P- ISSN 1991-8941 E-ISSN 2706-6703 *Journal of University of Anbar for Pure Science (JUAPS)* Open Access
2012,(6), (2) :70-74

TORDES-THE NEW SYMMETRIC KEY ALGORITHM

Ajay Bhushan* **Pawitar Dulari****

* Galgotias College of Engineering and Technology
**Govt. Degree College, Indora (Himachal Prdaesh)-INDIA.

ARTICLE INFO

Received: 00 / 00 /00
Accepted: 00 / 00 /00
Available online: 9/12/2012
DOI:10.37652/juaps.2012.63241

Keywords:
Block cipher,
Computer security,
Cryptography,
Data Encryption Algorithm,
TORDES algorithm.

ABSTRACT

The selective application of technology and related procedural safeguard is an important responsibility for cryptographic algorithm to its electronic data systems. This paper specifies the functionality of TORDES for encryption and decryption to protect the sensitive unclassified data. TORDES is made available within the context of a total security program consisting of physical security procedure.

Introduction

There has been a noticeable development in Internet and World Wide Web in the recent past, a socially fruitful outcome of which being, generated interest towards information technology and increased utility therefore of related applications by general population throughout the globe. Broad and easy exchange of confidential data belonging to various categories throughout the world over the network, both by experts and general populations is presently at its charm. A very big challenge in this field *(vide supra)* is Data hacking which, presently is a cynosure both among the data users as well as developer [1].

Encryption algorithms play a big role in providing data security over the network [2]. Encryption algorithm can be categorized into two types viz. symmetric key algorithms and asymmetric key algorithms.

The strengths of symmetric key Algorithms makes it to be much faster than asymmetric systems and hard to break if using a large key size and the limitation for the symmetric key algorithms is that the key distribution requires a secure mechanism to deliver keys properly[3].

A unique approach termed MODDES has earlier been introduced with block cipher algorithm [4]. This approach uses stack of operators and randomized delimiter along with some suitable mathematical operators and look up tables. A new cryptographic algorithm named TORDES has been proposed in the present study, which is meant for better encryption of data with enhanced security and performance (For more details see also [1] and [5]).

Review of Literature

Gope et al. [4] [6] introduced a new secret key algorithm named Multi Operator Delimiter based Data Encryption Standard (MODDES) which was successfully tested for protecting data belonging to various categories. In comparison to DES, MODDES has been found simple and efficient as later does not fully emphasize on the key. In addition, performance in terms of total execution time and data encrypting and decrypting capacity MODDES has an edge over DES, 3DES, AES.

Ayushi [7] proposed a new symmetric algorithm which achieved few goals like Confidentially, Data integrity and authentication of sending data. Dhanraj et al. [8] introduced an enhanced approach to DES in the form of partial symmetric key algorithm, which makes it less dependent on the key and for the same plain text it produces differently modified secure code sequences.

* Corresponding author at: Galgotias College of Engineering and Technology. E-mail address: ajay2007bhushan@gmail.com

Khanna et al. [9] introduced a new advanced symmetric key cryptographic method called NJJSAA. Ray et al. [10] dealt with new advanced symmetric key cryptographic method for multiple encryption and decryption of any file especially image file, sound file, video file, text file, executable file or any other file. Others had made an attempt is made to design a new model of Symmetric key Cryptography using Vigenere Cipher Technique and ECB Encoding

Algorithm for TORDES

A. Encryption Algorithm of TORDES

In this algorithm, we have taken two predefined stacks and a lookup table. Here the first stack consists of different combinations of operator strings and the other stack consists of combinations of delimiters, which are chosen randomly at the code sequence. The lookup table consists of the code words of the corresponding operators present in first stack. The steps of the algorithm have been presented in the ray diagram form (Fig. 1)

