Text Cryptography Based on Three Different Keys

Omar Fitian Rashid[1]
omar.fitian@hiuc.edu.iq

Mohammed Jasim Mohammed[2]
mohammed.jasim@hiuc.edu.iq

Mustafa Tareq[1]
mstfman@gmail.com

Abstract: Secure information transmission over the internet is becoming an important requirement in data communication. These days, authenticity, secrecy, and confidentiality are the most important concerns in securing data communication. For that reason, information hiding methods are used, such as Cryptography, Steganography and Watermarking methods, to secure data transmission, where cryptography method is used to encrypt the information in an unreadable form. At the same time, steganography covers the information within images, audio or video. Finally, watermarking is used to protect information from intruders. This paper proposed a new cryptography method by using three different keys to make the system harder to break by outsider attackers (where the 1st and 3rd encryptions keys are numerical keys, while the 2nd key is string). This system is done based on seven steps; the first step is converting the plaintext based on the first generated key that leads to substitute each character in plaintext, the second step is embedding second generated key with the message that want to send, the third step is done by converting text to their equivalent ASCII format. The fourth step is converting these ASCII format to Binary numbers; then, these numbers are shifted based on the third generated key. These binary numbers are converted to ASCII, and the last step is to convert ASCII to their equivalent characters. The achieved text is the ciphertext that will be sent.

Keywords: Text Cryptography; Cryptography; Plaintext; Ciphertext.

[1] Dr.: Department of Computer Technology Engineering, Al-Hikma University College, Baghdad, Iraq.
[2] Dr.: Department of Medical Instrumentation Engineering Techniques, Al-Hikma University College, Baghdad, Iraq

1. Introduction

Cryptography was firstly used in the past as nonstandard symbolic representations, the main purpose is to send a message in coded design, and the receiver can easily understand the message. After that, they were comprised of covering a move of paper around a chamber and afterwards denoting the message on the paper. The unrolled paper was then shipped off to the beneficiary, who could without much of a stretch decipher the message on the off chance that he knew the measurement of the special chamber [1].

Earlier cryptography methods were simple; these methods were called the classical cryptography methods. The evolution of the internet and its use also led to thinking of enhancing these methods or proposing new ideas for cryptography. This led to proposed more complex algorithms such as symmetric-key cryptography and asymmetric key cryptography. Symmetric key methods can implement either based on stream cipher or block cipher, where the stream cipher encrypts the plaintext by encrypting character by character, while block cipher encrypts as a whole. Symmetric key cryptography proved to be very effective unless Diffie and Hellman showed some of its loopholes in 1977 and proposed public-key cryptography [2]. After that, several new attempts were tried to build a new idea for encryption methods; an example of these methods is the systems proposed by [3, 4, 5, 6, and 7]. Any cryptography system must contain the following parts:

- **Plaintext:** it is the main text (original text) that the sender wants to send it to the receiver.
- **Ciphertext**: is the incomprehensible message is received after an encryption method is applied to the original text.
- **Encryption Algorithm:** It applied different methods, such as replacement and change on the plaintext to achieve the ciphertext.
- **Decryption Algorithm:** It is the inverse system of encryption strategy. To achieve the main plaintext, it used both ciphertext and key.
- **Secret key:** this key worth is free of plaintext and calculation. Contingent upon the key being utilized, the calculation gives a different yield. The specific activity performed on that calculation relies upon the key [8].

The encryption process is shown in Figure 1.

