International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459 (Online), An ISO 9001:2008 Certified Journal, Volume 3, Special Issue 2, January 2013)

National conference on Machine Intelligence Research and Advancement (NCMIRA, 12), INDIA.

Cryptanalysis with A Symmetric Key Algorithm TORDES

Pawitar Dulari[1], Ajay Bhushan[2]

1Department of Physics,Govt. Graduate.College, Indora,(Himachal Prdaesh)-INDIA
[2]Department of Information Technology, Galgotias College of Engineering and Technology,Greater Noida (Uttar Pradesh)–INDIA

E-mail: [1]pawitar.ibs@gmail.com,[2]ajay2007bhushan@gmail.com

Abstract

In today's epoch, most of the means of secure data and code storage and distribution rely on using cryptographic Schemes, such as certificates or encryption keys. This paper is devoted to the security and attack aspects of cryptographic techniques with new symmetric key algorithm TORDES. This algorithm is proposed to achieve the different goals of security i.e., Availability, Confidentiality and Integrity. We will also discuss the security threats in this algorithm.

***Keywords*- TORDES**; **Random**; Attack; **Security**; **Crypto analysis.**

I. INTRODUCTION

Today's cryptography is vastly more complex than its precursor.Unlike the innovative use of cryptography in its classical roots where it was implemented to conceal both diplomatic and military secrets from the enemy, the cryptography of today, even though it still has far-reaching military implications, has expanded its field, and has been considered to provide a cost-effective means of securing and thus caring large amounts of electronic data that is stored and communicated across corporate networks wide reaching. Cryptography offers the means for caring this data all the while preserving the privacy of critical personal financial, medical, and ecommerce data that might end up in the hands of those who shouldn't have access to it.

Modern high value encryption methods have few known flaws and are subjected to extensive attack by cryptography experts through cryptanalysis. This is a science (or art) of evaluation encrypted traffic without prior knowledge of key. Hence while considering as to what encryption to use, it is important to choose a well known method that has been thoroughly examined by the wider area. Many high secure algorithms have turned out to be eventually insecure. The cryptanalysis will be used against a condition, if someone tries to crack encrypted traffic. The methods used vary both due to the nature of the attacks and the encryption algorithm they are trying to crack.

Some well known attacks like Brute Force[7] is probably the most rigorous technical attack in use today, simply because most modern algorithms and their implementations have few known holes that attacker can exploit. An 8 bit key has 28 combinations (256), thus a typical pocket calculator has enough power to try out all these combinations against the cipher text in less than a second, by comparison a 40 bit key has 240 combinations (1,099,511,627,776) but this is still computable comparatively easily.

II. TORDES

Tordes is a block cipher algorithm (bhushan et al., 2012). It is unique independent approach which uses several computational steps along with string of operators with randomized delimiter selections by using some suitable mathematical logic. It is specially designed to produce different cipher texts by applying same key on same plain text. It is one of the best performing partial symmetric key algorithms particularly for the text message with limited size in its class. It also protects the cipher text from attacks because it is fully dependent on the key and code cannot be deciphered by applying all possible combinations of keys. The following information invariably used in TORDES For encryption Techniques.

1) Key Values
2) Code sequence string generated from a particular process.
3) Transformation of string.
4) Mirror image of string.

This shows that the security of text data is not only depends upon key value. This really increases the security of text file.

Encryption 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 look up 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 in figure1 as above.