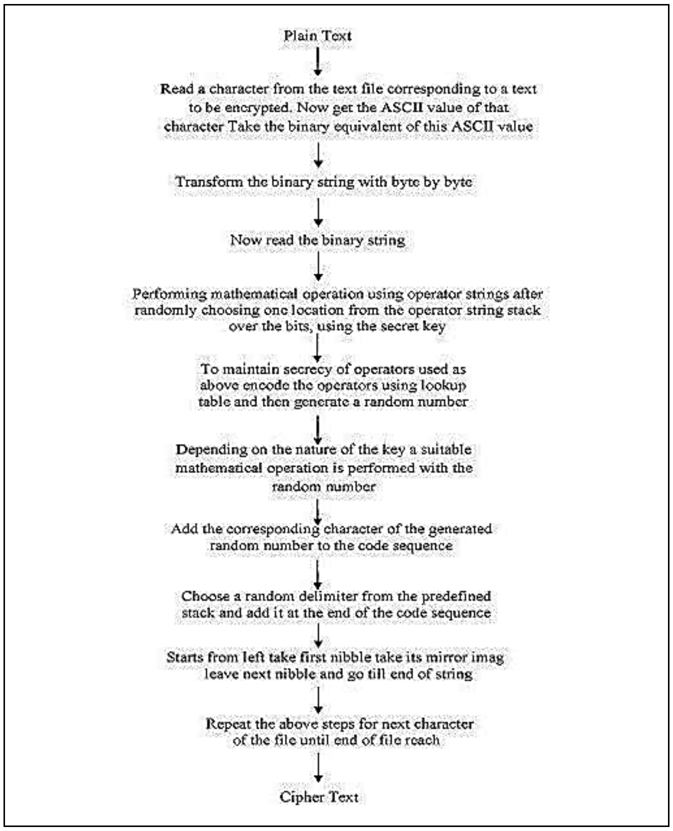

Plain Text
Read a character from the text file corresponding to a text to be encrypted. Now get the ASCII value of that character Take the binary equivalent of this ASCII value
Transform the binary string with byte by byte
Now read the binary string
Performing mathematical operation using operator strings after randomly choosing one location from the operator string stack over the bits, using the secret key
To maintain secrecy of operators used as above encode the operators using lookup table and then generate a random number
Depending on the nature of the key a suitable mathematical operation is performed with the random number
Add the corresponding character of the generated random number to the code sequence
Choose a random delimiter from the predefined stack and add it at the end of the code sequence
Starts from left take first nibble take its mirror imag leave next nibble and go till end of string
Repeat the above steps for next character of the file until end of file reach
Cipher Text

Figure 1. Encryption Procedure of TORDES

B. Decryption Algorithm of TORDES

Decryption is the process of conversion of cipher text to plain text. Entire algorithm corresponding to decryption of TORDES has been shown in the form of flow charts (Fig. 2).

