Open Access **Baghdad Science Journal** **P-ISSN: 2078-8665**
2020, 17(4):1320-1327 **E-ISSN: 2411-7986**

DOI: http://dx.doi.org/10.21123/bsj.2020.17.4.1320

Combining Several Substitution Cipher Algorithms using Circular Queue Data Structure

Noor A. Ibraheem* ***Mokhtar M Hasan***

Computer Science Department, College of Science for Women, University of Baghdad, Baghdad, Iraq.
*Corresponding author: *noorai_comp@csw.uobaghdad.edu.iq ,mokhtarmh@csw.uobaghdad.edu.iq
*ORCID ID: *https://orcid.org/0000-0003-4495-0772 , https://orcid.org/0000-0002-4702-4320

Received 28/10/2019, Accepted 19/7/2020, Published 1/12/2020

Abstract

With the revolutionized expansion of the Internet, worldwide information increases the application of communication technology, and the rapid growth of significant data volume boosts the requirement to accomplish secure, robust, and confident techniques using various effective algorithms. Lots of algorithms and techniques are available for data security. This paper presents a cryptosystem that combines several Substitution Cipher Algorithms along with the Circular queue data structure. The two different substitution techniques are; Homophonic Substitution Cipher and Polyalphabetic Substitution Cipher in which they merged in a single circular queue with four different keys for each of them, which produces eight different outputs for every single incoming letter. The present work can be applied efficiently for personal information security and network communication security as well, and the time required for ciphering and deciphering a message is less than 0.1 sec.

Key words: Circular queue, Homophonic substitution cipher, Polyalphabetic substitution cipher, Substitution cipher.

Introduction

Recently Information and communication systems witnessed fast developments of various technologies along with security issues, and a lot of information forms and communication systems considered as a core parts of our daily lives (1). With the proliferation of this information, communication, and network abilities there is growingly interest in these technologies.

Information network technology has various extensive applications which serve different social fields; however, since internet is a wide open system it is normally to face information security problems. These problems comprise hacker intruding, network attack, besides internet menaces such as tampering and interception network information (2-4). The spreading of mobile applications that upload and download data over the network increases the urgent need to secure and safe internet data communication (2).

Steganography is a technique for secret communication between the concerned parties. In steganography the secret communication hide the valuable information inside a transmitted file in a way that any change in the transmitted file information will not be noticeable (5,6). Cryptography is one of the effective methods for information security by converting the required message in a manner that only the authorized person has the ability to understand and decipher the message (7).

Both cryptography and steganography methods are utilized together to achieve system security by receiving and transmitting data over network communications (1). The transmitted information through transmission channel demands confidentiality introduced by the cryptography methods from end to end communication, and secret camouflaged information embedded via different multimedia files provided by Steganography methods (1).

The novelty of this work is clear by combining two Substitution Cipher types; Homophonic Substitution Cipher and Polyalphabetic Substitution Cipher using a single circular queue in order to create a new algorithm that is more secure and immune against breaking. The details of the proposed algorithm is explained in the following sections. The rest of the paper is organized as

follows. Section 2 introduces related work; Section 3 describes problem formulation and system methodology. Experimental results are presented in Section 4, while Section 5 gives some comparative factors with other related methods. Section 6 introduces the system analysis, and finally Section 7 shows the conclusion and future work.

Related Work

Various encryption techniques have been applied to assure network security as well as personal information security, however, it still as a challenge to combine them in a single unified structure (8). For example, researchers in (9) presented crypto-system for both personal data security and network security with an inclusive study of different cryptographic techniques. In (1), researchers introduced an efficient methodology of digital steganography system using an adaptive circular queue least significant bits (LSBs) substitution; the circular queue is applied dynamically between multiple communication users RSA cryptosystem is applied for information security authentication and privacy. In steganography technique the cover image is ordered in different circular queues blocks, the secret cypher blocks are dynamically adapted to be located in the circular queues, and from the other side the authorized user will determine the correct plain text in RSA decipherment according to the private key, the system is evaluated by MSE, PSNR and maximum embedding capacity (1). In (10), the researchers applied several encryption algorithms such as: Advanced Encryption Standard AES, Advanced Encryption Standard RSA, and Advanced Encryption Standard Proposal AESP under circular queue control to schedule the secret code generated by the control key where the entire secret code is changed with each decoded message. The proposed system has the ability to generate different multiple random keys according to the implemented encryption algorithm. The shortening of this system sets in its limitation of application into a specific area of multimedia field (10).

