International Journal of Scientific Research and Engineering Development-– Volume 4 Issue 5, Sep- Oct 2021

Available at www.ijsred.com

RESEARCH ARTICLE OPEN ACCESS

An Advanced Aes Algorithm Using Cascading Method on 400 Bits Key Size Used in Increasing the Security of Next Generation Internet of Things

Prof. Satish Soni[1], Abha Tiwari[2]

[1]PROFESSOR & HEAD OF COMPUTER SCIENCE DEPARTMENT, JNCT REWA M.P. 486001 INDIA

[2]SCHOLAR, COMPUTER SCIENCE DEPARTMENT, JNCT REWA M.P. 486001 INDIA

ABSTRACT-

This paper of cascaded AES recommends symmetrical block encryption utilizing 200 bit consecutive plain text and 400 bit key. The algorithm utilizes 400 bit key which is separated into 2 pieces of 200-200 pieces giving diverse keys to each rounds of cascading which will expand the security. Here AES-AES cascading is done which consist of 5 rounds instead of 10, thus it will omit the mix column twice from the original AES Encryption method. Discarding mix column single time diminish the intricacy from 248 to 216.Hence, it takes half time than basic AES algorithm to encode the block data. Since is AES is generally utilized worldwide standard encryption strategy and is additionally used to give security in space of remote LAN's hence, it very well may be utilized to give energy saving cryptographic procedure to myriad gadgets that are associated with network in, this outcome was declared in August 19, 2016 Conference on Cryptographic Hardware and Embedded Systems 2016(CHES 2016) Conference on Cryptographic Hardware and Embedded Systems 2016(CHES 2016).

Keywords— AES, Encryption techniques, Cascading technique, block encryption, Sequential and Parallel data, OpenCL, SIMD, multicore GPU and AMD, IoT.

1.INTRODUCTION

In the present period of device addiction; data storage, preparing and recovery are absolutely PC based this is the foundation of IoT. Since IoT gives a remarkable identifiers to every one of the gadgets associated with one another through network and the capacity to move information over network with no mediation of Human-Human and Human-Computer Thus, including IoT in cryptography is arising space. Thus, it turns out to be vital to give security to the data which is moved over network. This can be accomplished by scrambling the data for example changing valuable data into indiscernible structure by utilizing different scrambling calculation. AES (Advance Encryption Standard) is most strongest algotithm in the present time as it is simply vulnerable to savage power assault, which is extreme work for the cryptanalysts. On account of its affirmation to give security to the data it is generally utilized in banks, workplaces to get the significant information. By giving security to IoT by utilizing AES calculation. We can safely transfer information to the cloud.

 ©IJSRED:All Rights are Reserved

A. HISTORY

NationalInstituteofstandardsandtechnology(NIST)[1]invitedproposalsfortheAdvancedEncryption Standard(AES) in 1997.Among 15 proposed algorithms Rijndael wasselected as AES algorithm that adjust the number of roundsneededforeachkeysize.ItwasgivenbytwoBulgarianscientist John Daemen and Vincent Rijmen . It was introducedto replace 3DES [5] [10] and IDES [1] [5] which are known tobeencryptionstandardoftheirtime.

B. AES

Advance Encryption Standard i.e. AES [6] is not based onFeistel Structure [5] like 3DES, IDES hence able to processwhole block of data at once in single matrixduring eachroundsofpermutationandsubstitution.Itconsistsoffourseparate function or transformation [2] [4] for each round i.e.bytesubstitution,permutation,arithmeticoperationoverafinite field, XOR with a key. Hence, change in plaintext ineachroundandeachtransformation addsmore security todata.All tasks are performed more than 8-bit bytes .It utilizes forward s-box and backwards s-box for encryption and unscrambling separately. The s-box is created utilizing Galois field (GF). The code takes plaintext of square size of 128 pieces, 192 pieces and 256 pieces. Like that key length [6] could be additionally of 128,192 and 256 pieces. However, the calculation is alluded to as AES-128, AES-192, or AES-256, contingent on its key length. The key is depicted as square matrix of bytes. This key is then ventured an array of key schedule words. The first code key should be extended from 16 bytes to 16_(r + 1) bytes[11], where r signifies the quantity of rounds .Again there are four sorts of change that is acted in each rounds of AES calculation. They are:

1. Sub Byte: according to name suggest, it is a change stage in which content of every cell of the state array is subbed by the sections of the predefined 15*15 framework called replacement box. It gives non-linearity[12] and confusion[5].

