ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

A Symmetric Multiple Random Keys (SMRK) Model Cryptographic Algorithm

K. Vijaya Kumar[1], K.Somasundaram[2],

[1]Research Scholar (Karpagam University) & Assistant Professor, Dept. of CSE, Vignan Institute of Engineering for Women, Visakhapatnam, Andhra Pradesh, India.

[2]Professor, Dept. of CSE, Vel Tech High Tech Dr.RR Dr.SR Engineering College, Avadi, Chennai,Tamilnadu India.

ABSTRACT: In this digital world, which is currently involving a rapid change in technology, the security of digital information has become a primary concept. Cryptography plays a specific and important role to protect secret files and documents from unauthorized access. The cryptography algorithms are classified in to two categories, Public-key producing and symmetric-key producing algorithms. The principal goal of designing any encryption algorithm is to hide the original message and send the encrypted or secret text message to the receiver so that secret message communication can take place over the web. The strength and potentiality of an encryption algorithm depends on the difficulty of cracking the original message. A number of symmetric key encryption algorithms like DES, TRIPLE DES, AES, BLOWFISH have been developed to provide greater security affects one over the other. Although the existing algorithms have their own merits and demerits but in this we presents a new approach for data encryption and decryption based on multiple random keys generation. A new encryption algorithm based on block cipher generating mechanism is proposed herewith to analyze the time-consumed by the complete process (process starting from sender encryption to receiver decryption) of the selected cryptographic algorithms with proposed algorithm. Creating random keys for each block and interdependence of all keys in all stages of encrypting and decrypting provides high secure for the data. For the plaintext the corresponding key are generated by randomly. The expected results showing that, under the random keys generation and for the same size of the input block of data, the proposed algorithm will be about several times faster than existing algorithm, and there are other runtime characteristics which further highlight the difference between these cryptographic algorithms. This algorithm is safe against unauthorized attacks and runs faster than the popular existing algorithms. With this new approach we are implementing a technique to enhance the security level of this algorithm and to further reduce the time for encryption and decryption.

KEYWORDS: Cryptography, symmetric key, asymmetric key, random key, security, and security attacks.

I.INTRODUCTION

Cryptography plays a very vital role in keeping the information secure from unauthorized access in transit. The cryptography ensures that the message which is sent from source remains confidential and should be received only by the intended receiver at the other end. Cryptography converts the original message in to non readable format and sends the message over an insecure channel. The original message or the actual message that the source wishes to communicate with the receiver is defined as Plain Text. The message which is in encrypted from is called as Cipher Text. Encryption [1, 3, 8] is the process of converting plaintext into cipher text with a key. A Key is a numeric or alpha

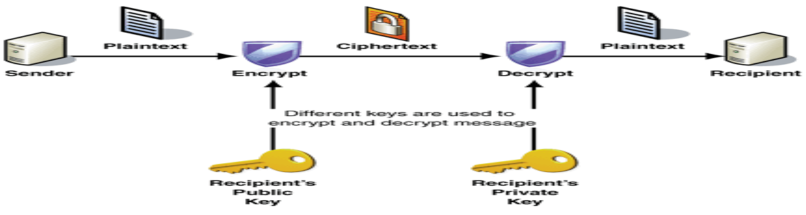


Figure 1: Encryption- Decryption process.

numeric text or may be a special symbol. A decryption [1] is a reverse process of encryption in which original message is retrieved from the cipher text. Encryption takes place at the sender end and Decryption takes place at the receiver end. Figure 1 shows the encryption/decryption process of a plaintext message. The input to the encryption process is plain text and that of decryption process is cipher text. Initially plaintext is passed through the encryption algorithm which encrypts the plaintext using a key and then the produced cipher text is transmitted. At the receiving end for decryption, the input cipher text is passed through the decryption algorithm which decrypts the cipher text using the same key as that of encryption. Finally we get the original plaintext message. Cryptography is broadly divided into two categories [9] depending upon the Key. They are Symmetric Key Encryption [7] and Asymmetric Key Encryption. Symmetric Key Encryption uses the same key for encryption and decryption processes [6]. This technique is simple yet powerful but key distribution is the chief problem that needs to be addressed Whereas, Asymmetric Key Encryption use two mathematically associated keys: Public Key & Private Key for encryption. The public key is available to everyone but the data once encrypted by public key of any user can only be decrypted by private key of that particular user [16].

