ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 3, Issue 2, August 2013.

A Secure Data Transmission Using Dynamic Random Key

B.T.Geetha, M.V.Srinath
geetha_bt@yahoo.co.in, sri_induja@rediffmail.com
Research Scholar, Sathyabama University, Chennai, India.
Head – Content Development, at Efuture Soft, Chennai,India.

Abstract: Today we are in the world where conservation of energy is very important. The amount of energy consumption used for encryption is high. The main aim is to reduce the energy needed for the encryption technique. Hence this paper proposes a new encryption algorithm, using which the energy required for encryption can be reduced. In this paper we are implementing a High Diffusion (HD) algorithm which conserves energy than the currently used Advanced Encryption Standard (AES) encryption algorithm.

Key words: **Key mixing, Transposition Layer, Substitution Layer, S-matrix, Inverse S-Matrix, High diffusion.**

I. INTRODUCTION

A. Network Security

In the field of networking, the area of network security consists of the provisions and policies adopted by the network administrator to prevent and monitor unauthorized access, misuse, modification, or denial of the computer network and network-accessible resources.

Authentication

Network security starts from authenticating the user, commonly with a username and a password. Access points support Medium Access Control (MAC) authentication of wireless clients, which means that only traffic from authorized MAC addresses, will be allowed through the access point. Unilateral authentication means that the access point authenticates the user, but the user does not authenticate the access point .

Encryption

Encryption is the process of transforming information (referred to as plaintext) using an algorithm to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key. The result of the process is encrypted information , referred to as cipher text .

Decryption

Decryption is the reverse process of encryption. It is the process of transforming encrypted information into readable information. There are different types of encryption available. This paper implements a new encryption technique.

II. LITERATURE SURVEY

The Table -1 gives us the comparative study about the different techniques used in cryptography[3][6].

III. PROPOSED SYSTEM

Proposed system consists of four layers.

1. Key mixing layer
2. Nonlinear substitution layer
3. Symbol transposition layer
4. HD encoding layer

The proposed system shown in Fig.1 has higher throughput when compared to the existing AES since the block size is higher.

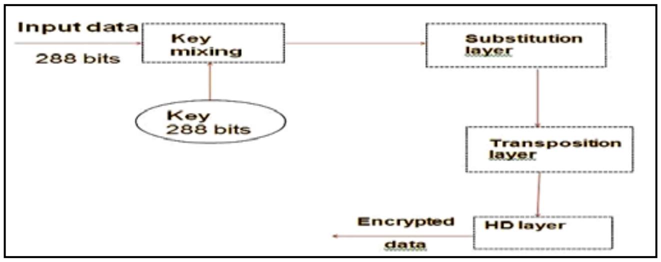

Fig 1: Block Diagram of propose system.

The energy consumption for encryption of data in the proposed system is less than the AES. The objectives of the proposed system are,

- ✓ To save the energy used for encryption of data.
- ✓ To make the encryption faster and reduce the number of encryption rounds to encrypt the message.
- ✓ To generate dynamic random key for encryption.

TABLE 1

COMPARATIVE STUDY OF DIFFERENT CRYPTOGRAPHIC TECHNIQUES

RC-4	WEP	TKIP	DES	AES
Rivest Cipher 4	Wired Equivalent Privacy	Temporal Key Integrity Protocol	Data Encryption Standard	Advanced Encryption Standard
Used by standards such as IEEE 802.11	Used by standards such as IEEE 802.11	Used by standards Such as IEEE 802.11i	Used by standards such as IEEE 802.11	Used by standards such as IEEE 802.11
Shared key stream cipher algorithm	WEP uses the stream cipher RC4 for confidentiality and the CRC-32 checksum for integrity.	TKIP utilizes the RC4 stream cipher with 128-bit keys for encryption and 64-bit keys for Authentication.	Data encryption using a private (secret) key	Symmetric block cipher that can encrypt and decrypt information.
The data stream is simply XORed with the generated key sequence	A 40 bit key is concatenated with a 24-bit initialization vector (IV) to form a 64 bit RC4 traffic key	TKIP enhances WEP by adding i) A per-packet key mixing function to de-correlate the public IVs from weak keys. ii) A rekeying mechanism to provide fresh encryption and integrity keys.	It takes a 64 bit key as input, of which only 56 bits are used. From these 56 bits, 48 bit sub keys are created.	Using cryptographic keys of 128, 192, and 256 bits to encrypt and decrypt data in blocks of 128 bits.
Vulnerable to analytic attacks of the state table.	WEP is vulnerable because of relatively short IVs and keys that remains static.	More resistant to cryptanalytic attacks involving key reuse.	Worked fine for small data sets, but Slowed down incredibly on larger blocks.	It has 10 rounds for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys.

