International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-8 Issue-6S, August 2019

Symmetric Random Biometric Key (Srbk) Based Cryptography

S.Pavithra, P.Muthu Kannan

Abstract-: In this paper, we propose a novel cryptographic algorithm namely Symmetric Random Biometric key (SRBK) algorithm. The key for this SRBK algorithm is obtained from two biometric features namely ear and lip. The key generated are flexible and can be altered based on the type of algorithm used. We also consider Advanced encryption standard (AES)algorithm for comparison with SRBK algorithm and finally it was proved that SRBK algorithm is better than AES algorithm on selected parameters.

Key words: Bi-modal biometrics, AES, Key generation.

I. INTRODUCTION

Security plays a vital role in transferring huge amount of data across the internet where the information is not safe guarded by any medium. Cryptography is an eminent component in communication which ensures secure transmission and reception takes place between authorized parties. The proper selection of cryptographic algorithm is important for security, efficiency and other parameters. In this paper, a novel method is proposed to generate keys using biometric features like ear and lip. The detailed generation of key by bi-modal method is discussed in [9]. Biometrics is an analysis from human physical and behaviour characteristics. Though many methods are available, we use human EAR and LIP because of its unique features for generating binary values(keys). The advantage of using this biometric feature is that the key generated is flexible. The bits generated at the final stage can be obtained based on the algorithm we use. In this paper, the biometric key is applied to AES algorithm and also to the novel method proposed. In AES, the key length is 128 bits, whereas in SRBK, the length is 16 bits.

1.1. GENERATION OF BIOMETRIC KEYS

Here the initial set of values for keys in terms of 16 bytes are generated from biometric features (Ear and Lip). Two features are taken as reference and 128 bits are generated from the two features.

The steps followed in key generation are:

- Input image
- Conversion from RGB to GRAY-
- Filtering-various filters were applied and analysed to know the better noise removal filter
- Enhancement- Tonal regularisation
- Image reshaping- Mean level of the pixel are adjusted
- Extraction- concentrating and extracting selective feature on the image
- Concatenation- Gradient calculation
- Gradient image
- Sorting- re-arranging the values
- Key generation. - binary value is generated as key.

The detailed method of key generation from Ear feature is discussed in [9].

The most popular standard algorithm which is widely used in today's scenario is AES algorithm. It is found to be several times faster than the triple-DES algorithm.

The features of AES are as follows

- Symmetric key /block cipher.
- Based on number of rounds, the key length is varied.
- Fast and stronger than triple –DES.
- Gives the entire specification and design details.
- Can be implemented in software tools.

II. BIOMETRIC KEY IN AES

The key obtained from biometric feature is flexible and therefore can be applied to AES based on number of rounds. The overview of key size and rounds is shown in table 1.

Table 1: Relationship between key size and number of rounds in AES.

KEY SIZE	NO.OF ROUNDS
128	10
192	12
256	14

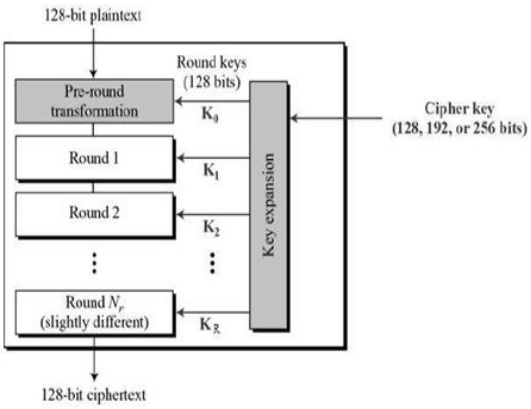


Fig 1: The general schematic of AES algorithm [3]

Manuscript published on 30 August 2019.
* Correspondence Author (s)
S.Pavithra, Research scholar, Saveetha Institute of Medical And Technical Sciences (SIMATS), Chennai, Tamilnadu, India(email: pavithrra1286@gmail.com)
Dr.P.Muthukannan, Professor, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Chennai, Tamilnadu, India(email: muthukannan@saveetha.com)

2.1 AES ANALYSIS USING BIOMETRIC KEYS

The keys obtained from ear and lip biometric features are given as input(key) to the encryption /decryption process of AES algorithm. The 128- bit key and 10 round operation is performed. The results are shown below.

