www.ijecs.in
International Journal Of Engineering And Computer Science ISSN: 2319-7242
Volume 4 Issue 8 Aug 2015, Page No. 14058-14062

Improving Playfair Algorithm To Support User Verification And All The Languages In The World Including Kurdish Language

Omed Hassan Ahmed, Aram Mahmood Ahmed, Sarkar Hasan Ahmed
College of Science and Technology
University of Human Development
aramteesside@yahoo.co.uk
Network Department/CSI
Sulaimani Polytechnic University
aram_mahmud@yahoo.com
Network Department/CSI
Sulaimani Polytechnic University
sarkarhasan@gmail.com

***Abstract* - communicating over any untrusted medium or network requires privacy and authentication; cryptography plays an important role in this area. Original Playfair cipher is one of the early cryptographic algorithms that uses a 5x5 matrix. It supports English language merely and can be cracked easily. It has being improved in different aspects. This paper, firstly, improves the algorithm to support the Kurdish language script. This is achieved by using a 256X256 matrix that meanwhile increases the security of the algorithm dramatically. Secondly, the proposed algorithm is coupled with a hash function (sha512) to achieve user verification. For this a software is designed and implemented based on software development concepts.**

keywords- playfair cipher, encryption, decryption, Unicode, computer network, software development, sha512, Kurdish

I. Introduction

Cryptography is the art of storing and transmitting data in a mangled form so that only authenticated users are able to read and process it. There are three types of cryptography: firstly, Secret Key cryptography which uses a single key for encryption and decryption; secondly, Public Key cryptography which uses one key for encryption and another for decryption. Finally, Hash function which uses a mathematical formula to encrypt information which is irreversible i.e. it is one way encryption[1]. Traditional Playfair is one of the secret key algorithms that had many shortcomings. Researchers have found different methods to enhance it such as extending the matrix, using LFSR(Linear Feedback Shift Register), using RSA concept, etc. Yet, despite of not supporting many available characters, it does not support kurdish language and many other languages. In addition, dictionary attack which is guessing the key through meaningful combinations of characters is also expected. In our approach a matrix will be created that holds the value of all the possible known characters in the world. Plus, a hash function will be used to stand against dictionary attack. sha512 technique is a decent candidate to be used as a hash function because it is proven to be more secure than the other techniques

DOI: 10.18535/ijecs/v4i8.78

II. Literature Review

Playfair algorithm was originally invented by Charles Wheatstone in 1854. It uses a 5x5 matrix to produce the cipher text. Researchers have so far improved it mainly in four aspects which are: extending the table, using Linear Feedback Shift Register (LFSR), using RSA algorithm, and using 3D-playfair cipher.

1. Extension of the table: originally the table was 5X5. Later, in order to overcome the restrictions (7X4, 6X6 ,16X16, etc.) matrices were proposed. For more details refer to [2].

2. Linear Feedback Shift Register (LFSR): LFSR was introduced in order to increase the security and performance of the algorithm by producing pseudo-random sequences. It is a number of connected flip-flops where their outputs will be the input for the next state using a linear function. The linear function of single bits are XOR and inverse-XOR. The initial value of LFSR is called seed; the output is determined by the previous state totally. Thus, in order to obtain pseudo random sequences, changing the taps is used which plays as a secondary key to the algorithm[3]. It is proven that LFSR enhances the security of the algorithm noticeably [4].

3. RSA algorithm: it is a public key cryptographic algorithm. It is basically meant to overcome the key transmission problems existing in single key algorithms. This is because in RSA two keys are used (public key for encryption and private key for decryption). The private key is only known to the receiver and he is supposed to be the only one who is able to decrypt the cipher. Considering time and resources, this is also breakable though. However it provides security to a decent extend. Reference [5] used RSA to help playfair algorithm transfer the key in a secure way by encrypting the playfair key using RSA. Next, modified RSA was used for the same purpose. This version of RSA is stronger because it uses four different keys in the process. For more details refer to [6,7].

4. 3D-playfair: it is introduced in order to obtain a great ratio of diffusion and confusion. It uses a 4X4X4 matrix. Furthermore, it divides the plaintext into groups of three letters known as trigraphs and treats them as a single unit. The text is mangled using substitution techniques[8]. Since the structure of the algorithm is well known, it can be breakable if part of the plain text was known to the intruder. Therefore additional bitwise operation technique can be coupled with the algorithm to overcome this restriction [9].

