Volume 4, Issue 9, September 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

An Enhanced Encryption Approach of Hiding Text Information through Word File

Fahim Multani*
CSE Department, SSSIST, Sehore,
M.P., India

Mr. Gajendra Singh
CS/IT Department, SSSIST, Sehore,
M.P., India

Abstract—Our daily life is dependent on secure transmission or communication of private information just likes payment through credit card at various agencies like banking sectors, online shopping portals at book shop etc., and mobile phone calls to other person or transferring the information through network like internet which require a way to maintain the information correct and safe. So to get a common idea of cryptography that is put it into context of common secure transmission or communication of information. Generally Cryptography provides a way where users can communicate securely or confidentially in adversarial environments. There are two type of cryptographic technique one is symmetric, if both the sender user and the receiver user are using the same key known as private key, as in the case of stream and block ciphers and message authentication codes. Hash functions are another type of symmetric technique in cryptographic, where neither sender user nor receiver user needs to know a confidential or private key. In contrast of this, cryptographic technique is asymmetric, if sender user and receiver user are using dissimilar keys, typically a "private" and a "public" one. Symmetric cryptography are extremely efficient as compare asymmetric cryptography, most of the applications are use to symmetric cryptography to make sure the secrecy, the integrity and the authenticity of confidential data. This paper presents a new encryption scheme which is based on symmetric cryptography concept. Furthermore, the security with performance of the presented encryption scheme is also evaluated. The combination of ASCII code and symmetric key approve the effectiveness of the proposed method, and the combination of ASCII code and symmetric key shows advantages of large key space and security with high level.

Keywords— Decryption, Encryption, Symmetric, Key, Asymmetric, Cryptography, Algorithm, Information security

I. INTRODUCTION

The importance of security has greatly increased over the years as most of critical functionality of the business and military enterprises became digitized. Text information is a primary part of any information system and they often hold confidential data. The security of the text data depends on physical security, OS security and DBMS security [13]. Text security can be compromised by obtaining confidential data, degrading or changing data availability of the text information. Though access control model were developed and found to ensure security, there were always chances of those access controls to be bypassed leading to a breach. To enforce the second layer of security, data being stored in the repository could be modified and stored in an encrypted format. This idea gave way to research in the design possibilities of proposed work. Two of such designs were Access Control Kernels and Encrypted file. Access Kernels were based on isolating and containing security policies inside separate modules [7]. The downside of this design was that the value-dependent access restrictions were not possible. The cryptographic technique of using keys to encrypt and store data was applied to achieve security. There were many restrictions and challenges like operations\computations on encrypted data, view-based protection, etc. This research focuses on a security solution for protection of data at rest, specifically protection/security of data that resides in file. [10] The scope of the research is to develop a technique that mediates the user and the operations to achieve text information security goals. People need to use the cryptographic operations in order to keep the personal sensitive information files to avert from foreigners in consideration of the security goals. The number of operations includes lots of algorithms to protect the attacks of foreigners to reach and read personal files that are located in personal computer or the owner would like to send somewhere [11]. Cryptographic operations consist of encryption and decryption techniques in computer and computer networking. In effort to keep information's in safety such as banking account information's or to provide file transaction without any problem such as password sharing caused such a security methods [11].

This paper has four parts. Part-I, presents introduction about cryptography and related with security, Part-II, presents proposed work where proposed encryption scheme are presented in details, Part-III presents experiment analysis of the proposed concept and Part-IV, presents conclusion and references.

II. PROPOSED WORK

In figure1 are showing the block diagram of the proposed concept where original text information and word file are executing with each other and performing encryption operation using a private Key by the assist of proposed encryption scheme [1-4]. During encryption or decryption identical key will utilize due to symmetric nature. Proposed Key length is

128 bits long so that security of proposed scheme is too high [13]. Proposed scheme is very efficiently due to its straightforwardness. Here proposed scheme take a smaller amount of time during execution as compared to the other scheme because only the essential or enough number of functions work during whole process that are essential for maintaining the confidentiality against the attacker or intruders. Now over all concept of proposed scheme are that original text and a word file executed with proposed encryption scheme and proposed encryption scheme call to propose key to produce another word file as a cipher output in this file original data hided but before hiding original text it encrypted through proposed encryption scheme. In reverse cipher output executed with proposed decryption scheme and this proposed decryption scheme call same proposed key to produce plain text.