2.1.1. Encryption:

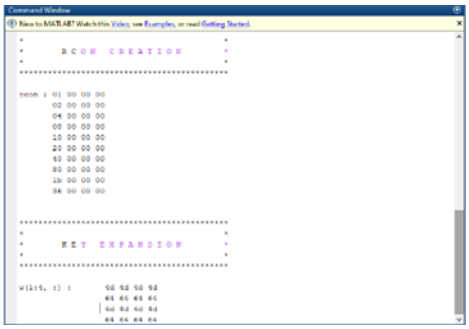


Fig 2: biometric key used in AES for Pre-round

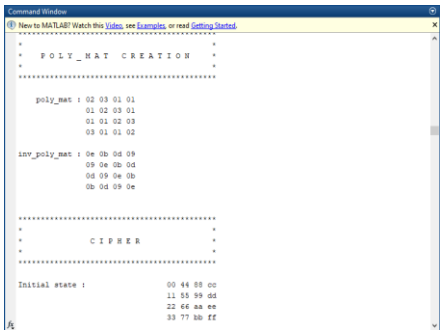


Fig 3: Cipher taken for process.

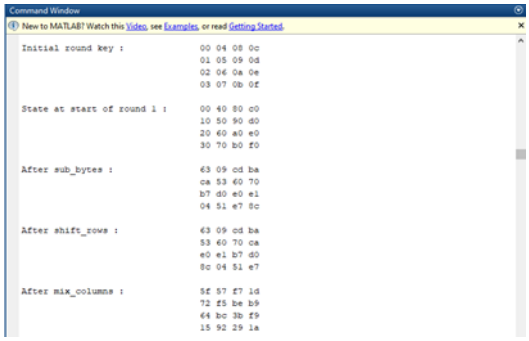


Fig 4: Initial round 1 process

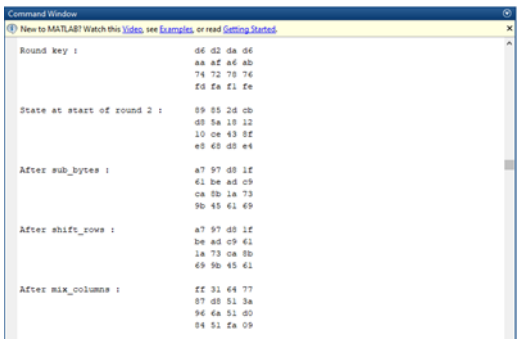


Fig 5: Round 2 process

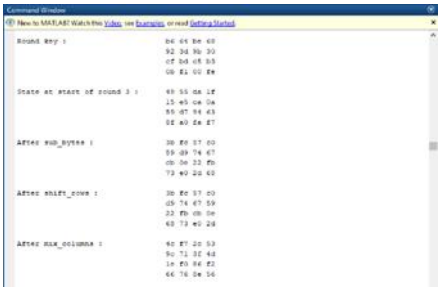


Fig 6: Round 3 –AES

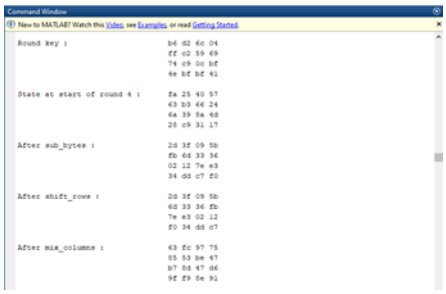


Fig 7: Round 4 –AES

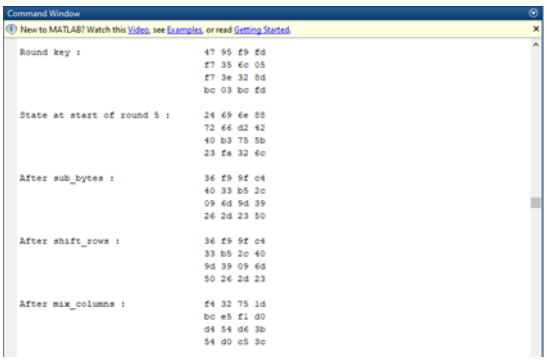
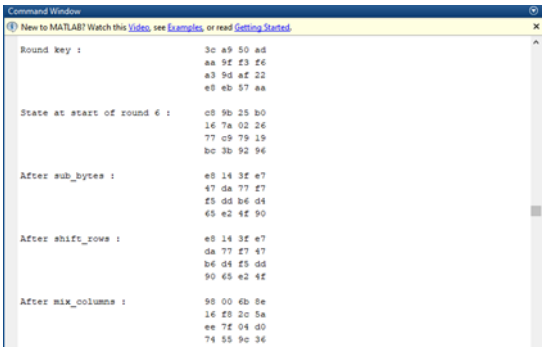


