IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 3 Issue 2, February 2016.
www.ijiset.com
ISSN 2348 – 7968

An Automatic Generated Symmetric key Based Technique for Encryption and Decryption of Text Data

Roshan M. Pandav[1], Vijay Kumar Verma[2]
ME Student[1], Asst. Professor[2], Lord Krishna College of Technology, Indore, M.P., India[1,2]
roshan.pandav67@gmail.com[1],vijayvermaonline@gmail.com[2]

Abstract:-Informationsecurity is one of the most challenging aspects ofcommunication.In symmetric key cryptographic algorithms singlekey is used for both encryption and decryption process. There are several algorithm have developed for symmetric encryptionfor example DES, AES, Blowfish, RC5, IDEA are some of them. Every algorithm usesdifferent block size, key size and processing method. Thesealgorithms only accept English alphabets, numerical valuesand special symbols as plaintext. The cipher text will be adocument which is in the form of alphabets or specialcharacters or numbers or combination of all. In this paper we proposed an efficient symmetric key cryptographic algorithm which automatically generate key based on the length of the text.

Keywords:-Symmetric, Asymmetric, Cryptography, Automatic, encryption, decryption.

1. INTRODUCTION

Symmetric key encryption scheme has five components 1.Plaintext, 2.Encryption algorithm, 3. Secret key, 4. Cipher text,5. Decryption algorithm.Cryptographic attacks are mainly classifiedas two types, namely passive attack and active attack. Goalof Passive attack is just read the information it does notchange the content of the message, for example of messagecontent it only read the content of message withoutpermission. Where as in active attack, not only read theinformation and also modifying the content of the message.For example replay attack accesses the message that send tothe receiver and it sent its own message content to thereceiver as like sender.

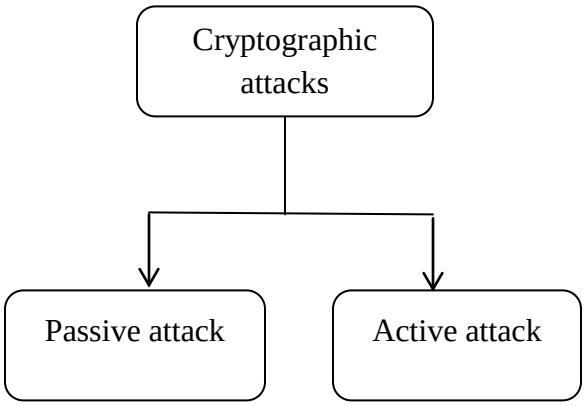

Figure 1 Types of cryptographic attacks

ISSN 2348 – 7968

II.CLASSIFICATIONS OF CRYPTOGRAPHY

A cryptography system is mainly classified into threetypes 1. Symmetric key cryptography, 2. Asymmetric keycryptography 3. Hash functions. A symmetric keycryptography uses same secret key by sender and receiverfor encryption and decryption respectively. Asymmetric orpublic key cryptography uses public key by sender forencryption which is known to all and private key whichknown by the receiver for decryption for example.The hash function usesmathematical transformation to irreversibly encryptinformation. Fig 2illustrates types of cryptographic techniques.

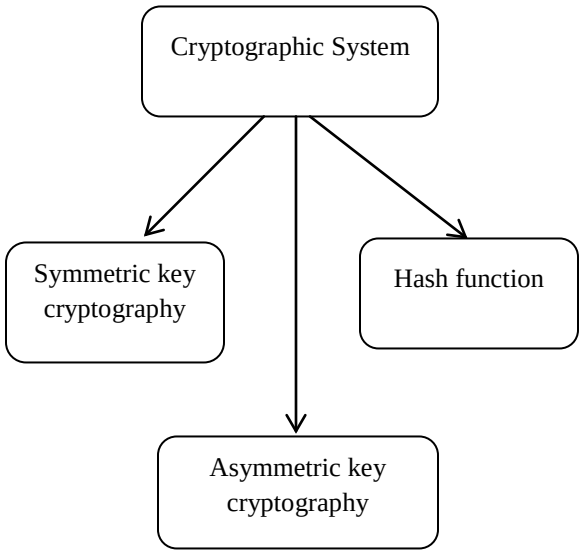

Figure 2 types of cryptographic techniques

III. LITERARTURE REVIEW

In 2011 K.Govinda and Dr.E.Sathiyamoorth proposed “Multilevel Cryptography Technique Using Graceful Codes. Theyproposed multilevel cryptography technique for data encryption-decryption using graceful codes[1].