II.RELATED WORK

In [1], author proposed a session based symmetric key cryptographic algorithm Matrix Based Bit Permutation Technique (MBBPT) is proposed where the plain text is a binary bit stream with finite number of bits. The bits of the each block fit diagonally upward starting from (1, 1) cell in a left to right trajectory into a square matrix of suitable order n. Then the bits are taken from the square matrix diagonally upward starting from (n, n) cell in a right to left trajectory to form the encrypted binary string. The same process is performed in reverse to get the plain text.

In [2] the main idea is taken from Importance of cryptography in network security By Susan Storm et al ,26th May 2003. It consist of Network security issues, the role of cryptography, the status of network security and finally what steps must be taken while implementing the efficient security policy.

Nitin K proposed strengthen secured communication [3] over the Network by enhancing the strength of the AES algorithm with Diffie-Hellman key exchange Protocol. The security strength of the AES algorithm can be enhanced by increasing the key length to 256 bit and thereby increasing the number of rounds in order to provide a stronger encryption method for secure communication. The author says, AES can be more strengthen by Diffie-Hellman Key Exchange Protocol which allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure communications channel.

The author proposes application of AVK (Automatic Variable Key) in curves [4] , AES, RSA, diffusion and message digest and it is shown that it increases security level during transmission. Gain in time complexity can be achieved by parallel computing and parallel reliability. It has been said that the most secured criteria is variable data with variable secret key with message transmission mode also being variable (i.e. both transmitter and receiver to use non-orthogonal measurement bases). It has also been shown how AVK can be applied in Vernum Cipher.

In this paper the author [5] proposed genetic algorithms (GAs) are a class of optimization algorithms. GA deals with the confidentiality of electronic data which is transmitted over the internet. The concept was genetic algorithms with pseudorandom function to encrypt and decrypt data stream. The encryption process is applied over a binary file so that the algorithm can be applied over any type of txt as well as multimedia data.

. In this paper the author [6] proposes different types of cryptographic approaches where the efficiency of these approaches depends on the message size and the key size. The author discussed, one of the most effective cryptography approach called Random Key cryptographic algorithm. He has defined the algorithmic approach adapted by the approach along with result analysis where the system shows the Random key Visual Cryptography is effectively efficient.

In this paper the author [7] presents a detailed study on various symmetric key encryption techniques, its comparison and the attacks to which they are vulnerable to. Cryptography plays an integral role in secure communication and it provides an excellent solution to offer the necessary protection against the data intruders. Over a significant time, data encryption techniques took a massive leap from simple methods to complicated mathematical calculations in order to achieve secure communication.

Deepti A. Chaudhari proposed a new intrusion detection system named Enhanced Adaptive ACKnowledgement (EAACK) [8] is specially intended for MANET. By the acceptance of MRA scheme, EAACK is capable of detecting malicious nodes regardless of the existence of false misbehaviour report. Enhanced Adaptive Acknowledgment (EAACK) has been developed with Hybrid cryptography (DES and RSA). By adopting this technique, it further reduces the network overhead which is caused by digital signature in previous system. To increase the security level of packet, prime number generation of RSA is done by Genetic Algorithm.

In this paper the author [9] explains various symmetric key encryption algorithms were observed from many angles. To overcome the problems in Symmetric Ciphers, Public Key Cryptography was developed, but it has its own loopholes. The strongest ciphers of today may become easier to decode with the onset of Quantum Computing. Ergo, there will always be a need for stronger encryption techniques & there is allot of scope for research in the mysterious field of Cryptography.

The author [10] explains digital signature scheme. Digital signature is the technique of cryptography which is used for providing security to the users. Not only this but it also ensures the information confidential, and also provides digital signature, authentication, secret sub-storage, system security and other functions. So encryption and decryption process is the solution of ensuring the non repudiation, confidentiality, integrity and authenticity of the data.

In this paper the author[11] analyzed different symmetric key algorithms for various file features like different data type, data density, data size and key size, and analyzed the variation of encryption time for different selected cipher algorithms. From the simulated results it is concluded that encryption time is does not dependent upon data type and date density of the file, it depends upon the number of bytes present in the file. It also revealed that encryption time and data size is proportional to each other. For all block cipher algorithms that are analyzed, with increase in key size, encryption time also increases, but reduces with increase in key size.

