International Journal of Computer Science and Software Engineering (IJCSSE), Volume 9, Issue 3, March 2020
ISSN (Online): 2409-4285 www.IJCSSE.org Page: 12-15

Mapping Character Position Based Cryptographic algorithm with Numerical Conversions

MahmudulHasan Moon[1], A K M Tanzimul Islam Tanim[2], Md. Zillani Shoykot[3], Md. Nahid Sultan[4], U.A. Md. Ehsan Ali[5] and Emran Ali[6]

[1, 2, 3, 4, 5, 6] Faculty of Computer Science and Engineering, Hajee Mohammad Danesh Science and Technology University (HSTU), Dinajpur-5200, Bangladesh

[1]mahmudulmoon123@gmail.com, [2]tanim_cse12@gmail.com, [3]shoykot_cse13@gmail.com, [4]nahid.sultan@hstu.ac.bd, [5]ehsan_cse@hstu.ac.bd, [6]emran.cse@hstu.ac.bd

ABSTRACT

Security of data is the challenging aspects of modern information technology. An improved cryptology algorithm is introduced in this paper to offer comparatively higher security. We divide our message into several blocks as 8bits per block then convert each character into its corresponding positional number, where uppercase letters, lowercase letters, digits and special characters are mapped into some range of numbers. Then replace each decimal number into their binary equivalent consisting of 7-bits. Then combine 8 blocks of binary numbers into a single string. After performing some operation on the data, we get the final encrypted message. For decryption, we use same method in reverse way. Taking the decrypted message we perform some basic operation as replacing by binary or equivalent decimal and position then we get the original message back. Though the length of the encrypted message is larger than original message in this proposed algorithm, it offers higher security for the real-time communications.

Keywords: *Cryptography, Encryption and decryption, Position based Cryptography, Higher level of security, ASCII conversions, Numerical Conversions.*

1. INTRODUCTION

During this time when the Internet provides essential communication between tens of millions of people and is being increasingly used as a tool for commerce, security becomes a tremendously important issue to deal with. There are many aspects to security and many applications, ranging from secure commerce and payments to private communications and protecting passwords .One essential aspect for secure communications is that of Cryptography [1].Cryptography is a big deal in the present era of information and communication technology. Though it has been used for thousands of years to hide secret messages, systematic study of cryptology as a science (and perhaps an art) just started around one hundred years ago [2]. The cryptography is the study of mathematical techniques related to aspects of information security such as confidentiality, data integrity, entity authentication and data origin authentication [3]. Also it means hidden writing, and it refers to the practice of using encryption to conceal text [4]. The major security goals that are of concern to the cryptography are confidentiality, authentication, integrity, non-repudiation and access control [5]. Among the available three modern security offering techniques namely cryptography, steganography and watermarking, cryptography is the base to understand and also easy to implement ensuring a higher level of security in the real-time security systems. In this paper, we proposed a new cryptographic algorithm which follows a different methodology from the traditional symmetric-key cryptography, asymmetric-key cryptography or numerical function.

2. RELATED WORK

Several works have been done to develop a new cryptographic algorithm for a higher level of security.
A new cryptographic algorithm for the Real Time Applications was proposed by A. H. Omari, M.B. Al-Kasasbeh, E. R. Al- Qutaish, and M. I. Muhairat to improve the time for encryption and decryption of data of end-to-end delay and to provide higher level of security [6].Some researchers have developed a secure hybrid mode-based cryptosystem which provides greater security level than that schemes based on a single hard problem. The enemy or adversary has to solve the two problems simultaneously which is unlikely to happen in order to read any secret message [7].A new cryptosystem based on factoring and discrete logarithm problems which provides longer and higher security level than that schemes based on a single hard problem was proposed by E.S. Ismail and M.S.N. Hijazi. The adversary has to solve the two problems simultaneously in order to recover a corresponding plaintext from the received cipher-text [8].

Some researchers have developed a new cryptosystem using multiple cryptographic assumptions which offers a greater security level than that schemes based on a single cryptographic assumption [9].S. Kumar, Addagarla, and Y. Babji made a comparative security study on symmetric key cryptosystem based algorithms such as DES, TDES, IDEA, and AES [10].A basic study on cryptography which is a solution for information security threats has been shown in [11].

