Wasit Journal for Pure Science

Journal Homepage: https://wjps.uowasit.edu.iq/index.php/wjps/index
e-ISSN: 2790-5241 p-ISSN: 2790-5233

Arabic and English Texts Encryption Using Modified Playfair Algorithm

Luheb Kareem Qurban[1], Amenah H. Abdulateef[2], Wisam Abed Shukur[3]*

[1,3]Computer Science Department, College of Education for Pure Science/Ibn Al-Haitham, University of Baghdad, IRAQ.
[2]Department of Biology/College of Science for Women, University of Baghdad, IRAQ.

*Corresponding Author: Wisam Abed Shukur

DOI: https://doi.org/ 10.31185/wjps.285
Received 10 December 2023; Accepted 16 January 2024; Available online 30 March 2024

ABSTRACT: To maintain the security and integrity of data, with the growth of the Internet and the increasing prevalence of transmission channels, it is necessary to strengthen security and develop several algorithms. The substitution scheme is the Playfair cipher. The traditional Playfair scheme uses a small 5*5 matrix containing only uppercase letters, making it vulnerable to hackers and cryptanalysis. In this study, a new encryption and decryption approach is proposed to enhance the resistance of the Playfair cipher. For this purpose, the development of symmetric cryptography based on shared secrets is desired. The proposed Playfair method uses a 5*5 keyword matrix for English and a 6*6 keyword matrix for Arabic to encrypt the alphabets of both languages. The result of our study shows that when compared to the classical method, the modified method requires less time. Similarly, the suggested method used less time to encode Arabic texts. For both Arabic and English texts, decryption using the suggested method was also quicker than the standard approach. The suggested technique's ciphertext is compared to the standard method's using the Normalized Cross-Correlation method to determine how effective the approach is for the identical plaintext. There is always a correlation coefficient between -1 and +1.

Keywords: Playfair cipher, security, proposed method, matrix, transmission channel.

1. INTRODUCTION

To increase complexity and security of cipher algorithm, Cryptographic techniques need to be modified in Scientific manner. The modification process is made by some changes of Basic parameters for traditional and Advanced cipher algorithms [1]. The Playfair cipher is one of the oldest block ciphers that based on substitution process and symmetric scheme. the operational Principle of Playfair cipher is simple and efficient [2]. The Substitution model of both standard and proposed method of Playfair cipher are depend of the neighboring character and positions [3]. The key of encryption is the root of square array that used in encryption process. The standard Playfair algorithm, which works on a 5x5 square matrix for 25 English character, The characters I and J are mixed in same cell. the standard algorithm deals with English texts only, in this work the algorithm has been developed to work with Arabic texts as well, using a 6x6 matrix for 28 Arabic letters, and 8 additional letters, which are (أ, إ, آ, ء, ؤ, ى, ئ, ة) in the proposed method. There are previous studies that encrypted Arabic texts using the traditional Playfair, which uses a block size of 2 characters. The proposed method developed the block size to 3 characters, in addition to using new rules for encryption and decryption, then stronger results were obtained. [4][5][29].

2. RELATED WORK

In 2019 ***Madeha Shaltagh Yousif*** [25] used an n×n matrix with permutation and transposition, where (n > 10), due to the high computation, make it withstand many well-known attacks.

In 2020, Tuti Alawiyah [16] used a Playfair cipher algorithm to generate a Hill cipher key as a rectangular matrix. The use of the Playfair Cipher algorithm makes it easy for users to remember key matrices, while remaining safe when distributed.

In 2020***, Dhamyaa A. Al-Nasrawi*** [24] proposed new method of 3 steps: the first, Romanizing Arabic text entails switching the Arabic script for the Latin script. The second is a romanized text encipher/decipher that uses a 6x8 matrix and unicode, along with the Playfair proposal. The Knight tour key is used to generate the encryption and decryption. The final stage, deromanizing the Arabic text to produce plain text, strengthens the system's resistance to third parity.