Mohammad Soltani, Young, the author [14] suggested a new robust cryptography algorithm to increase security in the Symmetric-key producing algorithm. At each stage creating five keys for cryptography, storing a part of secret file at one of the keys, Interdependence of all keys in all stages of encrypting and decrypting, To make the keys interdependent and to encrypt the secret file by each of them, there are 2 independent algorithms to select the type of algorithm needed to make the keys interdependent by the user, bigger changes in the physical structure of the encrypted file In case of wrong decryption and to make the resulting keys and encrypted file unique after the cryptography process.

In [15] the author gave a detailed theoretical study on the DES, 3DES, AES and Blowfish symmetric encryption algorithms and a comparative analysis has been made. These algorithms consume a significant amount of computing resources such as CPU time, memory and battery power. The comparison is made on the basis of these parameters: speed, block size, and key size etc. and concluded that Blowfish has better performance than other DES, 3DES, and AES algorithms.

The author [16] gave a detailed analysis of symmetric block encryption algorithms on the basis of different parameters to analyze the performance of the most popular symmetric key algorithms in terms of Authentication, Flexibility, Reliability, Robustness, Scalability, Security, and to highlight the major weakness of the mentioned algorithms, making each algorithm's strength and limitation transparent for application. It is observed that most of them have a tradeoff between memory usage and encryption performance with few algorithms been compromised.

III.THE PURPOSE OF CRYPTOGRAPHY- GOALS OF CRYPTOGRAPHY

The main purpose of cryptography is to provide security to the information in transit. This makes to design Cryptography to achieve number of goals to ensure the secrecy, privacy of data, non alteration of data and so on. Due to the great security advantages of cryptography it is widely used today. Following are the various goals of cryptography [2, 11].

A. *Confidentiality*

Information in computer is transmitted and has to be accessed only by the authorized party.

B. *Authentication*

The information received by any system has to check the identity of the sender that whether the information is arriving from a authorized person or a false identity.

C. *Integrity*

Only the authorized party is allowed to modify the transmitted information. No one in between the sender and receiver are allowed to alter the given message.

D. *Non Repudiation*

Ensures neither the sender, nor the receiver of message can deny the transmission.

E. *Access Control*

Only the authorized parties are able to access the given information.

IV.TYPES OF CRYPTOGRAPHY

Cryptography [16] is a process of converting plaintext (ordinary text, or clear text) into ciphertexts (a process called encryption), then back again (known as decryption). There are many ways to classify the various cryptographic algorithms. The most common are symmetric key cryptography which uses secret key and asymmetric key cryptography which uses public key cryptography.

A. Secret Key Cryptography

In secret key cryptography [9], a single key is used for both encryption and decryption. The key should be known to both the sender and the receiver. The key used by the sender is sent to the receiver by means of any secured lines which is difficult in this approach. The receiver applies the same key to decrypt the message and recover the plaintext. Because a single key is used for both functions, secret key cryptography is also called symmetric encryption.

B. Public Key Cryptography

In public or asymmetric key cryptography [9], pair of keys is used one private key and one public key. Both keys are required to encrypt and decrypt a message or transmission. The private key is just private. It is not to be shared with anyone and it will not be lost or compromised. On the other hand, the public key is just public. Public key cryptography intends for public keys to be accessible to all users. In fact, this is what makes the system strong. If a person can access anyone public key easily, usually via some form of directory service, then the two parties can communicate securely and with little effort, i.e. without a prior key distribution arrangement. In this paper multiple random number symmetric keys are being used.

C. Stream ciphers and block cipher methods

Stream ciphers [15] operate on a single bit (byte or computer word) at a time, and implement some form of feedback mechanism so that the key is constantly changing. A block cipher is so-called because one block of data is encrypted at a time using the same key on each block. In general, the same plaintext block will always encrypt to the same cipher text when using the same key in a block cipher whereas the same plaintext will encrypt to different cipher text in a stream cipher. Block ciphers can operate in one of several modes. They are Electronic Codebook (ECB), Cipher Block Chaining (CBC), Cipher Feedback (CFB) mode and Output Feedback (OFB).

The most common secret-key cryptography method using today is the Data Encryption Standard (DES), designed by IBM in the 1970s. DES is a block-cipher method, uses a 56-bit key that operates on 64-bit blocks. The DES method has a set of rules and transformations that employed specifically for a fast hardware and slow software implementations.

Several variants of DES are currently in use, including Triple-DES (3DES, also described in FIPS 46-3) and DESX. There are a number of other secret-key cryptography algorithms that are also in use today like CAST-128 (block cipher), RC2 (block cipher) RC4 (stream cipher), RC5 (block cipher), Blowfish (block cipher), Twofish (block cipher). In 1997, NIST initiated a new secure cryptosystem standard for U.S. government applications called, the Advanced Encryption Standard (AES), which became the official successor to DES in December 2001.

