Scientific Journal of Impact Factor (SJIF): 4.72

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 4, Issue 4, April -2017

Design of New Algorithm to improve Confidentiality and Integrity

Ritu Goyal
NorthCap University/CSE, Gurugram, 122001, India

MehakKhurana
NorthCap University/CSE, Gurugram, 122001, India

Abstract*—The cryptographic algorithm is designed to enhance security in real life with increased speed and less memory utilization. TEA is a kind of Feistel cipher which uses simple operations like XOR, ADD, Shift. 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. This paper presents a hybrid approach in which the response time is minimized. The data is encrypted using AES and Tiny Encryption Process. The hybrid Procedure is considered for easiness and improved performance. At encryption time, data is encoded using tiny-AES-128 encryption process which modifies it into an unreadable text. Encryption of data is done using all four AES steps with a little modification in S-Box used by substitute byte step. Identities for S-box are created by applying the concept of TEA which will be used during decryption. Our proposed approach will minimize computational time and memory utilization It is simulated in MATLAB 2014Ra.*

Keywords: Encryption, Decryption AES Encryption, Cryptography, security and TINY encryption.

I. OUTLINE

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.

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.

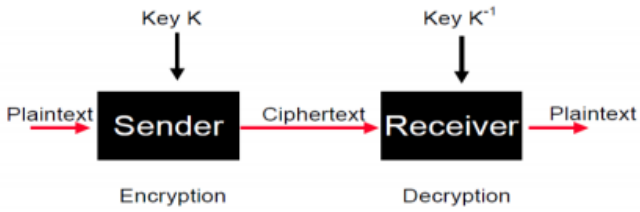

Fig. 1.Cryptographic technique.

III. TEA (TINY ENCRYPTION ALGORITHM)

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.

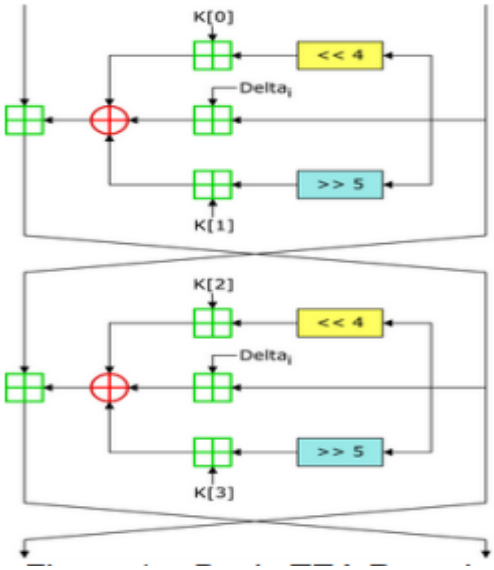

Fig.2.Simple Tiny encryption algorithm

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.Althoughthere are numerousaims to encode/encryptinformation, there are severalexplanations not to. Encryption does not resolve all safetydifficulties, and canuniformlymarkcertain problems inferior.

1. Encryption notResolve Access Control Problems

It simplyenhances the directly above of decrypting the informationearlieroperators can deliverit.If access panels are implemented wellbefore encryption adds tinyadded security within the folderthis one. Someuser who has pleasure to entrancestatisticsinside the folder has no furtheror any less pleasure as a consequence of encryption. Consequently, encryption should not ever be used to explain access control difficulties.

2. Encryption not able to defend alongside a Mischievous DBA

Certainorganizationstroubled which a malicious user capacityimprovementraised database administration (DBA) privileges throughpredicting a password conforming the suggestion of encodingstowed data to defendbesides this warning. Though, the precise solution to this difficult is to defend the DBA explanation, and to alteration defaulting passwords for addedadvantagedexplanations. The calmestmode to interruption into a file is thru using a avoidance password for a advantagedversion that an manager has allowable to continueunmovable.