Fig 8: Round 5-AES



Retrieval Number: F10670886S19/2019©BEIESP
DOI:10.35940/ijeat.F1067.0886S19
Journal Website: www.ijeat.org

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

Fig 9: Round 6-AES

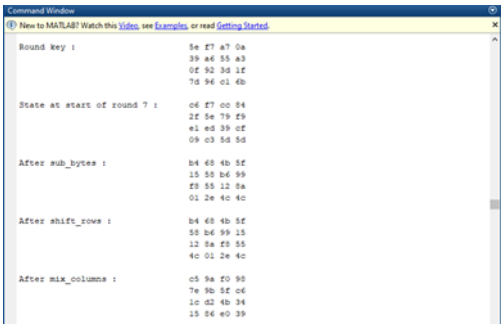


Fig 10: Round 7-AES

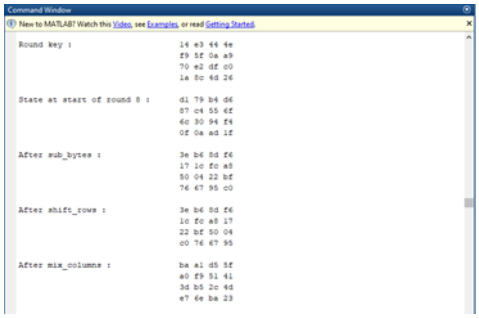


Fig 11: Round 8-AES

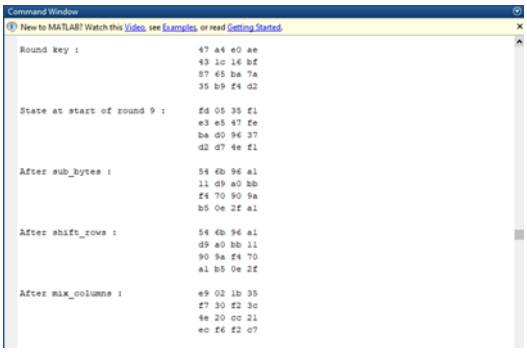


Fig 12: Round 9-AES

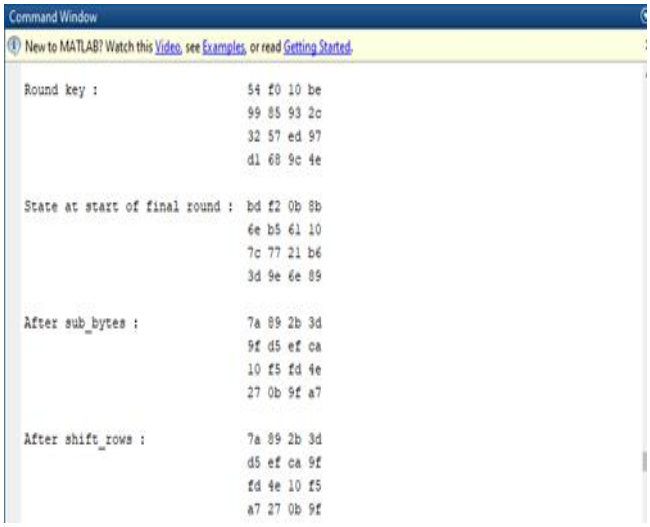


Fig 13: Final round 10-AES

Fig 14: Final key at the end of encryption and cipher text

2.1.2. Decryption:

The key and cipher text obtained from the final step of encryption process is given as input to the decryption. Fig 15 shows the first step in decryption and fig 16 shows the final key and plain text obtained.