While researchers in (8) applied circular substitution concept with reversal transposition, a symmetric polyalphabetic block cipher. The suggested method combined the principles of the simple character level displacement of the Caesar cipher, with the distribution of the Vernam polyalphabetic cipher and the diffusion of the transposition cipher adaptively, the system security are available for both white box and grey box models as well as black box models. In (11) researchers developed a symmetric cryptographic algorithm using circular queue and gray code. This suggested algorithm can be used for text, audio, image, and video files security. The gray code which is an ordered numeral binary system that utilized two successive differ in only one bit. The dimension of circular queue and beginning of the selected keyword character considered as the flexible factors; these features are used to retrieve the plaintext.

Kumar et al. in (2) suggested a new matrix scrambling technique based on random number selection, shifting and reversing techniques of circular queue. The random function is applied firstly to generate binary sequence, secondly to generate the row and column selections, and thirdly to select scrambling operations to exceed the regularity in the outcome ciphered text. The proposed method can be applied on text encryption, image encryption, and multimedia encryption.

Boneh et al. in (12), rs applied n-circular secure system based on the Decision Diffie-Hellman assumption; the suggested system suffering from several defects points such as, the system has to obtain a regular process at each n-encryption cycle, and to produce circular security for the selected ciphered text attacks, the system is weakly secure. The suggested algorithm can be applied on text, image, and multimedia encryptions, while Suri et al. in (13) applied ciphering on text using multiple circular arrays.

Wisam et al., and Nichat et al. in (14) and (15) submitted hybrid systems. Authors in (14) proposed a hybrid text cryptograph system depends on the circular queue using various encryption methods such as; Caesar, Vigenère, Affine, and multiplicative. In this method each character of input text is encrypted using one of the defined cipher techniques controlled by selected key. The system proved its efficiency and security in ciphering and deciphering sensitive data (14).

Genetic algorithms (GAs) have a lot of applications in various fields (16), for example, Nichat et al. in (15) suggested a hybrid model is proposed for image encryption using GA and chaotic function. At first, the system constructed some encrypted images using the key and chaotic function which will consider as the GA initial population, and then the GA is applied to produce the optimum solution represented by the best ciphered image with the highest entropy and lowest correlation coefficient (15). While Albahar, et al. in (17) suggested a novel algorithm based on combining RSA (Rivest-Shamir-Adleman), AES (Advanced Encryption Standard), and TwoFish methods to improve data exchange between Bluetooth devices securely. in (18), Mustafa A. proposed to implement video encryption using a

Baghdad Science Journal
P-ISSN: 2078-8665
E-ISSN: 2411-7986

combination of some encryption method which are; DES, Triple DES, Blowfish, AES using modes of operation and padding modes.

The proposed work used two Substitution Cipher types; Homophonic Substitution Cipher and Polyalphabetic Substitution Cipher using a single circular queue which is a new algorithm used for ciphering and deciphering a plaintext message.

Proposed System Methodology

The problem statement consists of applying circular queue data structure which will be used to combine Homophonic Substitution Cipher and Polyalphabetic Substitution Cipher methods to create a secure encryption for the input text letters, Fig. 1 shows the overall proposed system architecture.

Proposed Algorithm

In this paper, two different substitution techniques were combined, which are Homophonic Substitution Cipher and Polyalphabetic Substitution Cipher methods; they melted together into a single circular queue. In the encryption stage, the input message *M* is initially permutated to be *MP* text, then each character is ciphered using circular queue, to generate the encrypted message *C*. at the decryption stage, the encrypted message *C* is deciphered each character using queue architecture and the resultant message is re-permutated into *MP* text to finally extracted the original input message *M*. The details of the ciphering stage and deciphering along though circular queue is elaborated in the following subsections.

