UNICODE and Colors Integration tool for Encryption and Decryption

Maram Balajee[1]

[1] Asst. Prof., Dept. of IT, G M R Institute of Technology,
Rajam, Andhra Pradesh, 532127 , India.

***Abstract*---Cryptography, to most people, is concerned with keeping communications private. Indeed, the protection of sensitive communications has been the emphasis of cryptography throughout much of its history. Encryption is the transformation of data into some unreadable form. Its purpose is to ensure privacy by keeping the information hidden from anyone for whom it is not intended, even those who can see the encrypted data. Decryption is the reverse of encryption; it is the transformation of encrypted data back into some intelligible form.**

UNICODE is a computing industry standard for the consistent representation and handling of text expressed in most of the world's writing systems. Developed in conjunction with the Universal Character Set standard and published in book form as The UNICODE Standard, 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, such as character properties, rules for normalization, decomposition, collation, rendering, and bidirectional display order (for the correct display of text containing both right-to-left scripts, such as Arabic or Hebrew, and left-to-right scripts). This paper introduces a new technique for cryptography by using UNICODE and colors in universe (supported by computer).

***Index Terms*—Cryptography, UNICODE, Colors, Encryption, Decryption.**

I. INTRODUCTION

Generally we are using many techniques for encrypting data before sending. For this, there is a need of one common secret key between source and destination. By using that key, the sender encrypts the data. After receiving, the receiver decrypts the received data by using the shared secret key.

Now a days, many tools and techniques are available for crack those shared secret keys.

Now this paper proposed a new policy to encrypting the data by using UNICODE and Colors (supported by computer) in the following sections.

II. EXISTING SYSTEMS

A. *What is Cryptography*?

Cryptography is the study and practice of encoding data using transformation techniques so that it can only be decoded by specific users. In simpler words, it is a theory of secret writing. Practitioners of cryptography are known as cryptographers.

A cryptographic algorithm, or known as cipher, is a mathematical function used in the encryption and decryption method. A cryptographic algorithm functions by blending with a key to encrypt the plaintext. The plaintext can be encrypted in different ways with different keys. The security of cipher text is completely dependent on two things: the power of the cryptographic algorithm and the confidentiality of the key. A cryptographic algorithm, all potential keys and all the protocols that make cryptography work formulate a cryptosystem. Current cryptography methods overlap various subjects like mathematics, computer science, and engineering. ATM cards, computer passwords, and electronic commerce are few examples where cryptography is used.

B. *What is UNICODE?*

ASCII which stands for American Standard Code for Information Interchange became the first widespread encoding scheme. However, it is limited to only 128 character definitions. Which is fine for the most common English characters, numbers and punctuation but is a bit limiting for the rest of the world? They naturally wanted to be able to encode their characters too. And, for a little while depending on where you were, there might be a different character being displayed for the same ASCII code. In the end, the other parts of the world began creating their own encoding schemes and things started to get a little bit confusing. Not only were the coding schemes of different lengths, programs needed to figure out which encoding scheme they were meant to be using.

It became apparent that a new character encoding scheme was needed and the UNICODE standard was created. The objective of UNICODE is to unify all the different encoding schemes so that the confusion between computers can be limited as much as possible. These days the UNICODE standard defines values for over 100,000 characters and can be seen at the UNICODE Consortium. It has several character encoding forms, UTF standing for UNICODE Transformation Unit:

- UTF-8: only uses one byte (8 bits) to encode English characters. It can use a sequence of bytes to encode the other characters. UTF-8 is widely used in email systems and on the Internet.
- UTF-16: uses two bytes (16 bits) to encode the most commonly used characters. If needed, the additional characters can be represented by a pair of 16-bit numbers.
- UTF-32: uses four bytes (32 bits) to encode the characters. It became apparent that as the UNICODE standard grew a 16-bit number is too small to represent all the characters. UTF-32 is capable of representing every UNICODE character as one number.

