A new Symmetric Approach to Cryptography

Aamir Sohail[1]

[1]Department of Information Technology. Bahauddin ZakariyaUniversity,Multan,Pakistan

Abstract: Today data transmission is very important through different network. Need of Network security comes to secure data transformation from one network to another network. As the complexity of the systems and the networks are increasing, Weakness is also expanding and the task of securing the networks is becoming more convoluted. Duty of Securing is done by Cryptography techniques. A colossal amount of data is exchanged over public networks like the internet due to immense accommodation, and this includes personal details and confidential information. It is important to prevent the data from falling into the wrong hands. So due to this factor we use cryptography. Encryption and decryption are the basic terms that used in cryptography. There are Few Algorithms that working for encryption and decryption is AES, DES, 3DES and BLOWFISH. The main contribution of the paper is to provide an algorithm that is useful for data transformation in cognitive radio network. In this paper we draw a new symmetric key technique that is for cryptography use which helped to make the data saved from others.

Keywords: Network, Network Security, Cognitive Radio Network Cryptography, Encryption, Decryption, DES, 3DES, AES, BLOWFISH, Symmetric key

I. Introduction

Technology now days are common in our surroundings. With the passage of time the transformation of data increasing day by day and maintain an old data in a system increasing gradually. Security is important factor of transmission and saving the data. One important and essential aspect of communications is cryptography.Cryptography is the investigation of concealing data by changing over the touchy data into an ambiguous content utilizing an appropriate encryption system so it can't be comprehended by any unintended individual, and afterward changing over it back to its unique frame for the proposed beneficiary utilizing some decoding method [1].

The implementation of cryptography have been placed being used since antiquated Roman and Egyptian realms. "Caesar figure" imagined by Julius Caesar is one such illustration. Presently, the specialty of cryptography has been digitalized. PC calculations have modernized the specialty of cryptography. Cryptography has turned into a basic apparatus in shielding the delicate data from unapproved get to and to give data security. Cryptography has discovered its routines in protection ranges as well as in business field too. Organizations and firms utilize cryptography systems to shield their information and data from their enemies. Cryptography is likewise used to secure individual information and has broad application in our everyday lives [2].

Now days there are four basic objectives of cryptography are [3] Confidentiality, Integrity, Non-Repudiation,Authentication. Sometimes cryptography is referred as encryption. The Basic part of encryption is makes an irregular scrambled key and concealing the first information by making key and encode this with key and spare from gatecrasher. Encryption part is useful for securing the electronic transmission over unprotected systems.

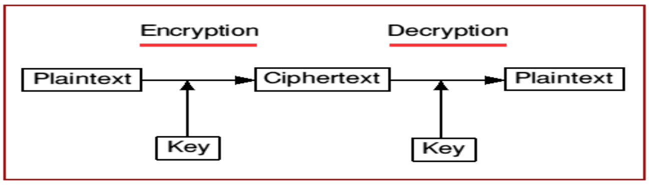


Figure1: Model for cryptography

Figure1: describing the encryption, decryption process. By performing some specific algorithm between 'plaintext and key' the cipher text is obtained, and this cipher text is transferred to the receiver. To get plain text again on the receiving end, perform some specific operation between cipher text and key. This thing is known as decryption process.

The rest of the paper is outlined in furthered different Section. Section II briefly describes the Cryptography types and Section III describes some popular algorithm that are in working position now days are explained. Section IV outlined with some issues found in old algorithms. Our purposed new technique is given Section V. Section VI has implantation and Section VII provides the performance evaluation of proposed algorithm. The conclusion is included in Section VIII.

II. Cryptography types

Basically Encryption has three types [13]

- Symmetric encryption
- Asymmetric Encryption
- Hashing

Symmetric Encryption

A sort of encryption that has just single key is known as symmetric encryption [11]. It is one of the most punctual utilized procedures of cryptography. There are different points of interest of this approach. Execution is decently high. This encryption sort is more secure and reasonable.