2. Shift Row: This is the solitary change stage [6] among every one of the changes. It circularly left moves each column of the state exhibit as indicated by the offset number of lines. Consequently, it gives inter column diffusion .

3. Mix Column: It is additionally a replacement stage which performs predefined activity between fixed matrix of 4*4 likewise called polynomial operation between fixed matrix and yield of the state exhibit from Shift Row. It gives diffusion .
4. Add Round Key: In it bitwise XOR of the current state array with a part of extended key [6] . It additionally gives disarray [5]. It gives security to the algorithm as just this stage utilizes key.

For Add Round Key; Key Expansion is done to give distinctive keys in various rounds of AES .Thus, Key Expansion measure comprise of activities like Rotate Word, Sub Byte and XOR with "Round Constant" framework [5].
In last round of AESthere are just three changes specifically Sub Byte, Shift Row and Add Round Key.

 ©IJSRED:All Rights are Reserved

AES Structure

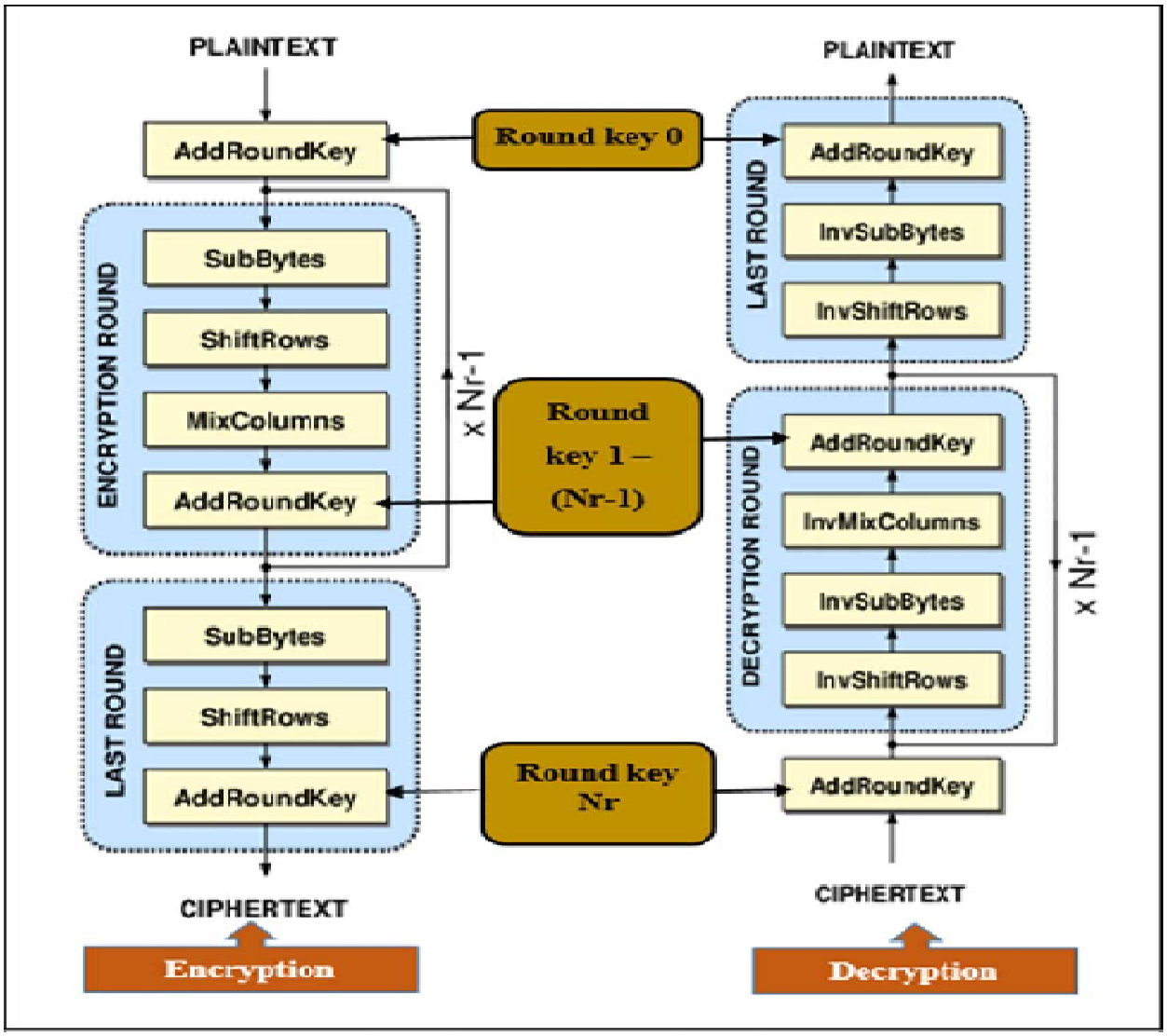


Fig1:Process of encryption and Decryption

 ©IJSRED:All Rights are Reserved

Cascaded cryptography [4] means multiple encryptions are theprocess of encrypting an already encrypted message [8] one ormore times either using same or different algorithms. It is alsoknown as cascaded encryption or cascaded ciphering, multipleencryption andsuper decipherment[9].

2.RELATEDWORK

AES algorithm is designated for encryption for a reason that it isfastandmoreprotectedincontrasttoIDESand3DESencryptionalgorithm.AESissymmetricblockcipherencryption algorithm which is one of the most extensively usedinternationalstandardencryptionprocesses.InAESwhole block of data is processed in a single matrix also knownasstate array.