In 2021, ***Raghad K. Salih*** [27] used a10×10 Playfair key matrix, which includes capital and small Alphabets, numbers, that increase the resistance of Playfair cipher.

In 2022, ***Subramaniyam.c.s*** [21] Numerical data and both uppercase and lowercase letters were encrypted using case-sensitive techniques. Use color substitution to replace plain text; color is used to facilitate encryption.

In 2019, ***Winarko Edi*** [11] Through the use of the Key Layer Matrix (KLM) approach, this study aims to modify the Playfair cryptographic algorithm key matrix. Specifically, the 5x5 key matrix is changed into two layers, resulting in a key combination of 25 x 25, which consists of upper and lower case letters. Two keys are utilized to perfect this modification: the layer 1 key and the layer 2 key. The computations using this approach result in a slower process complexity but a more difficult to hack system.

In 2018, ***Amalia M A Budiman and R Sitepu*** [12] This technique used a hybrid cryptosystem that included the symmetric Modification Playfair Cipher 16x16 algorithm and the asymmetric Knapsack Naccache-Stern algorithm.

3. STANDARD PLAYFAIR

All parties use cryptography as secure mechanism since it an effective and suitable way to safeguard information during transmission through unprotected media [6]. All cryptographic techniques use symmetric and asymmetric keys according to nature of used key generation [7] the stream and block cipher are two types of encryptions according to nature of sensitive information [8]. data security goals are secrecy, integrity, and availability that considered in encryption process [9]. The encryption process depends on either permutation process or substitution process.[10].

Playfair is a block symmetric substitution cipher and block size is two. It creates a 5*5 matrix and fill with 25 English alphabetic letters except j letter that merge with I letter [11][12]. The first row of created matrix must be containing the keyword or key considering to prevent duplicating of its letters [13]. the remained letters of alphabetic such as English or Arabic are distributed via other positions of created matrix. The letters that have fewer frequency for each alphabetic such as English or Arabic are located together in the same position of created matrix [14] [15].

While in the proposed method, the created matrix has size 6*6 and block size is 3. The applied rules on standard Playfair algorithm are different from applied rules on the proposed modified Playfair cipher algorithm [16] [17].

For classical Playfair encryption, there are several Applied rules that used to achieve encryption process. the first rule is separating the plaintext into blocks or pairs equally [18]. The Repeated letters are separated via different letter which is (x) letter such as "Hello" word, the Repeated letters are (ll) that must set x letter in between to result (lx and lo) [19]. The Second rule is if a plaintext letters in the same row of the created matrix, then each letter will shift to the right, the last letter in the row will follow the first one for same row but in circular manner [20]. Third rule is if two plaintext letters in the same column then each letter will shift to bottom once [21]. fourth rule is When two letters lie in different positions row and column that form square or rectangle then each letter will substitute with that letter in lies in same row, So for column [22].

For decryption, if two ciphertext letters are on the same row or Column, substitute them with the left or above letters. Respectively [23].

4. PROPOSED METHOD

The methodology of proposed modified Playfair method is divided in two phases, keyword generation and ciphering process. The block cipher of proposed method is 3 instead of 2 with in standard form. It is encrypted Arabic as well as English letters, and creates a 5*5 matrix fill with 25 English alphabetic letters except j letter that merge with I letter. For Arabic alphabetic the matrix has size 6*6 since the number of Arabic letters is 36.

For proposed Playfair encryption, there are several Applied rules that used to achieve encryption process. The first rule is separating the plaintext into blocks of three letters equally. The Repeated letters are separated via different letter which is (x) letter such as "Letters" word, the Repeated letters are (tte) that must set x letter in between to result (txt). The Second rule is if a three plaintext letters in the same row of the created matrix, then the first letter will shift to the

right one step, the second letter will shift to the right two, the third letter will shift to the right three step, if the letter in the last of row will follow the above rules but in circular manner. Third rule is if three plaintext letters in the same column then the first letter will shift to bottom ones, the second letter will shift to bottom twice, the third letter will shift to bottom three step, if the letter in the last of column will follow the above rules but in circular manner. Fourth rule is When three letters lie in diagonal positions the first letter will exchange with third letter and the middle letter will not change. The last rule if the letters lie in different positions will follow the same steps in second rule depending on its position.