IV. SYSTEM ARCHITECTURE

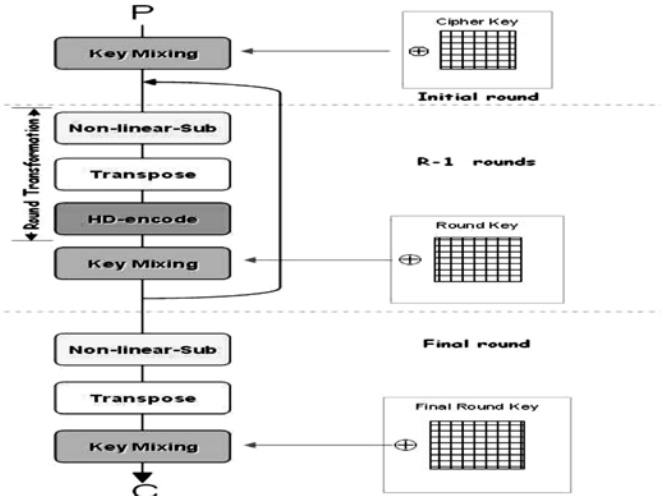

Fig 2: System Architecture

The Fig 2 above shows the system architecture of the proposedd algorithm.This algorithm performs 10 rounds for encryption.

In each round there are four layers.The layers are Key mixing layer, Non linear substituton layer, transposition layer and High diffusion encoding layer. These layer functions are carried out in both encryption and decryption.The data from the user is seperated into the blocks of size 288bits. These seperated user data are processed layer by layer.The detailed layer functions are discussed in the following section.

V. DETAILED DESIGN AND TEST PLAN

A. Decomposition Description

There are various components and modules present in our paper. Everything in the paper can't be done at the same time; hence we had decomposed our work in two different modules. Decomposition gives us an easier way to solve any type of big problems. It has a power to convert very huge things into a number of smaller ones.

B. Detailed Design

In this paper the modules had been designed based upon its work. The objective of this paper is to reduce the energy required for the encryption technique.

The following modules are carried out in both encryption and decryption . The data from the user are separated into the blocks of size 288 bits [1]. The user data are processed block by block.

1.) Key Mixing Layer

The key mixing layer is a bitwise XOR operation of the plain text with the round key . The output cipher text of the key mixing layer of round r-1 forms the input plain text to the next round r . The key size is 288 bits and it is represented by 6x6 matrix . The key generated is expanded to produce a round key for each round . Initially at the beginning the block of data is XORed with the initialization vector and then sent to the key mixing layer.

In decryption the block of cipher text is XORed with the round key generated .

2.) Nonlinear Substitution Layer

In substitution layer the input data bytes are substituted with the bytes in the S-Box (given in table 2) [2][5] . The S-Boxis the 16x16 matrix which contains the hexadecimal byte values up to 255 in the random order . The input data byte is split into two nibbles as upper 4 bits and lower 4 bits. The lower nibble is used to identify the row and the upper nibble is used to identify the column. The intersection of the rows and columns will give the new data byte which is to be placed as an input data byte.

3.) Symbol Transposition Layer

This layer is used to reduce the linearity among the input data , so that making the attacks harder .The aim of this layer is to change the position of the data using the permutation . The permutation function is stored in an array and it is used to make the transposition of the data.

In decryption the same permutation function is applied to the cipher state .

In decryption the cipher bytes are replaced with the bytes in the similar manner except that the inverse S-Box (given in Table 3) is used to reverse the process.

The permutation function used in this paper is given in Table 4.