III. The Proposed Algorithm Using 256X256 Matrix:

This algorithm can support all language scripts in the world; For this Unicode is being used and it requires a 256X256 matrix. This is because value of any character of any language around the world is between (0 - 65536). This way the user can encrypt any language including Kurdish language, space, symbols, special characters, etc. Next, a hash function of the key will be generated using Sha512 technique and then it will be merged with the cipher. This will be used to verify the Authenticity of the user and prevent the dictionary attack.

DOI: 10.18535/ijecs/v4i8.78

Algorithm:

Encryption:

1. Read Plain Text and keyword
2. Remove the repeated letters in the key.
3. create a 256X256 matrix then fill it with values of the key letters and the remaining values of unicode characters.
4. placing 'null' character if there were repeated characters in the same pair or the length of the plain text was odd.
5. Apply the traditional rules of Playfair cipher.
6. Hash the keyword by using sha256 algorithm to generate 128 characters. Then merging it with the cipher text. Now the message is ready to transfer.

Decryption:

1. Read the cipher text and the keyword
2. Split the first 128 characters from the cipher text.
3. Hash the given keyword using sha512 algorithm.
4. If the hashed key was equal to the spitted 128 characters, then it means the keyword is correct and the user is verified. Otherwise, the user is rejected and the process of decryption will be HALT.
5. Apply the traditional rules of playfair to decrypt the cipher.

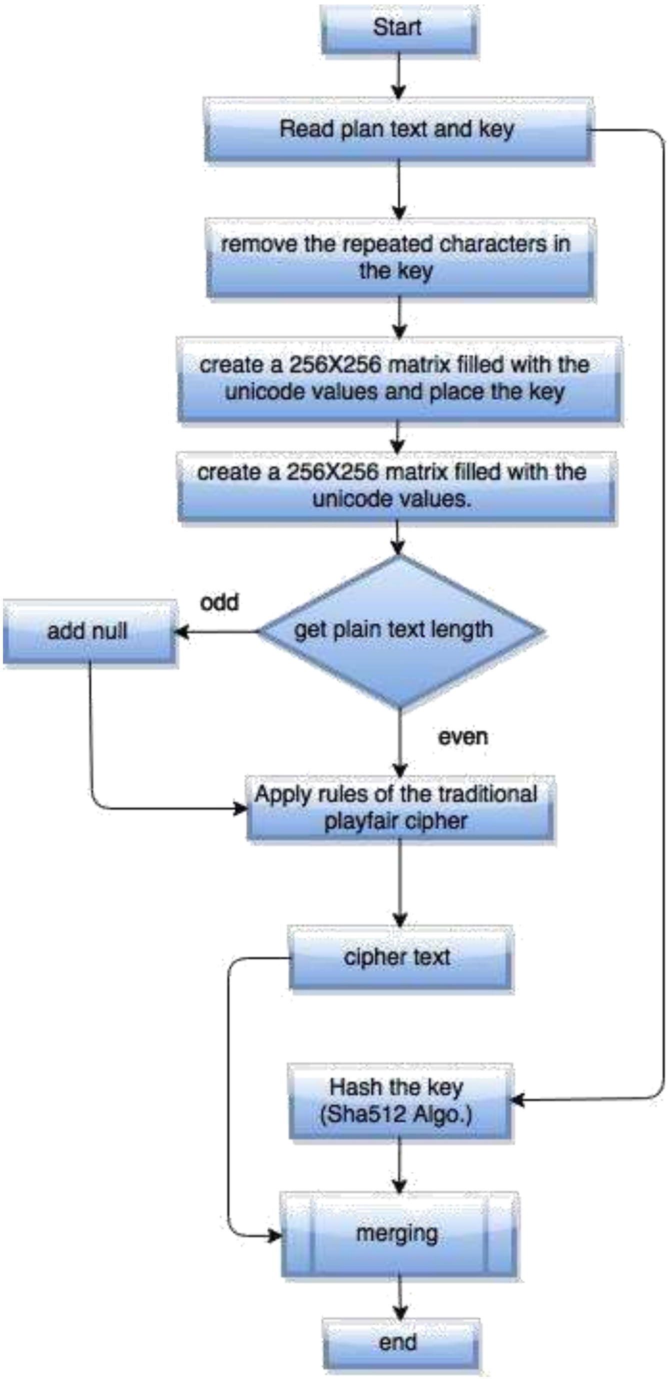
Start
Read plan text and key
remove the repeated characters in the key
create a 256X256 matrix filled with the unicode values and place the key
create a 256X256 matrix filled with the unicode values.
odd
add null
get plain text length
even
Apply rules of the traditional playfair cipher
cipher text
Hash the key (Sha512 Algo.)
merging
end

fig 3.1 flowchart of the encryption process.