Again for making original AESmore safe there are severalmodification is done in the original AES algorithm likevaryingthekeysize,s-box,e.tctoimprovetheperformance of the AES algorithm like increasing security andencrypting rate of data. The main purpose of modification inAES is to make it implementable on various hardware [3] andsoftware[3].

There are many research papers published on the modificationofAES as it is the standard for encrypting in today's era.Modificationslikeincreasingthesizeofkeymakeit lessprone to cryptanalysis, also varying the size of s-box make the whole algorithm more complex, thus make it lessvulnerabletobrute force attack.

Some modification done in the previous papers increase theefficiency of algorithm a lot but still research is going on forimplementing it parallel using ANN networks so it could beused for encrypting huge amount data parallel and increase theprocessing speed.

So, afterstudying many previous papers onthe modificationof AES we conclude a new technique which increases theprocessing speed as well as security of data which we haveappliedinourproposed work.

3.PROPOSEDWORK

TheproposedalgorithmcompriseofdiffusionofAESalgorithm with cascading technique which uses 200 bit plaintext and 400 bit key which is divided into two equal parts inorder to deliver different keys at different cascading level.There are only five rounds in place of 10 in new algorithm incascaded format .Thus, it will eliminate mix column [3] twicefromthewhole AESwhichinturndecreasestimecomplexity.

Thechangethathasbeendoneinproposedalgorithmare:

Cascading technique: The original AES doesn't have anycascadingconceptbuthereinproposedalgorithmcascadingon the AES algorithm has been done for two rounds usingdifferent keys for each rounds which adds more security to the algorithm and also there are only five rounds for each ofthetwocascadedlayers.Hence,Mix Columncouldbeeliminatedtwotimesfromthewholealgorithmwhichdecreasesitstimecomplexityfrom $2^{48}$to 2^{16}.