V.SMRK ALGORITHM

A. Encryption Algorithm:

```
Input: A data of size multiple of 8 if necessary do padding with ""(space).
Step 1: Data is divided into 8 characters each.
Step2: Each of these 8 characters is converted into their ASCII values.
Step3: Each ASCII character is converted into binary values of length 8 bit.
Step4: Two 8-bit binary values are concatenated and reverse operation is performed.
Step5: Random key of 16 bit is generated i.e.(0-   65,535).
Step6: Divide 16 bit reversed value with 16 bit random generated key.
Step7: The obtained remainder and quotient is individually padded to 16 bit.
Step8: Remainder and quotient of 16 bit each is concatenated.
Step9: To the above result 4 bit left shift is performed.
Step10: Each 8 bit in the 32 bit is converted to decimal and divided with 32.
Step11: The 32 bit value is generated by filling the positions obtained in the above step with each bit of keys complement.
Step12: The result of step 8 & step 11 are concatenated.
```

B. Flow chart of encryption:

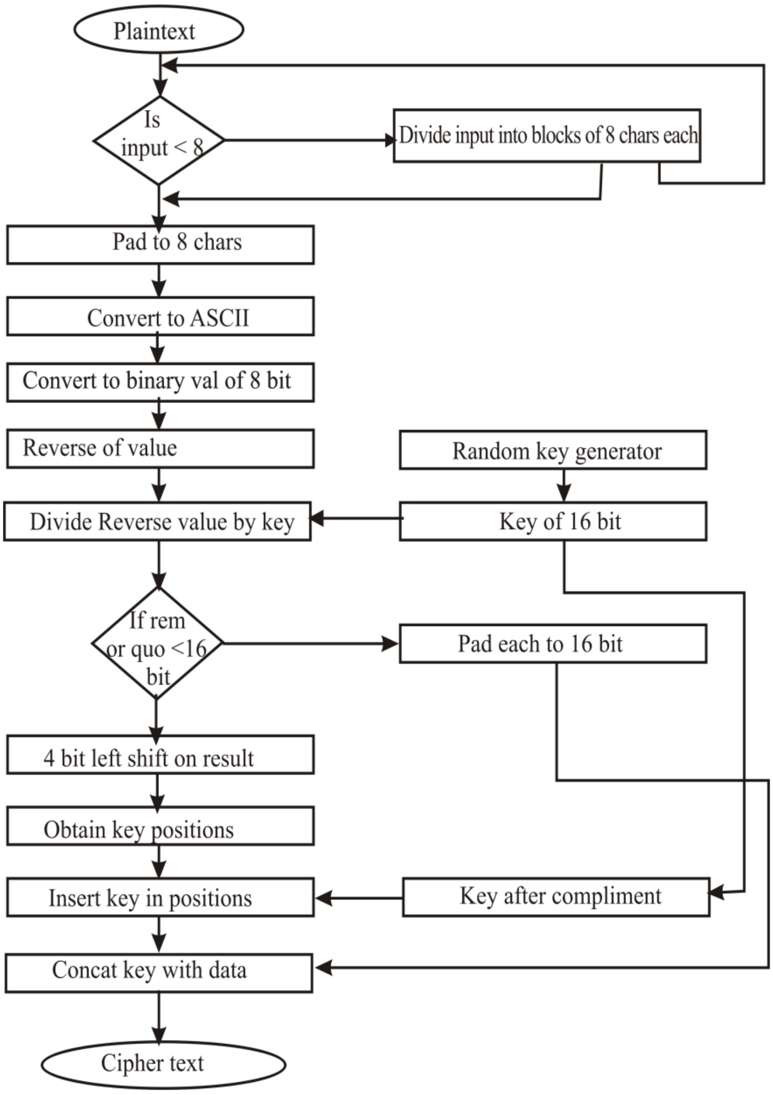


Figure 2: Flow chart of encryption algorithm

C. Decryption Algorithm:

Step 1: Cipher text is divided into 160 bits each.
Step 2: On the first 128 bits of the above step 4 bit left shift is performed for every 32bits.
Step3: Each 8 bit of every 32 bit of the above step is converted to decimal and divides with 32.
Step4: The 16 bit key is retrieved from the remaining 32 bits by taking each bit from the positions obtained in the above step.
Step5: Complement is performed on the obtained 16 bit value.
Step 6: Key is multiplied with last 16 bit and added with first 16 bit for every 32 bit of first 128 bits of cipher text.
Step7: Reverse operation is performed on each 16 bit obtained from the above step.
Step8: Each 8 bit value of the above step is converted to its decimal equivalent.
Step9: Each decimal value is converted to its equivalent ASCII character.