3. Encrypting not able to make Data Safe

Accessibility is a key feature of safety. In caseencoded informationcreatesnumbersinaccessible, or unfavorablymovesobtainabilityviaplummetingconcert, formerlyencodingall will generate a novelsafetydifficult. Accessibility is toounfavorablypreciousthru the database actualityunreachableonce encryption solutions are altered, as decentsafetyperformsneed on a consistentfoundation. Once the keys are to be altered, the database is unreachablethough data is decrypted and re-encrypted with a novel key or keys.

For above given problem we design awell-organized and real time feasible namelyAES and TINY systemwhichcustomssymmetric keys with encryption and

decryption afterward project a procedure for its use in many user data-centric requests.

V. METHOD

The projectedschemeconsidered into two parts: the sender's view and the receiver's view as presented in Fig.3 and Fig. 4.The secret txt is encodedthrough AES-128 encryption processusing 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.

A. Flow diagram

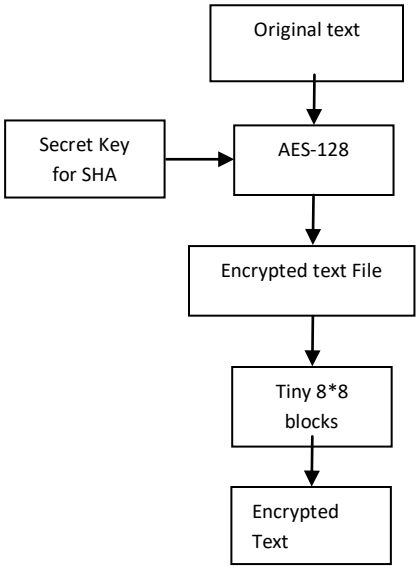

Fig.3. Block diagram from the sender's view

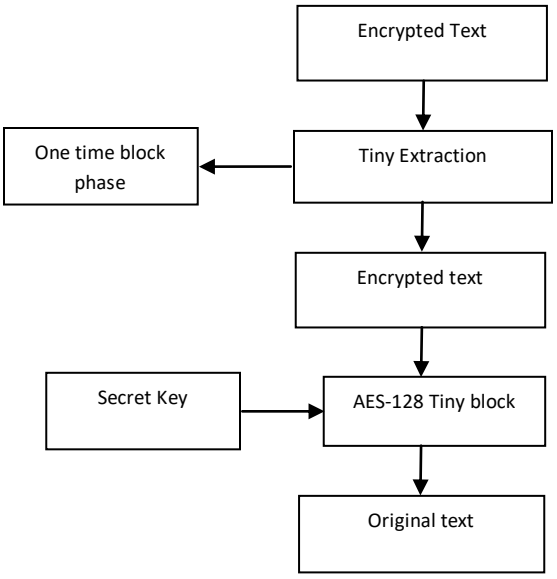

Fig. 4.Block diagram from the receiver's view

The encoded text is mined from the tiny blocks through using s-box miningsystem at the receiver's side. The mined secret text is decodedthrough the AES procedure with the mutual secret key and the unique message/packet is formerlycreated.

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 cryptographyprocedure. AES block cipher has 128, 192 or 256 bit keys to encode and decodeinformation in blocks of 128-bits. AES has a discrete key developmentstage for the increase of 128, 192 or 256-bit keys so that these keys can be helped in numerouscircles of cryptography process [11].

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

A non-linear sub-bytereplacementstageevery byte is substituted with alternativeallowing to a lookup counter (S-box). This stage is essentially a stand lookup exploiting a 16×16 matrix of byte standardstermed as s-box. This matrix includes of eachprobablearrangements 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 measuredmethod for formation the s-box tables [13]. Over the matrix that becomesfunctioned upon all over the encryption is identified as state. This alterationcompleted of 2phases: (i). Multiplicative inverses of every byte in the state. (ii). theoutcome in this step is gained from phase (i) by altering y = f(x) ChangeRows – aninversion 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 4^{th} line loop 3 bytes [10][9]. The Inverse Shift Rows revolutionachieves these circular shifts the furthertechnique 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 createscomplicatechanges to columns in the

state. Efficiently a matrix increase in GF (28) using prime poly m(x) =x8+x4+x3+x+1. AddRoundKey – 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 procedureamong 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 productivitythough it also affects all of state. A smallmodification 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 gottenthrough 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