 ©IJSRED:All Rights are Reserved

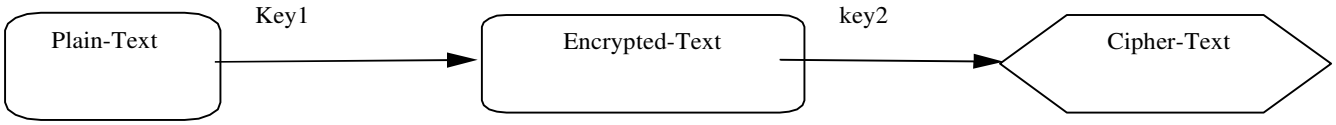


Fig2: Cascading technique We have taken;

Plaintext = 1234567890ABCDEF123456

KEY=FECDBA1357924680ABCDEF1234567890FEDCBA0987654321AB

Atfirst,plaintextisencryptedinfirstroundofcascadingbykey1

i.e.KEY1=FECDBA1357924567890ABCDEF123

Andinsecondroundofcascadingthesecondpartofkeyistakenas

KEY2=4567890FEDCBA0987654321AB

Againthealreadyencryptedplaintextisencryptedusingsecondkey.

1 .**Useof200bit blocksize**:Ourproposedalgorithmuses200bit instead of original 128 bit block for input data. Hence, toaccommodate whole 200 bit in single state array; size of statearray is increased from 4*4 to 5*5which brings changes instages of eachroundfore.g.

A. *SubByte:Transformation:Changeinsizeofplaintextdoesn't affectthis transformation.*
B. *ShiftRow:*Duetochangeinplaintext5ShiftRowoperation is performed in proposed algorithm insteadof4shiftoperation.

$SR_{0,0}$	$SR_{0,1}$	$SR_{0,2}$	$SR_{0,3}$	$SR_{0,4}$
$SR_{1,0}$	$SR_{1,1}$	$SR_{0,0}$	$SR_{1,3}$	$SR_{1,4}$
$SR_{2,0}$	$SR_{2,1}$	$SR_{2,2}$	$SR_{2,3}$	$SR_{2,4}$
$SR_{3,0}$	$SR_{3,1}$	$SR_{3,2}$	$SR_{3,3}$	$SR_{3,4}$
$SR_{4,0}$	$SR_{4,1}$	$SR_{4,2}$	$SR_{4,3}$	$SR_{4,4}$

Table1:BeforeShiftRowOperation:

 ©IJSRED:All Rights are Reserved

SR0,0	SR0,1	SR0,2	SR0,3	SR0,4
SR1,1	SR1,2	SR1,3	SR1,1	SR1,0
SR2,2	SR2,3	SR2,4	SR2,0	SR2,1
SR3,3	SR3,4	SR3,0	SR3,1	SR3,2
SR4,4	SR4,0	SR4,1	SR4,2	SR4,3

Table2*:* AfterShiftRowOperation

C. *MixColumn:*ThepolynomialequationforMixColumnis changes to $2X^4+4X^3+3X^2+X+1$.And the polynomialmatrixchangesfrom4*4to5*5.

$$\begin{pmatrix} 02 & 04 & 03 & 01 & 01 \\ 01 & 02 & 04 & 03 & 01 \\ 01 & 01 & 02 & 04 & 03 \\ 03 & 01 & 01 & 02 & 04 \end{pmatrix}$$

Fig3:FixedPolynomialmatrixfor5*5

$$\begin{pmatrix} E0\ 7D09\ 8A\ 4C & & & & \\ & 4C\ E07D\ 09 & 8A & & \\ & 8A\ 4C & E0\ 7D & 09 & \\ 09 & 8A & 4C\ E0\ 7D & & \\ 7D\ 09 & & 8A & 4C & E0 \end{pmatrix}$$

Fig4:InversePolynomialmatrix

 ©IJSRED:All Rights are Reserved

*D. AddRoundKey:*Numberofroundkeyoperationincreases as result of which number of words increasesfrom44to55.

3. **OmissionsofMixColumn**:InourproposedalgorithmMixColumn is omitted twice from whole algorithm which ismainlyresponsibleforreductionintimecomplexity2^{48}to2^{16}.