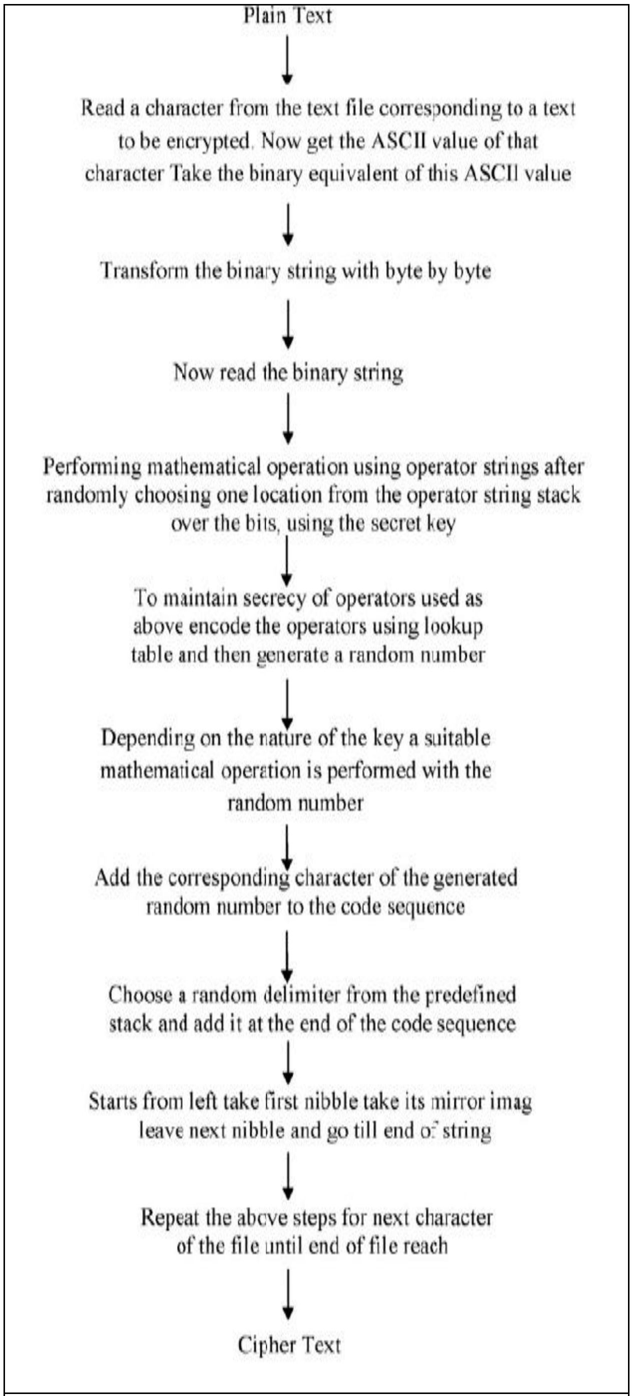

Plain Text
Read a character from the text file corresponding to a text to be encrypted. Now get the ASCII value of that character Take the binary equivalent of this ASCII value
Transform the binary string with byte by byte
Now read the binary string
Performing mathematical operation using operator strings 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 abcve steps for next character of the file until end of file reach
Cipher Text

Figure1:Showing Decryption in TORDES algorithm

Decryption algorithm of TORDES

Entire algorithm corresponding to decryption of TORDES has been shown in the form of flow charts

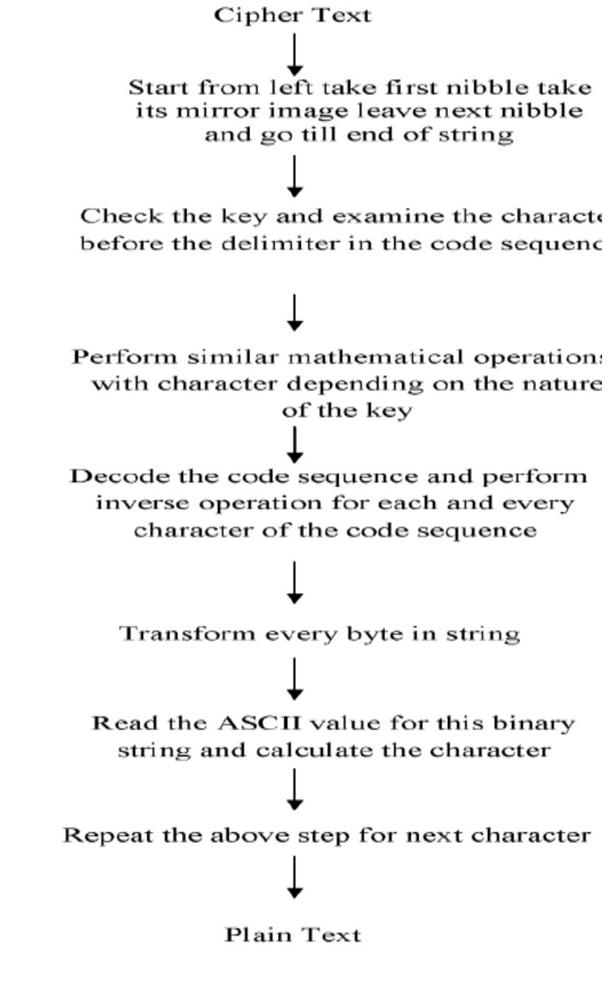

Cipher Text
Start from left take first nibble take its mirror image leave next nibble and go till end of string
Check the key and examine the characte before the delimiter in the code sequenc
Perform similar mathematical operation: with character depending on the nature of the key
Decode the code sequence 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

Figure2: Showing Decryption in TORDES algorithm

III. Security Analyses With Tordes

Security is an important aspect associated with both the encrypted objects and the encryption algorithms. Some security issues of the TORDES algorithm from the cryptographically point of view have been discussed herein.