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

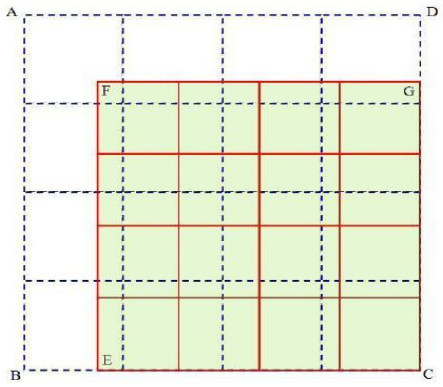

Fig. 5.Tiny S-Block based reconstruction from S-Box

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.

TheTEAis a kind of Feisteltypeciphers which usages operations from mixed(orthogonal)arithmetical groups XOR, ADD and SHIFT. Adualshiftcausesallbitsof thedataandkeytobeassortedcommonly.

Thekeyprogramprocessis modest;the128-bit keyKisseparatedintofour32-bitblocksK=(K [0],K[1],K[2], K[3]).Tiny encryption algorithm aspectstobeextremelyresilientto differencecryptanalysis(Bihamet al.,1992)andachieveswholedispersion(where a one bit alterationin the plaintext will cause about32bit differences inthe cipher text). Timeroutineonaworkstationisverystirring of this approach.

C. Steps involved in research

The Encoded fileisin printon MATLAB platformandacceptsa 32-bitwordsize.The128bitkeyisdividedintofour portionsandisputin storagek [0]- k [3]andtheDataiskeptinv[0] andv[1].

1. Makem×n non-overlapping block separating size of AES-128 matrix

2. Letdesignate 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 commonthrough both ends) and achieve the cypher text in every nominated blocks byevery 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 TEAusagesaddingandcalculationastheflexibleoperativesi nits placeofXOR.TheTEAencryption routinedepends onthe alternativeuseof XORandADDtodelivernonlinearity.The procedurehas32 cycles(64rounds).TEAisshortsufficientto inscribeintovirtuallysomesequenceronanycomputer.

The block basedTinyEncryptionAlgorithm(B-TEA)is a blockcipher encryption procedurethatisverymodesttodevicehasfastimplementatio ntime,andtakingsnominalstoringspace[2]

D. Integrity Chck using SHA-256

SHA-256 has a uniquebeneficiary hash purposes to SHA-1 & it is also one of the solidest hash purposesobtainable. Whereas SHA-1 has not been cooperated in real-world circumstances, SHA-256 is not much more composite to cipher. The 256-bit key creates it a decent partner utility for advance encryption algorithm. It is definite in the NIST (National Institute of Standards and Technology) typical'FIPS 180-4'. NIST similarlydeliver a no. of test vectors to confirmaccuracy of application.

- FIPS 180-4 requires the communication has a '1' bit attached, and is formerlyamplified to anentirequantity of 512-bit blocks, counting the textextent (in bits) in the last 64 bits of the previous block.
- Subsequently user must have a byte-stream fairly than a bit-stream;calculation a byte '10000000' (0x80) adds the compulsory bit "1".
- To change the text to 512-bit slabs, itcompute the no of slabsessential, N, formerly for every these it willgenerate a 16-integer (i.e. 512-bit) collection. For everythese numbers, It will take four bytes from the communication (using charCodeAt), and left-shift them through the suitablequantity to pack them into the 32-bit number.
- The charCodeAt() techniqueproceedsNaN for out-of-bounds, then the '|' operativechanges this to zero, so the 0-padding is completedindirectly on change into slabs.
- Formerly the measurement of the message (in bits) wants to be added in the last 64 bits, that is the lattertwo numbers of the concluding block. In code, this could be done.

```
M [N-1] [14] = ((msg.length-1)*8) >>> 32;
  M [N-1] [15] = ((msg.length-1)*8) &
0xffffffff;
```

On the other hand, JavaScript bit-ops change their influences to 32-bits, so n >>> 32 would provide 0. Therefore itusesmathematicsoperativesin its place: for the most-significant 32-bit quantity, it willdistribute the (unique) extentthrough 2^32, and use floor() change the consequence to an integer.