4.) HD Encoding Layer

The function of this layer is to securely expand the number of bits in the input data. The layer securely encrypt ‘ k ’ bit input data i.e. plain text into ‘ n ’ bit encrypted output data i.e. cipher text. Here the number of bits in the cipher text is greater than the number of bits in plain text. High encryption throughput is obtained when this layer function is used in Counter (CTR) mode [1]. In decryption the reverse process is carried out on cipher text to retrieve the plain text.

TABLE 2

S-BOX

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	01	DE	A5	63	6A	26	7E	C9	7F	67	A4	05	03	64	2E	32
1	AE	04	BA	B5	B2	50	3A	17	08	82	0F	94	ED	7C	F5	71
2	6C	24	8A	B9	D9	E2	CC	38	B0	6D	EC	8D	3D	CA	9D	A9
3	B1	6F	E3	80	35	3B	B6	4A	E7	21	55	B3	68	BD	6E	19
4	F0	16	6B	EB	59	28	1D	2C	D6	41	3F	D5	C7	3E	8F	89
5	36	88	45	8E	DD	8C	34	CD	2F	A2	22	F7	AF	29	9E	91
6	E9	86	C0	40	18	83	F6	25	C2	A1	54	AB	66	EF	A6	E8
7	B4	5A	84	C4	52	5F	E5	02	5D	EA	D4	DB	D2	85	5B	27
8	00	44	93	47	DF	46	1A	D7	37	51	49	A8	1C	B8	4F	F9
9	C5	43	60	20	0C	57	7B	A3	61	E1	2A	E4	33	C6	53	74
A	0B	9A	76	E6	65	FF	C3	3C	9F	75	56	F8	69	F3	9C	87
B	7D	F4	5E	FD	BF	23	0D	DA	AA	99	95	9B	0E	5C	96	39
C	D3	90	30	92	C1	2D	1B	E0	81	97	15	72	10	1F	98	62
D	78	4D	13	73	AC	CE	D0	1E	FE	8B	2B	0A	06	C8	4E	F2
E	CB	CF	58	7A	EE	A0	B7	DC	12	42	FB	FC	07	14	4B	AD
F	D8	48	77	11	D1	A7	BC	70	F1	FA	BB	79	09	BE	4C	31

VI. IMPLEMENTATION AND RESULT

A. Implementation

This paper proposes an encryption algorithm to encrypt the data efficiently saving the energy. The block size of this algorithm is higher when compared to the currently existing algorithms. The algorithm splits the user data into blocks of 288 bits. The data are processed block by block. This algorithm has ten rounds , each round consisting of four layers.

The key generation algorithm is invoked and the round keys are generated. The round keys are used in the key mixing layer. The blocks of data are then processed through the rounds of the algorithm. The encrypted data are obtained from the output of the final round and it is written to the file. This file is input to the decryption. Decryption is the reverse process of encryption carried out to get the plain text from the cipher text.

TABLE 3

INVERSE S-BOX

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	80	00	77	0C	11	0B	DC	EC	18	FC	DB	A0	94	B6	BC	1A
1	CC	F3	E8	D2	ED	CA	41	17	64	3F	86	C6	8C	46	D7	CD
2	93	39	5A	0B	21	67	05	7F	45	5D	9A	DA	47	C5	0E	58
3	C2	FF	0F	9C	56	34	50	88	27	BF	16	35	A7	2C	4D	4A
4	63	49	E9	91	81	52	85	83	F1	8A	37	EE	FE	D1	DE	8E
5	15	89	74	9E	6A	3A	AA	95	E2	44	71	7E	BD	78	B2	75
6	92	98	CF	03	0D	A4	6C	09	3C	AC	04	42	20	29	3E	31
7	F7	1F	CB	D3	9F	A9	A2	F2	D0	FB	E3	96	1D	B0	06	08
8	33	C8	19	65	72	7D	61	AF	51	4F	22	D9	55	2B	53	4E
9	C1	5F	C3	82	1B	BA	BE	C9	CE	B9	A1	BB	AE	2E	5E	A8
A	E5	69	59	97	0A	02	6E	F5	8B	2F	B8	6B	D4	EF	10	5C
B	28	30	14	3B	70	13	36	E6	8D	23	12	FA	F6	3D	FD	B4
C	62	C4	68	A6	73	90	9D	4C	DD	07	2D	E0	26	57	D5	E1
D	D6	F4	7C	C0	7A	4B	48	87	F0	24	B7	7B	E7	54	01	84
E	C7	99	25	32	9B	76	A3	38	6F	60	79	43	2A	1C	E4	6D
F	40	F8	DF	AD	B1	1E	66	5B	AB	8F	F9	EA	EB	B3	D8	A5