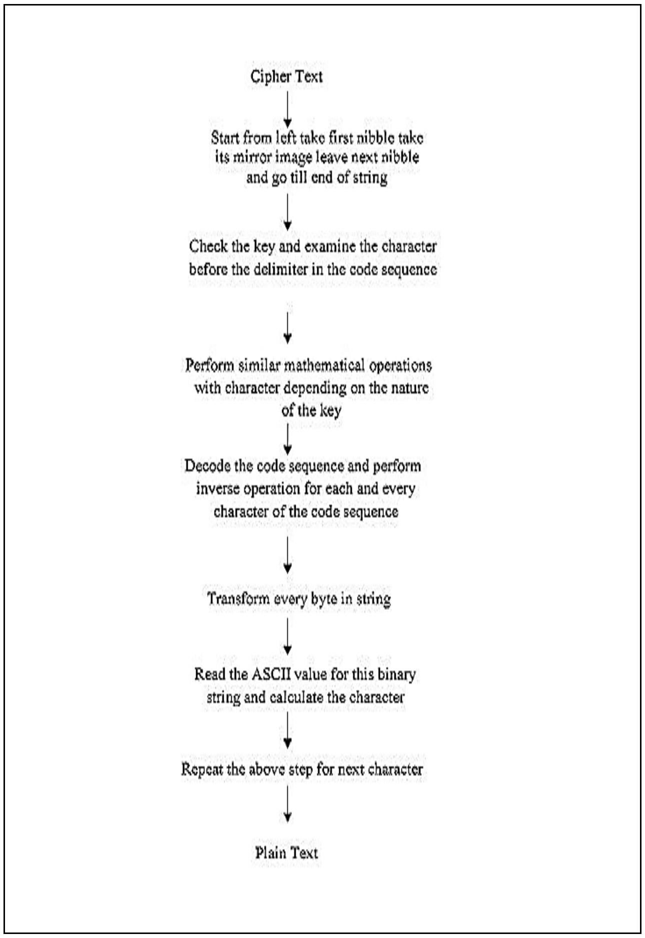

Cipher Text
Start from left take first nibble take its mirror image leave next nibble and go till end of string
Check the key and examine the character before the delimiter in the code sequence
Perform similar mathematical operations with character depending on the nature of the key
Decode the code sequence and perform inverse operation for each and every character of the code sequence
Transform every byte in string
Read the ASCII value for this binary string and calculate the character
Repeat the above step for next character
Plain Text

Figure 2. Decryption Procedure of TORDES

PERFORMANCE AND EVALUATION

A. Performance of TORDES

TORDES is practical implementation with a piece of software code written in Dot Net. This is done because of inbuilt future of security present in the Dot Net. Furthermore there is no such restriction that it be implemented only on Dot Net and not on java, pup or other languages.

B. Encryption/Decryption Execution time

We are using three parameters for execution of time first in encryption value, second in decryption and third in total encryption and decryption time which is shown in Table 1. A comparison of execution time encryption plain text on different existing cryptographic algorithm (DES, TDES, AES and MODDES) has been done in the present study.

In the present approach, values of some plaintext algorithm using TORDES have been generated and compared with existing algorithms (DES, TDES, AES and MODDES). The proposed method has been implemented based on multi-threading concept, which helps in efficient utilization of CPU. Hence encryption and decryption time is very optimum as compared to existing methods. Below table and graph shows the time (seconds) required for encryption and decryption of text file of size *20,527* bytes (See Fig. 3). Some snapshots of the current GUI of TORDES implementation are shown in Fig. 4.

Table 1: Shows the time (in seconds) required for encryption and decryption of text file of size 20,527 bytes.

Algorithm	Input Text file	DES	TDES	AES	MODDES	TORDES
Encryption	20,527 bytes	2	7	4	10	12
Decryption	20,527 bytes	17	58	62	4	4
Total	20,527 bytes	19	65	66	14	16