DOI: 10.18535/ijecs/v4i8.78

IV. Analysis Of The Proposed Algorithm:

1. It supports all the language scripts in the world including Kurdish language. in addition, it supports all the unicode characters including space, symbols, special characters, upper and lower case alphabets, etc.

Brute force attack attempts to gain the key systematically trying every possible mixture of characters. In the traditional playfair algorithm the attacker has to search in 26*26 diagrams. However, since the proposed system uses a 256X256 table, he/she has to search in 65536*65536 diagrams. it can be clearly seen, security of the proposed system has rapidly increased and it is much more resistible against the brute force attack.

2. Frequency analysis: it is an attempt to somewhat disclose the message by studying the frequency of letters or groups of letters contained in the cipher text. the traditional algorithm worked on 26 characters so the likelihood of occurrence is 1/26 = 0.0384. whereas the proposed algorithm works on 65536 characters and the likelihood of occurrence of a character in the algorithm is 1/65536 = 0.0000152. It can be easily noticed that the proposed algorithm is resistible to frequency analysis attack.

3. The proposed system has solved many shortcomings existing in the traditional algorithms. It removes the confusion in case of having odd number characters or repeating letters in the same pair by using *null* character. furthermore, i and j are not treated as one character.

4. The hashing technique makes the algorithm to stand against dictionary attack because it verifies legitimate users and prevents fraud users from keep entering false characters to guess the key.

References

1. Gary C. Kessler (2015) *An Overview of Cryptography,* Available at:http://www.garykessler.net/library/crypto.html#t ypes (Accessed: 24/7/2015).

2. S. Dhenakaran, S.; Ilayaraja, M. (06/2012) 'Extension of Playfair Cipher using 16X16 Matrix', *International Journal of Computer Applications,* vol. 48(issue 7), pp. pp. 37-41 [Online]. Available at: http://dx.doi.org/10.5120%2F7363-0192 (Accessed: 19/6/2015).

3. Vinod Kumar,Santosh kr Upadhyay,Satyam Kishore Mishra,Devesh Singh (June 2013) 'Modified Version of Playfair Cipher Using Linear Feedback Shift Register and Transpose Matrix Concept', *International Journal of Innovative Technology and Exploring Engineering (IJITEE),* Vol. 3(Issue-1), pp. [Online]. Available at:http://www.ijitee.org/attachments/File/v3i1/A0925063113.pdf (Accessed: 26/7/2015).

4. Srivastava, S.S. (5 June 2011) 'Security Aspects of the Extended Playfair Cipher',*Communication Systems and Network Technologies (CSNT),* Vol. 3(Issue-1), pp. 144 - 147 [Online]. Available at: http://www.ijitee.org/attachments/File/v3i1/A0925063113.pdf(Accessed: 26/7/2015).

5. Surendra Singh, ChauhanHawa SinghRam, Niwas Gurjar (2014) 'Secure Key Exchange using RSA in Extended Playfair Cipher Technique', *International Journal of Computer Applications,* Volume 104 (15), pp. 144 - 147

DOI: 10.18535/ijecs/v4i8.78

[Online]. Available at:*http://www.ijcaonline.org/archives/volume104/number15/18277-9180* (Accessed: 21/6/2015).

6. Zubair Iqbal, Kamal Kr. Gola, Bhumika Gupta, Manisha Kandpal (2015) 'Dual Level Security for Key Exchange using Modified RSA Public Key Encryption in Playfair Technique', *International Journal of Computer Applications,* 111 (13), pp. 5-9 [Online]. Available at: *http://research.ijcaonline.org/volume111/number13/pxc3901408.pdf*(Accessed: 22/6/2015).

7. Kamal Kr. Gola, Bhumika Gupta, Zubair Iqbal (2014) 'Modified RSA Digital Signature Scheme for Data Confidentiality', *International Journal of Computer Applications,*106(13), pp. 14-17 [Online]. Available at:*http://research.ijcaonline.org/volume106/number13/pxc3899848.pdf* (Accessed: 25/6/2015).

8. Kaur, A. (2013) '3D — Playfair cipher using LFSR based unique random number generator', *Contemporary Computing (IC3),* 16(), pp. 18 - 23 [Online]. Available at:*http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=6612193&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D6612193*(Accessed: 25/6/2015).

9. Verma, V.,Kaur, D. ,Singh, R.K. (2013) '3D - Playfair cipher with additional bitwise operation', *Control Computing Communication & Materials (ICCCCM), 2013 International Conference on,* (), pp. 1 - 6 [Online]. Available at:*http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=6612193&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D6612193*(Accessed: 25/6/2015).