Representing Kurdish Letters by using Partition Theory

[1]*Zana Ali Mahmood* [2*]*Awreng Baiz Mahmood*

[1]Academic researcher, Kurdistan, Iraq

[2]College of Sciences, University of Salahaddin, Kurdistan, Iraq

[1]zanaeducatin2024@gmail.com

[2*]awring2002@yahoo.com

Representing Kurdish Letters by using Partition Theory

[1]*Zana Ali Mahmood* [2*]*Awreng Baiz Mahmood*

[1]Academic researcher, Kurdistan, Iraq

[2]College of Sciences, University of Salahaddin, Kurdistan, Iraq

[1]zanaeducatin2024@gmail.com

[2*]awring2002@yahoo.com

Abstract

Given the importance of encryption and maintaining the confidentiality of information and not penetrating it, this paper included encoding letters and words of Kurdish through Abacus James diagram in partition theory. This paper is an extension of the work of many researchers, such as Awreng, Ammar and Ahmed on encoding letters and words using Abacus James diagram for letters in the English language. It is completely natural that this method will have new and very difficult methods as an entrance to a new type of encryption process.

Keywords: Partition theory, e-abacus diagram, encryption and decryption process.

المستخلص

نظراً لأهمية التشفير والحفاظ على سرية المعلومات وعدم اختراقها، تناولت هذه الورقة ترميزا

لحروف وكلمات اللغة الكردية باستخدام مخطط أباكس جيمس في نظرية التجزئة. يعتبر هذا البحث امتداداً لعمل العديد من الباحثين، مثل أورنك وعمار وأحمد، على ترميز الحروف والكلمات باستخدام مخطط أباكس جيمس للحروف في اللغة الإنجليزية. ومن الطبيعي أن تتطور هذه الطريقة بطرائق جديدة وصعبة للغاية كمدخل إلى نوع جديد من عمليات التشفير.

1. Introduction

James abacus with $\boldsymbol{\gamma}$ −number is one of the graphical representations for any partition of a non-negative integer and it can be divided into several chains which consist of outer and inner chains. Also, numbers can be represented by a diagram called $\boldsymbol{e}$ −abacus diagram, where every $\boldsymbol{\gamma}$ − number will be represented by a (□) and the rest of the sites by $(-)$.

Let $\boldsymbol{n}$ be a positive integer. **A composition** of $\boldsymbol{n}$ is a sequence $\boldsymbol{\mu} = (\boldsymbol{\mu_1}, \boldsymbol{\mu_2}, \dots)$ of non-negative integers such that $\boldsymbol{n} = |\boldsymbol{\mu}| = \sum_{\boldsymbol{i}} \boldsymbol{\mu_i}$. The integers $\boldsymbol{\mu_i}$ for all $\boldsymbol{i} \geq \boldsymbol{1}$ are the parts of $\boldsymbol{\mu}$ and $\boldsymbol{\mu_i} = \boldsymbol{0}$ if $\boldsymbol{i} > \boldsymbol{k}$, we identify $\boldsymbol{\mu}$ with $(\boldsymbol{\mu_1}, \boldsymbol{\mu_2}, \dots, \boldsymbol{\mu_k})$**.** A composition $\boldsymbol{\mu}$ is **a partition** if $\boldsymbol{\mu_j} \geq \boldsymbol{\mu_{j+1}}$, for all $\boldsymbol{j} \geq \boldsymbol{1}$. Now, Let $\boldsymbol{\sigma}$ be the number of redundant partsof the partition $\boldsymbol{\mu}$ of $\boldsymbol{n}$, then we have $\boldsymbol{\mu} = (\boldsymbol{\mu_1}, \boldsymbol{\mu_2}, \boldsymbol{\mu_3}, \dots, \boldsymbol{\mu_r}) = \left(\boldsymbol{\lambda_1^{\sigma_1}}, \boldsymbol{\lambda_2^{\sigma_2}}, \dots, \boldsymbol{\lambda_m^{\sigma_m}}\right)$ such that: $|\boldsymbol{\mu}| = \sum_{\boldsymbol{i=1}}^{\boldsymbol{r}} \boldsymbol{\mu_i} = \sum_{\boldsymbol{k=1}}^{\boldsymbol{m}} \boldsymbol{\lambda_k^{\sigma_k}}$, [1]. To clarify the above concepts, we take the partition of $\boldsymbol{4}$ by $(\boldsymbol{4}) = (\boldsymbol{4^1})$ are $(\boldsymbol{3}, \boldsymbol{1}) = (\boldsymbol{3^1}, \boldsymbol{1^1})$ or $(\boldsymbol{2}, \boldsymbol{2}) = (\boldsymbol{2^2})$ or $(\boldsymbol{2}, \boldsymbol{1}, \boldsymbol{1}) = (\boldsymbol{2^1}, \boldsymbol{1^2})$ or $(\boldsymbol{1}, \boldsymbol{1}, \boldsymbol{1}, \boldsymbol{1}) = (\boldsymbol{1^4})$.