B.1. Code Points

A code point is the value that a character is given in the UNICODE standard. The values according to UNICODE are written as hexadecimal numbers and have a prefix of "U+". For example to encode the characters I looked at earlier, "A" is U+0041, "a" is U+0061, "1" is U+0031, "#" is U+0023. These code points are split into 17 different sections called planes. Each plane holds 65,536 code points. The first plane, which holds the most commonly used characters, is known as the basic multilingual plane.

B.2. Code Units

The encoding schemes are made up of code units. They are way to provide an index for where a character is positioned on a plane. For instance, with UTF-16 each 16-bit number is a code unit. The code units can be transformed into code points. For example, the flat note symbol " " has a code point of U+1D160 and it lives on the second plane of the UNICODE standard. It would be encoded using the combination of the following two 16-bit code units: U+D834 and U+DD60.

B.3. How many Colors supported by Computer:

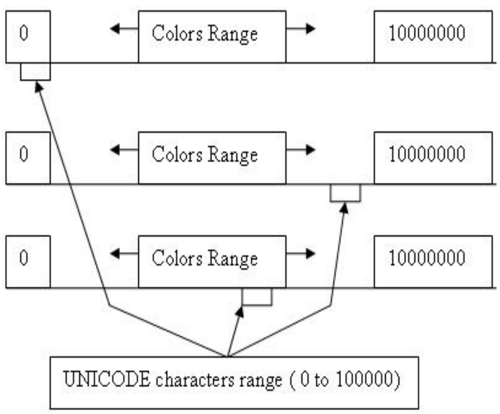
Careful measurements of our visual system’s best performance have been made by psychophysicists (people who study human responses, like seeing color, to things in the world, like light). They have shown that we can see about 1000 levels of light-dark, 100 levels of red-green, and 100 levels of yellow-blue for a single viewing condition in a laboratory. This means that the total number of colors we can see is about 1000 x 100 x 100 = 10,000,000 (10 million). A computer displays about 16.8 million colors to create full color pictures, really more than necessary for most situations. However, the answer is not quite so simple. What color looks like is greatly affected by the viewing conditions. These conditions include the color of the lighting, the amount of lighting, and other colors in the scene. Colors also appear in different modes when they appear on different objects such as surfaces, light sources, or within volumes. Different people also have slight differences in the way they see color. Since we can see at least 10-million colors in a single viewing condition and the variety of viewing conditions and observers is endless, then the only truly correct answer is infinity. If we have 10-million colors, times 10-million lighting types, times 10-million lighting levels, times 10-million surrounding colors, times 6-billion people in the world, times 3 modes of viewing we get a really huge number. The result of that multiplication is 18 followed by 33 zeros (18,000,000,000,000,000,000,000,000,000,000,000), or 18 decillion. That might not quite be infinity, but is close enough since all those estimated numbers are probably on the low side. And there is no way to exactly measure each of them.

III. PROPOSED SYSTEMS

A. *New Policy for Proposed System:*

This proposed policy is fully based on Private-key cryptography. In secret-key cryptography schemes, a single key is used to encrypt data. A secret key may be held by one person or exchanged between the sender and the receiver of a message. If secret-key cryptography is used to send secret messages between two parties, both the sender and receiver must have a copy of the secret key. However, the key may be compromised during transit. If you know the party you are exchanging messages with, you can give them the key in advance. However, if you need to send an encrypted message to someone you have never met, you'll need to figure out a way to exchange keys in a secure way. One method is to send it via another secure channel or even via overnight express, but this may be risky in some cases.

In this proposed new policy, the sender will decide the range of colors which will be assigned to 1, 00,000 UNICODE characters. The selection of Colors is in the following way:



In this proposed new policy, the sample binding between character / symbol/digit, UNICODE and Color is in the following way:

Char	UNICODE	Color
a	U+0041	
b	U+0042	
c	U+0043	
d	U+0044	
e	U+0045	
f	U+0046	
g	U+0047	
h	U+0048	

Fig 1: Sample mapping of Char/symbol/digit, UNICODE and Color.