D. Flow chart of decryption:

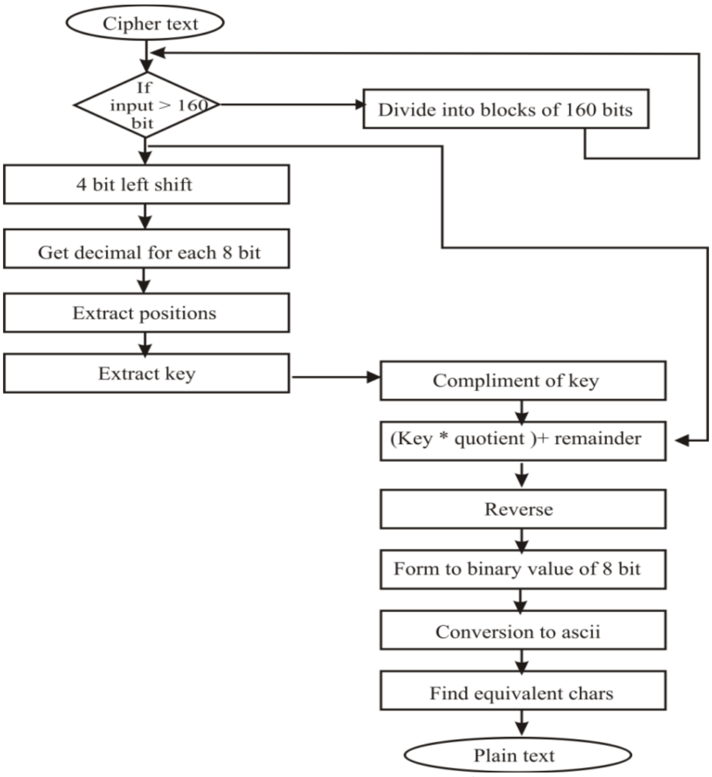
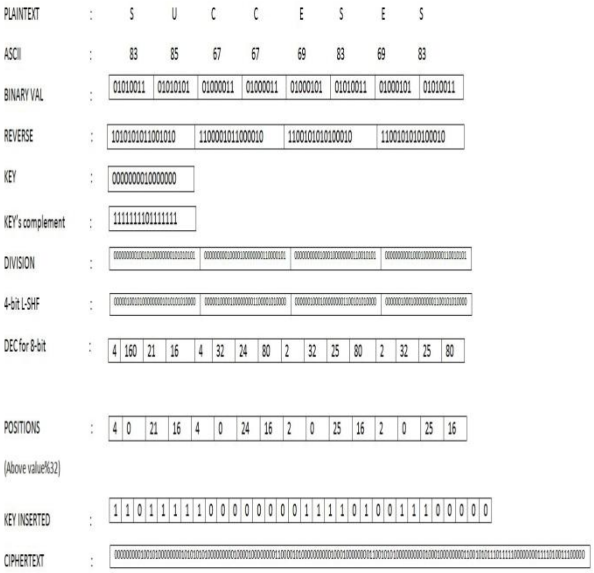


Figure 3: Flow chart of decryption algorithm

VI.NUMERICAL ANALYSIS

Encryption



PLAINTEXT : S U C C E S E S

ASCII : 83 85 67 67 69 83 69 83

BINARY VAL : 01010011 | 01010101 | 01000011 | 01000011 | 01000101 | 01010011 | 01000101 | 01010011

REVERSE : 1010101011001010 | 1100001011000010 | 1100101010100010 | 1100101010100010

KEY : 0000000010000000

KEY's complement : 1111111101111111

DIVISION : 00000000010010100000000101010101 | 00000000010000100000000110000101 | 00000000001000100000000110010101 | 00000000001000100000000110010101

4-bit L-SHF : 00000100101000000001010101010000 | 00000100001000000001100001010000 | 00000010001000000001100101010000 | 00000010001000000001100101010000

DEC for 8-bit : 4 | 160 | 21 | 16 | 4 | 32 | 24 | 80 | 2 | 32 | 25 | 80 | 2 | 32 | 25 | 80

