ISSN No. 0976-5697

Volume 4, No. 8, May-June 2013

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

UNICODE and Color Integration Technique for Encryption and Decryption

Anil Kumar
Deptt. of computer science
TIT&S BHIWANI, Haryana
Yadavanil82@gmail.com

Ritu yadav
Deptt. of Electronics & Communication
TIT&S BHIWANI, Haryana
Ritu12june@gmail.com

Rajesh Kumar
Senior Programmer Deptt. of computer science
TIT&S BHIWANI, Haryana
rajeshgoyal@titsbhiwani.ac.in

Abstract: A wide variety of techniques have been employed for encryption and decryption but cryptanalysis has simultaneously cracked these encryption techniques from time to time. UNICODE is one of the consistent representation and handling of text expressed in most of the world's writing systems. The latest version of UNICODE consists of a repertoire of more than 107,000 characters covering 90 scripts, a set of code charts for visual reference, an encoding methodology and set of standard character encodings, an enumeration of character properties such as upper and lower case, a set of reference data computer files, and a number of related items. This paper introduces a new technique and an algorithm that focuses on cryptography by using UNICODE and colors available in the universe (supported by computer).

Keywords: Unicode, Encryption, Decryption, Software Localization and Cryptanalysis.

I. INTRODUCTION

The rapid growth of internet in the recent days and the wide spread availability of networks have lead to the development of powerful and creative applications. Almost all the software applications are becoming online, not to mention the Google Docs and Microsoft Office Live. Hence, the networks have become more open and accessible .Consequently, an adversary is not limited to eavesdropping but may take a more important role by activities like a Man in the Middle Attack. The last decade witnessed a lot of the sea-attacks [1]. Therefore, the security for the huge amount of data transferred is at stake. The science of Cryptology dates back to Caesar's time. Since then, a variety of heuristics have been proposed for secured communication. But, cryptanalysis has simultaneously cracked these encryption techniques from time to time . Hence, the fundamental task of cryptography is not only to protect the secrecy of messages transmitted over public communication lines but also to resist such cryptanalytic attacks which tend to evolve with the passage of time . The Data encryption techniques can be broadly classifieds symmetric and asymmetric key cryptography [2].

In symmetric key cryptography, the same key is used by the sender and the receiver for encryption and decryption respectively. The representative algorithms of this approach are AES, TDES,RC5 [3] and the likes. Asymmetric or public key cryptography uses two keys namely, private key which is kept by the receiver and public key which is announced to the public [4]. Cryptosystems like RSA, PGP and ECC fall under this category. Other recent data encryption techniques include Quantum Cryptography [5]. Although, a wide variety of techniques have been employed for encryption and decryption, the use of a multilingual approach for the same is not prevalent. Motivated by this, here, we propose a novel algorithm that focuses on encryption of plain text over a range of languages supported by Unicode [6]. The use of mapping techniques makes the algorithm fast, efficient and easier to implement. Further, the replacement strategy used ensures better security. The rest of the paper is organized as follows. In Section II we present the proposed algorithm with examples. Next, in Section III we discuss and illustrate the functioning of the algorithm .Conclusion and future works are mentioned in Section IV.

A. What is Unicode?:

Fundamentally, computers deal with numbers. They store letters and other characters by assigning a unique number for each one. Before Unicode was invented, there were hundreds of different encoding systems. There was no single encoding system that could contain enough characters: for example, the European Union alone requires several different encodings to cover all its languages [7]. Even for a single language like English, no single encoding was adequate for all the letters, punctuation, and technical symbols in common use.

These encoding systems also conflict with one another. That is, two encodings can use the same number for two different characters, or use different numbers for the same character. Any given computer (especially servers) needs to support many different encodings[8]; yet whenever data is passed between different encodings or platforms, such data always run the risk of corruption .Unicode provides a unique number for every character, which is independent from the platform, program, and language .

B. User Defined Codes (UDC):

According to the Unicode standard, Unicode values range from 0000-FFFF, which contains 65535 characters. Thus each language has its own range of character mapping according to the Unicode standard [10].

II. PROPOSED ALGORITHM

a. Convert the character into its Corresponding Unicode.
b. Convert the Unicode to 16-bit Binary Number.
c. Now Add 8-bits to the left of the 16-bit Binary Number and these 8 bits are calculated as follows :

1st bit can be calculated by XORing the 1st and 16th bit of Unicode.

2nd bit can be calculated by XORing the 2nd and 15th bit of Unicode.