For decryption, if three ciphertext letters are on the same row, follow the second rule of encryption but shift to the left side as well as when the three letters in the same column will shift up based on third rule. The last rule if the letters in diagonal position will follow the fourth encryption rule exactly.

TABLE 1-The Playfair 5*5 English matrix

A	B	C	D	E
F	G	H	I/J	K
L	M	N	O	P
Q	R	S	T	U
V	W	X	Y	Z

TABLE 2-The Playfair 6*6 Arabic matrix

ب	ل	ي	ف	ر	غ
ة	ج	و	ا	س	ك
ء	آ	أ	ؤ	إ	ئ
ت	ث	ح	خ	د	ذ
ز	ش	ص	ض	ط	ظ
ع	ق	م	ن	ه	ى

5. THE ALGORITHM OF STANDARD AND PROPOSED METHOD PLAYFAIR

5.1 ALGORITHM 1: ENCRYPTION PROCESS

Step1: Input keyword
Step2: generate 5*5 keyword matrix for English alphabet and 6*6 for Arabic.
Step3: split plaintext into blocks of three letters
Step4: if there are duplicated letters then insert (x) between them.
Step5: if three letters are in the same row then go to step 6
Else if three letters are in the same column then go to step 7
Else if three letters in diagonal position then go to step 8
Else go to step 6
Step6: shift first letter one step to right and second two steps and third three steps.
Step7: shift first letter one step to bottom and second two steps and third three steps.
Step8: exchange first and third letter but the second will not change
Step9: if any letter lies in the last row or column then follow the above rules but in circular manner.