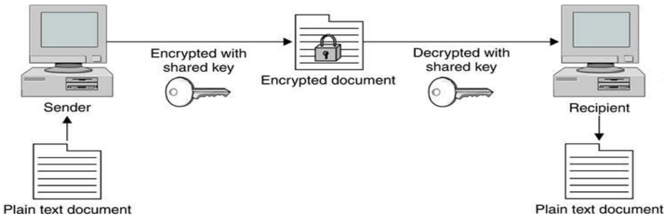


Figure2: Symmetric Encryption

Asymmetric Encryption

Asymmetric encryption [12] utilizes two distinctive keys for encryption and decoding. The private key can just decode the encoded message. No key other than private key can be utilized for unscrambling.

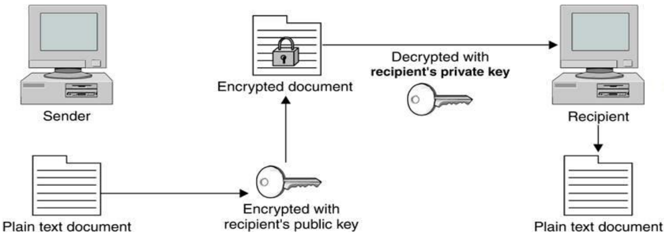

Sender
Encrypted document
Decrypted with recipient's private key
Recipient
Plain text document
Encrypted with recipient's public key
Plain text document

Figure3: Asymmetric Encryption

Hashing

Hash function is one way encryption method and no key is required for encryption and decryption.

III. Related Work and Popular Algorithms

Almost 4000 years ago Cryptography [5] [4] Concepts came in Egypt. Around in 2000 B.C Hieroglyphics were user for the tombs decoration of deceased rulers and kings. These symbols describe the story of Kings and rulers lifestyle. These Symbols was cryptic in special meaning to describe the words. As time passed these indications were become more common and Text hiding importance through these indications decreased. With the passage of time deciphering with symbols becomes more complicated and People intention decreased with this approach.

The Arabs were the first that works in this field. QALQASHANDI name Arabic author was the first man that introduces the technique for solving the ciphers [14]. His strategy clarifies that record all figure content letters and subsequent to recording tally the recurrence of every images. By utilizing the normal recurrence of each letter of dialect the plain content can be composed out by utilizing this strategy. After Arabic author a Frenchman named ANTOINE ROSSIGNOL worked on this. In 1628 he helped his army force to defeat the Huguenots by decrypting the captured message. His style for solving ciphers was depends on methods of two lists.

Decius Wadsworth was the man that developed a cipher system in 1817. His cipher system was very helpful and used at the end of World War II. His cipher system was consists of two disk. The outer disk and the inner disk, the outer disk contains the 26 alphabet and 2 to 4 numbers and the inner disk had only 26 letter of alphabet. The disks were adapted to each other at the ratio of 26:33. To encode a data, the interior plate is turned until the point that the coveted letter is at the best position with the amount/number of turns required for this result as the figures. Because of adapting discs together a ciphers for a character did not repeat till the all thirty three characters used for plaintext [6].

Tomographic cipher was developed in 1859 by PLINY EARLE CHASE. His Method indicate that two digit number allocated to every single character of text by method for table and these numbers were written at the end first numbers formed a row on top of the second numbers. A row that is on bottom side should be multiplied by 9 and correspondingly pairs are stored into table to make a cipher text.

There are different popular encryptions methods exist in the cryptography which are

AES[18]stand for Advanced Encryption Standard. Advance Encryption Standard is symmetric 128 bit block length and 128,192 & 256 bits key length data encryption techniques to encrypt sensitive data which is used by U.S governments to protect important information. AES is included in the ISO/IEC 18033-3 standard. In this assault calculation aggressor utilize vocabulary of words in English and discover the words which is utilized as key[7].

DES [19] stands for data encryption standard. It is an Encryption algorithm that is introduced in 1997 [8]. The DES takes maximum of 2^56 attempts to find the correct key. One of the main draw back in working with the DES is data vomiting that is lack of security for the data which is contained.

3DES[20]stand for Triple data encryption standardTriple DES is expansion of DES which includes rehashing the essential DES calculation three times utilizing either a few special keys for a size of 112 or 168 bits [8].

IV. Issues Found in Algorithms

There are so many issues found during study of all algorithms.

