Available online at www.qu.edu.iq/journalcm
JOURNAL OF AL-QADISIYAH FOR COMPUTER SCIENCE AND MATHEMATICS
ISSN:2521-3504(online) ISSN:2074-0204(print)

# *Cryptography model based on the principles of the geometric Series*

**Sundus Hatem Majeed**

**Baghdad University , Baghdad ,Iraq. E-mail : saohhatem@yahoo.com**

**ARTICLE INFO**

*Article history:*
Received: 08 /08/2021
Rrevised form: 30 /08/2021
Accepted : 19 /09/2021
Available online: 09 /10/2021

*Keywords:*

sequences, attack , cryptography, key.

**ABSTRACT**

Given the rapid advancement of data innovation and the massive volume of data exchanged over the Internet, which needs protection from electronic theft and extortion, there are many encryption algorithms that developed to protect data. Development in the field of coding (Cryptography) has always been accompanied by a development in the field of decoding and Cryptanalysis. This led to the Weakness of many encryption algorithms. Therefore, the need to develop a new methods are necessary. In this paper, a method based on geometric series for encrypting data was proposed, where two keys are used, the amount of the incremental in sequence represents the first key; the number of terms in the sequence represents the second key. The proposed model has been tested using a number of appropriate attack techniques; the proposed model has proved its efficiency and strength against attacks several technique of attacks are applying on the propose model, the results proved that the strength of the proposed method. As a contribution, this paper using a sequence to concatenate the values of the sequence terms to hide the origin character ASCII code which adds fuzzy cryptography to guess the correct ASCII code.

MSC. 41A25; 41A35; 41A36.

DOI : https://doi.org/10.29304/jqcm.2021.13.3.851

## 1. Introduction

The art and science of ensuring security by secret writing messages to create them decipherable are known as cryptography. The rapid advancement of network technology has

*Corresponding author : *Sundus Hatem Majeed*
Email addresses: *saohhatem@yahoo.com*
Communicated by: Dr.Rana Jumaa Surayh aljanabi.

resulted in a common data-sharing culture. Hence, you are more vulnerable to data being copied and redistributed by hackers.

Therefore, info should be protected whereas it's being transmitted, touchy info like credit cards, bank exchange, also Numbers associated with Social Security must be saved. There are several encryption algorithms available for this purpose. Within In the last several days, of communication over the air, encoding acts an awfully critical part in protective information in on-line transmission, primarily that specialize in wireless technology's security. Various secret writing techniques are utilized to shield confidential information from unauthorized access. Encoding could be a quite common technique wont to promote info security. The progress of the cryptography is heading towards unlimited possibilities. New encryption strategies are being discovered every day. This document covers some of the recent existing encryption techniques and their comparison. [10],[6].

In this paper a new technique through using geometric series was proposed, where the new technique consist of three phases, the first phase is key generation phase and the second is the encryption phase where the third phase is decryption phase, for evaluating the proposed method , many cryptanalysis techniques were applied to test the security and the efficiency for the proposed method as discussed in the result and discussion section .

**2-Sequence and Series Definition**

Any item or group of numbers may be arranged in a specified arrange, which is called a sequence, following a certain rule. In case of a1, a2, a3, a4, . . ., etc. identify the elements or teems of the sequence, so 1,2,3,4,… .. denote the term's position . The number of elements or terms can be used to determine the sequence, that is, an endless sequence. In case a1, a2, a3, a4, . . . is a sequence, then the equivalent series has the form SN = a1 + a2 + a3 + .. + aN. A series is summation of a sequence, for a finite sequence made up of numbers; it is possible to get the series by adding up individual terms. Series can be found for infinite sequences also.[2].

**3-Sequence and Series Types**

The following are some of the most popular sequences:

A: arithmetic sequence is a series of numbers generated by adding or subtracting a given number from the preceding number.

B: Geometrical Sequence is the sequence wherein each item is acquired by divided or multiplied a particular item by the previous item.

C: Fibonacci Numbers form an interesting sequence of numbers in which each element is obtained by adding two preceding elements, and the sequence begins with 0 and1.

The arrangement is characterized as F0 = 0 and F1 = 1 and Fn. = fn-1 + fn-2 .

Fibonacci sequence, create an intriguing series of numbers in which each member is created by adding two preceding items, starting with 0 and 1.

D: Harmonic Sequence: If the reciprocals of all of the components of a number series form an arithmetic sequence, it is said to be in a harmonic sequence.[2],[5].