TABLE 4
PERMUTATION FUNCTION

0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**
6	**12**	**30**	**23**	**8**	**25**	**19**	**1**	**13**	**17**	**7**	**22**	**2**	**21**	**15**	**32**	**5**	**0**
18	**19**	**20**	**21**	**22**	**23**	**24**	**25**	**26**	**27**	**28**	**29**	**30**	**31**	**32**	**33**	**34**	**35**
11	**24**	**18**	**31**	**35**	**3**	**14**	**33**	**34**	**10**	**16**	**27**	**4**	**28**	**26**	**20**	**29**	**9**

The following steps explain the algorithm

1. Begin
2. Separate the input file into blocks of 288 bits
3. Read the data block from the file
4. Perform key expansion
5. Initialize the count variable round to 1
6. Perform key mixing operation
7. Perform substitution function
8. Perform the transposition operation
9. Perform high diffusion operations.
10. Repeat steps 6 to 9 until counter variable is 10
11. Write the encrypted data to the file.
12. Repeat steps 3 to 11 until end of file is reached.
13. End

B. Result

The time consumed by a full 10 round 288- bit (key stream length) HD cipher, and a 256-bit AES [11] is measured in two different systems of different configurations with different sizes of files are given as input . The results obtained are tabulated in Tables 5 and 6 and its corresponding graphs are shown in figures 3 and 4 respectively,

System 1:

RAM : 4GB Hard Disk: 320GB
Processor: AMD 2.3GHz

TABLE 5
COMPARISON TABLE FOR SYSTEM-1

Size of the file	**Time taken in AES (micro seconds)**	**Time taken in HD (micro seconds)**
1Kb	16	15
2Kb	500	16
7Kb	531	31
22Kb	547	78

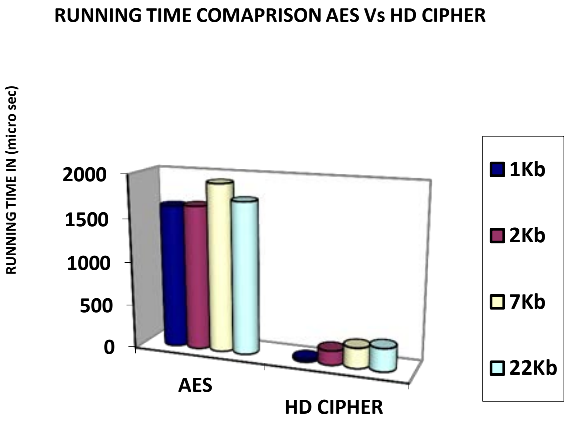

Fig 3: Comparison Chart1

System 2:

RAM : 2GB ,Hard Disk: 500GB
Processor: Intel Pentium P6200 2.13GHz

TABLE 6
COMPARISON TABLE FOR SYSTEM-2

Size of the file	**Time taken in AES (micro seconds)**	**Time taken in HD (micro seconds)**
1Kb	1637	29
2Kb	1652	165
7Kb	1920	234
22Kb	1738	265

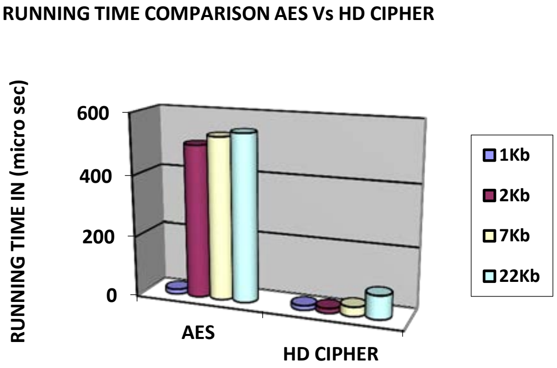

Fig 4: Comparison Chart2

VII. CONCLUSION

This paper proposes an encryption algorithm that securely encrypts a larger key stream of 288 bits. Replacing the AES with the HD cipher allows us to achieve higher encryption throughput. The running time analysis experiments reveal that HD cipher consumes less time compared to the traditional AES . Also the proposed system performs significantly better when larger frame lengths are used .