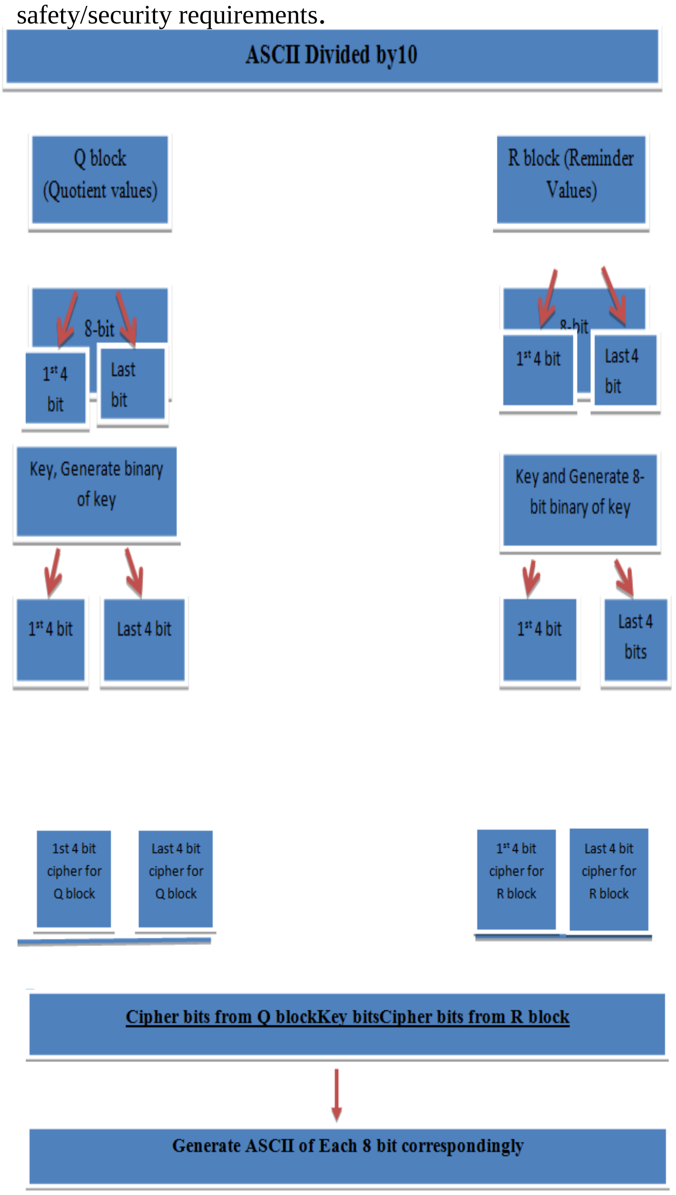
- Complex structure, more time executing, predictable due to short key as like DES algorithm and key length.
- The more perplexing structure of calculation builds the season of execution. So the structure of calculation ought to be easy to make Algorithim speedier.
- The more extended the length of key gives higher security as contrast with shorter length of key and furthermore increment the speed of execution of scheming [15].

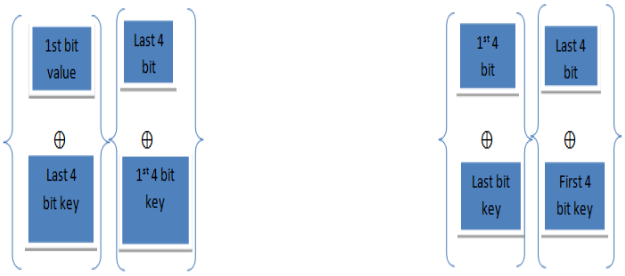
- The general execution of any calculation relies on choice of numerical as well as sensible operations connected on plain content, key and figure content.

In network security there are two types of attacks. The first one is Active attack. Active attack is tried to modify the systems resources and it effects operations performed in a system. Active attacks are categorized as Replay, Modification of message, Forgery. The second one is passive attack. Passive attack is a try which monitors the data transmission without affecting the operation performed in a system. [9] The passive attack is categorized as Eavesdropping, Collecting private data.

V. Proposed Algorithm

Security of data relies on secure encryption. For every Successful system it is important that it satisfy the data safety/security requirements.