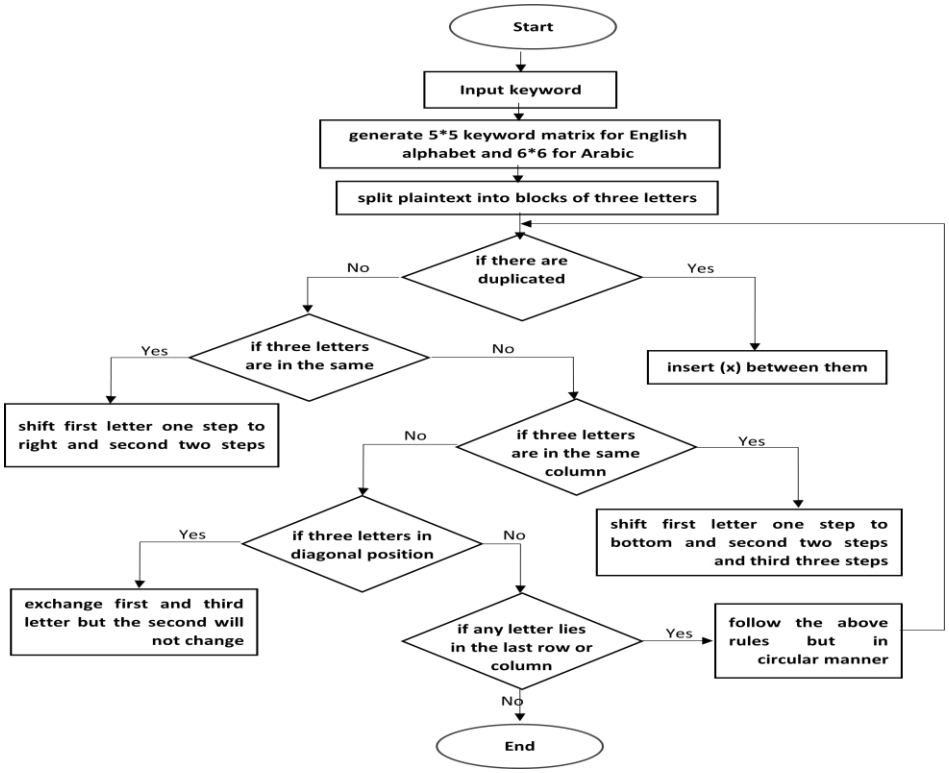


FIGURE 1. The encryption process

5.2 ALGORITHM2: DECRYPTION PROCESS

Step1: Input keyword
Step2: generate 5*5 keyword matrix for English alphabet and 6*6 for Arabic.
Step3: split ciphertext into blocks of three letters
Step4: if there are duplicated letters then insert (x) between them.
Step5: if three letters are in the same row then go to step 6
Else if three letters are in the same column then go to step 7
Else if three letters in diagonal position then go to step 8
Else go to step 6
Step6: shift first letter one step to left and second two steps and third three steps.
Step7: shift first letter one step up and second two steps and third three steps.
Step8: exchange first and third letter but the second will not change
Step9: if any letter lies in the last row or column then follow the above rules but in circular manner.

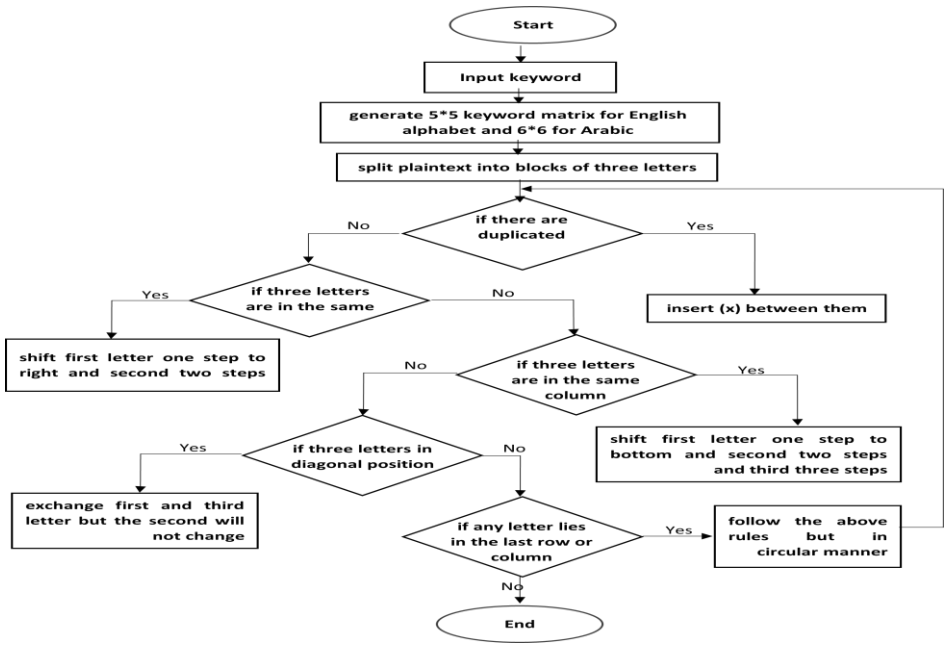
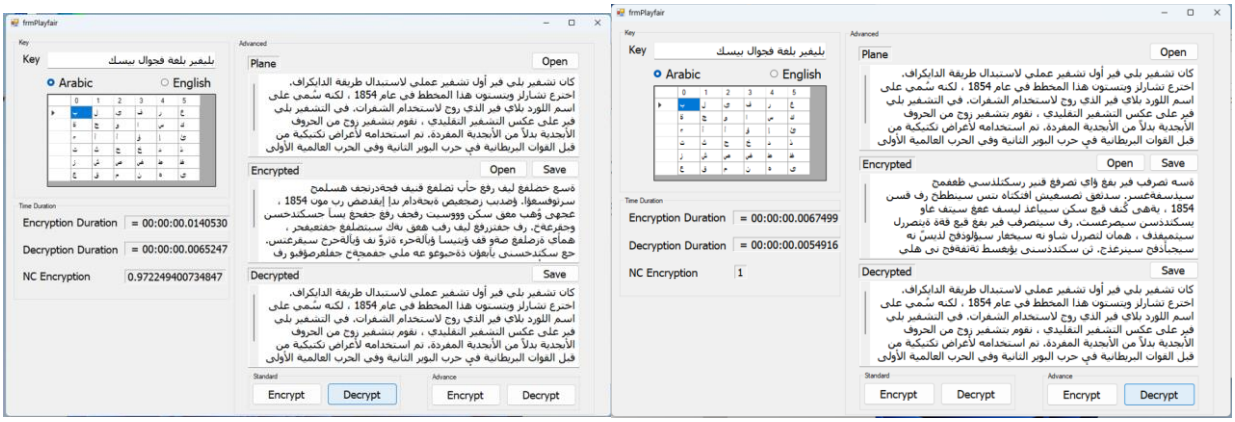