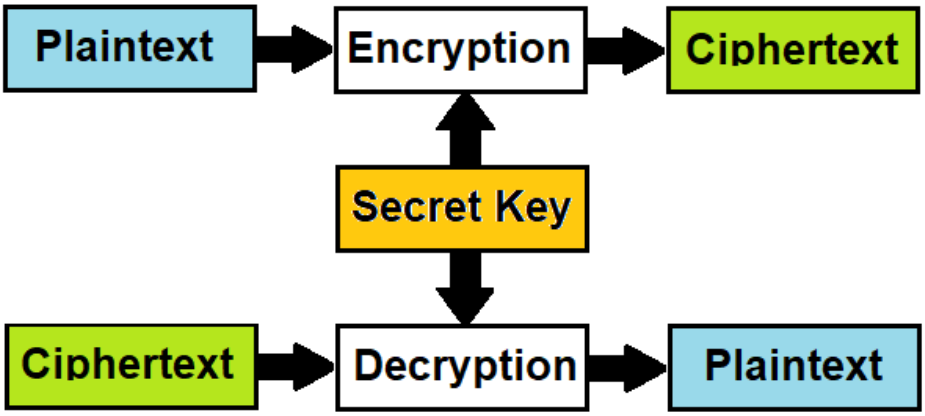

Figure 1: The encryption processes

2. Materials and Methods

The proposed cryptography method consists of two phases; encryption and decryption. This system is done based on seven steps; the first step is converting the plaintext based on the first generated key that leads to substitute each character in plaintext, the second step is embedding second generated key with the message that want to send, the third step is done by converting text to their equivalent ASCII format. The fourth step is converting these ASCII format to Binary numbers; then, these numbers are shifted based on the third generated key. These binary numbers are converted to ASCII, and the last step is to convert ASCII to their equivalent characters. The achieved text is the ciphertext that will be sent.
Where the encryption phase is located on the sender side and used to encrypt the message before sending it to the receiver, this phase contains five steps of data conversion, as shown in Figure 2.

Step 1: Replace each character in plaintext with its equivalent character based on the key-value (first encryption key).
Step 2: Embed a string key (second encryption key) with the encryption text.
Step 3: Convert each character in encryption text to their equivalent ASCII value (example: character “a” equal to 99 in ASCII).
Step 4: Convert each ASCII value into binary format (example: 99 in ASCII equals 01100011 in binary).
Step 5: Shift each number in binary based on the key-value (third encryption key).

Step 6: Convert every eight binary number to an ASCII value (example: 01100011 in binary equals 99 in ASCII).
Step 7: Convert each ASCII value to its equivalent character (example: 99 in ASCII equals to the character "a"). The achieved text is the ciphertext that will be sent.