3rd bit can be calculated by XORing the 3rd and 14th bit of Unicode.

4th bit can be calculated by XORing the 4th and 13th bit of Unicode.

5th bit can be calculated by XORing the 5th and 12th bit of Unicode.

6th bit can be calculated by XORing the 6th and 11th bit of Unicode.

7th bit can be calculated by XORing the 7th and 10th bit of Unicode.

8th bit can be calculated by XORing the 8th and 9th bit of Unicode.

a) Now we get a 24-Bit Binary Number.
b) Convert this 24-bit binary Number to Hexadecimal number.
c) Now encrypt this new Number with its corresponding color.

A. Encryption:

The text to be encrypted is read character by character and the Unicode value of each is obtained. . Convert the Unicode to 16-bit Binary Number. Now Add 8-bits to the left of the 16-bit Binary Number and these 8 bits are calculated as explained in the above algorithm. After getting the 24-Bit Binary Number. Convert this 24-bit binary Number to Hexadecimal number. Now encrypt this number with its corresponding color.

B. Decryption:

The cipher text is scanned convert the color to its corresponding hexadecimal number. After this convert the hexadecimal number to the 24 bit binary number. Remove the 8 starting bits to make the number 16 bit binary number and convert the 16 bit number to corresponding Unicode and then the value of that particular character.

III. EXAMPLES AND DISCUSSION

A. Example of Encryption:

Suppose we have to encrypt a String "Monga".

B. Encryption of 'M':

a. Unicode of M is 0x004d.
b. Binary Conversion of this is :0000000001001101
c. 8 bits that are attached to left of this number are :01001101
d. 24 bit number is : 010011010000000001001101
e. Hexadecimal Conversion is : 4D004D
f. Color corresponding to this value is : ■

C. Encryption of 'o':

a. Unicode of o is 0x006f.
b. Binary Conversion of this is: 0000000001101111.
c. 8 bits that are attached to left of this are: 01101111
d. 24 bit number is : 011011110000000001101111
e. Hexadecimal conversion is : 6F006F
f. Color corresponding to this value is : ■

D. Encryption of 'n':

a. Similarly for n color is :6E006E ■

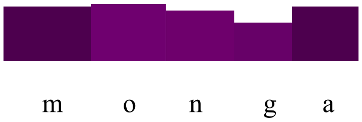
E. Encrption of 'g':

a. Similarly for g color is : 670067 ■

F. Encryption of 'a':

a. Similarly for a color is : 610061 ■

G. Encrption of "Monga":



H. Decryption of"":

a. Hexadecimal Value corresponding to this color is 4D004D.
b. Binary conversion is 010011010000000001001101.
c. Take 16 bits from right that is : 0000000001001101
d. Hexadecimal Number corresponding to this is: 004D
e. Value corresponding to Unicode 004D is 'M'.

I. Similarly we can decrypt the whole colors and get the string "Monga":

IV. CONCLUSION AND FUTURE WORK

By using different colors in the universe (supported by computer) and UNICODE characters, we can implement encryption and decryption. This proposed policy is very simple to implement. But the future projects will provide high security by using different colors and UNICODE characters.

V. REFERENCES

[1]. Ross J. Anderson, "Why Cryptosystems Fail", Communications of the ACM, New York, USA, 1994, pp. 32-40.

[2]. Mulet : A Multilanguage encryption technique 978-0-7695-3984-3/10 © 2010 IEEE 2010 Seventh International Conference on Information Technology .

[3]. R.L. Rivest, "The RC5 encryption algorithm", Proceedings of the 1994 Leuven Workshop on Fast Software Encryption, Springer-Verlag, 1995, pp.86-96.

[4]. William C . Barker, " Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher", National Institute of Standards and Technology, NIST Special Publication 800-67, 2008.

[5]. R.W Collins, " Software localization for Internet software, issues and methods", Software, IEEE, Florida, USA, 2002, pp. 74-80.

[6]. P. Wayner, Disappearing Cryptography : Information Hiding: Steganography and Watermarking. Morgan Kaufmann, 2nd edition, 2002.

[7]. N. F . Johnson and S . Jajodia. Steganalysis of imges created using current steganography software. In IHW'98 – Proceedings of the International Information hiding workshop. April 1998.

[8]. D. R . Stinson, "Cryptography Theory and Practice" CRC Press, Inc., 2002.

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

[10]. Maram Balajee, "Unicode and colors Integration tool for encryption and Decryption" , Vol. 3 No. 3 Mar 2011, IJCSE , ISSN : 0975-3397