## 4. Literature review

Al-din, B. N., et. al. propose a new algorithm through classify the characters of the message into groups and exchange the keys between the groups to be difficult on the cryptanalytics to follow the path of constructing the system, also using the different cryptanalysis techniques to evaluate the proposed algorithm.[3]

Mansara (AM) and Aldin (BN) use advanced Caesar ciphers by embracing two private keys connected to character's positions (that is, odd and even) in order to encrypt and/or decode

data. The two private-keys are mapped to the public-key and transferred toward the direction of the receiver. Finally, the results show that the new cryptosystem is inevitable for cryptanalysis attacks. It also reduces the size of the ciphertext and reduces available memory. The creation of public keys has shown to be a one-way process that is based on a binary matrix that is created and exchanged by the two communication parties.[7]

Abed, B. N. et. al. . A new cryptosystem was introduced using a one-variable third-order equation and by employing Cardano's strategy to solve a cubic equation to make the suggested cryptosystem more secure and sophisticated. Since then, there are four possible symmetric-keys and a variable equation formula, several cryptoanalyses have been applied to the suggested cryptosystem to make certain the reliability and confidentiality of the suggested algorithm, all showing the cryptosystem's resistance to attacks, as described in the Results section shown in.[1]

Norman, S. A., et. at. New methods of data encryption are being suggested. The suggested approach is based on the Taylor series and involves selecting a constant value and a Taylor expression as a two keys. The first key (constant value) then replaces the plain-text into Taylor expression. The decryption phase is required to calculate the Taylor inversion. Several types of attacks, such as A D F G V X dictionary attacks, frequency attacks, and autocorrelation attacks, are employed to assess the suggested method's effectiveness.. The Taylor series makes the ciphertext even more complicated. The range of values used to assign the value x (range 0 to n) increases the likelihood of breaking cryptography, so the proposed cryptosystem is n * n! [9,].[8]

Ansah, R. K., et. al..This paper gives a basic introduction to elliptic curve cryptography (ECC) and its applications in cryptography. Elliptic curve cryptography has exactly the desired properties that help in making secured messages hardly to be hacked.[4].

## 5-Methodology

Figure (1) shows a flowchart that summarized the methodology of the proposed model

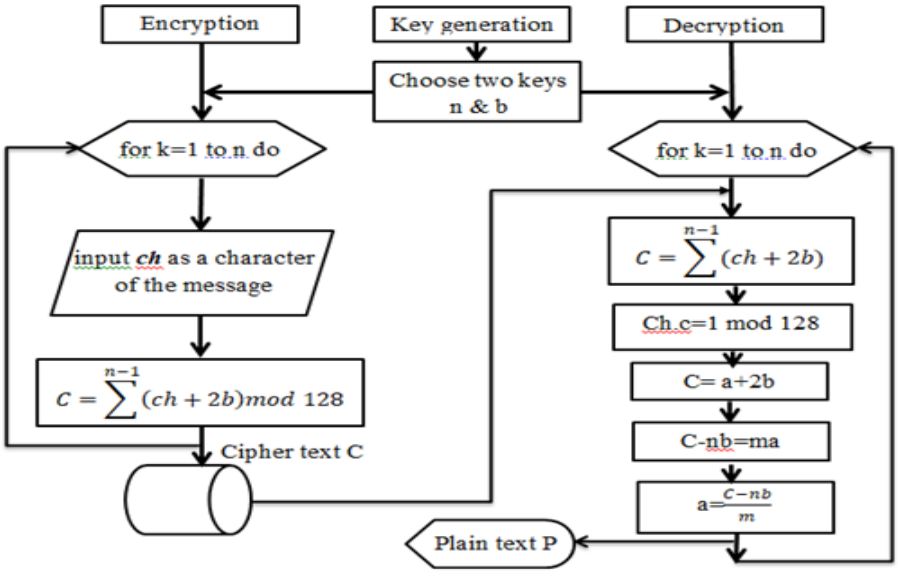



Fig. (1): A flowchart of the proposed model

### 5.1. Key generation

Int *n* the first key
Int *c* the second key // which represent the number of terms in sequence

### 5.2. encryption

Increment value *b*
Input *ch* // character of the message
Input c the number of terms in sequence
Convert message characters to ascii code