1 Chosen cipher text attack

This attack model refers to the situation where attacker tries to deduce secret keys by studying various cipher texts and corresponding plaintexts. This kind of attack has more chances of success if encryption process uses limited key values and does not change the image data too much. TORDES algorithm has been planned to counter such attacks as it uses two keys which are chosen randomly for different pixels; hence deduction of encryption keys will be practically impossible.

2 Cipher text-only attack

In this attack model, the attacker tries to deduce the original text by studying different ciphered text. If text can be found without finding out secret key, it is quite easy to find real text. Here, TORDES encrypts very text, thereby is much effective against any such type of attack.

3 Chosen-plain text attacks

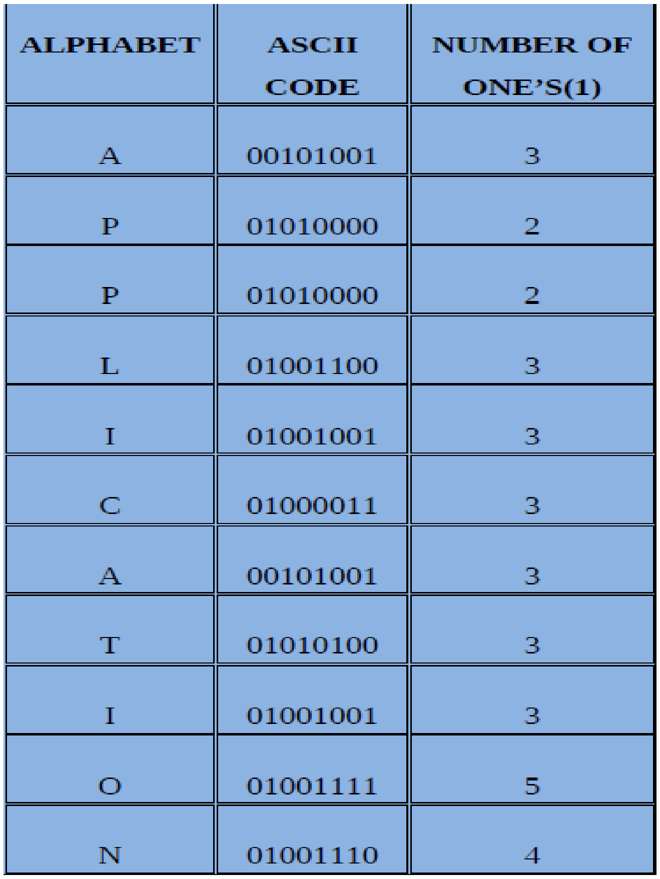
In this attack model, an attacker chooses a number of plaintexts and then interprets their respective cipher texts. The attack can crack the encrypted text without knowing details of encryption algorithm and secret key. But symmetric key algorithm TORDES has an edge over this type of attack as it uses transformation and also changes the data and locations even when it is resized.

4 Brute-force attacks

Efficiency of TORDES against this type of attack can be demonstrated by considering the following example. For decryption of the word “APPLICATION”, the key value and four operators used in encryption algorithm are known.

Machine Intellegence & Advancement Group (MIRAG)
IJETAE
EXPLORING RESEARCH AND INNOVATIONS
International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459 (Online), An ISO 9001:2008 Certified Journal,Volume 3, Special Issue 2, January 2013)
National conference on Machine Intelligence Research and Advancement (NCMIRA, 12), INDIA.