FIGURE 2. The decryption process

6. RESULTS

In this section, we conducted an experimental result to verify our proposed algorithm in processing English and Arabic texts. The performance of the modified Playfair algorithm is evaluated against the standard Playfair. Fig.1 below utilize the encryption and decryption processes. In the encryption process, the data set is English or Arabic file containing the plain text to be encrypted and uploaded from the computer. While the decryption process, the English or Arabic file containing the cipher text that are decrypted and uploaded from the computer or directly from the text after encryption process. both algorithms are studied and evaluated under the same conditions and evaluation metrics as shown in Fig. 1.



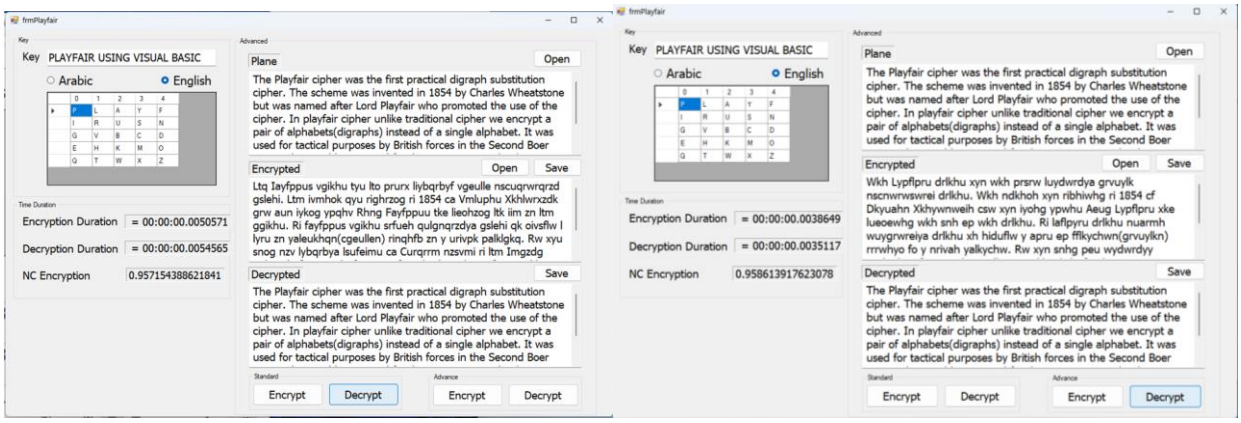


FIGURE 3. main menu for encryption and decryption procedure of standard and modified Playfair.

The results were compared with the standard Playfair to validate the efficiency of the modified Playfair based on the considered evaluation factors, and show its capability to cope with English and Arabic texts. As shown in Table 3, several evaluation factors were exploited to evaluate the performance of the modified Playfair against the standard Playfair based on ciphering and deciphering times, security, coding block size, robustness, complexity, keys type, keyword matrix size and efficiency. Unlike the standard Playfair algorithm, the modified Playfair exhibit an improvement in term of security, speed, robustness, and efficiency. In addition, the complexity is high in the modified Playfair.