ASCII Divided by10
Q block (Quotient values)
R block (Reminder Values)
8-bit
1st 4 bit
Last bit
8-bit
1st 4 bit
Last 4 bit
Key, Generate binary of key
Key and Generate 8-bit binary of key
1st 4 bit
Last 4 bit
1st 4 bit
Last 4 bits
1st 4 bit cipher for Q block
Last 4 bit cipher for Q block
1st 4 bit cipher for R block
Last 4 bit cipher for R block
Cipher bits from Q blockKey bitsCipher bits from R block
Generate ASCII of Each 8 bit correspondingly



VI. Implementation of Encryption

1) Read the user file and Generate Correspondingly ASCII value of each character in file. Let's Suppose User file has word **Hi**, ASCII of **H** is **072** and ASCII of **i**is **105**.

2) Divide every character ASCII value by 10. Calculate Quotient, Reminder and Quotient values stored in Q block, Reminder values stored in R block correspondingly.

$$Q[7,10]R[2,5]$$

3) Calculate 8-bit binary value for each value that is in R block and Q block correspondingly.

$$Q[00000111, 00001010]$$
$$R[00000010,\ \ 00000101]$$

4) Take key from user. Key should be set of one or more special character. Calculate ASCII value of sequence correspondingly and convert it into 8-bit binary. Let's suppose user entered $$. ASCII is <u>**3636**</u> and binary is <u>**00100100 00100100**</u>.

5) Every 8 bit binary key is divided into 4 4 bits also Every 8 bit binary value in Q block and R block is divided in 4 4 bits correspondingly.

$$Key[key1key2key3key4]$$
$$Key[0010010000100100]$$

$$Q[Q1Q2Q3Q4]R[R1R2R3R4]$$
$$Q[0000011100001010]$$
$$R[0000001100000101]$$

6) Take XORs of Q1 with Key2, Q2 with key1, and Q3 with key4 and Q4 with key3 also take XORs of R1 with key2 and R2 with key1, R3 with key4 and R4 with key3.

$$Q[Q1\oplus key2Q2\oplus key1Q3\oplus key4Q4\oplus key3]$$
$$R[R1\oplus key2R2\oplus key1R3\oplus key4R4\oplus key3]$$

7) Obtained cipher blocks as *Q'* and *R'* from pervious step. The result will be in this form.

$$Q'[Q1'Q2'Q3'Q4']R'[R1'R2'R3'R4']$$
$$Q'[0100010101001000]R'[0100000001000111]$$

8) Combine *Q'* cipher text block and *R'* cipher text block by using sequence key (in bit form) in between Q' and R'

$$Q'\$\$R'$$

010001010100100000100100001001000100000001000111

9) convert each 8-bit into ASCII and Save ASCII value correspondingly. Finally get and save cipher text. Obtained result is **EH$$@G**

Implementation of Decryption

1) Read Cipher text, User entered Sequence key. Convert cipher text and key into binary value.
2) Identify Sequence key and remove. Two blocks obtained that is *Q'* and *R'*
3) Divide 8- bits of each block(*Q'* and *R'*) in 4 4 bits and make a 4 4 bits of key

$$Q^{'}[0100010101001000]R^{'}[0100000001000111]$$

$$Q^{'}[Q1^{'}Q2^{'}Q3^{'}Q4^{'}]R^{'}[R1^{'}R2^{'}R3^{'}R4^{'}]$$
$$Key[key1key2key3key4]$$
$$Key[0010010000100100]$$

4) Take XORs as like

$$Q'[Q1^{'}\oplus key2Q2^{'}\oplus key1Q3^{'}\oplus key4Q4^{'}\oplus key3]$$
$$R'[R1'\oplus key2R2'\oplus key1R3'\oplus key4R4'\oplus key3]$$

5) Combine the 4 bits to 8 bits and Result obtained in the form of Q block and R block

$$Q[0000011100001010]$$
$$R[0000001000000101]$$

6) Calculate ASCII value/symbols for each 8 bit in blocks. Obtained result is

Block size (Byte)	Encryption Time (sec)	Decryption Time
8	38 sec	36 sec
16	48 sec	47 sec
32	53 sec	54 sec

$$Q[7,10]R[2,5]$$

7) Multiply each value in Q block by 10 and in result add value from R block correspondingly. Obtained result be in this form

$$7 \times 10 = 70,10 \times 10 = 100$$
$$70+2,100+5$$
$$72,105$$

8) Take value correspondingly from ASCII table. Obtained result is **H and i**

Cipher text was: **EH$$@G** Original text is **Hi**

VII. Experimental Turnout of Algorithm

Turnout is Considered into two process. One is "Encryption" and the second one is "Decryption". Results are obtained using WINDOWS operating system and software used for implementation is Visual Studio 2010.