Most important is thatrefunded is the recorded hexadecimal symbol of the second hash. This can be valuable for example for storage hashed PINs, but if it will want to usage the hash as a key to an encryption routine, for instance, you will famine to use the dualworth not this writtenillustration.

E. Encryption using Tiny-Block hybridization in AES-128

BLOCK –TINY

TEA is a modest but influential encryption procedure (grounded on a 'Feistel cipher'). TEA is a light-weight explanation more suitable for certainuses than 'manufacturing strength' methods such as AES which can be valuable for web uses that need safety or encryption. It will provideprotected cryptology,robust encryption in a few outlines of brief. TEA form is nearer than the innovative (64-bit block form) when encoding longer slabs (ended 16 chars), and is newsafe ('an individual bit will alterationaround one partial of the minutes of the whole block, parting no place where the variations start'). It is also modest to implement for encoding arbitrary-length manuscripts (presencemutable block size, it needs no 'mode of operation'). The tiny encryption algorithmusages a 128-bit key which is used for increased safety and an encoded or hashed form of the complete password.

1. BLOCK-TINY and AES-128 operation

- Tiny encryption algorithmworks as a Feistel system (a symmetric slabcode) that usages a mixture of bit unstable, XOR, and enhanceprocesses to generate the essentialdispersal and misperception of data.
- It fixes these processes on 32 bit argumentsslightly than single bytes, anidenticalsignificant optimization that the authors avoid "progressive the authority of a processor." It customs a 128 bit (4 word) key, involvement in its separate word mechanisms in an actual key agenda.
- The innovativeoperationworks on 64 bits (two words) of facts at a time, thoughoptions (such as Block TEA) permit arbitrary-sized blocks.

2. AES-128

Weconfine to depiction of a characteristic round of advance encryption algorithm. Every round include of four sub-processes. The 1st round procedure is represented below:-

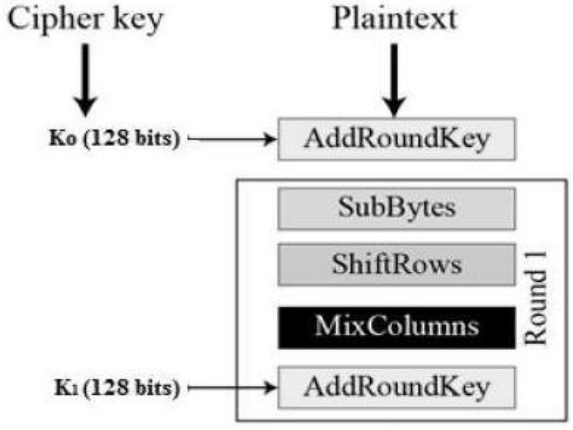

Fig. 6: Operation process of AES-128

Byte Substitution (SubBytes)

The 16 input bytes are replacedinobserving up a secure table (S-box) assumed in strategy. The consequence is in a matrix of 4 rows and 4 columns.

Shiftrows

All of the 4 rows of the matrix areremoved to the left-hand. Someaccesses that 'fall off' are re-inserted on the correctcrosswise of row. Shift is approved out as surveys –

- 1st row is not removed.
- 2nd row is removed 1 (byte) location to the left.
- 3rd row is removed 2locations to the left.
- 4th row is removed 3 positions to the left.
- The consequence is a novel matrix containing of the similar 16 bytes but removed w.r.t each other.

MixColumns

Every column of 4 bytes is currentlyaltered using a singularexactpurpose. This purpose taking as input the four bytes of one column and productions four entirely new bytes, which change the unique column. The consequence is alternativenovel matrix containing of 16 novel bytes. It must be well-known that this stage is not achieved in the previous round.