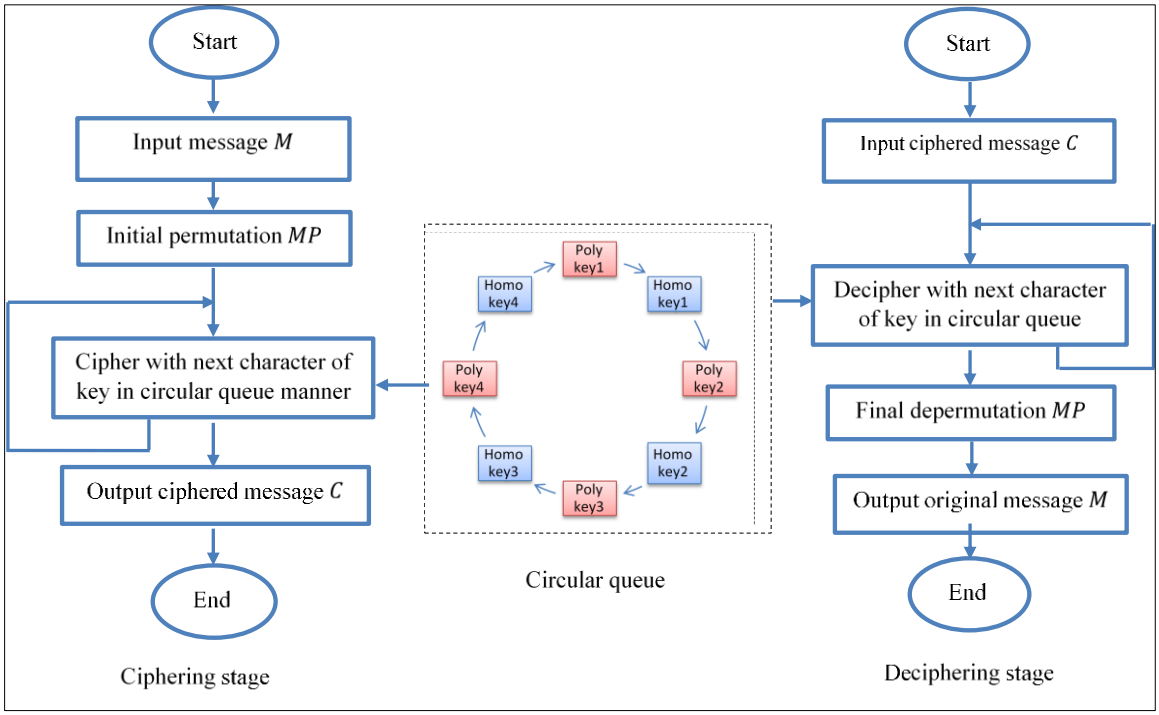

Figure 1. Proposed system architecture.

Homophonic Keys Generation

In order to prepare the keys permutations of the homophonic cipher, random algorithm along with the original alphabetic are used together to generate different key at a time. Each generated homophonic key is created randomly from the original alphabetic to obtain more sophisticated key and therefore the algorithm will be hard/ strong against text breaking, four keys in total are required for the final purpose, as shown in Fig. 2.

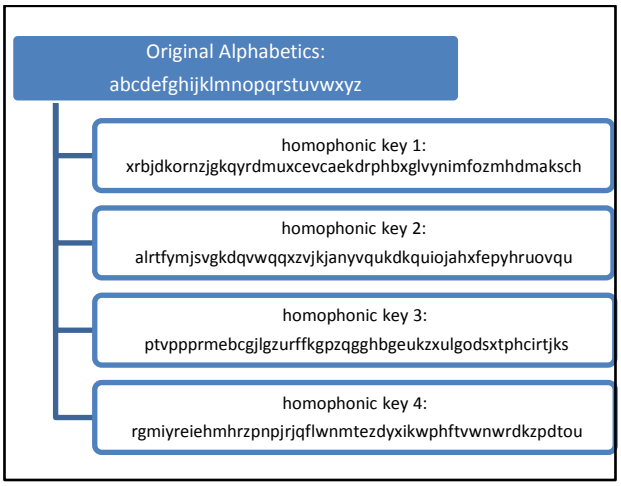

Figure 2. Four keys are extracted from the original alphabetic characters.

Baghdad Science Journal
P-ISSN: 2078-8665
E-ISSN: 2411-7986

We can notice that all the generated keys are 52 letters as length, so that each single input letter will be replaced by two different letters which will increase the complexity of the proposed algorithm.

Polyalphabetic Keys Generation

In Polyalphabetic keys generation, the number of keys in polyalphabetic is equal to the number of keys used in homophonic, these four keys are generated by using a different keyword for each one. The following keywords have been utilized for this purpose.

Keywords are: computer, monarchy, sophisticated, and irritation.

The final polyalphabetic keys are recognized as demonstrated in Fig. 3:

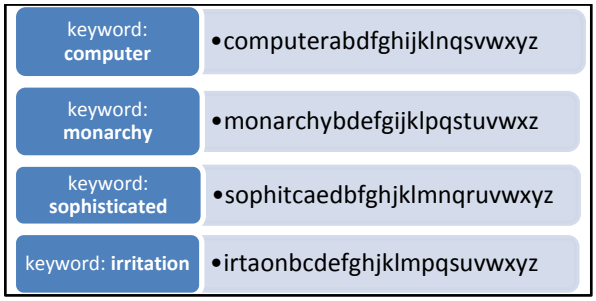

Figure 3. Four keys are generated for polyalphabetic cipher using different keyword for each.