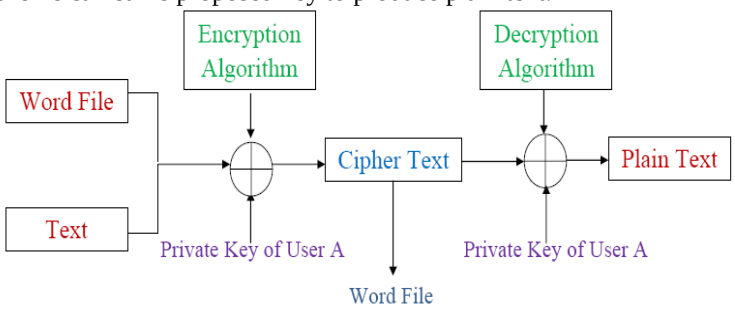


Fig 1: Proposed Concept Block Diagram

A. Proposed Encryption Scheme Architecture:

Figure 2 is viewing proposed encryption process architecture. In this figure proposed encryption process started via start function. Initially it taking 128 bits original text which is dividing into two part equally 64 bits left plain text (LPT) and 64 bits right plain text (RPT). Again these plain text are dividing into four parts equally LPT_1, LPT_2, LPT_3, LPT_4 for left plain text and RPT_1, RPT_2, RPT_3, RPT_4 for right plain text. Then each part are performing right circular shift, left circular shift and XOR operation with each other with the help of key. Finally proposed encryption process produced cipher text of 128 bits as an output. Details of each operation are exposed in the figure 2. And step of the encryption scheme is defined next.

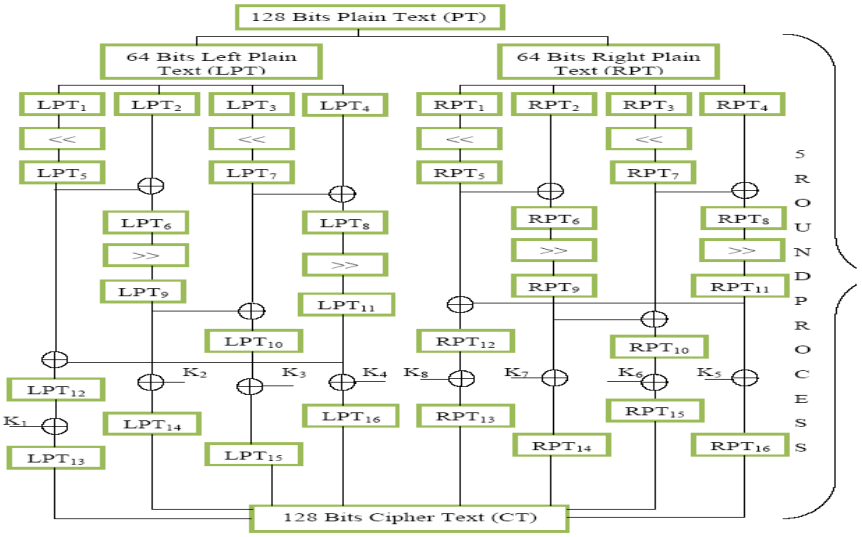


Figure 2: Proposed Encryption Architecture

- **Encryption Algorithm Step**

1. Input 128 bits plain text (PT).
2. Divide PT into two equal parts Left Plain Text (LPT) and Right Plain Text (RPT).
3. Select LPT and divide it into four equal parts LPT_1, LPT_2, LPT_3, LPT_4. Similarly RPT_1, RPT_2, RPT_3, RPT_4 for RPT.
4. Select LPT_1, LPT_3 and apply 2-bits left circular shift on each. Resultant will be LPT_5 & LPT_7.
5. Perform XOR operation on (LPT_2, LPT_5) and (LPT_7, LPT_4). Resultant will be LPT_6, LPT_8.
6. Select LPT_6, LPT_8 and apply 2-bits right circular shift on each. Resultant will be LPT_9, LPT_{11}.
7. Perform XOR operation on (LPT_9, LPT_7) and (LPT_{11}, LPT_5). Resultants will beLPT_{10} and LPT_{12}. Respectively.
8. Similarly Select RPT_1, RPT_3 and apply 2-bits left circular shift on each. Resultant will be RPT_5 & RPT_7.
9. Perform XOR operation on (RPT_2, RPT_5) and (RPT_7, RPT_4). Resultant will be RPT_6, RPT_8.
10. Select RPT_6, RPT_8 and apply 2-bits right circular shift on each. Resultant will be RPT_9, RPT_{11}.
11. Perform XOR operation on (RPT_9, RPT_7) and (RPT_{11}, RPT_5). Resultants will beRPT_{10} and RPT_{12}. Respectively.
12. Select Key value of 128 bits. And Divide it into eight equal parts similar to K_1, K_2, K_3, K_4, K_5, K_6, K_7, K_8.
13. Perform XOR operation Between Key and text value in following way.