POSITIONS : 4 | 0 | 21 | 16 | 4 | 0 | 24 | 16 | 2 | 0 | 25 | 16 | 2 | 0 | 25 | 16

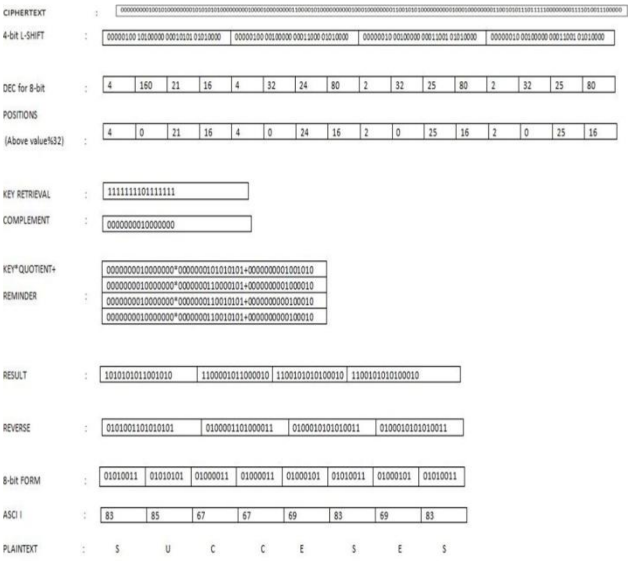
(Above value%32)

KEY INSERTED : 1 | 1 | 0 | 1 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 0 | 1 | 0 | 0 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 0

CIPHERTEXT : 00000000100101000000000101010101000000000010000100000000110000101000000000001000100000000011001010100000000000100010000000001100101011101111100000000011110100111000000

Figure 4: Case study of encryption algorithm

Decryption



CIPHERTEXT : 00000000100101000000000101010101000000000010000100000000110000101000000000001000100000000011001010100000000000100010000000001100101011101111100000000011110100111000000

4-bit L-SHIFT : 00000100 10100000 00010101 01010000 | 00000100 00100000 00011000 01010000 | 00000010 00100000 00011001 01010000 | 00000010 00100000 00011001 01010000

DEC for 8-bit : 4 | 160 | 21 | 16 | 4 | 32 | 24 | 80 | 2 | 32 | 25 | 80 | 2 | 32 | 25 | 80

POSITIONS

(Above value%32) : 4 | 0 | 21 | 16 | 4 | 0 | 24 | 16 | 2 | 0 | 25 | 16 | 2 | 0 | 25 | 16

KEY RETRIEVAL : 1111111101111111

COMPLEMENT : 0000000010000000

KEY*QUOTIENT+ REMINDER :
0000000010000000*0000000101010101+0000000001001010
0000000010000000*0000000110000101+0000000001000010
0000000010000000*0000000110010101+0000000000100010
0000000010000000*0000000110010101+0000000000100010

RESULT : 1010101011001010 | 1100001011000010 | 1100101010100010 | 1100101010100010

REVERSE : 0101001101010101 | 0100001101000011 | 0100010101010011 | 0100010101010011

8-bit FORM : 01010011 | 01010101 | 01000011 | 01000011 | 01000101 | 01010011 | 01000101 | 01010011

ASCI I : 83 | 85 | 67 | 67 | 69 | 83 | 69 | 83

PLAINTEXT : S U C C E S E S

Figure 5: Case study of decryption algorithm

VII.EXPERIMENTAL RESULTS AND ANALYSIS

In this section the comparative study between AES, DES, 3DES, RC6 and SMRK has done on 10 files of sizes varying from 40 Kb to 7310 Kb. Analysis includes comparison of encryption time, decryption time, CPU process time for encryption , decryption , average CPU process time and throughput. Table I & Table II shows the calculations and comparative study for encryption time and decryption time in milliseconds. The proposed SMRK is done against the different files where it takes very less time to encrypt/decrypt than Triple-DES and little bit more time than AES. Figure 6 & Figure7 show the graphical representation of encryption time and decryption time against different file sizes. For this analysis we use MATLAB in a laptop with 2.4 GHz CPU, in which performance data is collected. It encrypts and decrypts different file size ranges of data.

The encryption time is considered the time that an encryption algorithm takes to produce a cipher text from a plaintext. Encryption time is used to calculate the throughput of an encryption scheme. It indicates the speed of encryption. The throughput of the encryption scheme is calculated as the total plaintext in bytes encrypted divided by the encryption time.