Circular Queue

Circular Queue as known is a linear data structure in which the operations are performed based on the principle of FIFO (First In First Out), so the last position is connected back to the first position to make a circle. Circular Queue can be applied in information security to make the message hardly divulged or interpreted (19). The use of this structure will insert some factors that provide the encryption/decryption process with strength and complexity, these elements are established for both sender and receiver before starting the encryption process. In this work, the circular queue is applied to combine the homophonic and polyalphabetic substitution keys together in order to produce a complex cipher algorithm, the suggested combination is shown in Fig. 4:

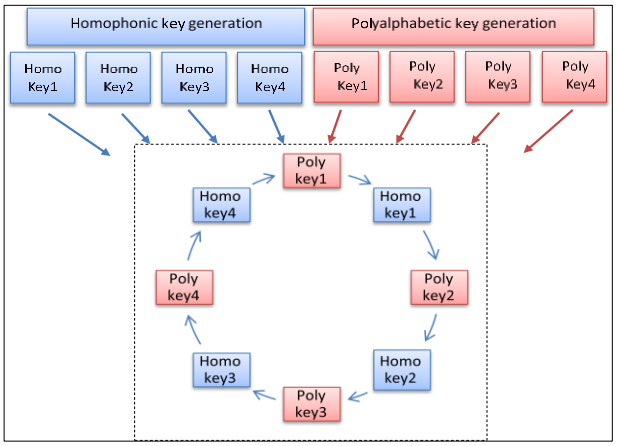

Figure 4. Circular queue represents the order of encryption the incoming letter.

As elucidated in Fig 4 above, in the circular queue arrangement, each incoming letter to be encrypted is applied on the next slot of the circular queue, so that the outcome result is different letter since next letter goes to next method that has different key and so on, this operation is repeated every 8 letters, it is worth to mention that the number of slots in the circular queue can be increase to involve more and different cipher algorithms, the ultimate resultant is more powerful and secure ciphered text.

Input Message

Before we start with the encryption process, we permutated the input message (*M*) randomly as explained in Fig. 5 where the length of the message is assumed to be consisted of 22 letters. The permutated message is the same length of the input massage with changing the positions of the input characters:

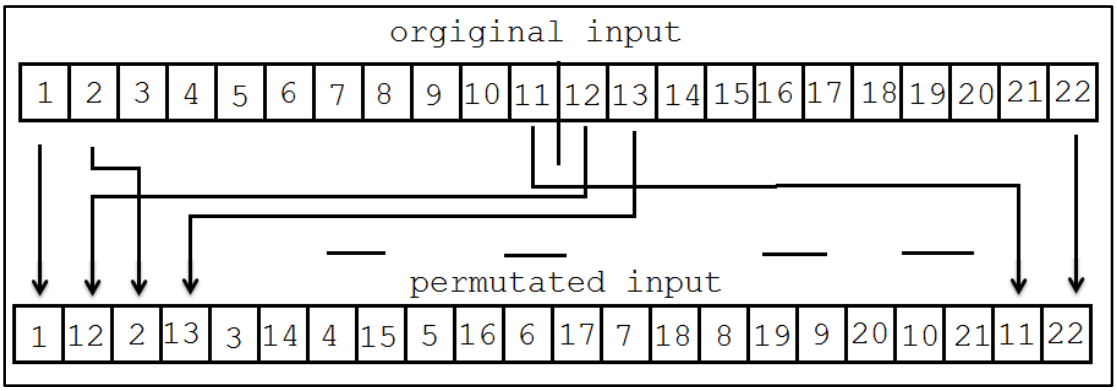

Figure 5. The initial permutation of the input message (M), assuming the message length is 22 letters.

Baghdad Science Journal
P-ISSN: 2078-8665
E-ISSN: 2411-7986

Ciphering Phase

After preparation of the homophonic keys and polyalphabetic keys; the system now is ready to accept messages for ciphering and deciphering. Each message received for ciphering operation is permutated as explained before; the aim of this operation is to complicate the resulted text.

The permutated message is ciphered using the generated circular queue as explained before, each letter is goes to next slot of the circular queue and the outcome is aggregated in a buffer, the operation is continuous until all letters of the permuted text is done, Fig. 6 shows the operation of the ciphering process.