In 2012 Monika Agrawaland Pradeep Mishra proposed “A Comparative Survey on Symmetric KeyEncryption Techniques”. They present a detailed study of most ofthe symmetric encryption techniques with their advantages and limitations over each other.They give a detailed study of the popular symmetric key encryption algorithms such as DES, TRIPLEDES, AES, and Blowfish. Symmetric Key algorithms run faster than Asymmetric Key algorithms such as RSAetc. and the memory requirement of Symmetric algorithms is lesser than Asymmetric encryption algorithms [2].

In 2013 Krishna Kumar PandeyandVikasRangari Proposed “An Enhanced Symmetric Key Cryptography Algorithm to Improve Data Security “.The proposed work uses enhanced symmetric key encryption algorithm, in which same structure of encryption and decryption procedure algorithm is used. In conventional encryption methods the key for encryption and decryption is same and remain secret. The algorithm uses key generation method by random number in algorithm for increasing efficiency of algorithm. The algorithm use key size of 512 bits for

ISSN 2348 – 7968

providing better security and it also provide the concept of internal key generation at receiver end on the basis of 512 bits key which will entered by the sender[3].

In 2013 Sruthi B. Asok, P. Karthigaikumar, Sandhya R and Naveen Jarold K, Siva Mangai "IRIS Based Cryptography". Theyimplemented Iris based cryptography in proposed work. Secret key is generated from iris image. Randomness checkis conducted for the key sequence. In AES information isencrypted and decrypted using the key[4]

In 2013 Deepak Nagde, Raviraj Patel, Dharmendra Keld proposed"New Approach for Data Encryption using Two WayCrossover". They proposed a new approach for datasecurity. They use the concept of genetic algorithms incryptography along with the randomness properties of MASmethod. This total way of transferring secret information ishighly safe and reliable. So without the knowledge of thepseudorandom sequence no. one will be able to extract themassage.In the feature work we plan to design sophisticated softwarebased on this technique which will target to use in highlysecure multimedia data transmission application[5].

In 2014 Mitali1, Vijay Kumar and Arvind Sharma proposed "A Survey on Various Cryptography Techniques".The survey is done on some of the more popularand interesting cryptography algorithms currently in use andtheir advantages and disadvantages are also discussed. Theypaper provides a fair performance comparison between thevarious cryptography algorithms on different settings of datapackets. They presents the performanceevaluation of selected symmetric algorithms. The selectedalgorithms are AES, 3DES, Blowfish and DES. Thepresented simulation results show the numerous points.Firstly it was concluded that Blowfish has betterperformance than other algorithms followed by AES.3DES has least efficient of all the studied algorithms[6].

In 2014 Ashwini R. Tonde, Akshay P. Dhande proposed "Review Paper on FPGA Based Implementation of Advanced Encryption Standard (AES) Algorithm". They proposed FPGA-based implementation of the Advanced Encryption Standard(AES) algorithm. This implementation is compared with other works to show the efficiency. The design uses an iterativelooping approach with block and key size of 128 bits, lookup table implementation of S-box [7].

ISSN 2348 – 7968

IV. PROPOSED METHOD

Encryption Method

Consider a simple text NETWORKS

Now the length of original string NETWORKS is counted, which is 8. Now the length of original string NETWORKS is counted, which is 8.

Since 8 is even number, the Key is generated using (n/2) i.e. 8/2=4 or else the key generated should be (n+1)/2).

Now the key i.e. letter at position 4 is W and key chosen will be word‟s corresponding numeric value i.e. k=23 (consider A=1, B=2… Z=26)

Original text	NV	D=(NV+K)/26 replace with ASCII value
N	14	75
E	5	81
T	20	76
W	23	72
O	15	66
R	18	84
K	11	79
S	19	80

Table 1 original text and its ASCII text after apply round 1 of proposed method

Now apply round 2

Binary Value	Logical NOT	Convert into decimal and replace with ASCII Character
01001011	10110100	-|
01010001	10101110	«
01001100	10110011	|
01001000	10110111	Π
01000010	10111101	ᵛ
01010100	10101011	½
01001111	10110000	¿
01010000	10101111	»

Table 2cipher text after round 2 proposed methods

Finally we got so finally the chipper text is

-|«|Πᵛ½¿»

Decryption Process

Apply the revers procedure of encryption technique

Decimal Equivalent of encrypted data	Binary Value with logical NOT	ASCII Value
180	10110100	11
174	10101110	2
179	10110011	17
183	10110111	20
189	10111101	12
171	10101011	15
168	10110000	8
175	10101111	16

Table 3reverses of round 2 of proposed method

Text Obtained – KQLHBTOP

Apply Reverse Transposition as Text Obtained: - KBQTLOHP

Numeric Value	Numeric value and Corresponding Alphabet
11	N
2	E
17	T
20	W
12	O
15	R
8	K
16	S

Table 4original text after applying revers of round 1 proposed

ISSN 2348 – 7968

V. PROPOSED ALGORITHM

Step 1: Count the length of String

Step 2: If length is evenCalculate key (K) for using n/2, Calculate a numeric Value by Considering A=1, B=2 …Z=26and

elseCalculate key (K) for using n/2, Calculate a numeric Value by Considering A=1, B=2 …Z=26

Step 3: calculate Key (K) (n+1)/2, Calculate a numeric Value by Considering A=1, B=2 …Z=26.

