INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS…..

INTRODUCTION TO A NEW ENCRYPTION APPROACH HAS+ AND COMPARISON OF TIME COMPLEXITY OF DIFFERENT ENCRYPTION ALGORITHMS

[1]Urvashi, [2]Ms. Pooja

M.Tech Scholar[1], Asst. Prof.[2]
R.N. Engineering College
Maharishi Dayanand University, Rohtak (Haryana), India
[1]urvashisharma701@gmail.com

ABSTRACT: *Symmetric key encryption (the same key used for encryption and decryption) is the oldest branch in the field of cryptography, and is still one of the most important ones today. In this research, we are creating new encryption technique in which we do not only work on the key, but also on data (plain text) too, so, that we can achieve highly secure information of the cipher text. HAS+ Encryption Technique with Key Rotation Based on ASCII Value" is using two algorithms first work with key and data using ASCII value and second for Key generation and will compare its complexity with existing algorithms.*

KEYWORDS: *Time Complexity, Encryption Algorithm, HAS+, Symmetric ASCII based Encryption.*

1. INTRODUCTION

Cryptography is the combination of two Greek words Crypto which means "Secret" and graphy which mean "writing". So, cryptography is a way to change the message/information (plain text) from one form to another secret form which is different from the original with the help of a secret key and this process is called Encryption [4, 5]. The changed value of a secret message is called cipher text and to get the original message from a cipher is called decryption. The detailed 1 operation of a cipher text is monitored by both the algorithm used and in each instance by a key. Modern cryptography divided into several disciplines of mathematics, electrical engineering and computer science.

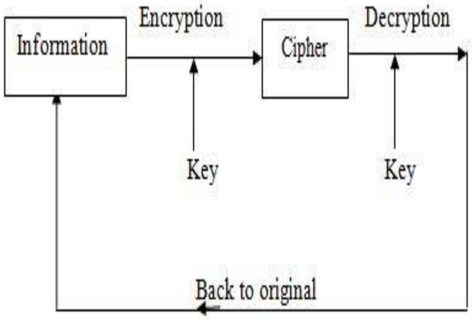

Figure 1.1: Encryption\Decryption process

According to key, cryptographic algorithms can be divided into two types

1.1 Secret key cryptography:

The key used for encryption and decryption process is same. It is likewise termed as symmetric key cryptography such as AES and DES [8].

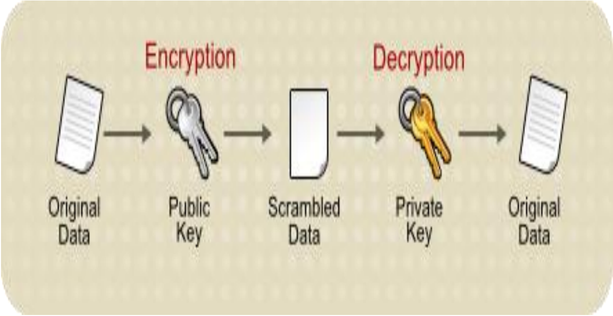

Figure 1.2: Secret key Cryptography [3]

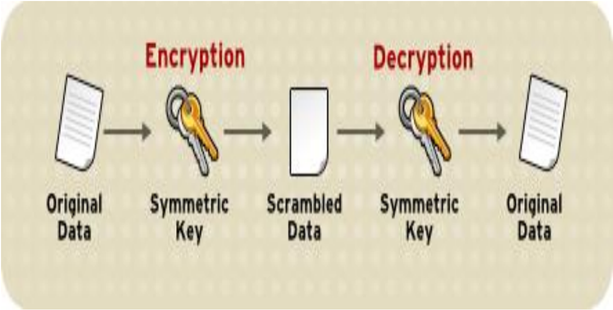

Figure 1.3: Public key Cryptography [3]

1.2 Public key cryptography:

Two different keys are used. One for converting data in cipher and another key for deciphering to data. It is also known as asymmetric key cryptography such as RSA [11].

There are many cryptography algorithms have been already developed such as XOR, RSA, AES, DES, TDES and BLOWFISH etc. Every one of these has its own advantages and disadvantages.

2. RESEARCH WORK

Existing algorithms change their key after each round using some pre-defined function for example like S-Box, Shift Rows, Permutation, etc. But in this technique, the key rotates is be done after when each character or element of key is used and generate new key by using ASCII value of the previous key. The key is rotated in a circular way to the left side, each character of the key is shifted left side and the first character goes to the end of the key. This process is continued until the last character of the file is to be encrypted.