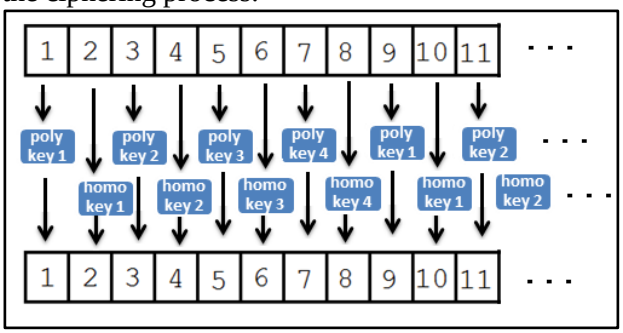

Figure 6. Ciphering operation using circular queue.

Deciphering phase

As known, this operation represents the reversion of the ciphering phase, in this step, circular queue is generated using the same presented method explained previously, but the difference in the reversing of the operation of each of homophonic and polyalphabetic is recognized.

Experimental Results:

We have provided experimental examples to explain and clarify the ciphering operation as well as deciphering operation, different lengths texts have been implemented to show the reliability and flexibility of the proposed algorithm. Example 1, Example 2, Example 3 which is an example applied in (5) which is extracted from famous story "Alice's Adventures in Wonderland" by Lewis Carroll.

Example 1:

Input message:

Circular queue is a linear data structure in which the operations are performed based on first in first our principle

Output ciphered message:

eucwlewjakazouynizimbzrgslriqlitelrgyjkkrpxunabe
nlrwcsvxvrnwutxtkdhysiazvuyoqlxjabrgltxwlekjako
zwjkfvmiuniuvhexyrpmrtvrgeejvtpbjapozyakqvmtz
mmzztlr

Decipher operation:

circularqueueisalineardatastructureinwhichtheoperat
ionsareperformedbasedonfirstinfirstourprinciple

Example 2:

Input message:

In a normal queue we can insert elements until queue becomes full but once queue becomes full we cannot insert the next element even if there is a space in front of queue

Output ciphered message:

kqdbiqftevuvijktkruqiizzntpekdymwvnwouyglrbpue
ezenxolrvbavcchpzuleiexzgmvlrslrqtemktgexgkdvqi
kccumcikdryvtezclrnxivtehozgnxiqlmexjgmylretpst
euqkgtxgijkbalzcfucnpzjteuqkvuycqlrunpazyuyslez
pumozwewskrjtemedwlr

Decipher operation:

Inanormalqueuewecaninsertelementsuntilqueuebeco
mesfullbutoncequeuebecomesfullwecannotinsertthe
nextelementevenfifthereisaspaceinfrontofqueue

Example 3:

Input message:

Alice was beginning to get very tired of sitting by her sister on the bank, and of having nothing to do: once or twice she had peeped into the book her sister was reading, but it had no pictures or conversations in it, 'and what is the use of a book,' thought Alice 'without pictures or conversation?' So she was considering in her own mind (as well as she could, for the hot day made her feel very sleepy and stupid), whether the pleasure of making a daisy-chain would be worth the trouble of getting up and picking the daisies, when suddenly a White Rabbit with pink eyes ran close by her. There was nothing so VERY remarkable in that; nor did Alice think it so VERY much out of the way to hear the Rabbit say to itself, 'Oh dear! Oh dear! I shall be late!' (when she thought it over afterwards, it occurred to her that she ought to have wondered at this, but at the time it all seemed quite natural); but when the Rabbit actually TOOK A WATCH OUT OF ITS WAISTCOAT-POCKET, and looked at it, and then hurried on, Alice started to her feet, for it flashed across her mind that she had never before seen a rabbit with either a waistcoat-pocket, or a watch to take out of it, and burning with curiosity, she ran across the field after it, and fortunately was just in time to see it pop down a large rabbit-hole under the hedge. In another moment down went Alice after it, never once considering how in the world she was to get out again.

Output ciphered message:

clezwknxbkloyabyveisbadbderswkksbzvmh
erpeinxbnwoigkhruwuitlqythvdszkfmtttpamvbyhmq
uwlthgorllxfbkhlegvemxdtqwnlekorshmtwodwtmve
psbmlolerudsmxbaqwvxmswkwxbfwohthvdspvlew
odpaotjrkfxttuabpetixdwlqhdsvveiuidlocrvpihkbrett
qmchihmhmidfhabijbbhmbbkfgkcjbslxvttwjagettlw
zvmvwhketqlxttxyvvuqzllxeuwjthoorilxcbkylegvex
xdmqwfleworrhmbwoiwtvvemsbvlodercdswxbkqw