4. **Increase in key size**: size of key is increased from 128 bitto 400 bit adds more security to the algorithm. Here, 400 bitkeyisdividedinto200-200bit.

4.PROPOSEDALGORITHM

Heretakeplaintextas'p'andkeyas'k'thatdividesintwopart.
Casciphertext
Initialization:i=0,count=0,j=0

- *fori=0to24by11.1K1[i]=k[i+j];*
- *Keyexpansion(k1);*
- *doinitialtransformation*
- *fori=1to4by1*

{

- *substitutionbyte();*
- *shiftrow();*
- *mixcolumn();*
- *addroundkey();}*

- *substitutionbyte();*
- *shiftrow();*
- *addroundkey();*
- *count++*

- *if(count<2)*
  - *p=c*

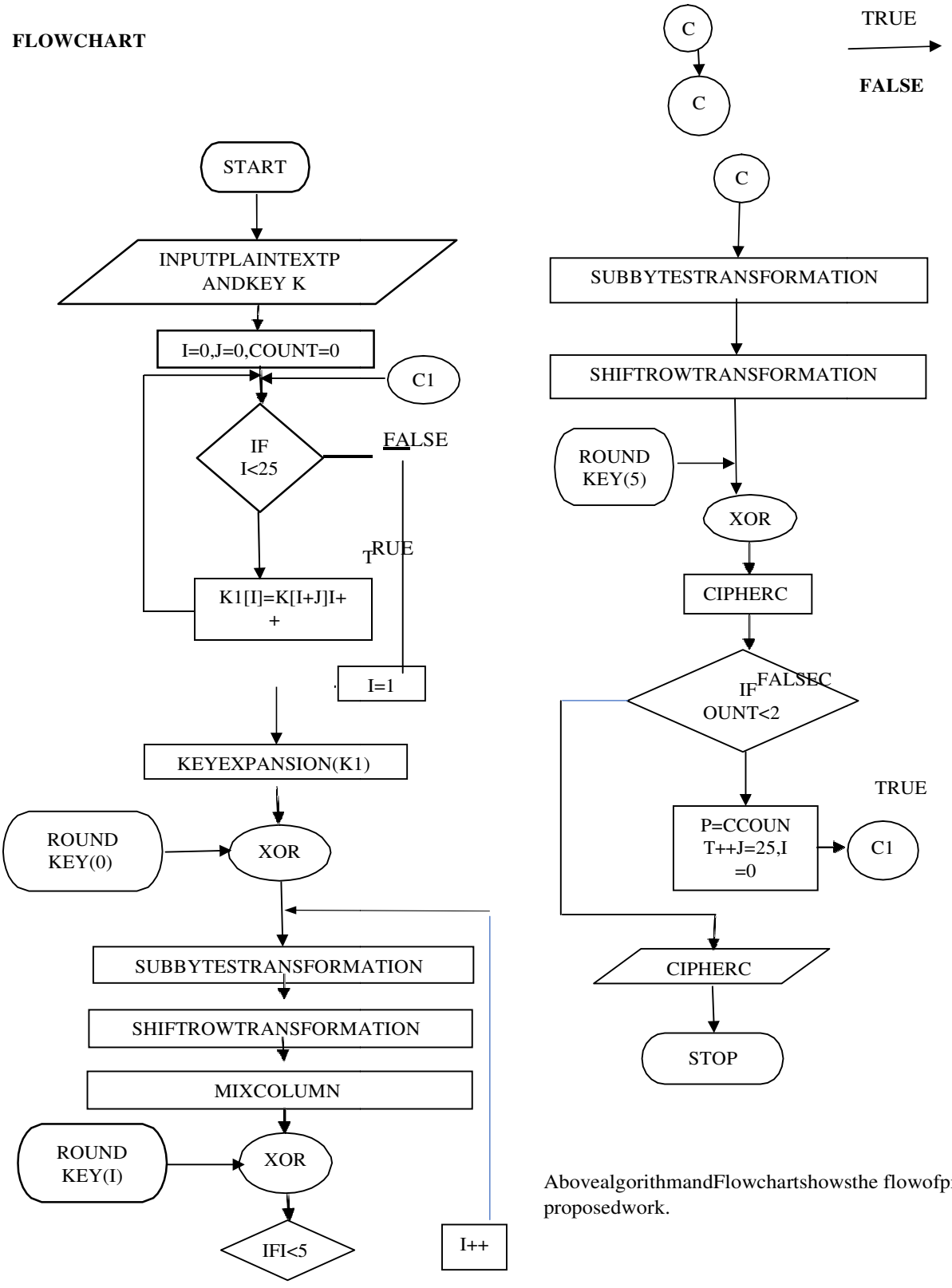
9.2 i=09.3j=25

- *gotostep1*

10.elseexit

 ©IJSRED:All Rights are Reserved

5. FLOWCHART



AbovealgorithmandFlowchartshowsthe flowofprogramofour proposedwork.

 ©IJSRED:All Rights are Reserved

- Here, firstly we have taken a plain text of 200 bitsandakeyofsize400bits.

- Further,the400bitskeyisdividedintotwoequalhalves of 200-200 bits. In that way we could maketwodifferentkeysfordifferentturns ofcascadedencryptiontechniquewhichwouldmaketheencryptionprocessless pronetoBruteforceattack.