3. ENCRYPTION PHASE

In the encryption phase of the proposed algorithm, at first the input characters of the text to be encrypted are divided into several packets of N characters taking in order from the beginning character, where the value of N is 8 which may vary only for the last packet as the last packet contains the remaining characters. For example, if a text consists of 20 characters, the first 8 characters constitute the first packet, the subsequent 8 characters constitute the second packet and the remaining 4 characters constitute the last packet. Secondly, convert each character into its corresponding positional number, where uppercase letters are mapped into 1-26 and lowercase letters are mapped into27-52,digits are mapped into 53-62 and special characters are mapped into 63-90.Then replace each decimal number into their binary equivalent consisting of 7-bits because to represent the special characters we need to take minimum of 7-bits and combine 8 blocks of binary numbers into a single string. Then convert whole binary string that we got from previous step into its decimal equivalent and again convert each digit of the decimal number into its ASCII value and create binary matrix[18,6] by converting the ASCII values to its binary equivalent.The total bits needed to represent the 8 characters is 56 i,e 8*7=56 and the number of rows must be 18 i,e (2^57)-1=18 digit number. Now to represent the 18 bits binary number we need to take at least 6 bits decimal digits i,e (2^19)-1=6 digit decimal number. For each column, at last, we got the encrypted message as 6-digit decimal number by converting binary number.

3.1 Pseudo code of Encryption

1. Input original message.
2. Divide the original message into several blocks of 8 characters.
3. For each packet:
a. Convert each character into its corresponding positional number, where uppercase letters are mapped into 1-26 and lowercase letters are mapped into27-52, digits are mapped into 53-62 and special characters are mapped into 63-90.
b. Convert each decimal number into their binary equivalent.
c. Combine the 8 binary numbers into a single string.
d. Convert whole binary string that we got from previous step into its decimal equivalent.
e. Convert each digit of the decimal number into its ASCII value.
f. Create binary matrix by converting the ASCII values to its binary equivalent.
g. For each column:
i. Convert the binary number to its 6-digit decimal number.
ii. Combine each 6-digit decimal number to a single string.
4. End of encryption.
5. Finally got the encrypted message.

4. DECRYPTION PHASE

In the decryption phase of the algorithm, at first, convert the 6-digit decimal number into its binary equivalent and put them in column wise to create a binary matrix. Consider the each row, Convert the binary number to its decimal equivalent and consider this decimal number as ASCII value and replace them with their equivalent character. Then combine all the characters as a single string and consider it as a single decimal number and convert this decimal number into its binary equivalent. Divide the whole binary string into several blocks of 7-bits. For each 7-bit block, convert the binary number to its equivalent decimal. Replace each decimal positional number with their mapped character. At last, we got the decrypted original message by combining each block of 8 characters to a single string.

4.1 Pseudo code of Decryption

1. Input encrypted message.
2. For each packet:
a. Divide the encrypted string into 6-digit decimal number.
b. Convert the 6-digit decimal number into its binary equivalent and put them in column wise to create a binary matrix.
c. For each row:
i. Convert the binary number to its decimal equivalentand consider this decimal number as ASCII value and replace them with their equivalent character.
ii. Combine all the characters as a single string and consider it as a single decimal number.
d. Convert this decimal number into its binary equivalent.
e. Divide the whole binary string into several blocks of 7-bits.
f. For each 7-bit block:
i. Convert the binary number to its equivalent decimal.

g. Replace each decimal positional number with their mapped character.
h. Combine each block of 8 character to a single string.
3. End of Decryption.
4. Finally got the decrypted main message.

5.1 Implementation of Encryption

As an example, let's consider that the user wants to encrypted then conceal the message "My No-12LOW". According to the discussion the algorithm divides the input into 2 packets, where the first one contains the first 8 characters "My No-12" and the last contains the subsequent three characters "LOW" as shown below:

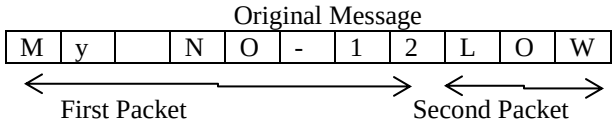

Fig-5.1: Dividing the Original Message into 2 Packets

As the explanation in the encryption phase the characters of each packet are converted to their equivalent positional number. Then using the 7-bit binary equivalent of the positional number. Then combine all 8 binary numbers into a single string and convert the binary string into into corresponding decimal number.

M	y	blank	N	o	-	1	2
13	51	63	14	41	68	54	55
0001101	0110011	0111111	0001110	0101001	1000100	0110110	0110111

7544818275261239

Now, Convert each digit of the decimal number into its ASCII value and convert the value to its equivalent binary.

Character ASCII value Binary equivalent

Character	ASCII	Binary
7	55	110111
5	53	110101
4	52	110100
4	52	110100
8	56	111000
1	49	110001
8	56	111000
2	50	110010
7	55	110111
5	53	110101
2	50	110010
6	54	110110
1	49	110001
2	50	110010
3	51	110011
9	57	111001

Now create binary matrix by using the binary equivalent,

1	1	0	1	1	1
1	1	0	1	0	1
1	1	0	1	0	0
1	1	0	1	0	0
1	1	1	0	0	0
1	1	0	0	0	1
1	1	1	0	0	0
1	1	0	0	1	0
1	1	0	1	1	1
1	1	0	1	0	1
1	1	0	0	1	0
1	1	0	1	1	0
1	1	0	0	0	1
1	1	0	0	1	0
1	1	0	0	1	1
1	1	1	0	0	1
065535	065535	002561	061648	033206	050379

Now combine the each 6-digit decimal number into a single string.