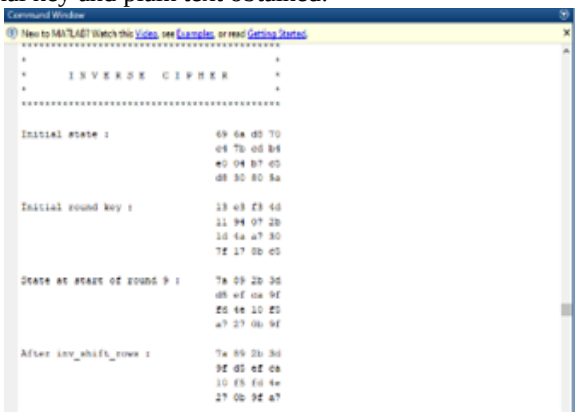


Fig 15: Decryption process- key and cipher text to plain text conversion

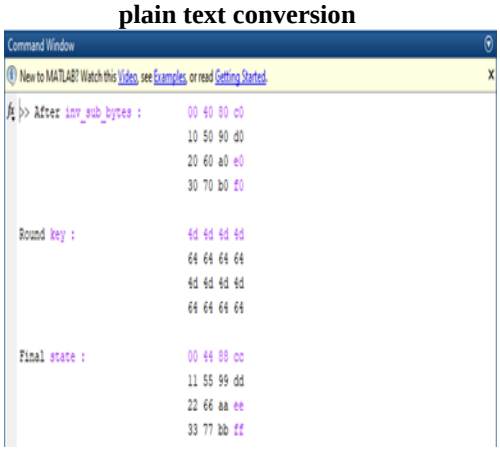


Fig 16: Final key and plain text at the end of decryption

In today's scenario, AES is widely used and accepted for hardware and software implementation. Till date, no practical cryptographic attack has been identified or reported. Additionally, AES has built –in- key flexibility which improves the overall advantage of the process. However, similar to DES, AES security is assured only if it is correctly implemented with the proper key management techniques. [2]

III. THE PROPOSED NOVEL METHOD: SYMMETRIC RANDOM BIOMETRIC KEY (SRBK)

3.1. ENCRYPTION

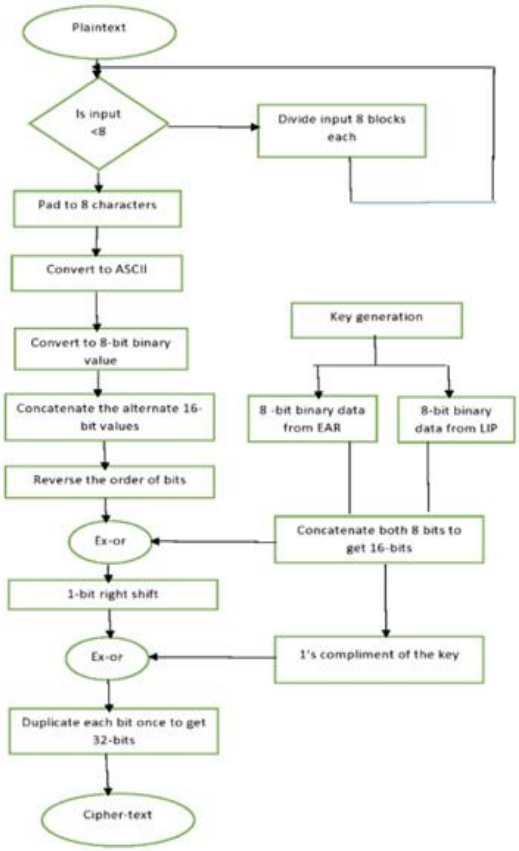


Fig 17: Flow chart of SRBK Encryption

Step 1: Initial data of size multiple of 8 is taken, if necessary do padding.

Step 2: Data is divided into 8 characters each

Step 3: Convert into its corresponding ASCII equivalent.