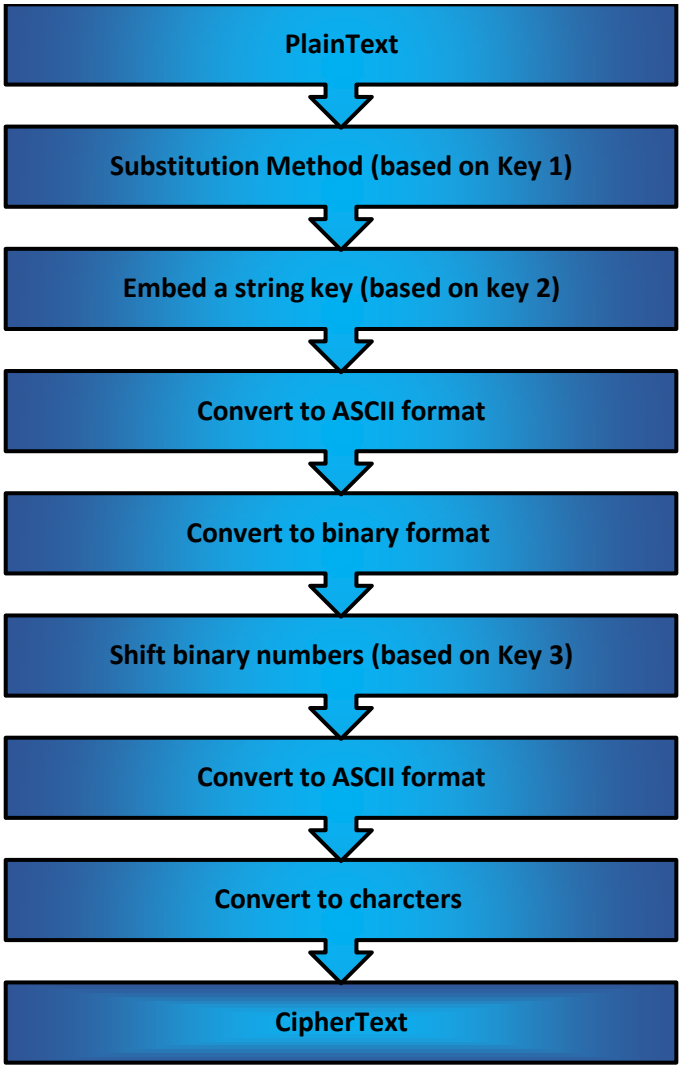

Figure 2: Encryption phase

While decryption phase is located on the receiver side, and it is used to decrypt a message received from the sender. This phase contains five steps which are the same steps on the sender side but in reverse order, as shown in Figure 3. These steps are:

Step 1: Convert each character in ciphertext to their equivalent ASCII value.
Step 2: Convert each ASCII value into binary format.
Step 3: Shift each number in binary based on the key-value (third encryption key).
Step 4: Convert every eight binary numbers to ASCII value.
Step 5: Convert each ASCII value to its equivalent character.
Step 6: Remove a string key (second encryption key).
Step 7: Replace each character in ciphertext with its equivalent character based on the key-value (first encryption key). The achieved text is the original text (plaintext).

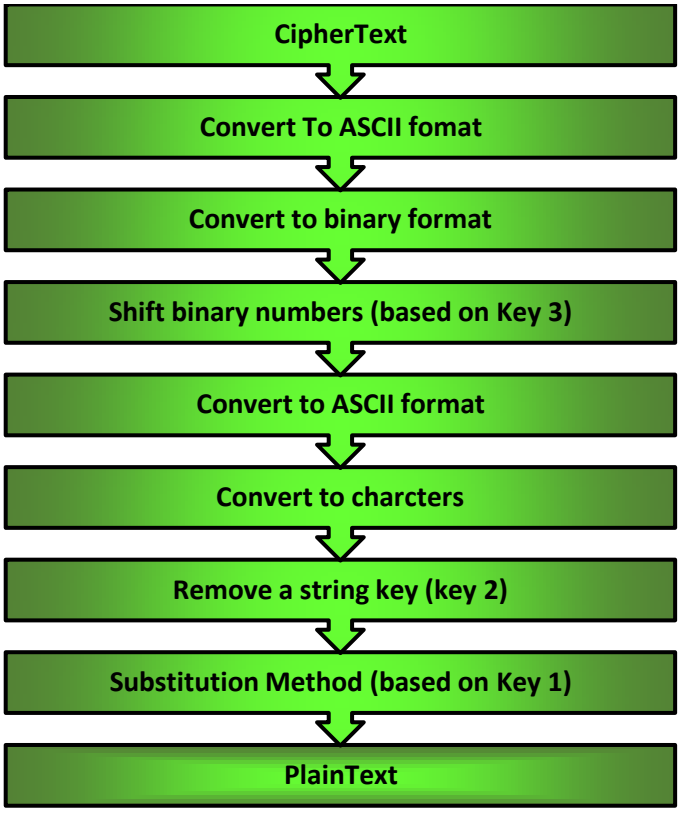

Figure 3: Decryption phase

3. Results and Discussions

To perform the above procedure of encryption to secure the transferred information, the following example will highlight the result of the currently proposed method.

Encryption steps example, where the plaintext is "An example of plaintext to test the encryption steps", where the 1st encryption key is 7, 2nd encryption key is “String key”, and 3rd encryption key is 5.