Step 4: Apply using formula C= (NV+K) / 26; where C is cipher text, NV plain text numeric value and key K and replace with ASCII value.

Step 5: Convert into binary format and apply logical NOT.

Step6: Generator Decimal number and replace with corresponding character.

Step7: Final got chipper text.

VI. GRAPHS AND ANALYSIS

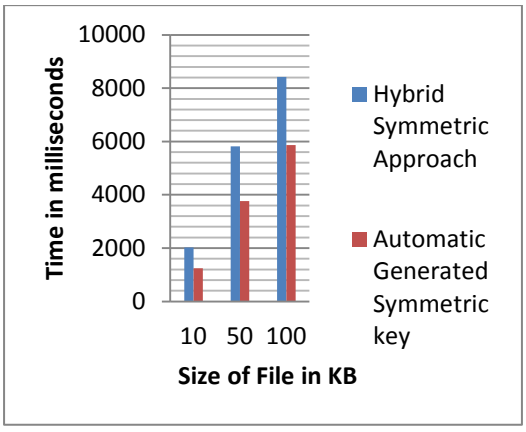

Figure 3 Analysis graph

We have implemented the proposed algorithm and Hybrid symmetric approach using VB Dot net 2010 .We use simple text file to encrypt and decrypt the data . From the graph it clear that the proposed method perform well as compared to hybrid symmetric approach.

VII. CONCLUSION

We proposed an efficient anautomatic generated symmetric key based technique for encryption and decryption of Text Data. The main objective is to convert the text into a crypt from so analysis becomes tedious and confusing. The algorithm providesautomated generated key, so that the key cannot be identifiedeasily. In future we can apply some numerical calculation and can also be applied to the image database. The algorithmcan also be applied to the numeric data in future.

VIII. REFERENCE

[1] Prof K.Govinda, Dr.E.Sathiyamoorth proposed " Multilevel Cryptography Technique Using Graceful Codes" Volume 2, No. 7, July 2011 Journal of Global Research in Computer Science

[2] Pratap Chandra Mandal Evaluation of performance of the Symmetric Key Algorithms: DES, 3DES, AES and Blowfish Volume 3, No. 8, August 2012 Journal of Global Research in Computer Science

ISSN 2348 – 7968

[3]Monika AgrawalPradeep Mishra"A Comparative Survey on Symmetric KeyEncryption Techniques"International Journal on Computer Science and Engineering (IJCSE)ISSN:ISSN : 0975-3397 Vol. 4 No. 05 May 2012

[4] Deepak Nagde, Raviraj Patel, Dharmendra Kelde "New Approach for Data Encryption using Two WayCrossover"International Journal of Computer Science and Information Technologies, Vol. 4 (1) , 2013, 58 – 60

[5] Krishna Kumar PandeyVikasRangariAn Enhanced Symmetric Key Cryptography Algorithm to Improve Data Security International Journal of Computer Applications (0975 – 8887) Volume 74– No. 20, July 2013

[6]Sruthi B. Asok, P. Karthigaikumar, Sandhya R, "Naveen Jarold K4, Siva MangaiIRIS Based Cryptography" International Journal of Advanced Research in Computer and Communication EngineeringVol. 2, Issue 2, February 2013

[7]Mitalil, Vijay Kumar and Arvind SharmaA Survey on Various Cryptography TechniquesInternational Journal of Emerging Trends & Technology in Computer Science (IJETTCS)Web Site: www.ijettcs.org Email: editor@ijettcs.orgVolume 3, Issue 4, July-August 2014 ISSN 2278-6856

[8]Surabhi Shah Megha Singh Neha Joshi A New Encryption Algorithm to Increase Performance & Security through Block Cipher Technique Volume 4, Issue 9, September 2014 ISSN: 2277 128X International Journal of Advanced Research in Computer Science and Software Engineering

[9] Udepal Singh, Upasna Garg"An ASCII value based text data encryption System" . International Journal of Scientific and Research Publications, Volume 3, Issue 11, November 2013 1 ISSN 2250-3153.

[10]Soubhik Kumar Dey, Mr. Tarak Nandy, "A Symmetric Key Cryptographic AlgorithmIPASJ International Journal of Computer Science (IIJCS)Volume 2, Issue 1, January 2014 ISSN 2321-5992