$K_1 \oplus LPT_{12} \rightarrow LPT_{13}$
$K_2 \oplus LPT_9 \rightarrow LPT_{14}$
$K_3 \oplus LPT_{10} \rightarrow LPT_{15}$
$K_4 \oplus LPT_{11} \rightarrow LPT_{16}$
$K_5 \oplus RPT_{12} \rightarrow RPT_{13}$
$K_6 \oplus RPT_9 \rightarrow RPT_{14}$
$K_7 \oplus RPT_{10} \rightarrow RPT_{15}$
$K_8 \oplus RPT_{11} \rightarrow RPT_{16}$

14. Combine all LPT_{13} ,LPT_{14} , LPT_{15} , LPT_{16} , RPT_{13} , RPT_{14} , RPT_{15} , RPT_{16} into one . Resultant will be Cipher Text (CT).
15. Exit.

B. Architecture of Proposed Decryption Scheme:

Figure 3 is viewing proposed decryption process architecture. In this figure proposed decryption process started via start function. Initially it is taking 128 bits cipher text which is dividing into two parts equally of 64 bits left cipher text (LCT) and 64 bits right cipher text (RCT). Again this cipher text are dividing into four parts equally LCT_1, LCT_2, LCT_3, LCT4 for left cipher text and RCT_1, RCT_2, RCT_3, RCT4 for right text. Then each part is performing right circular shift, left circular shift and XOR operation with each other with the help of key. Finally proposed decryption process produced original text of 128 bits as an output. Details of each operation are exposed in the figure 3. And step of the decryption scheme is defined next.