Table 3
Crypto-analysis to determine efficiency of TORDES



ALPHABET	ASCII CODE	NUMBER OF ONE'S(1)
A	00101001	3
P	01010000	2
P	01010000	2
L	01001100	3
I	01001001	3
C	01000011	3
A	00101001	3
T	01010100	3
I	01001001	3
O	01001111	5
N	01001110	4

Table 1: Crypto-analysis to determine efficiency of TORDES

Thus, the possible number of attempts to break this word based on three operators is

3^3 * 3^2 *3^2 *3^3 *3^3 * 3^3 *3^3 *3^3 *3^3 *3^5 *3^4 = (3) ^34

On the basis of numbers of one's available in the bits position in the last octet of the binary string is **3^34** possible numbers of combinations of modified secure code sequence string. The transposition of characters also gives **11! ,** *i.e.* number of combinations. Mirror Nibble will give 22! So, total number of combinations required to decipher the text "APPLICATION" is

3^34 +11! +22! = 1124017405*10^21combinations
(3^34 +11! +22!) / (2.4*(10) ^9)*3600*24*365 = 14850.98 years (theoretically)

"APPLICATION" in case of MODDES, with known key value and three operators, the number of attempts required breaking is

3^34 = 16677181699666569 combinations, i.e. 1.9 days approx.

5 Dictionary attack

A dictionary attack uses a targeted technique of successively trying all the words in an exhaustive list called a dictionary (from a pre-arranged list of values). In difference with a brute force attack, where a large proportion key space is searched systematically, a dictionary attack tries only those possibilities which are most likely to succeed, typically derived from a list of words for example a capital (hence the phrase dictionary attack) or a country etc. Generally, dictionary attacks succeed because many people have a tendency to choose passwords which are short (7 characters or fewer), single words found in dictionaries or simple, easily-predicted variations on words, such as appending a digit. However these are easy to defeat. Adding a random number in the middle can make dictionary attacks untenable. TORDES has used this technique to protect the data from dictionary attack.

6 Man in the middle attack:

It differs from the above in that it involves tricking individuals into giving way their keys. The cryptanalyst places him in the communication channel between sender and receiver who wish to exchange their data for secure communication. The cryptanalyst then performs a key exchange with each party, with the original parties believing they are exchanging keys with each other. The two parties then end up using keys that are known to the cryptanalyst. This type of attack can be defeated by the use of a hash function. TORDES used hash function which is capable to defeat this kind of attack.

7 Timing/differential power analysis:

It is a new technique made public in the mid 1998, particularly useful against the smart card that erasures differences in electrical use over a period of time when a microchip performs a function to secure information. This technique can be used to put on information about key computations used in the encryption algorithm and other functions pertaining to security.

The technique can be rendered less effective by introducing random noise into the computations, or altering the sequence of the executables to make it harder to monitor the power fluctuations. This type of analysis was first developed by Paul Kocher of Cryptography Research, though Bull Systems claims it knew about this type of attack over four years before.

IV. Strength Of Tordes

The MODDES (Gope et al., 2009) 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.

V. Conclusion

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 size.

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

REFERENCES

[1] W. Stallings “Cryptography and network security principles and practice,” Fourth edition, Prentice hall, 2007

[2] Gope, P., Ghosh, D., Chelluri, A.R.K. and Chattopadhyay,P., 2009. Multi Operator Delimiter based Data Encryption Standard (MODDES). ICCNT. Chennai,

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

[4] NIST, “Advanced Encryption Standard Call”, NIST, 1997.

[5] Bhushan , A., 2012. “TORDES A New Approach to Symmetric Key Encryption”, LAP Lambert Academic Publishing, **ISBN-13**: 9783659218415

[6] Bhushan, A2012. Transform Operator Random Generator Delimiter based Encryption Standard (TORDES).CCIT2012, Iraq.

[7] Bhushan, A., D, Pawitar., “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

[8] Bhushan , A., 2012. “TORDES A Symmetric Key Algorithm” **Anbar University Journal for Engineering Sciences,** ISSN: 19979428.

[9] National Bureau of standards-Data encryption Standard,

[10] FIPS Publications, 46. 1997.

[11] Tanenbaum, A. S., 2004. Computer Networks. New Delhi, Prentice Hall Inc.

[12] Charles, P.P. and Shari, P.L., 2008. Security in Computing: 4th edition,Prentice-Hall, lnc.

[13] Jing, F. and Xian Z., 2009. Data Encryption by Two Keys.

[14] NIST data for DES

[15] NIST data for TDES

[16] NIST data for AES