This Proposed solution is on ASCII value of key and that is also uses in this paper “Simple Encryption/Decryption Application” [16]. In this new pattern is design to use the ASCII key value for unique key generation technique, in which key uses its own data for encryption.

2.1 HAS+ ENCRYPTION

“HAS+ Encryption Technique with Key Rotation Based on ASCII Value” using two algorithms first work with key and data using ASCII value and second for Key generation.

2.1.1 Algorithm design

Step 1: Read original file as ‘P’
Step 2: Read key as ‘K’
Step 3: Find the ASCII value of K.
Step 4: Convert the ASCII value into its equivalent binary.
Step 5: Count Number of 1’s occurred in the binary value of key as ‘count’.
Step 6: while EOF

- Perform XOR operation on element of P with the element of K as the resultant ‘C’ produced.
- For i=1 to count
    - o Add 1 bit to C
- Add new value of C to cipher.txt
- IF all elements of key are used
    - o K1[i]=KEY_GENERATION (K[i], count).
    - o Call Steps 3, 4 and 5 for count new value.
- Update ‘K’ by K1.

Step 6: Repeat step 3 until EOF.
Step 7: Stop

2.1.2 Algorithm for Key_Generation (key[i], count)

Step 1: Left Circular Rotation on Key.
Step 2: For i=0 to key length
If ((key[i] * count)> 4098)

- ▪ Key[i]= key[i] XOR count

Else

- ▪ Key[i]= key[i]+ count

Step 3: Return Key.

Flow chart for key generation:

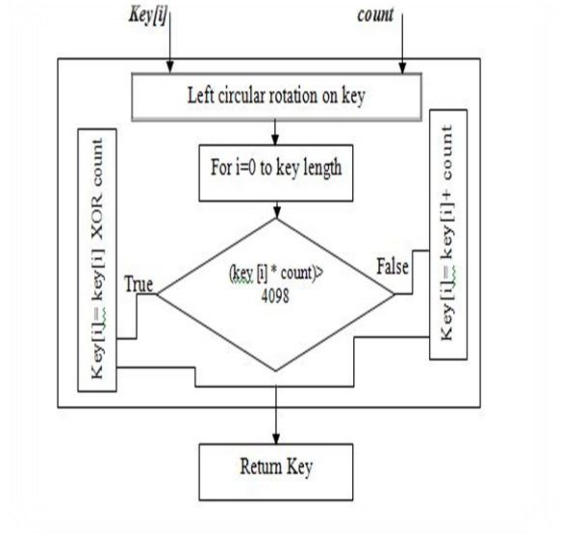

Figure 2.1: Flow chart of Key Generation

Flow chart for HAS+ Encryption Algorithm:

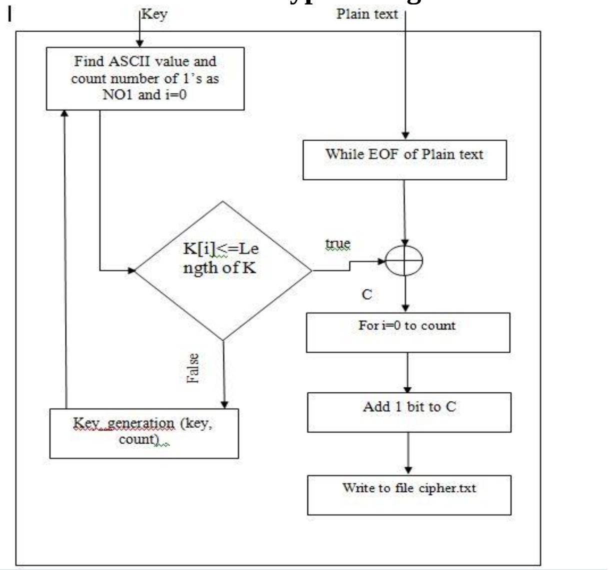

Figure 2.2: Flow chart of HAS+ Algorithm

2.2 HAS+ ADVANTAGES

1.A new Stream cipher technique is using a variable length key.
2.Key is randomly generating using ASCII value of base key.
3.Easy to implement.
4.Faster execution on both software and hardware.
5.Fiestel Network support

2.3 Time Complexity Comparison Result

If a file of 10 kb is encrypted by using four algorithms, two times separately then we can analyse the results given below, in that the time (in millisecond) taken to encrypt a 10 KB file is given below.

HAS+ , DES, TDES, Blowfish: Comparison based on Encryption time. For file size 10 KB. The result may varies on different condition like- Architecture of Operating System, processing speed, Random Access Memory size, Language used (c, c++, Java, etc), way of implementation of algorithm and others feathers.