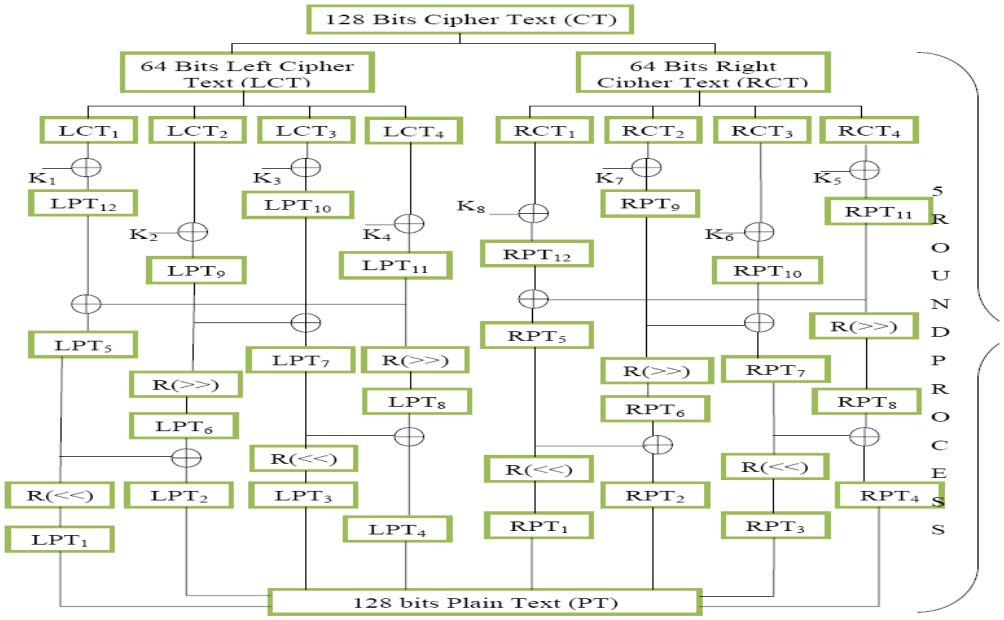


Figure 3: Proposed Decryption Architecture

- **Decryption Algorithm Step**

1. Input 128 bits plain text (CT).
2. Divide CT into two equal parts Left Plain Text (LCT) and Right Plain Text (RCT).
3. Select LPT and divide it into four equal parts LCT_1 , LCT_2 , LCT_3 , LCT_4 . Similarly RCT_1 , RCT_2 , RCT_3 , RPT_4 for RCT.
4. Select Key value of 128 bits. And Divide it into eight equal parts like K_1 , K_2 , K_3 , K_4 , K_5 , K_6 , K_7 , K_8.
5. Perform XOR operation Between Key and text value in following way.
   $K_1 \oplus LCT_1 \rightarrow LPT_{12}$
   $K_2 \oplus LCT_2 \rightarrow LPT_9$
   $K_3 \oplus LCT_3 \rightarrow LPT_{10}$
   $K_4 \oplus LCT_4 \rightarrow LPT_{11}$
   $K_5 \oplus RCT_1 \rightarrow RPT_{12}$
   $K_6 \oplus RCT_2 \rightarrow RPT_9$
   $K_7 \oplus RCT_3 \rightarrow RPT_{10}$
   $K_8 \oplus RCT_4 \rightarrow RPT_{11}$
6. Perform XOR operation on (LPT_{12}, LPT_{11}) and (LPT_{10}, LPT_9). Resultants will be LPT_5 and LPT_7. Respectively.
7. Perform XOR operation on (RPT_{12}, RPT_{11}) and (RPT_{10}, RPT_9). Resultants will be RPT_5 and RPT_7. Respectively.
8. Select LPT_9 , LPT_{11} and apply 2-bits left circular shift on each. Resultant will be LPT_6 & LPT_8.
9. Select RPT_9 , RPT_{11} and apply 2-bits left circular shift on each. Resultant will be RPT_6 & RPT_8.

10. Perform XOR operation on (LPT_5, LPT_6) and (LPT_7, LPT_8). Resultants will beLPT_2 and LPT_4. Respectively.
11. Perform XOR operation on (RPT_5, RPT_6) and (RPT_7, RPT_8). Resultants will be RPT_2 and RPT_4. Respectively.
12. Select LPT_5, LPT_7 and apply 2-bits right circular shift on each. Resultant will be LPT_1, LPT_3.
13. Select RPT_5, RPT_7 and apply 2-bits right circular shift on each. Resultant will be RPT_1, RPT_3.
14. Combine all LPT_1 ,LPT_2 , LPT_3 , LPT_4 , RPT_1 , RPT_2 , RPT_3 , RPT_4 into one . Resultant will be Plain Text (PT).
15. Exit.

III. RESULTS

Here proposed algorithm is implemented in .Net programming language. In this proposed scheme performance factors are throughput, encryption time and decryption time, RAM uses, CPU uses [5, 6 & 8]. Mainly proposed scheme is evaluating encryption and decryption scheme on various size of files using identical key. During experiment, a desktop machine was used with the Intel Pentium Dual Core E2400 2.36 Ghz, and 1 GB of RAM. Evaluated results are environment (platform) dependent so it can vary on other platform. During experiments, the proposed system encrypts/decrypt lots of text file of various sizes. In this proposed system executed n times each time, various plaintext are respectively encrypted by "Proposed Scheme". Finally, the outputs of the assessment system are Throughput; CPU uses, execution time, and RAMS uses.

- Encryption/Decryption time of Various Text files comparisons shown in table 1,
- Throughput of Various Text files comparisons shown in table 2,
- CPU Uses of Various Text files comparisons shown in table 3
- RAM Uses of Various Text files comparisons shown in table 4

TABLE 1: TEXT ENCRYPTION/DECRYPTION ANALYSIS OF PROPOSED ALGORITHM

S.NO	File Size in KB	Proposed Algorithm Execution Encryption Time in Second(Approx)
1	1	0.0
2	2	0.15
3	3	0.31
4	4	0.66

TABLE 2: THROUGHPUT ANALYSIS OF PROPOSED ALGORITHM

S.NO	File Size in KB	Proposed Algorithm Throughput(Approx)
1	1	Very High
2	2	136.53
3	3	99.09
4	4	62.06