Step 4: Concatenate the alternate set of binary values

Step 5: Reverse the order of bits from step 4

Step 6: Bringing the concatenated biometric key from ear and lip

Step 7: Ex-or the result of step 5 and step 6

Step 8: Perform 1-bit right shift with result obtained from step 7

Step 9: 1's compliment the values of step 6

Step 10: Ex-or the result of step 8 and step 9

Step 11: Duplicating each bit once to get 32-bit cipher text

PLAIN TEXT	S	U	C	C	E	S	E	S
ASCII	83	85	67	67	69	83	69	83
BINARY VALUE	1010011	1010101	1000011	1000011	1000101	1010011	1000101	1010011
CONCATENATE THE ALTERNATE BITS	101001101000011	101010101000011	100010101000101	101001101010011				
REVERSE THE ORDER	1100001011001010	1100001010101010	1010001010100010	1100101011001010				
KEY CONCATENATE FROM EAR AND LIP	0100111001100100							
KEY'S COMPLIMENT	1011001100110111							
XOR-ING THE REVERSE BITS WITH KEY	1000110010101100	1000110011001110	1110111011000110	1000010010101110				
1 BIT RIGHT SHIFT	0100011001010110	0100011001100111	0111011101100011	0100001001010111				
XOR-ING WITH KEY'S COMPLIMENT	1111011111001101	1111011111111100	1100011011111000	1111001111001100				
DUPLICATING EACH BIT ONCE TO GET THE CIPHERTEXT	11111111001111111111000011110011111111110011111111111111111111000011110000001111001111111110000001111111110000111111 11000011110000							

Retrieval Number: F10670886S19/2019©BEIESP
DOI:10.35940/ijeat.F1067.0886S19
Journal Website: www.ijeat.org

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

3.2. DECRYPTION:

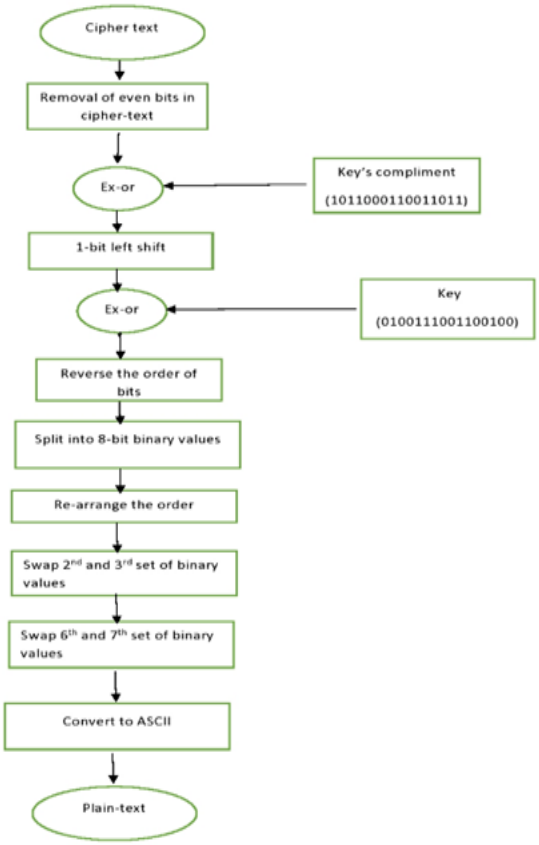


Fig 18 : Flow Chart – Decryption

Step 1: The 32-bit cipher text is obtained, in which the even number of bits are removed.

Step 2: The data is divided into four sets of 16 bit values.

Step 3: The key's compliment value is obtained which is ex-ored with step 2.

Step 4: Perform 1-bit left shift with the result obtained from step 3.

Step 5: Ex-or the key value with the left shifted bits.

Step 6: Reverse the order of bits with the result from step 5.

Step 7: Split into 8 sets of 8-bit binary values.

.

CIPHER TEXT	11111111001111111111100001111001111111111100111111111111111111110000111100000011110011111111110000001111 11111000011111111000011110000							
REMOVAL OF SUCCESSIVE EVEN BITS	11110111111001101		11110111111111100		1100011011111100		11110011111001100	
KEY'S COMPLIMENT	1011000110011011							
XOR-ING THE OBTAINED BIT WITH THE ABOVE 1'S COMPLIMENT OF THE KEY	01000110010101110	01000110011001111	01110111011000011	01000010010101111				
1-BIT LEFT SHIFT	10001100101011100	10001100110011110	11101110110001110	10000100101011110				
XOR-ING THE LEFT SHIFTED BIT WITH THE KEY	11000010110010010	11000010101010110	10100010101000010	11001010110010010				
REVERSE THE ORDER	01010011010000011	01001010101000011	01000101010001101	01010011010100011				
SPLIT INTO 8 BITS EACH	01010011	01000011	01001010 1	01000011	01000101	01000101	01010011	01010011
SWAPPING (2ND AND 3RD & 6TH AND 7TH)	01010011	01001010 1	01000011	01000011	01000101	01010011	01000101	01010011
ASCII	83	85	67	67	69	83	69	83
PLAINTEXT	S	U	C	C	E	S	E	S

Step 8: Swap the 2nd and 3rd byte values and 6th and 7th byte values.