bxmgpxugkchfxzgpttythywkiheauuedschfrxbjwocw
hfihjuirbpkpabruoimvdbhvvjwailxztxqabkjbsimulqc
lepihluirpaujakveihmlenfgkcvexlxflqjthsvbkvxwbk
ohenhfhhmnubqhefetylwydfythjvbwvxtlqfdsoveczg
zttuthfwkjxbpvmgfxftjnkfmvmyxmnwkzuivubtpam
vexhmlbpycbghfxwultxcthbdshimanlnerwruulcqqcf
abktjpxbvlqndsjlmixbrwovotvvejhecvmffxgwaivla
wowuhfmeihmwlozrvorufhebtxkrvbwavrvvwkjlxztt
yleydsiimaubpabcihxkfyvmclepwdlimsvmqabjwdm
hmenlsthtdsibrubpcerfwkpkfivmvpanhfmlwznlpvvh
wklxdatxnrvpwatwqeqcfxmweillxitxferkdsgxdmtxv
rvvjbnvleubexmkvebhdsvmqlejruiimeensvvowazim
klojrvcvechmbttilehhfxlcypagthkdsfwuyqcnabqjbpi
mrqccabfjbximpnlyerttjfvljqcdfxwdsblwjqwueradsx
mdoqwkuhhhlximrlqfvvhwawvlpdbfersdselwztxiabj
ihilxvttcotfveqhmsbkbabcihpbryqcdabshfqhmiubnm
cgqzesbpwogthbvbwvxydbythvdsmkfouuwstuwapx
bgqwcfxvetslxdimgfxfjbfimnnlnergvbzvlnuuclefihh
xdslocabvjbtimpenethivezuyzubyerfwdxlxwvmjlese
twlxkttbxmceibbrsqwjlesdssuihwoaerjdsyimbbpqcb
vtjivldloyblyqzsxdelqfthsvbwlxeqcxjjcveblxgqwjfx
wvewimjqcoabvlmfhmbuwvpavihmwukwoceromei
vlinlvgkoveqsbyttmmcgrumxbulqgdsrihuuycvmcstv
vbjzgevmclehdsckfrvmudsnvefzghfcvrvketmhmmtt
hxmvihplxmtxtrvowafwqsqwcjjvvefhmclqvpaiihiw
uywofwhavexhmwlqqerymefxbeuuurvvhfkbrylqqrv
iwaxxbolqzxmkveyhdfvmyleoihqhmauunrveorshmi
wovfxdettzgtvmelegetbhmafcpdsrihpwubqcixmmds
jkflvmcwhhihqsbbbpupapwkhkfkvmjwhshfsxdhlqo
vvtbzzimvlqgvvrqzslxvttugknhfnxbkwo

Decipher operation:

alicewasbeginningtogetverytiredofsittingby
hersisteronthebankandofhavingnothingtodoonceort
wiceshehadpeepedintothebookhersisterwasreadingb
utithadnopicturesorconversationsinitandwhatistheus
eofabookthoughtalicewithoutpicturesorconversation
soshewasconsideringinherownmindaswellasshecoul
dforthehotdaymadeherfeelverysleepyandstupidwhet
herthepleasureofmakingadaisychainwouldbeworthth
etroubleofgettingupandpickingthedaisieswhensudde
nlyawhiterabbitwithpinkeyesranclosebyhertherewas
nothingsoveryremarkableinthatnordidalicethinkitsov
erymuchoutofthewaytohearthrabbitsaytoitselfohde
arohdearishallbelatewhenshethoughtitoverafterward
sitoccurredtoherthatsheoughttohavewonderedatthisb
utatthetimeitallseemedquitenaturalbutwhentherabbit
actuallytookawatchoutofitswaistcoatpocketandlooke
datitandthenhurriedonalicestartedtoherfeetforitflash
edacrosshermindthatshehadneverbeforeseenarabbit
witheitherawaistcoatpocketorawatchtotakeoutofitan
dburningwithcuriositysheranacrossthefieldafteritand
fortunatelywasjustintimetoseeitpopdownalargerabbi
tholeunderthehedgeinanothermomentdownwentalice
afteritneveronceconsideringhowintheworldshewasto
getoutagain

Comparative Factors

This section presents a comparison of factors for various discussed encryption techniques, as explained in Table 1, where the comparative factors used are the media type, the particular technique utilized, and the existing of circular queue data structure. It is worthwhile to mention the Performance measures usually performed using several performance metrics when ciphering images, audio, or even video files but not for ciphering text. The most common measures are; The Peak-to-Signal-Ratio (PSNR), which measures the difference between original and reconstructed image pixels, and Structural similarity index Structural similarity (SSIM) which a new metric to measure the similarity between original image and reconstructed image based on the concepts of human visual system (HSV)(1).

Table 1. Comparison between different encryption methods.