TABLE 3- Comparison between Standard and Modified Playfair

Evaluation metric	Standard Playfair	Modified Playfair
Security level	High	Very-high
Coding block size	Two	Three
Encryption/decryption complexity	High	Very-high
Effectiveness	Moderate	High
Robustness	Moderate	High
Type of Keys	Symmetric key	Symmetric key
Size of keyword matrix	5*5	5*5 or 6*6
Encryption/Decryption Speed	Fast	Faster

The encryption process time is used to evaluate any encryption algorithm, which is rely on two aspects: size of the keyword and the total size of the plaintext block. The encryption time in the obtained experimental results is measured in a millisecond. Generally, the performance of encryption process is influenced by the encryption time. In contrast, the decryption time can be described as the spent time to retrieve a plaintext from encrypted text.

When encrypting a paragraph consisting of approximately 6 lines of English text, we noticed that the time taken by the updated method is less compared to the classical method. Likewise, as for encoding Arabic texts, the time was less with the proposed method.

Also decryption using the proposed method was also faster than the standard method for Arabic and English texts.

The efficiency of the method is measured by using Normalized Cross-Correlation method to find out the correlation between the ciphertext of the standard method and the proposed one for the same plaintext, The correlation coefficient always lies between -1 to +1. The time of encryption and decryption and Normalized Cross-Correlation coefficient is shown in Table 4 and 5.

TABLE 4- The time of encryption and decryption and Normalized Cross-Correlation for English text

Utilized cipher method	Encryption-Time in a millisecond	Decryption-Time in a millisecond	Normalized Cross-Correlation
Standard Playfair	00:00:00.0050571	00:00:00.0054565	0.957154388621841
Modified Playfair	00:00:00.0038649	00:00:00.0035117	0.958613917623078

TABLE 5- The time of encryption and decryption and Normalized Cross-Correlation for Arabic text

Utilized cipher method	Encryption-Time in a millisecond	Decryption-Time in a millisecond	Normalized Cross-Correlation
Standard Playfair	00:00:00.0140530	00:00:00.0065247	0.972249400734847
Modified Playfair	00:00:00.0067499	00:00:00.0054916	1

7. CONCLUSIONS

modified method outperforms the standard algorithm and scores higher in the average time analysis. Due to the similarity, it's not possible to get different times for the same input when performing encryption and decryption. The proposed algorithm sets the plaintext block size to 3 instead of the normal form 2, and thus serves as a reliable and efficient data encryption method. You can also use the 5*5 or 6*6 keyword matrix method to encrypt the English and Arabic alphabets. However, special characters and spaces are not encrypted.

In this case, the security of encryption technology can be further enhanced. Expanding Playfair Increases Security.

One of the ways to develop the proposed algorithm is to encrypt numbers and symbols as well. Or enlarge the block size to 4.

8. CONTRIBUTIONS OF AUTHORS

Luheb Kareem Qurban conceptualized, applied, formulated, and analyzed Amenah H. Abdulateef wrote the original manuscript and prepared it, while Wisam Abed Shukur reviewed and edited it and developed the model, software, verification analysis of the data, and visualization.

Each author has reviewed the published version of the manuscript and given their approval.

9. ACKNOWLEDGMENT

We would like to express our sincere gratitude to our **Firas A. Abdullatif**, for his valuable guidance and support throughout the research process. His expertise and insights were invaluable in shaping our research and helping us to overcome challenges.

We also want to thank our colleagues at **University of Baghdad** for their helpful feedback and support. In particular, we would like to thank **Dr. Bilal Bahaa Zaidan** National Yunlin University of Science and Technology contributions to our research.