Step 9: Convert into corresponding ASCII from the result obtained in step 8.

Step 10: The 8-character plain text is obtained

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

3.3. Symmetric Random Biometric Key- Features

- The proposed algorithm will be several times faster than the existing algorithm.
- This algorithm is safe against unauthorized attacks and runs faster than the popular existing algorithm.
- With this new approach we are implementing a technique to enhance the security level of this algorithm and further reduce the time for encryption and decryption.

IV. RESULTS AND DISCUSSIONS

Comparison is made between the AES algorithm and SRBK algorithm. Memory occupied by SRBK is several times lower than AES algorithm. The encryption time (time taken by the algorithm to convert from plain text to cipher text) is calculated for both the algorithms. Since the number of steps for encryption and decryption is less for SRBK, the overall encryption and decryption time is lesser than AES. The throughput is obtained based on the encryption time. It shows the speed of encryption and decryption. The speed at which the total plaintext encrypted divided by encryption time. The throughput is higher for SRBK compared to AES.

Fig 19: Memory occupied by AES and SRBK

Fig 20: Input data in Kb and CPU process time for encryption in milliseconds

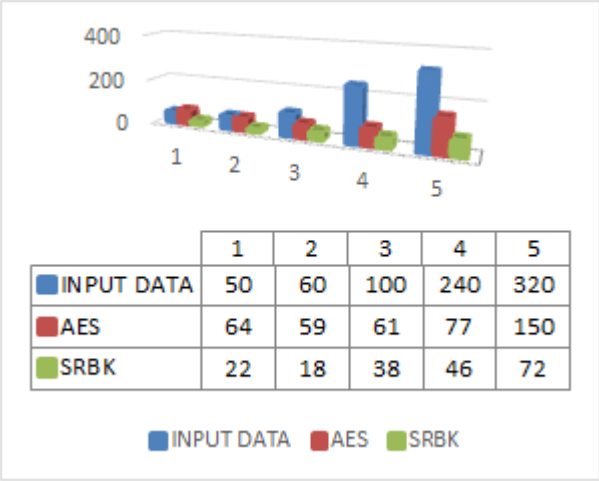


Fig 21: Input data in Kb and CPU process time for

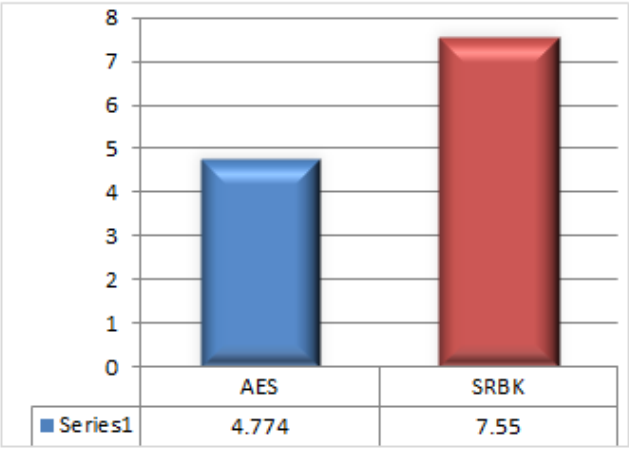


Fig 22: Throughput (Mb/sec)- ENCRYPTION Decryption in milliseconds

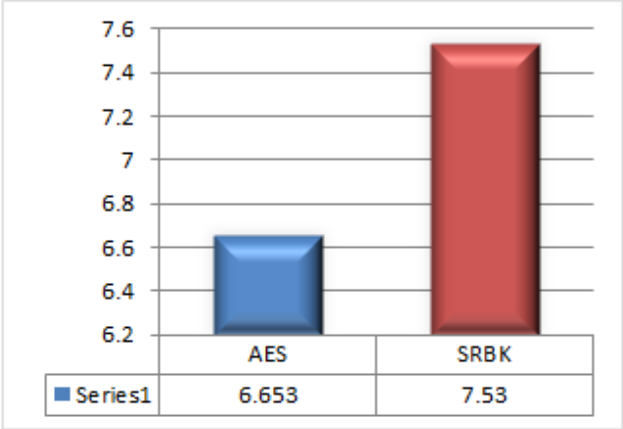


Fig 23: Throughput (Mb/sec)- DECRYPTION

V. CONCLUSION AND FUTURE WORK

Thus the proposed algorithm occupies less memory and encryption and decryption time proving it is better than existing encryption algorithm. The biometric key used for encryption and decryption is flexible and the number of bits can be changed based on the plain text used. We also say that the key is secure since it is generated from our own biological trait.