Step 1: Replace each character in plaintext to its equivalent character based on 1st encryption key:

Hu'l□htwsl'vm'wshpu{l□{'{v'{lz{'{ol'lujy€w{pvu'z{lwz

Step 2: Embed 2nd encryption key with the encryption text:

HSut'rli□nhgt wksely'Svtmr'iwnsgh pkue{ylS□t{r'i{nvg' {klezy{S't{roiln'gl ukjeyy€Swt{rpivnug' zk{elywSzt

Steps 3 & 4: Convert each character in encryption text to their equivalent ASCII value, then convert these values into binary format:

010010000101001101110101011101000010011101110010011011000110100101
111111011011100110100001100111011101000010000001110111011010110111
001101100101011011000111100100100111010100110111011001110100011011
010111001000100111011010010111011101101110011100110110011101101000
001000000111000001101011011101010110010101111011011110010110110001
010011011111110111010001111011011100100010011101101001011110110110
111001110110011001110010011100100000011110110110101101101100011001
010111101001111001011110110101001100100111011101000111101101110010
011011110110100101101100011011100010011110110011101101100001000000 1
110101011010110110101001100101011110010111100110000000010100110111
011101110100011110110111001001110000011010010111011001101110011101
010110011100100111001000000111101001101011011110110110010101101100
011110010111011101001101111010011101 00

Step 5: Shift each number in binary based on 3rd encryption key:

101000100100001010011011101010111010000100111011100100110110001101
001011111110110111001101000011001110111010000100000011101110110101
101110011011001010110110001111001001001110101001101110110011101000
110110101110010001001110110100101110111011011100111001101100111011
010000010000001110000011010110111010101100101011110110111100101101
100010100110111111101110100011110111011001000100111011010010111101
101101110011101100110011100100111001000000111101101101011011011000
110010101111010011110010111101101010011001001110111010001111011011
100100110111101101001011011000110111000100111011001110110110000100
000011101010110101101101010011001010111100101111001100000000101001
101110111011101000111101101110010011100000110100101110110011011100
111010101100111001001110010000001111010011010110111101101100101011
011000111100101110111010100110111101001 1

Steps 6 & 7: Convert every eight binary number to an ASCII value, then convert each ASCII value to their equivalent character, which is considered as the cipher text for this example:

¢B›«¡;“cKûsC;¡————————————————»[›+cÉ:›³£k‘;K»s›;A
————————————————ƒ[«+ÛËb›û£Û‘;KÛs³99
————————————————Û[c+ÓËÚ™;£Û“{Kcq;;a
————————————————«[S+ËÌ›»£Û“ƒK³s«99————————————————
Ó[Û+cË°›Ó

Encoding and decoding times are calculated for the proposed system, the times for encryption and decryption steps in terms of milliseconds (ms) for two files with different sizes (1K and 5K) are shown in Table 1.

Table 1: Encryption and decryption times

Size	Total Characters numbers	Encryption Time (ms)	Decryption Time (ms)
1K	1001	1.221	1.893
5K	5160	8.182	11.412

4. Conclusions

In this paper, a new cryptography method is proposed to secure the transmission of text over the internet. This is done by using three keys to make the system more difficult to broke by outside attackers. This system is done by first converting the plaintext base on first generated key by substitution each character in plaintext, then embedding second generated key with the message that wants to send, after that, convert it to their equivalent ASCII format, then convert ASCII format to Binary number, then these numbers are shifted based on third generated key, then these binary numbers are converting to ASCII, and finally convert ASCII to their equivalent characters. The achieved text is the ciphertext that will be sent. For future work, the proposed method can be enhanced by add another level of encryption, or use more complicated encryption techniques.

References

[1] Kumar Sharma, D., Chidananda Singh, N., Noola, D. A., Nirmal Doss, A., & Sivakumar, J. (2021). A review on various cryptographic techniques & algorithms. Materials Today: Proceedings.

[2] Bhardwaj, A. & Som, S. (2016). 'Study of different cryptographic technique and challenges in future. 2016 1st Int. Conf. Innov. Challenges Cyber Secur. ICICCS 2016, 208–212.

[3] Singh, V. K., Pandey, S., Degadwala, S. & Vyas, D. (2022). DNA and KAMLA Approaches in Metamorphic Cryptography: An Evaluation. 2022 Second International Conference on Artificial Intelligence and Smart Energy (ICAIS), 1173-1178.