10. REFERENCES

[1]. D. Kurniawan, A. L. Hananto, and B. Priyatna Modification Application of Key Metrics 13x13 Cryptographic Algorithm Playfair Cipher and Combination with Linear Feedback Shift Register (LFSR) on Data Security Based on Mobile Android, [Journal] // Int. J. Comput. Tech. - 2018. - vol. 5, no, pp. 65-70.

[2]. Ritchell S. Villafuerte Ariel M. Sison, Ruji P. Medina An Improved 3d Playfair Cipher Key Matrix With Dual Cipher Block Chaining Method [Journal] // INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH. - OCTOBER 2019. - 10 : Vol. 8. - pp. 1013-1016.

[3]. E. Elahi H. Raza, and S. Ali A new 3D Playfair based secure cipher generation model [Conference] // 13th International Conference on Emerging Technologies (ICET). 2018-Janua, pp. 1–4.

[4]. Ritchell S. Villafuerte Ariel M. Sison, Ruji P. Medina i3D-Playfair: An Improved 3D Playfair Cipher Algorithm [Journal] // IEEE Eurasia Conference on IOT, Communication and Engineering. - 2019. - pp. ISBN : 978-1-7281-2501-5.

[5]. Sakshi Agarwal, Dr. Gaurav Agarwal Pllay--Faiir Encrypttiion Allgoriitthm – A Reviiew [Journal] // International Journal of Computer Science & Communication. - 2019. -. Vol 10 • pp. 201-210

[6]. Wisam Abed Shukur, Ahmed Badrulddin, Mohammed Kamal Nsaif A proposed encryption technique of different texts using circular link lists [Journal] // Periodicals of Engineering and Natural Sciences. - 2021. - Vol. 9. - pp. .1115-1123.

[7]. Kubba, Zaid M. Jawad, and Haider K. Hoomod. "Developing a lightweight cryptographic algorithm based on DNA computing." In *AIP Conference Proceedings*, vol. 2290, no. 1. AIP Publishing, 2020.

[8]. Kubba, Zaid M. Jawad, and Haider K. Hoomod. "Modified PRESENT Encryption algorithm based on new 5D Chaotic system." In *IOP Conference Series: Materials Science and Engineering*, vol. 928, no. 3, p. 032023. IOP Publishing, 2020.

[9]. Wisam Abed Shukur, Luheb Kareem Qurban, Ahmed Aljuboori Digital Data Encryption Using a Proposed W-Method Based on AES and DES Algorithms [Journal] // Baghdad Science Journal. – 2023.

[10]. Firas A. Abdullatif, Alaa A. Abdullatif, Namar A. Taha Data hiding using integer lifting wavelet transform and DNA computing [Journal] // Periodicals of Engineering and Natural Sciences. - 2020. - Vol. 8. - pp. .58-66.

[11]. Winarko Edi Modification of Playfair Chiper to Strengthen Playfair Chiper Algorith with 2 Key Layer Matrix (KLM) Method [Journal] // International Journal of Innovation, Creativity and Change. - 2019. - Vol. 5. - pp. 602-619.

[12]. Amalia M A Budiman and R Sitepu File text security using Hybrid Cryptosystem with Playfair Cipher Algorithm and Knapsack Naccache-Stern Algorithm [Conference] // IOP Conf. Series: Journal of Physics: Conf. Series. - 2018.

[13]. Wu Zeyu Hybrid Playfair: a modified Playfair cipher combining 2D and 3D Playfair [Conference] // Third International Conference on Electronics and Communication, Network and Computer Technology. - Harbin, China 2021.

[14]. Ritchell S. Villafuerte, Ariel M. Sison, Alexander A. Hernandez, Ruji P. Medina Randomness Evaluation of the Improved 3D-Playfair (i3D) Cipher Algorithm [Conference] // 12th International Conference on Communication Software and Networks. – 2020.