TABLE 3: CPU USES OF PROPOSED ALGORITHM

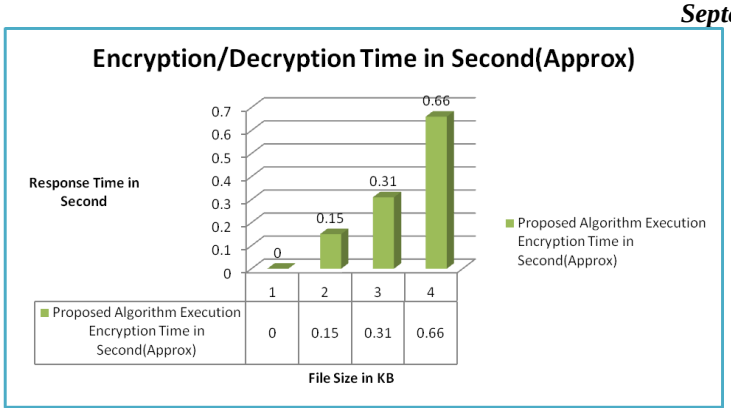
S.NO	File Size in KB	Proposed Algorithm CPU Consumption (Approx)
1	1	6
2	2	50
3	3	50
4	4	50

TABLE 4: RAM USES OF PROPOSED ALGORITHM

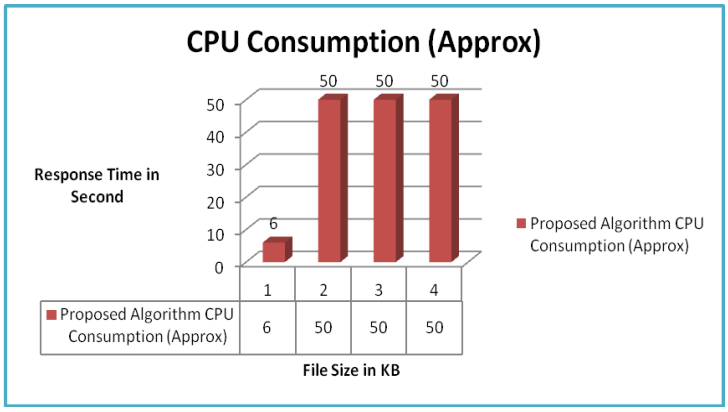
S.NO	File Size in KB	Proposed Algorithm RAM Uses in Second (Approx)
1	1	1423
2	2	1423
3	3	1457
4	4	1457

A graphical representation for the table 1 to 4 is shown in graph 1 to 3 with blue line for "Proposed Scheme (PS)". According to the graph, there is an inclination that encryption /decryption time for proposed scheme are good on different files of various size.

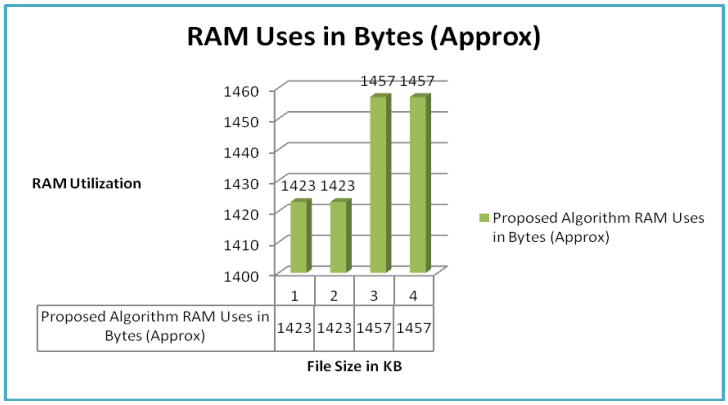
- A graphical representation for the table 1 is shown in graph 1,
- A graphical representation for the table 3 is shown in graph 2,
- A graphical representation for the table 4 is shown in graph 3



Graph 1: Text Encryption/Decryption Time of Proposed Algorithm



Graph 2: CPU Utilization of Proposed Algorithm



Graph 3: RAM Utilization of Proposed Algorithm

IV. CONCLUSION

From the results discussion it can clearly see that the proposed algorithm has better results than any of the other algorithms and hence can be incorporated in the process of encryption of any plain text. Also, we can see that the previous encryption algorithms (Classical and modern), etc [13]. have very less efficiency in terms of execution time and hence cannot be used for encryption of larger messages. The modern encryption techniques are better than classical ciphers as they have higher efficiency [9]. However it is also clear from table 1 to 5 that, by applying proposed algorithm to the files of different sizes highly security is obtain as compare to different other encryption algorithm. In execution time, CPU uses and RAM Uses the proposed algorithm have quite good results as compared to different other encryption algorithm. Table 1 showing the encryption time where various file size are producing different time according to size, if 2 kb file are executing through proposed algorithm are taking 15 second. Similarly at the time of decryption by proposed algorithm taking 15 second.