Finally get the encrypted message.

065535065535002561061648033206050379

5.2 Implementation of Decryption

Divide the encrypted message into 6 digit decimal number. Then convert the decimal number into equivalent binary and put them in column wise to create a binary matrix.

065535065535002561061648033206050379

065535	065535	002561	061648	033206	050379
1	1	0	1	1	1
1	1	0	1	0	1
1	1	0	1	0	0
1	1	0	1	0	0
1	1	1	0	0	0
1	1	0	0	0	1
1	1	0	0	1	0
1	1	0	0	1	1

1	1	0	0	1	0
1	1	0	1	1	1
1	1	0	1	0	1
1	1	0	0	1	0
1	1	0	1	1	0
1	1	0	0	0	1
1	1	0	0	1	0
1	1	0	0	1	1
1	1	1	0	0	1

Now convert the binary number of each row into its decimal equivalent and consider this decimal value as ASCII value and replace them with their equivalent character.

Binary	ASCII	Character
110111	55	7
110101	53	5
110100	52	4
110100	52	4
111000	56	8
110001	49	1
111000	56	8
110010	50	2
110111	55	7
110101	53	5
110010	50	2
110110	54	6
110001	49	1
110010	50	2
110011	51	3
111001	57	9

Now combine the each character into a single decimal string.

7544818275261239

Convert this decimal number into binary equivalent and divide the binary number into several blocks of 7-bits.Then convert the each 7-bit binary number into decimal equivalent and replace them with their mapped position.

7544818275261239

0001101	0110011	0111111	0001110	0101001	1000100	0110110	0110111
13	51	63	14	41	68	54	55
M	y	blank	N	o	-	1	2

6. CONCLUSION

As cryptography is a big deal in all type security systems, this developed algorithm will be a great part for the same. We presented the algorithm based on numerical conversions. We emphasized mainly on the concealing of the encrypted message ensuring a better security. Our method essentially block cipher method and it will take less time if the file size is large. The important thing of our proposed method is that it is almost impossible to break the encryption algorithm without knowing the exact key value. We ensure that this method can be applied for data encryption and decryption in any type of public application for sending confidential data.

REFERENCES

[1] Ayushi, ”A Symmetric Key Cryptographic Algorithm”, International Journal of Computer Applications (0975-8887) Volume 1 - No. 15, 2010.
[2] Sidhpurwalahuzaifa. A Brief History of Cryptography.[Online]. Available: https://securityblogs.redhat.com/2013/08/14/a-brief-history-of-cryptography.
[3] E. Cole, R. Krutz and J. W. Conley, Network Security Bible, Wiley Publishing Inc, 2005.
[4] A. Menezes, V. Oosrschot and A. Vanstone, Handbook on Applied Cryptography, CRC Press Inc., NY, USA, 2000.
[5] D. Stinson, Cryptography Theory and Practice, CRC Press Inc., NY, USA, 1995.
[6] S. Hebert, “A Brief History of Cryptography”, an article available at http:// cybercrimes.net/aindex.html
[7] A. H. Omari, B. M. Al-Kasasbeh, R. E. Al-Qutaish, and M. I. Muhairat, “A New Cryptographic Algorithm for the Real Time Applications”, Proc. of the 7th WSEAS International Conference on INFORMATION SECURITY and PRIVACY (ISP), pp. 33-38, 2008.
[8] E.S. Ismail and S. Baharudin, “Secure Hybrid Mode-Based Cryptosystem”, American Journal of Applied Sciences, vol.9, no.3, pp.289-292, 2012.
[9] E.S. Ismail and M.S.N. Hijazi, “A New Cryptosystem Based on Factoring and Discrete Logarithm Problems”, Journal of Mathematics and Statistics, vol. 7, no.3, pp. 165-168, 2011.
[10] E.S. Ismail and M.S. Hijazi, “New Cryptosystem Using Multiple Cryptographic Assumptions”, Journal of Computer Science, vol. 7 no.12, pp. 1765-1769, 2011.
[11] S. Kumar, Addagarla, and Y. Babji, “A Comparative Security Study Review on Symmetric Key Cryptosystem Based Algorithms”, International Journal of Computer Science and Mobile Computing, vol. 2, no.7, pp.146– 151, 2013.
[12] M.V. Kumar, “Cryptography – A solution for information security Threats”, Golden Research Thoughts, vol. 2, no.1, 2013.