$$for\ b = 0\ to\ n-1\ do$$

$$C = \sum_{b=0}^{n-1} ch + 2b$$

$$C1 = C\ mod\ 256$$

Do for all characters in the message

### 5.3. decryption

Input the two secret keys *n* , *c*
Input the cipher text C1

$$C1 = \sum_{b=0}^{n-1}(ch + 2b)$$

$$For\ k = 1\ to\ n\ do$$

$$C = mod^{-1}(C1)$$

$$C = m * ch + 2b_{0\ to\ n-1}$$

$$C - b_{0\ to\ n-1} = m * ch$$

$$ch = \frac{C - b_{0\ to\ n-1}}{m}$$

$$Plain\ text\ P$$

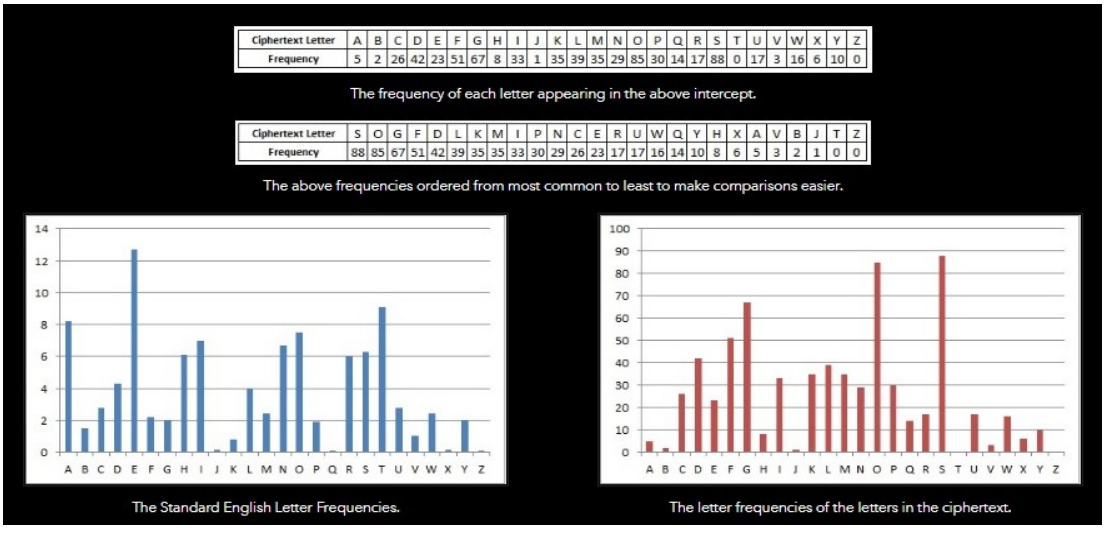
**a. example:**

**key generation phase**
let n=4
c=3
**encryption**
plain text = ARE YOU THERE
ch=A
ascii=65
C1= 65+67+69=201
207 mod 256 = 201
201=…
Do for all message characters
Cipher text = … ′ ┌ <DC1> Ū <ENQ> <STX>I] ┌ ′ ┌
**Decryption**
b=4 ,n=3

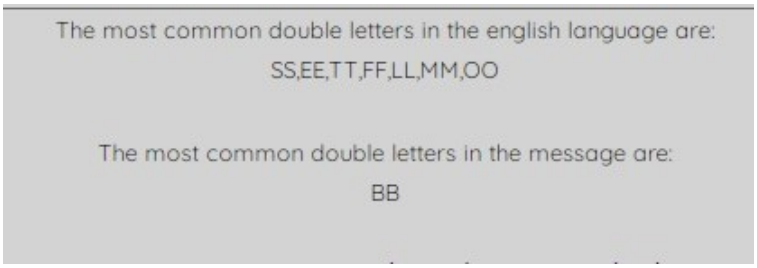
cipher text= … ′ ┌ <DC1> Ū <ENQ> <STX>Ⅎ ┌ ′ ┌ch.a=1 mod 128
first character …=201
201= x+(x+2)+(x+4)
3x=201-6
$x = \frac{195}{3} = 65$
x=65=A
do steps 1 -7 until end of cipher text
plain text = ARE YOU THERE
end

## 6-result and discussion

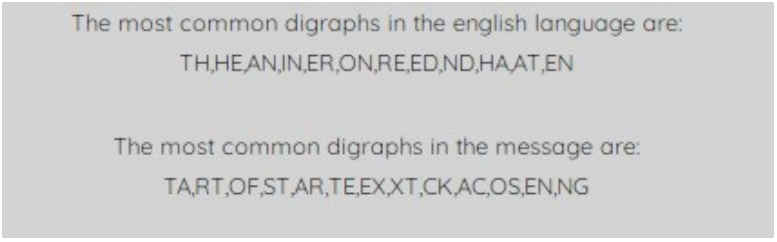
Different attack techniques are applied to test the proposed model, the results shown in the figure (2), the aim is to test the possibility of breaking a cipher text of the proposed model. By comparing the frequency of characters in the encrypted text, with the standard character frequency of the English language, as the results of applying this analysis to the encrypted text, showed a big difference between frequency values in English characters and the frequency values of the encrypted text characters, as shown in figures (2.a). Another attack is to determine the most common double_letters that found in the English alphabet, the results showed that it was no way to specify any double letter, as shown in figure (2.b). Also, to determine the most common digraphs characters as in English letters or what is known conventionally, as the results showed that it is not possible to specify any digraphs, as shown in figure (2.c). the fourth attack is the most common trigraphs attack as shown in figure (2.d).