- The sizeofstatearray ischangedfrom4x4to5x5intoaccommodateall200bitofplaintextsimultaneously.
- Proposed algorithm do encryption twice on sameplaintextusingsameAESalgorithmandtwodifferentkeysforbothturnsofencryption.
- Thenumberofroundsisbeingdecreasedfrom10to5roundsforeachturnofencryption
- Thus, for each last MixColumn is omitted in that it isomitted twicefrom thewhole algorithmwhichisresponsiblefordecreaseinencryptiontimeofdata.

6. ImplementationandResult

Wehavecomparedourproposedalgorithm,referencedalgorithm and original algorithm on different set of data blockfor encryption time and our proposed algorithm shows goodresult in comparison to the other to algorithm i.e. original andreferenced AES ; it shows speedup to 65% from the originalAES and 15% from referenced AES. The table3, givenbelow shows the variation in encryption time of the differentAES on different data size. Here sizeof the data is takenMegabytes(MB)andencryptiontimeisin millisecond(ms).

DATA(MB)	ORG. AES (ms)	REFAES(ms)	PROAES(ms)
0.15	130	48	40
0.50	593	280	245
1.00	1189	515	476
1.50	1795	781	711
2.00	2376	1055	995
2.50	2953	1297	1136
3.00	3547	15667	1483