Addroundkey

The 16 bytes of the matrix are currentlymeasured as 128 bits and are XORed to the 128 bits of the round key. In case this is the most recent round formerly the productivity is the cipher text. Then, the subsequent 128 bits are construed as 16 bytes and we instigateadditionalcomparable round.

VI.RESULT

This work presents the hybridcryptography of the Tiny Encryption and AES-128Set of rules. In this investigation we reviewed the bestcollectiveapproaches in the cryptography of a slab 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 encode a communication, but the message can only be decipheredthrough 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 communicationusages the procedure and the receiver's public key to do so. Aviewer may have both the procedure and the public key, but will still not be capable to decode the text. 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.7: 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.7: 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

----Proposed Technique encryption/decryption using (TINY+AES) using 128 bit key----

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

Encryption-

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.

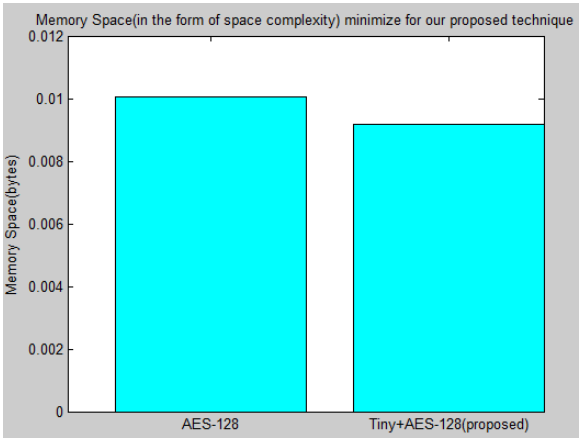

Fig.8: Memory space (in the form of space complexity) minimize for our proposed technique

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

This plannedschemeefforts on the secure approach of light weight cryptographic procedure. Tiny Encryption Algorithm to adjust with countless real time restraintslike memory space. The proposed scheme uses block based Tiny to produce the random key creation it safer for delicatedatatransmission in numerous real-time submissions.

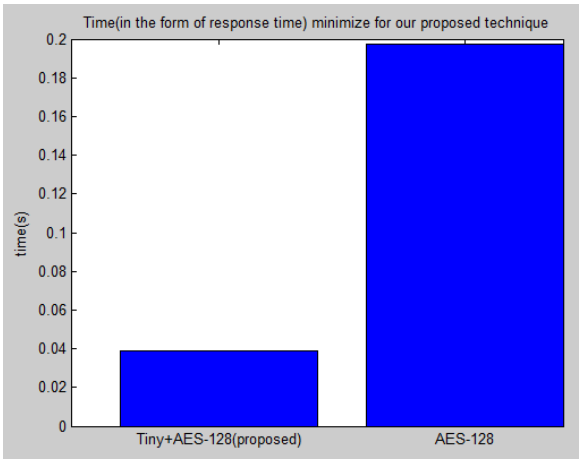

Fig.9: Comparison between AES-128 and Tiny-AES-128 with respect to tiny.

Apart from that the figure 6.4 show the basic AES-128takes 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) arithmeticalcollections and aenormousamount of circles to attain security with easiness. At two, sixty-four (64) Feistel rounds, aentire number of rounds are used in the TEA-AES-128 encryption process with smallest timenext encoded, the encodedfiles is embedding in a random text by using the idea of cryptography and formerly this text file directed 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 correctappeal by the user which minimize.

REFERENCES

[1] F.Mace, F.X Standert, J JQuisquater "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, YaserJararweh, 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] MehakKhurana, MeenaKumari, "Security Primitives: Block and Stream Ciphers", International Journal of Innovations & Advancement in Computer Science (IJIACS), ISSN 2347 – 8616, Vol. 4, March 2015.
[15] MehakKhurana, MeenaKumari, "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.

MehakKhurana is currently working as assistant professor in The NorthCap University in CSE & IT and has around 6 years of experience. She completed her MTech 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)