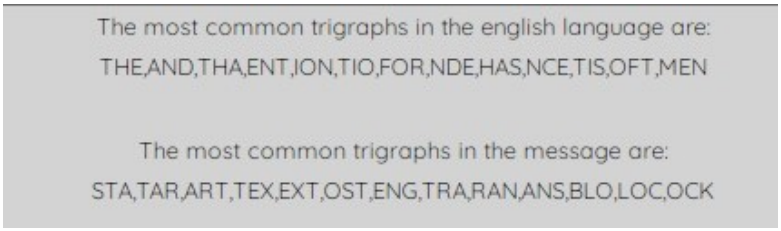

a. The frequency attack.




b. The most common double letters attack.




c. The most common digraphs attack.




d. The most common trigraphs attack.

Fig.(2): Different attack techniques are applied to test the proposed model :(a):The frequency attack , (b): The most common double letters attack. (c): The most common digraphs attack. (d): The most common trigraphs attack

## 5. Conclusion

In this paper, a new algorithm for encrypt and decrypt the information proposed based on the principle of the mathematical model that used the summation of the sequence, where the sequence consist of number of the terms that increment by the fixed value, the proposed algorithm determine the number of terms and the incremental value that used as a two keys in the algorithm. Using a variety of assault methods to break the ciphertext, all result show that the cipher text was unbreakable and attack techniques doesn't guess the keys.

## References

[1] Abed, B. N.,Kamil, B. Z., Hameed, M. A., & Abdullah, J. N. (2020, November). Using Cardano's method for solving cubic equation in the cryptosystem to protect data security against Cyber attack. In *2020 2nd Annual International Conference on Information and Sciences (AiCIS)* (pp. 127-131). IEEE. 55

[2] Alcock, L., & Simpson, A. (2005). Convergence of sequences and series 2: Interactions between nonvisual reasoning and the learner's beliefs about their own role. *Educational studies in mathematics*, *58*(1), 77-100. 22

[3] Al-din, B. N., Manasrah, A. M., & Noaman, S. A. (2020). A Novel Approach by Using a New Algorithm: Wolf Algorithm as a New Technique in Cryptography. *Webology*, *17*(2), 817-826. 33

[4] Ansah, R. K., Effah-Poku, S., Addo, D. A., Adjei, B. A., Bawuah, B. K., & Antwi, P. (2018). Relevance of elliptic curve cryptography in modern-day technology. *Journal of Mathematical Acumen and Research*, *3*(2). 77

[5] G. B. Thomas, R. L. Finney, M. D. Weir and F. R. Giordano, "Thomas' calculus: Addison-Wesley Reading", 2003.

[6] M. Viswanath and M. Ranjithkumar, "A secure cryptosystem using the decimal expansion of an Irrational number", *Applied Mathematical Sciences*, vol. 9, pp. 5293-5303, 2015.

[7]. Manasrah, A. M., & Al-Din, B. N. (2016). Mapping private keys into one public key using binary matrices and masonic cipher: Caesar cipher as a case study. Security and Communication Networks, 9(11), 1450-1461. 44

[8] Mitali, V. K., & Sharma, A. (2014). A survey on various cryptography techniques. International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), 3(4), 307-312. 11

[9] Noaman, S. A., Abed, B. N. A. D., & Abdul-Kader, S. A. A. (2020, July). A New Mathematical Model to Improve Encryption Process Using Taylor Expansion. In 2020 1st. Information Technology To Enhance e-learning and Other Application (IT-ELA (pp. 35-40). IEEE. 66

[10] O. M. Mendoza, "Taylor series variance estimation for selected indirect demographic estimators", the University of North Carolina at Chapel Hill, 1982.

[11] H. Noman Abed, “Robust and Secured Image Steganography using LSB and Encryption with QR Code”, JQCM, vol. 9, no. 2, pp. Comp 1-9, Aug. 2017.

[12] Z. Fahad Mhawes, “Dihedral Cryptographic Technique”, JQCM, vol. 10, no. 1, pp. Math Page 26 - 31, Jan. 2018.

[13] M. Hasan Abdulameer, “Image Encryption Using Columnar Transportation Technique and Bits Reversing”, JQCM, vol. 10, no. 1, pp. Comp Page 54 - 62, Jan. 2018.

[14] A. M. Abduldaim, “Weak Armendariz Zero Knowledge Cryptosystem”, JQCM, vol. 9, no. 2, pp. Math 1-6, Aug. 2017.\

[15] A. Kareem Wanas and S. Swamy, “Differential Subordination Results for Holomorphic Functions Related to Differential Operator”, JQCM, vol. 11, no. 2, pp. math 46-53, Aug. 2019.