The CPU process time is the time that a CPU is committed only to the particular process of calculations. It reflects the load of the CPU. The more CPU time is used in the encryption process, the higher is the load of the CPU. The analysis have been done for different file sizes of data where it is observed the throughput is much more better than the existing algorithms like AES, DES, 3DES and RC6.Individual CPU process time is calculated for both encryption and decryption process of different file sizes.

TABLE 1:Calculations and comparative study of different algorithms for encryption					
Input data in Kb and CPU process time for encryption in milliseconds					
Input size	*AES*	*DES*	*3DES*	*RC6*	*SMRK*
49	56	29	54	41	28
59	38	33	48	24	35
100	90	49	81	60	48
247	112	47	111	77	76
321	164	82	167	109	86
694	210	144	226	123	65
899	258	240	299	162	71
963	208	250	283	125	44
5345.28	1237	1296	1466	695	153
7310.336	1366	1695	1786	756	193
Average CPU process time	374	452	389	217	79.9
Throughput (Mb/sec)	4.174	3.45	4.01	7.19	14.8

TABLE 2:Calculations and comparative study of different algorithms for decryption					
Cipher data in Kb and CPU process time for decryption time in milliseconds					
Input size	*AES*	*DES*	*3DES*	*RC6*	*SMRK*
49	63	50	53	35	21
59	58	42	51	28	17
100	60	57	57	58	36
247	76	72	77	66	45
321	149	74	87	100	71
694	142	120	147	119	46
899	171	152	171	150	78
963	164	157	171	116	79
5345.28	655	783	853	684	143
7310.336	882	953	1101	745	165
Average CPU process time	242	246	275.6	210	70.1
Throughput (Mb/sec)	6.452	5.665	5.665	7.43	16.17

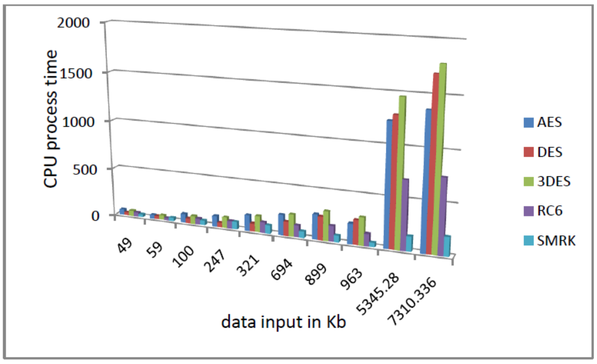


Figure 6: graphical representation of CPU process time Vs data size for decrypting cipher data.

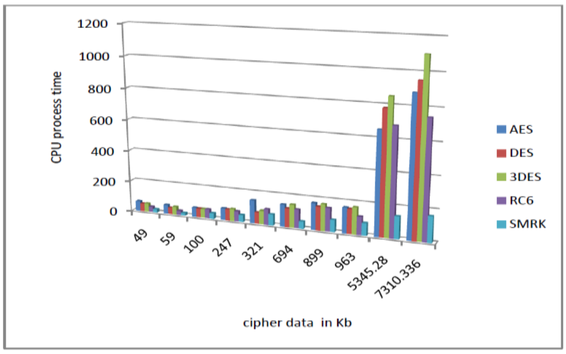


Figure 7: graphical representation of CPU process time Vs data size for encrypting input data.

VIII.CONCLUSION

This algorithm is used for secured communication between trusted parties. This is a cryptographic algorithm proposed by eliminating drawbacks of existing algorithms like symmetric and asymmetric algorithms. It is compatible on various types of data. In this 8 characters of plaintext and 160 bits of cipher text are processed at one time, the processing can be carried out simultaneously on the remaining data by using multiprocessing systems. This algorithm uses a 16-bit key for each 8 characters of the plaintext and 128 bits of the cipher text. In the proposed SMRK algorithm multiple symmetric keys are used. The encrypted keys are shared between the parties by including within the cipher text. This algorithm uses simple operations. This algorithm takes less processing time and will work faster for encryption and decryption with maximum throughput. It is concluded that the proposed algorithm SMRK will produce better performance than other common encrypted algorithms in terms of time taken for encryption and decryption process. The symmetric multiple random keys are generated for every 160 bits of data provides more secure for encrypting and decrypting the data. Our future work will include experiments/simulation on the above parameters on different file sizes of text, audio and video data and focus will be to improve encryption ratio and reduce process time and memory usage. The future study also includes increasing the key size and input data length to overcome brutal attacks.