Research number	Media type	Applied methods	Circular queue used
Reference (2)	Text, image, and multimedia.	Matrix scrambling technique based on random number selection, shifting and reversing techniques of circular queue.	Yes
Reference (8)	Text	circular substitution concept with reversal transposition	Yes
Reference (10)	Image	Advanced Encryption Standard AES, Advanced Encryption Standard RSA, Advanced Encryption Standard Proposal AESP using circular queue	No
Reference (12)	Text, image, and multimedia.	Decision Diffie-Hellman assumption	Yes
Reference (14)	Text	various encryption methods such as; Caesar, Vigenère, Affine, and multiplicative	Yes
Reference (15)	Image	genetic algorithm (GA) and chaotic function	No
Reference (3)	Text	Multiple Access Circular Queues	Yes
Reference (13)	Text, image, and multimedia.	Multiple Circular Arrays	No
Reference (11)	text, audio, image, and	Circular Queue and Graycode	Yes
Reference (18)	video files	Combination set of encryption algorithms (DES, Triple DES, Blowfish, AES)	No
Proposed method	Text	Combined Homophonic Substitution Cipher and Polyalphabetic Substitution Cipher using Circular queue	Yes

System Analysis

Java application language was developed to test the proposed algorithm, lots of experiments were performed on different length's characters. The proposed method for both encryption and decryption operations can be completed in n time if (n) is the total number of characters used in the plaintext. The suggested algorithm does not require any additional space for computational stage of the algorithm. The time complexity for the proposed work is O (n^2). In homophonic cipher, Each generated homophonic key is created randomly from the original alphabetic to obtain more sophisticated key and therefore the algorithm will be hard/ strong against text breaking, four keys in total are required for the final purpose. While In Polyalphabetic keys generation, the number of keys in polyalphabetic is equal to the number of keys used in homophonic, these four keys are generated by using a different keyword for each one. The homophonic and polyalphabetic generated keys are combined together in a single circular queue in order to produce a complex algorithm. Experimental results shows the strength of the proposed algorithm, in example 3, a large paragraph with special characters is used; the algorithm removed all the spaces and special characters.

The Advantages of the proposed work is that it is complex and immune against breaking, and there is no fixed size for the entered set of characters. Even the proposed system has been tested on text only, however, it can be applied easily on other media types such as image, and video files. The main shortening of the algorithm lies in the misuse of the key's selection, and the generated keys are used for stream not block ciphering. Finally the algorithm has not been examined for special input characters.

Conclusion and Future Works:

Message ciphering is an important issue in every single communication done in our life, due to the widespread of electronic devices that can break many cipher texts. Single algorithm for ciphering and deciphering can produce unsecure text. However, combining several methods can produce more sophisticated and complex cipher text that can be immune to break. This work suggested a combination of two encryption algorithms; homophonic substitution and polyalphabetic substitution techniques, these two methods are combined together using the significant circular queue data structure with four different keys for each technique, and this combination produced eight different outcomes results for each single incoming letter. The time required for ciphering and deciphering a non-short massage is less than 0.1 sec.

This proposed method can be expanded in general by combining more than two ciphering algorithms as well as using several circular queues for the encryption of each next incoming letter sequentially.

Authors' declaration:

- Conflicts of Interest: None.
- We hereby confirm that all the Figures and Tables in the manuscript are mine ours. Besides, the Figures and images, which are not mine ours, have been given the permission for re-publication attached with the manuscript.
- Ethical Clearance: The project was approved by the local ethical committee in University of Baghdad.

References

1. Jain M, Lenka SK, Vasistha SK. Adaptive circular queue image steganography with RSA cryptosystem. Perspectives in Science. 2016 Sep 1;8:417-20. Doi: http://dx.doi.org/10.1016/j.pisc.2016.04.093 2213
2. Kumar MK, Azam SM, Rasool S. Efficient Digital Encryption Algorithm Based On Matrix Scrambling Technique. IJNSA. 2010; 2(4). Doi: 10.5121/ijnsa.2010.2403
3. Phull S, Som S. Symmetric cryptography using multiple access circular queues (MACQ). InProceedings of the Second International Conference on Information and Communication Technology for Competitive Strategies. 2016 Mar 4 (pp. 1-6). https://doi.org/10.1145/2905055.2905166
4. Ogla RA. Symmetric-Based Steganography Technique Using Spiral-Searching Method for HSV Color Images. Baghdad Sci. J. 2019;16(4):948-58. DOI: http://dx.doi.org/10.21123/bsj.2019.16.4.0948
5. Swain G, Lenka SK. A novel steganography technique by mapping words with LSB array. IJSISE. 2015 Jan 1;8(1-2):115-22.
6. Agarwal P, Agarwal N, Saxena R. Data encryption through fibonacci sequence and unicode characters. MIT International Journal of Computer Science and Information Technology. 2015 Aug;5(2):79-82.
7. Eric C. Hiding in plain sight, Stegnography and the art of Covert Communication. Wiley, Indianapolis, Indiana, ISBN. 2003;10:0471444499. Available at: https://dl.acm.org/citation.cfm?id=862089
8. Isaac ER, Isaac JH, Visumathi J. Reverse Circle Cipher for personal and network security. In2013 International Conference on Information Communication and Embedded Systems (ICICES) 2013 Feb 21 (pp. 346-351). IEEE. Available at: https://www.researchgate.net/publication/261054865_Reverse_Circle_Cipher_for_personal_and_network_security
9. Kallam Ravindra Babu, S.Udaya Kumar, A.Vinaya Babu, "A Survey on Cryptography and