There are different bytes that indicate the execution time period of my algorithm. The experimental result is dived into three sections. Every section has system of different specification.

i. Model Name: HP G3450

Generation: i5 (6th Generation) RAM: 8GB

Block Size (Byte)	Encryption Time (sec)	DecryptionTime (sec)
8	20 sec	18 sec
16	38 sec	36 sec
24	45 sec	43 sec

Table1: Results Obtained Using 8GB RAM

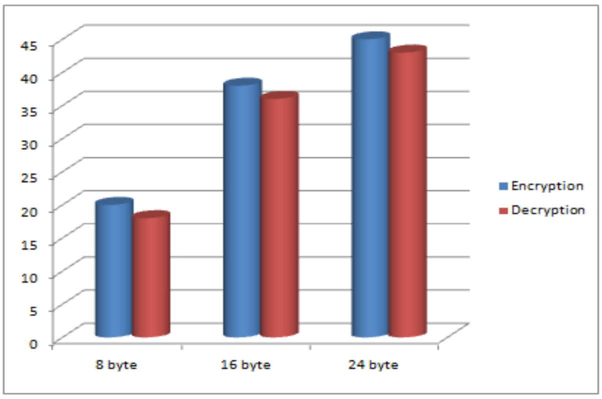


Figure5: Results Obtained Using 8GB RAM

ii. Model Name: HP1000

Generation: i3 (2nd Generation) RAM: 2GB

Table2: Results Obtained Using 2GB RAM

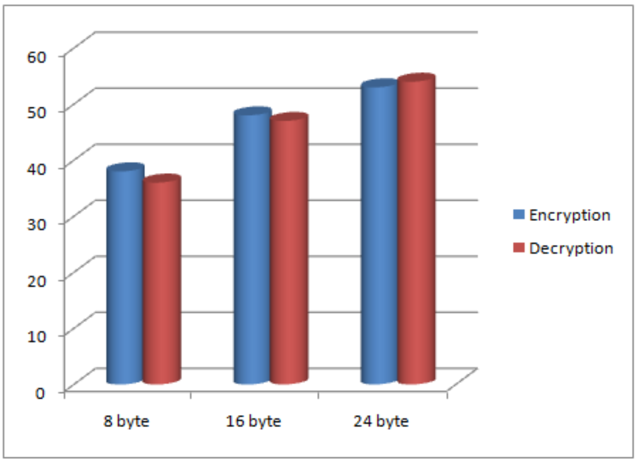


Figure6: Results Obtained Using 2GB RAM

iii. Model Name: Dell 6210

Generation: i3 (3rd Generation) RAM: 3GB

Table3: Results Obtained Using 3GB RAM

Block size (Byte)	Encryption Time (sec)	Decryption Time (sec)
8	35 sec	37 sec
16	44 sec	42 sec
24	50 sec	51 sec