REFRENCES

1. Manas Paul , Jyotsna Kumar Mandal ," A General Session Based Bit Level Block Encoding Technique Using Symmetric Key Cryptography to Enhance the Security of Network Based Transmission", International Journal of Computer Science, Engineering and Information Technology (IJCSEIT), Vol.2, No.3, pp-31-42,June 2012
2. Dayanand Sharma , Abhijit Kulshreshtha, Shrawan Ram, "Network Security Challenges and Cryptography in Network Security", J. Comp. & Math. Sci. Vol.2 (1), 25-30 (2011)
3.]Nitin K. Jharbade,Rajesh Shrivastava, "Network based Security model using Symmetric Key Cryptography (AES 256– Rijndael Algorithm) with Public Key Exchange Protocol (Diffie-Hellman Key Exchange Protocol)", IJCSNS International Journal of Computer Science and Network Security, VOL.12 No.8, pp 69-74, August 2012
4. P. Chakrabarti, B Bhuya, A.Chowdhuri, C.T.Bhunia, "A novel approach towards realizing optimum data transfer and Automatic Variable Key(AVK) in cryptography", IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.5,pp-241-250, May 2008
5. Suvajit Dutta, Tanumay Das, Sharad Jash, Debasish Patra, Dr.Pranam Paul," A Cryptography Algorithm Using the Operations of Genetic Algorithm &Pseudo Random Sequence Generating Functions", International Journal of Advances in Computer Science and Technology, Volume 3, No.5, pp 325-331, ISSN 2320 – 2602,May 2014.
6. Aruna Tomar, Sunita Malik, " A Random Key Based Visual Cryptography Approach for Information Security ", International Journal of Computer Science and Mobile Computing, Vol. 3, Issue. 6, pg.432 – 437, ISSN 2320–088X, June 2014.
7. Saranya K, Mohanapriya R, Udhayan J, "A Review on Symmetric Key Encryption Techniques in Cryptography", International Journal of Science, Engineering and Technology Research (IJSETR), Volume 3, Issue 3 pp 539-544, ISSN: 2278 – 7798,March 2014
8. Deepti A. Chaudhari, Prof. S. B. Javheri, "An Intrusion Detection System for MANET using Hybrid Cryptography", International Journal of Advance Researn in Computer Science and Management Science, Volume 3, Issue 1, pp 347-352, ISSN 2321 – 7782,January 2015.
9. Preeti Singh, Praveen Shende, "Symmetric Key Cryptography: Current Trends" , International Journal of Computer Science and Mobile Computing, ISSN 2320–088X,IJCSMC, Vol. 3, Issue. 12, December 2014, pg. 410 – 415.
10. Neha Garg , Partibha Yadav ,"Comparison of Asymmetric Algorithms in Cryptography", International Journal of Computer Science and Mobile Computing, ISSN 2320–088X,IJCSMC, Vol. 3, Issue. 4,April 2014, pg.1190-1196.
11. Ranjeet Masram, Vivek Shahare, Jibi Abraham, Rajni Moona , "Analysis And Comparison Of Symmetric Key Cryptographic Algorithms Based On Various File Features", International Journal of Network Security & Its Applications (IJNSA), Vol.6, No.4,pp 43-52, July 2014.
12. Monika Agrawal, PradeepMishra , "A Modified Approach for Symmetric Key Cryptography Based on Blowfish Algorithm",International Journal of Engineering and Advanced Technology (IJEAT),ISSN: 2249 – 8958, Volume-1, Issue-6, August 2012
13. S. William, "Cryptography and Network Security: Principles and Practice", 2nd edition, Prentice-Hall, Inc.,
14. Mohammad Soltani, Young,"A New Secure Cryptography Algorithm Based on Symmetric Key Encryption" , Journal of Basic and Applied Scientific Research, ISSN 2090-4304 www.textroad.com.
15. K.Gary,"An Overview of Cryptography", an article available at www.garykessler.net/library/crypto.html04.
16. Narender Tyagi, Anita Ganpati, " Comparative Analysis of Symmetric Key Encryption Algorithms", International Journal of Advanced Research in Computer Science and Software Engineering(IJARCSSE), Volume 4, Issue 8, pp 348-354, August 2014.
17. Mansoor Ebrahim, Shujaat Khan, Umer Bin Khalid, " Symmetric Algorithm Survey: A Comparative Analysis", International Journal of Computer Applications (0975 – 8887) Volume 61, No.20, pp 12-19,January 2013.