Steganography Methods for Information Security", IJCA, Vol.12, No.2, pp. 0975 – 8887, 2010.
10. Jabbar KK, Hilal HA, Mohammed RS. Text Cryptography Using Multiple Encryption Algorithms Based on Circular Queue via Cloud Computing Environment. JATIT . 2018 Jun 30;96(12).
11. Sumayya KA, Abraham JP. Data Security Algorithm Using Circular Queue and Graycode. InProceedings of ICETIT 2019 2020 (pp. 993-1004). Springer, Cham.
12. Boneh D, Halevi S, Hamburg M, Ostrovsky R. Circular-secure encryption from decision diffie-hellman. InAnnual International Cryptology Conference 2008 Aug 17 (pp. 108-125). Springer, Berlin, Heidelberg. Available at: https://link.springer.com/chapter/10.1007/978-3-540-85174-5_7
13. Suri PR, Deora SS. A Cipher based on Multiple Circular Arrays. IJCSI. 2013 Sep 1;10(5):165.
14. Wisam A S, Khalid K J, Luheb K Q. A Proposed Hybrid Text Cryptographic Method Using Circular Queue. IJCET. 2018; 9(7) :1123–1132.
15. Nichat SP, Sikchi SS. Image encryption using hybrid genetic algorithm. IJARCSSE. 2013 Jan;3(1):427-31.
16. Ibraheem NA. Finger Identification and Gesture Recognition Using Gaussian Classifier Model. IJAER. 2016 Jan;11(10):6924-31.
17. Albahar MA, Olawumi O, Haataja K, Toivanen P. Novel Hybrid Encryption Algorithm Based on Aes, RSA, and Twofish for Bluetooth Encryption. Journal of Information Security. 2018 Feb 12;9(2):168-76. Doi: 10.4236/jis.2018.92012
18. Mustafa A. Calculation of encryption algorithm combination for video encryption using two layers of AHP. In2016 10th International Conference on Telecommunication Systems Services and Applications (TSSA). 2016 Oct 6 (pp. 1-7). IEEE. DOI**:** 10.1109/TSSA.2016.7871099
19. Harini K, Pravallika N, Sashi R K. Enhancement of Data Security using Circular Queue Based Encryption Algorithm. IJITEE. 2019; 8 (12): 65-67.

دمج مجموعة طرق الاستبدال باستخدام هيكل بيانات الطابور الدائري

نور عدنان ابراهيم **مختار محمد حسن**

قسم الحاسوب، كلية العلوم للبنات، جامعة بغداد، بغداد، العراق.

الخلاصة:

مع التوسع الثوري في الإنترنت ، تتزايد المعلومات العالمية في تطبيق تكنولوجيا الاتصالات، ويعزز النمو السريع لحجم البيانات الكبير الحاجة إلى تحقيق تقنيات آمنة وقوية وواثقة باستخدام خوارزميات فعالة مختلفة. تقدم هذه الورقة نظامًا تشفيريًا يجمع بين عدة خوارزميات لشفرة الاستبدال جنبًا إلى جنب مع هيكل بيانات طابور دائري . تقنيات الاستبدال المستخدمة هي: شفرة هوموفونك وشفرة بولي الفابيتك، قد دمجت في طابور دائري واحد مع أربعة مفاتيح مختلفة لكل منهما، والتي تنتج ثمانية مخرجات مختلفة لكل حرف وارد واحد. العمل الحالي ممكن تطبيقه بكفاءة لأمنية المعلومات الشخصية وأمنية اتصالات الشبكة كذلك.

الكلمات المفتاحية: الطابور الدائري، شفرة الاستبدال، شفرة استبدال هوموفونك، وشفرة استبدال بولي الفابيتك.