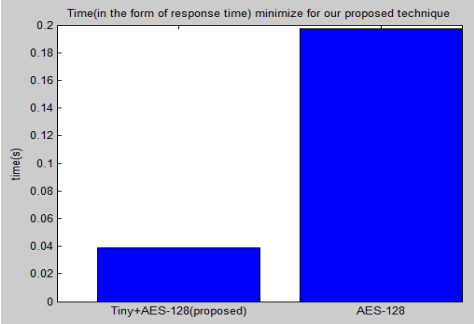

Fig.11. Comparison between AES-128 and Tiny-AES-128 with Respect To Tiny.

Apart from that the figure 6.4 show the basic AES-128 takes more time as compare to Hybrid Tiny + AES.

VII. Conclusion

Our proposed approach will define an emerging scheme in which two methods, encryption and decryption are shared, which offers a robust support for its safety and the method to protected data or message with verification and signature verification in our hybrid method which goes to modify the innovation of the records files into encrypted form using Tiny-AES-128 encryption procedure that variations it into an illegible cipher text and plaintext is cryptography using the processes from mixed (orthogonal) arithmetical collections and a enormous amount of circles to attain security with easiness. At two, sixty-four (64) Feistel rounds, a entire number of rounds are used in the TEA-AES-128 encryption process with smallest time after encryption, the encrypted data is embedding in a random text by using the idea of cryptography and then this text file sent via user and Processing time for block cipher, response time for senders, minimizing space consumption of s-box simulate in MATLAB.

In future, the reversal procedure as of which should be in a position to decrypt for FPGA hardware processor for original format upon the correct appeal by the user which minimize.

Acknowledgment

We are thankful to the Department of Computer Science and Engineering of Northcap University, Gurugram, India for giving us the platform for planning and developing this work in the departmental laboratories.

References

[1] F.Mace, F.X Standert, J J Quisquater "FPGA implementation(s) of a Scalable Encryption algorithm" IEEE Transactions on VLSI Systems, Vol.16, 2008, pp. 212-216.

[2] Francois-Xavier Standaert, Gilles Piret, Neil Gershenfeld, Jean-Jacques Quisquater "SEA a Scalable Encryption Algorithm for Small Embedded Applications" in Proc. CARDIS, 2006, pp 222-236.

[3] Andem, Vikram Reddy .—A Cryptanalysis of the Tiny Encryption Algorithm‖, 2003.

[4] Atul Kahate, — Cryptography and Network Security‖, TMH, 2003.

[5] Behrouz A. Forouzan, (2006)—Cryptography and Network Security‖, Firstedition, McGraw- Hill.

[6] V. Shoup and R. Gennaro: Securing Threshold Cryptosystems against Chosen. Ciphertext Attacks. Eurocrypt'98, LNCS 1404, pp. 1{16, 1998.

[7] Y. Tsiounis and M. Yung, On the Security of ElGamal Based Encryption. PKS'98, LNCS 1431, pp. 117-134, 1998.

[8] Y. Zheng and J. Seberry, Practical Approaches to Attaining Security against Adaptively Chosen Ciphertext Attacks. Crypto'92, LNCS 740, pp. 292-304, 1992.

[9] J. Pichel, D. E. Singh, and J. Carretero. Reordering algorithms for increasing locality on multicore processors. 10th IEEE International Conference on High Performance Computing and Communications, 2008, pages 123-130, 2008.

[10] Moh'd, Abidalrahman, Yaser Jararweh, and L. Tawalbeh. "AES-512: 512- bit Advanced Encryption Standard algorithm design and evaluation." In Information Assurance and Security (IAS), 2011 7th International Conference on, pp. 292-297. IEEE, 2011.

[11] Rewagad, P.; Pawar, Y., "Use of Digital Signature with Diffie Hellman Key Exchange and AES Encryption Algorithm to Enhance Data Security in Cloud Computing," in Communication Systems and Network Technologies (CSNT), 2013 International Conference on , vol., no., pp.437-439, 6-8 April 2013 doi: 10.1109/CSNT.2013.97.

[12] A. Menezes, P. van Oorschot, and S. Vanstone, Handbook of Applied Cryptography, CRC Press, New York, 1997, p. 81-83.

[13] Mohamed, E.M.; Abdelkader, H.S.; El-Etriby, S., "Enhanced data security model for cloud computing," in Informatics and Systems (INFOS), 2012 8th International Conference on, vol., no., pp.CC-12-CC-17, 14-16 May 2012.

[14] Mehak Khurana, Meena Kumari, "**Security Primitives: Block and Stream Ciphers",** International Journal of Innovations & Advancement in Computer Science (IJIACS), ISSN 2347 – 8616, Vol. 4, March 2015.

[15] Mehak Khurana, Meena Kumari, "**Variants of Differential and Linear Cryptanalysis"**, International Journal of Computer Applications (0975 – 8887) Volume 131 – No.18, PP 20-28, December 2015.

Authors' Profiles

Ritu Goyal, B.Tech in IT from BSA College of Engineering & Technology. (UPTU), Uttar Pradesh, India. Worked as assistant lecturer in SGI group in CSE & IT and has around 3 years of experience. Currently pursuing M.Tech in CSE from NorthCap University, Haryana and doing her research work. Her current research interests include: cryptography, information sharing, Cyber Security.

Mehak Khurana is an assistant professor in The NorthCap University in CSE & IT and has around 6 years of experience. She completed her M.Tech from USIT, GGSIPU in 2011 and B.Tech from GTBIT, GGSIPU in 2009. Her key areas of interest are Cryptography, Information Security and Cyber Security. She is lifetime member of Cryptology Research Society of India (CRSI).

How to cite this paper: Ritu Goyal, Mehak Khurana,"New Design of Tiny-Block Hybridization in AES", International Journal of Computer Network and Information Security(IJCNIS), Vol.9, No.9, pp.46-53, 2017.DOI: 10.5815/ijcnis.2017.09.06