VIII. FUTURE WORK

The future work involves the use of increased block size for the data used in the algorithm . The key generation algorithm can be modified to increase the complexity of the encryption . The number of rounds for the encryption of data can also be increased significantly based on the increased block size of the data.

REFERENCES

[1]. Chetan Nanjunda Mathur and K.P. Subbalakshmi Media Security, Networking and Communications (MSyNC) Lab, “Energy Efficient Wireless Encryption”.

[2]. Hani Ragab Hassen et...al, “An Efficient Key Management Scheme for Content Access Control for Linear Hierarchies”, Author manuscript, published in "Computer Networks 56, 8 (2012) 2107-2118" Preprint submitted to Elsevier February 4, 2012.

[3]. B.T.Geetha, Dr.M.V.Srinath “A Study on various Cryptographic Key Management and Distribution system in Secure Multicast Communications” 2012 International Conference on Advances in Mobile Network, Communication and Its Applications, 978-0-7695-4720-6/12 © 2012 IEEE DOI10.1109/MNCApps.2012.18

[4]. Zia Saquib et…al, “A Configurable and Efficient Key-Management scheme for SCADA Communication Networks”, International Journal of Research and Reviews in Information Security and Privacy (IJRRISP) ,Vol. 1, No. 2, June 2011,ISSN: 2046-5718,Copyright © Science Academy Publisher, United Kingdom.

[5]. V. Ch. Venkaiah and Srinathan Kannan, “Variations to S – Box and Mix Column Transformations of AES.

[6]. W.H.D Ng, H.Cruickshank, and Z.Sun,”Scalable Balanced Batch Rekeying For Secure Group Communication,” Elsevier Computers and Security, Vol.25, pp.265-273, June. 2006.

[7]. Seung-Jae Jang ,Young-Gu Lee , Kwang-Hyung Lee , Tai-Hoon Kim and Moon-Seog Jun “A Study on Group Key Agreement in Sensor Network Environments Using Two-Dimensional Arrays “ , Sensors 2011, 11, 8227-8240; doi:10.3390/s110908227. ISSN 1424-8220.

[8]. D.SuganyaDevi. et al..”Secure Multicast Key Distribution for Mobile Adhoc Networks”, (IJCSIS) International Journal f Computer Science and Information Security,Vol. 7, No. 2, 2010.

[9]. Lein Harn and Changlu Lin “Authenticated Group Key Transfer Protocol Based on Secret Sharing” IEEE Transactions on Computers, Vol. 59, No. 6, June 2010.

[10]. Naim Ajlouni, Asim El-Shwikh and Abdullah Rashed , “A New Approach In Key Generation And Expznsion In Rijndael Algorithm” December 2004.

[11]. www.people.eku.edu/styere/Encrypt/JS-AES.html

Mrs.B.T.Geetha received her M.E in Applied Electronics from MKU, Madurai in 2000 and B.E in EEE from MSU, Tirunelveli in 1998.Currently she is pursuing her Research in Sathyabama University , Chennai in the field of Network Security.

She is Life member in various Professional Societies like IETE (M200016),I.A.C.S.I.T(80332111) and I.S.T.E(LM32127) She is presently with Maamallan Institute of Technology, Chennai as an Associate professor in the Department of Electronics and Communication Engineering.

Dr.M.V.Srinath is Leading the Instructional Design team at current position in developing resources which includes CBT, e-Learning and Instructional materials for clients and in house .

He has published more than 35 Journals in National and International level and he also presented more than 60 papers in the National and International conferences. He has delivered more than 50 key note addresses and invited talks to different Universities and Colleges. He is a member of different Professional bodies like ISTE,CSI, Member, Member World Council for Curriculum and Instruction, Member Indian Society for Training and Development and etc..