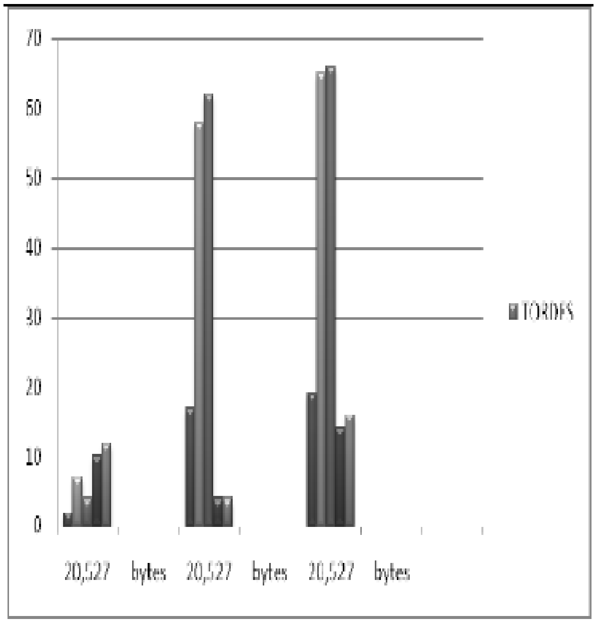
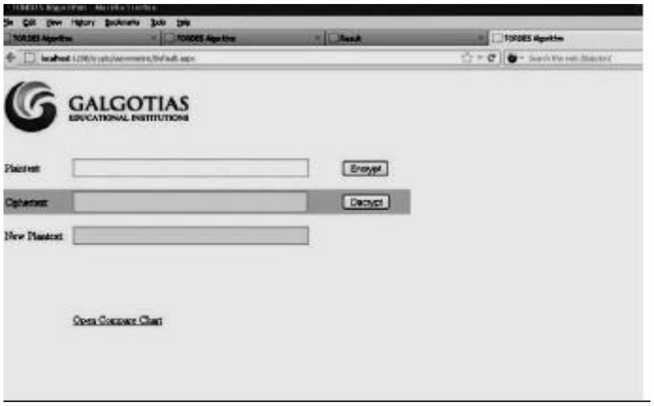
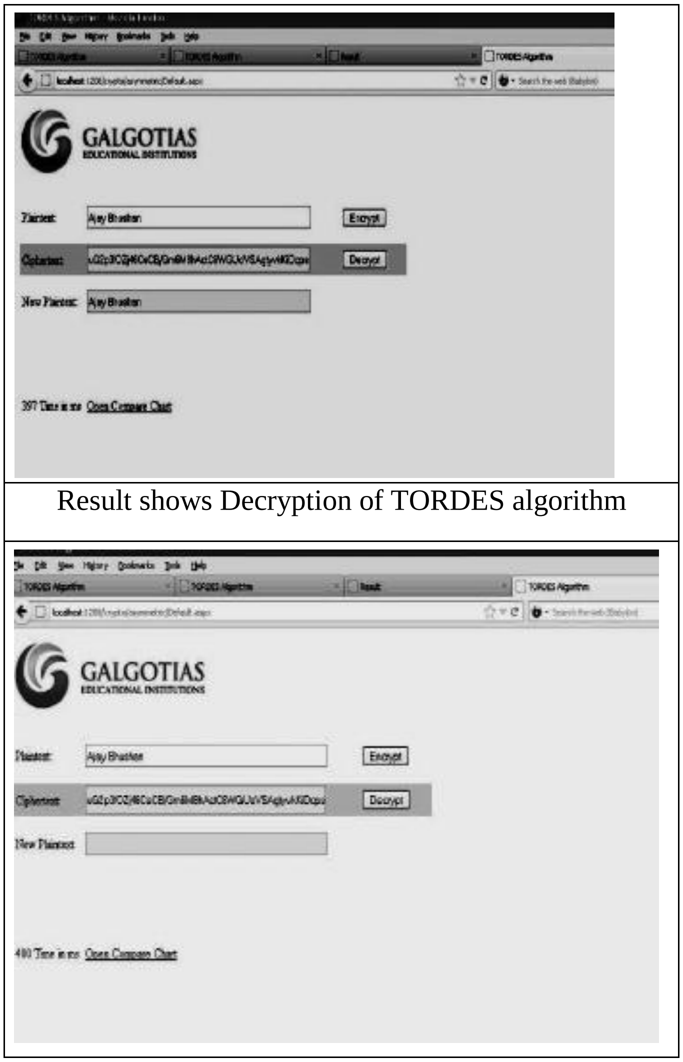


Figure 3. Performance values of different algorithms

View of webpage that contains TORDES algorithm



Result shows Encryption of TORDES algorithm



Plaintext: Ajay Bhushan

Ciphertext: uG2p3CQj/6CaCB/Gm8M8hAdC8WGLkVSAgtyvAKDcqu

New Plaintext: Ajay Bhushan

397 Time in ms

Result shows Decryption of TORDES algorithm

Plaintext: Ajay Bhushan

Ciphertext: uG2p3CQj/6CaCB/Gm8M8hAdC8WGLkVSAgtyvAKDcqu

New Plaintext:

400 Time in ms

Figure 4. GUI and results of TORDES

C. Advantages of TORDES

The main advantage of proposed system is that it is not fully dependent on the key and for the same plain text it produces different modified secure codes. In the present work, an effort has been made to benchmark performance analysis of popular secret key algorithms i.e. DES, TDES, and AES, MODDES with TORDES algorithm.

D.Strength of TORDES

The MODDES [4] was tested on P4 (2.4) processor and it was well worked and came out to be much secure for the purpose it was designed for. But today it is easy to crack this algorithm with the advent of second generation processor. For this algorithm to be much secure and functional as per second generation processor, it is necessary to modify MODDES so we have added some new steps on MODDES on same bit key. A new Algorithm TORDES was introduced which overcome these drawback of old algorithm and make it secure over communication channels. These are secret key that does not totally depend on the key. As such, if the key value becomes known, then we can decipher it without the knowledge of code sequence generated from that particular processing. And the related decryption algorithm which will make TORDES highly secure on second generation machine tested with result.