[4] Kumar, M., Soni, A., Shekhawat, A. R. S. & Rawat, A. (2022). Enhanced Digital Image and Text Data Security Using Hybrid Model of LSB Steganography and AES Cryptography Technique. *2022 Second International Conference on Artificial Intelligence and Smart Energy (ICAIS), 1453-1457.*

[5] Ji, X., Wang, B., Hu, F., Wang, C. & Zhang, H. (2022). New advanced computing architecture for cryptography design and analysis by D-Wave quantum annealer. In Tsinghua Science and Technology, 27(4), 751-759.

[6] Kundi, D., Zhang, Y., Wang, C., Khalid, A., O'Neill, M. & Liu, W. (2022). Ultra High-Speed Polynomial Multiplications for Lattice-based Cryptography on FPGAs. in IEEE Transactions on Emerging Topics in Computing.

[7] Rashid, O. F. (2021). Text Encryption Based on DNA Cryptography, RNA, and Amino Acid. The 5th International Multi-Conference on Artificial Intelligence Technology (MCAIT 2021).

[8] Hilarie, O. (2014). Recent Parables in Cryptography. IEEE Internet Computing, 18(1), 82–86.

تشفير النص بالاعتماد على ثلاثة مفاتيح مختلفة

عمر فتيان رشيد[1] محمد جاسم محمد[2] مصطفى طارق عبد[1]
omar.fitian@hiuc.edu.iq mohammed.jasim@hiuc.edu.iq mstfman@gmail.com

المستخلص: أصبح النقل الآمن للمعلومات عبر الإنترنت مطلبًا مهمًا في اتصال البيانات. في هذه الأيام ، تعد المصداقية والسرية من أهم الاهتمامات في تأمين اتصالات البيانات. لهذا السبب ، يتم استخدام طرق إخفاء المعلومات ، مثل أساليب التشفير وإخفاء المعلومات والعلامات المائية ، لتأمين نقل البيانات ، حيث يتم استخدام طريقة التشفير لتشفير المعلومات في شكل غير قابل للقراءة. في الوقت نفسه ، طرق إخفاء المعلومات تستخدم لاخفاء المعلومات في الصور أو الصوت أو الفيديو. أخيرًا ، يتم استخدام العلامة المائية لحماية المعلومات من المتسللين. اقترحت هذه الورقة طريقة تشفير جديدة باستخدام ثلاثة مفاتيح مختلفة لجعل اختراق النظام أكثر صعوبة من قبل المهاجمين الخارجيين (حيث يكون مفتاحا التشفير الأول والثالث مفاتيح رقمية ، بينما المفتاح الثاني عبارة عن سلسلة). يتكون هذا النظام من سبع خطوات ؛ تتمثل الخطوة الأولى في تحويل النص العادي بناءً على المفتاح الاول الذي تم إنشاؤه والذي يؤدي إلى استبدال كل حرف في نص عادي ، والخطوة الثانية هي تضمين المفتاح الثاني الذي تم إنشاؤه مع الرسالة التي تريد إرسالها ، ويتم تنفيذ الخطوة الثالثة عن طريق تحويل النص إلى قيم ASCII. الخطوة الرابعة هي تحويل تنسيق ASCII إلى أرقام ثنائية ؛ بعد ذلك ، يتم تحريك هذه الأرقام بناءً على المفتاح الثالث الذي تم إنشاؤه. ثم يتم تحويل هذه الأرقام الثنائية إلى ASCII ، والخطوة الأخيرة هي تحويل ASCII إلى الأحرف المكافئة لها. النص الذي تم تحقيقه هو النص المشفر الذي سيتم إرساله.

الكلمات المفتاحية: تشفير النص، التشفير، النص العادي، النص المشفر

[1] مدرس دكتور: قسم هندسة تقنيات الحاسوب - كلية الحكمة الجامعة – بغداد – العراق
[2] مدرس دكتور: قسم هندسة تقنيات الاجهزة الطبية - كلية الحكمة الجامعة – بغداد - العراق