B. *What is the use of Private-key?*

A computer displays about 16.8 million colors to create full color pictures, really more than necessary for most situations. Now we are considering 10 million Colors only. And the UNICODE standard defines values for over 100,000 characters and can be seen at the UNICODE Consortium.

Now 10 million colors and 100,000 characters are available in a computer system.

Now we can create a dynamic mapping table like Fig 1. If private key is 225,001. The 225,001st color is assigned to the first UNICODE character. The 225,002nd color is assigned to the second UNICODE character. And so on. Finally the 325,000th color is assigned to 100,000 UNICODE character.

C. *Encryption:*

This is new kind of cryptography is fully based on UNICODE and colors. First of all, it checks each and every character in the given file. Then it finds what the equaling UNICODE of each character is. Then simply give the corresponding color for each UNICODE character according to the predefined mapping.

In this way, we can create a color-chart of each page of text. In private-key cryptography, a single key is shared by sender and receiver.

According to the private-key, the dynamic mapping table is created before encryption.

Next, it takes the first character from text and finds the UNICODE. According to the UNICODE, it will take the equaling color. Then it will take the 2nd character and so on.

Now all characters are translated into corresponding colors. It means, all characters are encrypted into colored-charts.

D. Decryption:

The sender and receiver know the private-key. According to private-key, the receiver prepares a mapping between alphabet/special character/digit, UNICODE and Color. By using this chart, the receiver easily identify the COLOR->UNICODE->character.

IV. EXPLANATION WITH EXAMPLE

A. Encryption & Decryption - Pictorial Representation:

Suppose we want to encrypt the following message: “balajeem”

Now the above message is translated into the following:

The message “balajeem” is translated into the following UNICODE characters:

balajeem->U+0042 U+0041 U+006C U+0041 U+0051 U+0045 U+0045 U+006D

B. Encryption:

Then these UNICODE characters are translated into the following colored-chart.

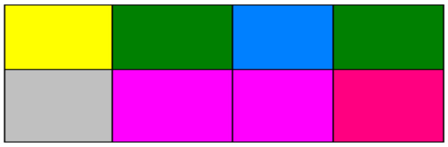


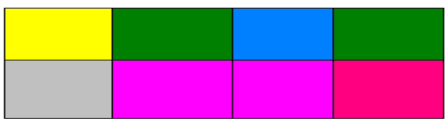
Fig 2: Colored Chart of Message

After receiving the colored-chart, the receiver prepares Mapping between alphabet / special character / digit, UNICODE and Color. According to private-key it is very simple to find equaling UNICODE then character.

C. Decryption:

By using the mapping table like Fig 1, we can decrypt the encrypted message like the following:

Step 1:



Step 2:

 =>U+0042=>b

=>U+0041=>a

=>U+006C=>l

=>U+0041=>a

=>U+0050=>j

=>U+0045=>e

=>U+0045=>e

=>U+006D=>m

Step 3:

It collects and combines each character. In this way, it will get back the original string “balajeem”.

V. CONCLUSION

By using different colors 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 colors and UNICODE characters.

References

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

[2] 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.

[3] http://en.wikipedia.org

[4] http://www.joelonsoftware.com

[5] D. R. Stinson, “Cryptography Theory and Practice” CRC Press, Inc., 2002.

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

AUTHOR [1]: MARAM BALAJEE, is working as a Asst. Prof in GMR Inst. Of Tech., Rajam, Andhra Pradesh, INDIA. Educational Qualifications are M.Sc(IT) and M.E(CSE) from Anna University. I presented 5 papers in National Conferences, 2 papers in International Conferences and 1 journal (IJRTE 2010- May Issue). And he is a Member of MIACSIT & MCSI.