CONCLUSION AND FUTURE WORK

Security is a very complex topic. It is very important to build systems and networks in such a way that the user is not constantly reminded of the security system around him. Users who find security policies and systems too restrictive will find ways around them. The proposed system is implemented based on threading concept so it reduces the CPU utilization hence it reduces the time required for encryption and decryption. The proposed system is successfully tested on text. The performance and security provided by proposed system is better than other secret key algorithm for the message of fixed sizeWe were able to come up with a primitive design of the camera to perform magnification at 2x, 3x and 4x respectively. However implementing other features as mentioned in the improvements section could make the design better. As a future work, the algorithm can be implemented on image, speech and video. It can be used on embedded systems. It can be also only through hardware.

REFERENCES

[1] Bhushan, A. (2012). TORDES A Symmetric key algorithm. *LAP Publishers*.

[2] Seth, S. and Mishra, R. (2011). Comparative Analysis Of Encryption Algorithms For Data Communication. *IJCST*, Vol. 2, Issue 2, June 2011, ISSN : 2229-4333(Print).

[3] Stallings, W. (2007). Cryptography and Network Security Principles and Practice. Fourth Edition, *Prentice Hall*.

[4] Gope, P., Ghosh, D., Chelluri, A. and Chattopadhyay, P. (2009). Multi Operator

Delimiter based Data Encryption Standard (MODDES). *ICCNT Conference*. Chennai, India, June 27 – 29, 2009.

[5] Bhushan, A. and Dulari, P. (2012). Component of Symmetric key Algorithm TORDES with its Functionality. *IJCEM International Journal of Computational Engineering & Management*, Vol. 15 Issue 5, September 2012 ISSN (Online): 2230-7893

[6] Gope, P., Kaushik, A., Arora, K. and Kumar, N. (2010). X-MODDES (Extended Multi Operator Delimiter Based Data Encryption Standard, *Proceedings of the 2nd International Conference on Future Networks (ICFN)*, China, March, 2010, pp 399-403.

[7] Ayushi, A. (2010). A Symmetric Key Cryptographic Algorithm. *International Journal of Computer Application.*

[8] Dhanraj, C. Nandini, N. and Tajuddin, M. (2011). An Enhanced Approach for Secret Key Algorithm based on Data Encryption Standard. *International Journal of Research and Reviews in Computer Science (IJRRCS)*, Vol. 2, No. 4, August 2011, ISSN: 2079-2557.

[9] Khanna, N., Nath, N., James, J., Chakrabarti , A., Chakrabort, S., and Nath, A., (2011). New Symmetric key Cryptographic algorithm using combined bit manipulation and MSA encryption algorithm: NJJSAA symmetric key algorithm. *International Conference on Communication Systems and Network Technologies.*

[10] Ray, J., Sanyal, J., Das, D., Nath, A. (2012). A new Challenge of hiding any encrypted secret message inside any Text/ASCII file or in MS wordfile: RJDA Algorithm. I. J. Modern Education and Computer Science, 2012, 5, 1-9 Published Online June 2012 in MECS.

توردس – الشفرة التناظرية المفتاح الجديدة

أجاي بوشان باويتار دولاري

ajay2007bhushan@gmail.com
pawitar.ibs@gmail.com

الخلاصة:

ان التطبيق الانتقائي المناسب للتكنولوجيا والاجراءات الأمنية المتعلقة بها هي مسؤولية كبرى لخوارزميات التشفير تجاه الانظمة الالكترونية التي يتم حمايتها بواسطة تلك الخوارزميات. والهدف الرئيسي لهذا البحث هو فعالية الشفرة التناظرية الجديدة "توردس" في استخدامها للتشفير وفكه اثناء حماية البيانات. وقد تم تطبيق "توردس" كجزء من اطار متكامل للحماية الأمنية يتضمن اجراءات أمنية مادية وليس برمجية فحسب.