REFERENCES

[1] [1] Rishav Ray, Jeeyan Sanyal, Debanjan Das, Asoke Nath A new Challenge of hiding any encrypted secret message inside any Text/ASCII file or in MS word file: RJDA Algorithm IEEE International Conference on Communication Systems and Network Technologies 2012

[2] [2] Debanjan Das, Megholova Mukherjee, Neha Choudhary, Asoke Nath and Joyshree Nath "An Integrated Symmetric key Cryptography Algorithm using Generalised modified Vernam Cipher method and DJSA method: DJMNA symmetric key algorithm" 978-1-4673-0126-8/11/$26.00 c_2011 IEEE

[3] [3] Neeraj Khanna, Joyshree Nath, Joel James, Amlan Chakrabarti, Sayantan Chakraborty and Asoke Nath " New Symmetric key Cryptographic algorithm using combined bit manipulation and MSA encryption algorithm: NJJSAA symmetric key algorithm" IEEE International Conference on Communication Systems and Network Technologies 2011.

[4] [4] Dripto Chatterjee, Joyshree Nath, Suvadeep Dasgupta, Asoke Nath "A new Symmetric key Cryptography Algorithm using extended MSA method: DJSA symmetric key algorithm" published in 2011 International Conference on Communication Systems and Network Technologies, 978-0-7695-4437-3/11 $26.00 © 2011 IEEE

[5] [5] Joyshree Nath, Sankar Das, Shalabh Agarwal and Asoke Nath "Advanced Steganographic Approach for Hiding Encrypted Secret Message in LSB, LSB+1, LSB+2 and LSB+3 Bits in Non standard Cover Files" International Journal of Computer Applications (0975 – 8887) Volume 14– No.7, February 2011

[6] [6] Yan Wang and Ming Hu "Timing evaluation of the known cryptographic algorithms "2009 International Conference on Computational Intelligence and Security 978-0-7695-3931-7/09 $26.00 © 2009 IEEE DOI 10.1109/CIS.2009.81

[7] [7] Diaa Salama Abdul Minaam, Hatem M. Abdual-Kader, and Mohiy Mohamed Hadhoud "Evaluating the Effects of Symmetric Cryptography Algorithms on Power Consumption for Different Data Types" International Journal of Network Security, Vol.11, No.2, PP.78-87, Sept. 2010

[8] [8] IEEE Transactions on Circuits and Systems for Video Technology: Special Issue on Authentication, Copyright Protection, and Information Hiding, Vol. 13, No. 8, August 2003.

[9] [9] Nadeem.A, "A performance comparison of data encryption algorithms," IEEE Information and CommunicationTechnologies, 2006

[10] [10] Md. Nazrul Islam, Md. Monir Hossain Mia, Muhammad F. I. Chowdhury, M.A. Matin "Effect of Security Increment to Symmetric Data Encryption through AES Methodology" Ninth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing 978-0-7695-3263-9/08 DOI 10.1109/SNPD.2008.101 IEEE 2008.

[11] [11] R. Venkateswaran Dr. V. Sundaram "Information Security: Text Encryption and Decryption with poly substitution method and combining the features of Cryptography" International Journal of Computer Applications (0975 – 8887)Volume 3 – No.7, June 2010

[12] [12] Akhil Kaushik, Manoj Bamela and AnantKumar "Block Encryption Standard for Transfer of Data" IEEE International Conference on Networking and Information Technology 2010.

[13] [13] Diaa Salama Abdul Minaam, Hatem M. Abdual-Kader, and Mohiy Mohamed Hadhoud "Evaluating the Effects of Symmetric Cryptography Algorithms on Power Consumption for Different Data Types" International Journal of Network Security, Vol.11, No.2, PP.78{87, Sept. 2010.

[14] [14] Gary C. Kessler, 1998, An overview of cryptography, [online]:

[15] http://www.garykessler.net/library/crypto.html , date accessed: 23/07/06