[15]. S.Karthiga T.Velmurug Enhancing Security in Cloud Computing using Playfair and Ceasar Cipher in Substitution Techniques [Journal] // International Journal of Innovative Technology and Exploring Engineering (IJITEE). - 2020. - Vol. 9.

[16]. Alawiyah, Tuti, Agung Baitul Hikmah, Wildan Wiguna, Mira Kusmira, Herlan Sutisna, and Bambang Kelana Simpony. "Generation of rectangular matrix key for hill cipher algorithm using Playfair cipher." In *Journal of Physics: Conference Series*, vol. 1641, no. 1, p. 012094. IOP Publishing, 2020.

[17]. Maiya Din, Saibal K. Pal, S.K. Muttoo, Sushila Madan A Hybrid Computational Intelligence-based Technique for Automatic Cryptanalysis of Playfair Ciphers [Journal] // Defence Science Journal. - 2020. - Vol. 70. - pp. 612-618.

[18]. S M Hardi J T Tarigan, N Safrina Hybrid cryptosystem for image file using elgamal and double Playfair cipher algorithm [Conference] // 2nd International Conference on Computing and Applied Informatics. - 2018.

[19]. Archi Seth, Siddhartha Sankar Biswas Chaotic Genetic Enhancements to the Modified Playfair Algorithm [Journal] // International Journal of Computer Sciences and Engineering. - 2018. - Vol. 6. - pp. 245-250.

[20]. Arnold C. Licayan, Alexander A. Hernandez Performance Analysis of Playfair CipherColor Substitution Variants [Conference] // 11th IEEE Control and System Graduate Research Colloquium (ICSGRC 2020). - Malaysia, 2020.

[21]. Subramaniyam.c.s, Sukanya sargunar.v Implementation of Playfair cipher by using 7 by 9 matrix and colour substitution [Journal] // International Journal of Engineering Associates. - 2022. - Vol. 5. - pp. 13-17.

[22]. Ashish Pandey, Neelendra Badal A Modified Circular Version of Playfair Cipher [Conference] // 2nd INTERNATIONAL CONFERENCE ON ADVANCED COMPUTING AND SOFTWARE ENGINEERING (ICACSE-2019). - 2019.

[23]. Maherin Mizan, Maha Md Masuduzzaman, Abhijit Bhowmik An Effective Modification of Play Fair Cipher with Performance Analysis using 6X6 Matrix [Conference] // ICCA: Proceedings of the International Conference on Computing Advancements. - Bangladesh, 2020.

[24]. Inas R. Shareef Noor D. Al-Shakarchy, Enaam Hadi Abd. Dhamyaa A. Al-Nasrawi, Huda F. Al-Shahad and Hiba J. Aleqabie New Cryptographic System of Romanized Arabic Text Based on Modified Playfiar [Journal] // Journal of Engineering and Applied Sciences. - 2019. - pp. 1331-1338.

[25]. Madeha Shaltagh Yousif Raghad Kadhim Salih and Nadia Mohamed Ghanim Alsaidi A new modified Playfair cipher [Conference] // AIP Conference Proceedings 2086,030047. - 2019.

[26]. Maherin Mizan Maha Md Masuduzzaman, An Effective Modification of Play Fair Cipher with Performance Analysis using 6X6 Matrix [Conference] // ICCA. - Dhaka, Bangladesh, 2020.

[27]. Raghad K. Salih* Madeha Sh. Yousif Playfair with Multi Strata Encryption [Journal] // Iraqi Journal of Science. - 2021. - Vol. 62, pp: 3237-3242.

[28]. Richard M. Marzan Dr. Ariel M. Sison An Enhanced Key Security of Playfair Cipher Algorithm [Conference] // ICSCA. - Penang, Malaysia, 2019.

[29]. Shukur, Wisam Abed, and Zaid M. Jawad Kubba. "Arabic and English Texts Encryption Using Proposed Method Based on Coordinates System." *International Journal of Advances in Soft Computing & Its Applications* 15, no. 2 (2023).