Time (ms)		*HAS+*	*DES*	*TDES*	*AES*
1st Time	*Encryption*	*65*	*61*	*109*	*78*
	Decryption	*59*	*58*	*97*	*62*
2nd Time	*Encryption*	*73*	*71*	*90*	*74*
	Decryption	*64*	*62*	*91*	*63*

Table No. 1 Comparison based on time for Encryption/Decryption

3. CONCLUSIONS

"*HAS+ Encryption Technique with Key Rotation Based on ASCII Value*" algorithm provides more security than existing algorithm because all existing stream cipher techniques use the same predefine sequence for the key generation but in this algorithm we are rotating key and also generate new key with using the ASCII value of the initial key for providing better security. Stream cipher techniques are replaced by the block cipher because of the simple key mechanism but HAS+ techniques has a complex key mechanism. Sometimes it is also secured than block cipher algorithm like DES. DES is not secure because of its key length. But this algorithm support variable length of the key. In HAS+ algorithm no limit for the size of the key but default key value is referred to the size of 128 bits.

4. FUTURE SCOPE

The future work on this algorithm technique is to increase the complexity of key mechanism to secure from different attacks. Enhance the key length for better result. Also design it for Block Cipher.

REFERENCES

[1] Niraj Kumar, Pankaj Gupta, Monika Sahu and Dr. M A Rizvi," Boolean algebra based Effective and Efficient Asymmetric Key Cryptography Algorithm: BAC Algorithm", 978-1-4673-5090-7/13/$31.00 ©2013 IEEE.

[2] Rajani Devi.T, "Importance of Cryptography in Network Security", 978-0-7695-4958-3/13 $26.00 © 2013 IEEE DOI 10.1109/CSNT.2013.102.

[3] Introduction to cryptography, https://access.redhat.com/site/documentation/enUS/Red_Hat_Certificate_System_Common_Criteria_Certification/8.1/html/Deploy_and_Install_Guide/Introduction_to_Public_Key_Cryptography.html#Introduction_to_Public_Key_Cryptography-Encryption_and_Decryption, last accessed on 27/05/2015

[4] History of cryptography, available at, http://en.wikipedia.org/wiki/History_of_cryptography, last accessed on 6-6-2015.

[5] Anjali Patil, Rajeshwari Goudar, "A Comparative Survey of Symmetric Encryption Techniques for Wireless Devices", International Journal Of Scientific & Technology Research Volume 2, Issue 8, August 2013.

[6] Block Cipher, available at, "http://homepage.usask.ca /~dtr467/400/", last accessed on 06/06/2015

[7] Cigenere cipher, http://en.wikipedia.org/wiki/Vigen %C3%A8re_cipher, last accessed on 29-05-2015.

[8] Vikendra Singh and Sanjay Kumar Dubey, "Analysing the space complexity or various Encryption Algorithms", International Journal of Computer Engineering and Technology (IJCET), Volume 4, January- February 2013.

[9] Shabnam Samina, Ratnakirti Roy and Suvamoy Changder, "Secure Key Based Image Realization Steganography", Second Internationla Conference on Image Information Processing (ICIIP), IEEE, 2013.

[10] Scytale, http://en.wikipedia.org/wiki/Scytale_(Dune), last accessed on 25-05-2014

[11] Christof Paar, Jan Pelzl, "Introduction to Public-Key Cryptography", Chapter 6 of "Understanding Cryptography, A Textbook for Students and Practitioners". (companion web site contains online cryptography course that covers public-key cryptography), Springer, 2009.

[12] William Stallings, "Cryptography and Network Security" Pearson 2011 page no 59 to 79.

[13] Xinqiang Li, Lili Yu, "The Application of Hybrid Encryption Algorithm in

[14] Software Security", 978-1-4799-2860-6/13/$31.00 ©2013 IEEE

[15] Delfs, Hans & Knebl, Helmut, "Symmetric-key encryption". Introduction to cryptography: principles and applications. Springer. ISBN 9783540492436. Page no. 11 to 29.

[16] Raymond G. Kammer, "DATA ENCRYPTION STANDARD (DES)", FIPS PUB46-3 1999October 25.

[17] E. Anupriya, Sachin Soni, Amit Agnihotri and Sourabh Babelay, "Encryption using XOR based Extended Key for Information Security – A Novel Approach", International Journal on Computer Science and Engineering (IJCSE) Vol. 3 No. 1 Jan 2011.