Table3:tableofresult

- ORGAES-OriginalAES

 ©IJSRED:All Rights are Reserved

- REFAES-ReferencedAES
- PROAES-ProposedAES

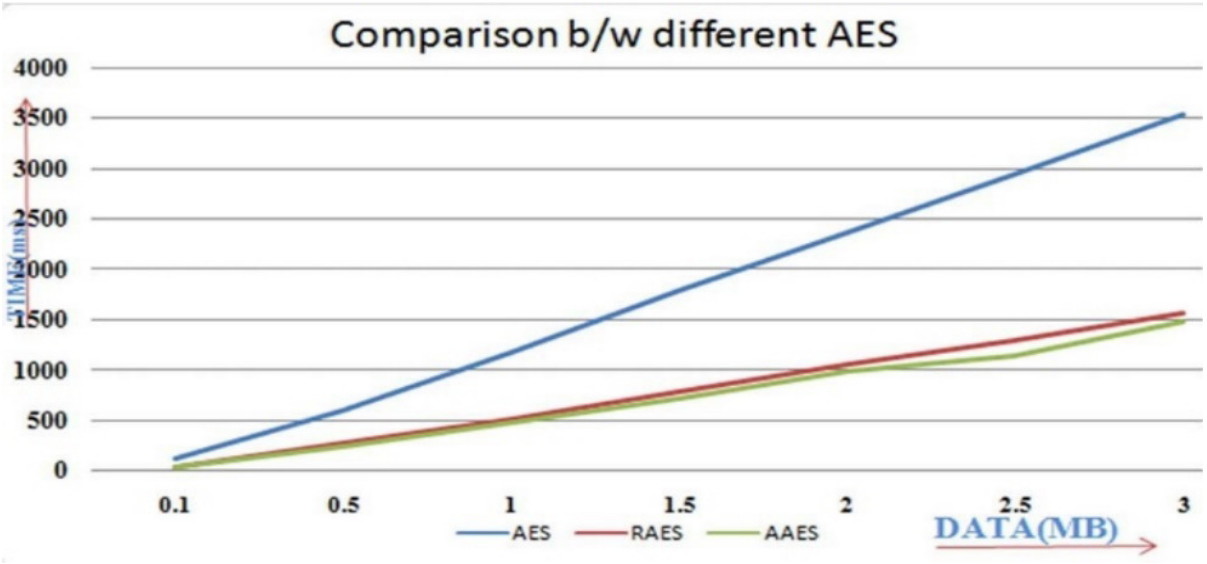


Fig5:ComparisonbetweendifferentAES

Our algorithm uses 200 bit block of data for encryption at atime which allows it to encrypt more data than the normalalgorithm in a single round making it faster than the originalalgorithm. Fig5 shows the graphical result of the comparisonbetweenthreeAES algorithm

New algorithm also uses Cascading which will increase thesecurityof dataaswellasmaketheexecutionfaster.

7.CONCLUSION

In our proposed work we have worked on the productivity of AES algorithm by utilizing Sequential 200 bit plain text as input and 400 bit as key in cascaded format. Because of AES-AES cascading and division of 400 bit key into two 200 bit key which will make it less prone to brute force attack.Exclusion of mix column twice from calculation decreases time complexity from 2^48 to 2^16. Consequently, we reason that new calculation saves encryption time upto 60% more than unique because of expulsion of mixed column and enhance security because of cascading and increase by key size.

REFERENCES

[1]. William E. (Bill) Burr "Selecting the AES" published by the IEEE computer society, 1540-7993/03/$17.00 © 2003 IEEE.

[2].Xinmiao Zhang and Keshab K.Parhi" Approaches for the advanced encryption Standard Algorithm" published by the IEEE computer society,1531- 636x/12/$10.00 © 2002 IEEE.

[3]. Chih –Hsu yen and Bing-Fie Wu, Senior Member ,IEEE" Simple Error Detection

 ©IJSRED:All Rights are Reserved

Method For Hardware Implementation Of Advance Encryption Standard", IEEE Transactions On Computers, Vol.55, NO.6, June 2006.

[4] Harshika, Rajeshkumar Rana & Prashant P Pittalia "Advances in cascaded cryptography" International journals of Advance Research in Computer Science and Management Studies, Volume 3, Issue in April 2015.

[5]. Stallings W, Cryptography and Network Security, Pearson Prentice Hall, New Delhi, 6th Impression, (2008).

[6]. Douglas Selent"Advance Encryption Standard" Insight: rivier academic journal, volume 6, number 2, fall 2010.

[7]. www.tutorialspoint.com,Book on "Cryptography just for beginners".

[8]. Rupali Gawade, Priyanka Shetye, Vaibhavi Bhosale & P N. Sawantdesai "Data Hiding Using Steganography For Network Security" International Journal of Advanced Research in Computer and Communication EngineeringVol. 3, Issue 2, February 2014

[9]. Geeta D. Rote, and Dr. A. M. Patil" Steganography with Cryptography Technique for Data Hiding" International Journal of Science and Research (IJSR) ISSN (Online): 2319-7064 Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

[10]. Priyadarshini Patil, Prashant Narayankar, Narayan D G, Meena S M" A Comprehensive Evaluation of Cryptographic Algorithms: DES, 3DES, AES, RSA and Blowfish" International Conference on Information Security & Privacy (ICISP2015), 11-12 December 2015, Nagpur, INDIA.

 ©IJSRED:All Rights are Reserved