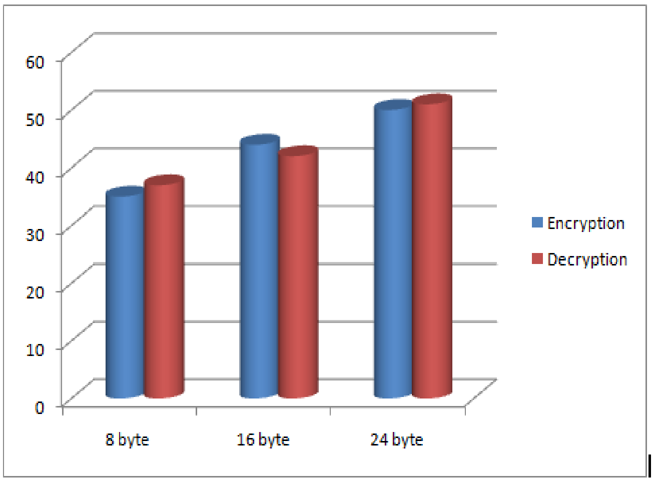


Figure7: Results Obtained Using 3GB RAM

VIII. Conclusion

The encryption of information/records is among the most straightforward routes utilized in shielding the substance of archive from being gotten to without approval. In this paper, we have found another approach for accomplishing a secured information transmission in an upgraded way. The new approach is a symmetric key calculation and will read each plain text one by one and convert it into cipher text by performing some operations. This proposed algorithm is effectual and easy to appliance. From the result, it has been evident that this approach is more relatable, faster than others. This Algorithm is superior to low level algorithm as well as compared to old algorithm.

REFERENCES

[1] Vishwa, G., Gajendra, S., &Ravindra, G. (2012). Advance cryptography algorithm to improve data security. Advance cryptography algorithm to improve data security, 43.

[2] Kessler, G. C. (2017, April 27). An Overview of Cryptography. Retrieved April 28, 2017, from Gary Kessler Associates: http://www.garykessler.net/library/crypto.html

[3] Kaushik, V., Singh, V., & Vats, M. (2014). Data Encryption Techniques for dependable and secure cloud computing. Data encryption techniques for dependable and secure cloud computing, 5.

[4] Abdalla, M., Bellare, M., Catalano, D., Kiltz, E., Lee, J. M., Paillier, P., et al. (2008). Searchable encryption revisited: Consistency properties, relation to anonymous IBE, and extensions. Journal of Cryptology, 42.

[5] Alexey Cheptsov, Bastian Koller, DavideAdami, Franco Davoli, Szymon Mueller, Norbert Meyer, Paolo Lazzari, Stefano Salon, Johannes Watzl, Michael Schiffers, Dieter Kranzlmueller, e Infrastructure for Remote Instrumentation, Computer Standards & Interfaces , Volume 34 Issue 6 ,November 2012.

[6] Wadsworth, D. (1883, januray 06). Decius Wadsworth. Retrieved december 07, 2016, from Wikipedia: https://en.wikipedia.org/wiki/Decius_Wadsworth

[7] Mainka, C., Somorovsky, J., &Schwenk, J. (2012). Penetration Testing Tool for Web Services Security". Penetration Testing Tool for Web Services Security", 7.

[8] Stallings, W. (2005). Data and Computer Communications . Upper Saddle River, New Jersey: Pearson Education.

[9] Stallings, W., & Brown, L. (2015). Computer Security. New jercy: Pearson..

[10] Khattab, A., Perkins, D., &Bayoum, M. (2013). Cognitive Radio Networks: From Theory to Practice. neyyork: Springer.

[11] Bishop, M. (2004). Introduction to Computer Security 1st Edition. Davis: Addison-Wesley Professional.

[12] Bishop, M. (2004). Introduction to Computer Security 1st Edition. Davis: Addison-Wesley Professional.

[13] Trappe, W. (2005). Introduction to Cryptography with Coding Theory 2nd edition. Newyork: Pearson.

[14] Shamir, A. (2017, 03 01). BekimDauti's Blog. Retrieved 04 12, 2017, from bekimdautiwordpress: https://bekimdauti.wordpress.com/2017/03/

[15] Encyclopaedia. (2016, 03 18). Key size. Retrieved 05 03, 2017, from the free encyclopedia: https://en.wikipedia.org/wiki/Talk:Key_size

[16] PunitaMellu&Sitender Mali, ―AES: Asymmetric key cryptographic System‖, International Journal of Information Technology and Knowledge Management, 2011, Vol, No. 4 pp.113-117.

[17] Shah Kruti R, BhavikaGambhava "New Approach of Data Encryption Standard Algorithm" International Journal of Soft Computing and Engineering(IJSCE) ISSN:2231-2307, Vol-2, Issue-1, March 2012

[18] "The Cryptography Guide: Triple DES". Cryptography World. Retrieved 2010-07-11.