Retrieval Number: F10670886S19/2019©BEIESP
DOI:10.35940/ijeat.F1067.0886S19
Journal Website: www.ijeat.org

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

The future work can be extended with the additional novel method with increase number of rounds for better security and the increased key length for encryption and decryption. Additional algorithm can also be used for comparison.

REFERENCES

1. "A Comparative Survey on Symmetric Key Encryption Techniques"- Monika Agrawal, Pradeep Mishra, International Journal on Computer Science and Engineering (IJCSE), Vol. 4 No. 05 May 2012, ISSN 0975-3397,Page no.877-882.
2. "Advanced Encryption Standard (AES) Algorithm to Encrypt and Decrypt Data" -Ako Muhamad Abdullah-Research gate-Publication Date: June 16, 2017
3. XAdvanced Encryption Standard - Tutorialspoint https://www.tutorialspoint.com/cryptography/advanced_encryption_standard.html
4. "A Survey on Cryptography Algorithms" Omar G. Abood, Shawkat K. Guirguis-International Journal of Scientific and Research Publications, Volume 8, Issue 7, July 2018 495 ISSN 2250-3153
5. "A Survey on Common Symmetric Encryption Algorithms" Arvind Kumar Sharma and Hitesh Sharma-International Journal of Engineering Research & Technology (IJERT) IJERT ISSN: 2278-0181 Vol. 3 Issue 12, December-2014.
6. "A SURVEY ON ENCRYPTION ALGORITHMS USING MODERN TECHNIQUES" Venkat Prasad.K, S. Magesh,-International Journal of Pure and Applied Mathematics Volume 117 No. 16 2017, 673-678.
7. "A Survey on the Cryptographic Encryption Algorithms" -Muhammad Faheem Mushtaq, Sapiee Jamel, Abdulkadir Hassan Disina, Zahraddeen A. Pindar, Nur Shafinaz Ahmad Shakir, Mustafa Mat Deris-(IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 8, No. 11, 2017.
8. "Encryption Algorithms: A Survey"-Swathi S V, IILahari P M, IIIBindu A Thomas-International Journal of Advanced Research in Computer Science & Technology (IJARCST 2016)- Vol. 4, Issue 2 (Apr. - Jun. 2016).
9. .Formulation of Ear Biometric Key with an Eminent Noise Immune Filter to Provide High Security in Authentication - Ms.S.Pavithra, ,Dr.P.Muthukannan, Mr.V.Prabhakaran, Jour of Adv Research in Dynamical & Control Systems, Vol. 10, 07-Special Issue, 2018
10. "Foundations of Computer Security" Lecture 52: Diffie-Hellman Key Exchange Dr. Bill Young Department of Computer Sciences University of Texas at Austin.
11. "Generation of Cryptographic Keys from Personal Biometrics: An Illustration Based on Fingerprints" By Bon K. Sy and Arun P. Kumara Krishnan.
12. Lecture Notes on "Computer and Network Security" by Avi Kak (kak@purdue.edu)
13. "Performance Analysis of AES and DES Cryptographic Algorithms on Windows & Ubuntu using Java", Shraddha Dadhich, International Journal of Computer Trends and Technology (IJCTT) - Volume 35 Number 4 - May 2016.
14. "Performance Analysis of AES, DES and RSA Cryptographic Encryption Algorithms: A Novel Study"-Nitin Arora, Kritika Metha, Km. Anjali, Manisha Bhatt, Km. Aradhana, Krishan Chandra Mishra, Mamta Martolia-International Journal of Electrical Electronics & Computer Science Engineering Volume 3, Issue 3 (June, 2016) | E-ISSN : 2348-2273 | P-ISSN : 2454-1222.
15. "SURVEY ON DIFFERENT TYPE OF ENCRYPTION ALGORITHM'S"- Namdev Choure, Prof. Shrikant Dhamdhere-open access international journal of science and engineering-|| Volume 3 || Special Issue 1 || March 2018