Definition 1.1: An $\boldsymbol{e}$ −Abacus is a Chinese abacus with $\boldsymbol{e}$ vertical runners, labeled $\boldsymbol{0}, \boldsymbol{1}, \boldsymbol{2}, \boldsymbol{3}, \dots, \boldsymbol{e-1}$ from left to right. We label the positions on the abacus $\boldsymbol{0}, \boldsymbol{1}, \boldsymbol{2}, \dots$ from left to right, top to bottom, [2].

Definition 1.2: The γ −numbers are defined by fix μ as a partition of n, choose an integer b greater than or equal to the number of parts of μ and define $\gamma_i = \mu_i + b - i, 1 \leq i \leq b$. The set $\{\gamma_1, \gamma_2, \ldots, \gamma_b\}$ is said to be a set of γ −numbers for μ, [2]. In the following diagram we will represent γ −numbers, by many runners depending on e is an integer number greater than or equal to 2, as follows in Table 1.

Table 1.1. *e*-Abacus Diagram

Run.1	Run.2	Run.3	…	Run.e
0	1	2	…	$e-1$
e	$e+1$	$e+2$	…	$2e-1$
$2e$	$2e+1$	$2e+1$	…	$3e-1$
.	.	.	…	.
.	.	.	…	.

James was the first to come up with the idea an e-abacus diagram in 1978 [2].This topic is important in many topics, especially in the field of encryption and maintaining the security or confidentiality of information. The word "**cryptography**" is derived from the Greek words **Krypto's**, meaning hidden, and **Graphene**, meaning to write. Historians believe Egyptian hieroglyphics, which began about 1900 B.C.E., to be an early instance of decipherment. The topic of e-abacus diagram was given great attention in the eleventh century by linking it to cryptography. There is more than one method used to encode the letters which depends on the concepts of partition theory. Eman and others encrypted English letters in 2015 by studying the concept of orbit, [3]. Hadil and Ammar encoded the Syriac letters in 2017 using the e-abacus diagram [4]. Awreng and Ammar also introduced another new technology for encrypting words and sentences in the English language, based on e-abacus diagram in 2019, [5,6]. After that, Ahmed and Ammar encrypted the letters and sentences by linking e-abacus diagram to directed graph theory

[7]. In 2021, the question that was asked in the source: Is it possible to break up any fairly large chart into smaller charts? The answer was yes, as formulas were found to provide division for many cases, [8]. And in 2022, Hiba and Ammar found connection between partition theory and mapping, which we will describe as the initial steps toward convergence with other types of mapping by merging a process between them, [9]. In addition, new methods were found by integrating Young's diagram with graph theory, [10]. In 2024, both Ammar and Juan added a row (rows) to the e-abacus diagram,[11]. To learn more concepts about partition theory, e-abacus diagram and Young diagram, you can see the references [12-14]. For this reason, we had to present an encoding of the Arabic-Kurdish letters in this article on the basis of the e-abacus diagram.

Finally, the goal of this paper is to create a database of Kurdish characters to encrypt and decode messages in future papers.

2. Encrypt The Specific Kurdish Alphabet:

The Kurdish alphabet means the letters of the Kurdish alphabet, that is, the basic letters that make up phrases, sentences, or words. These letters are divided into two parts:

i. The first section: silent letters or so-called consonants, which are as follows:

(ئ، ب، پ، ت، ج، چ، ح، خ، د، ر، ڕ ، ز، ژ، س، ش، ع، غ، ف، ڤ، ق، ک، گ، ل، ڵ، م، ن، هـ)

ii. The second section is the vowels, that is, the vowels which are as follows:

ا ، ه، و، وو، ۆ، ی ، ێ)(

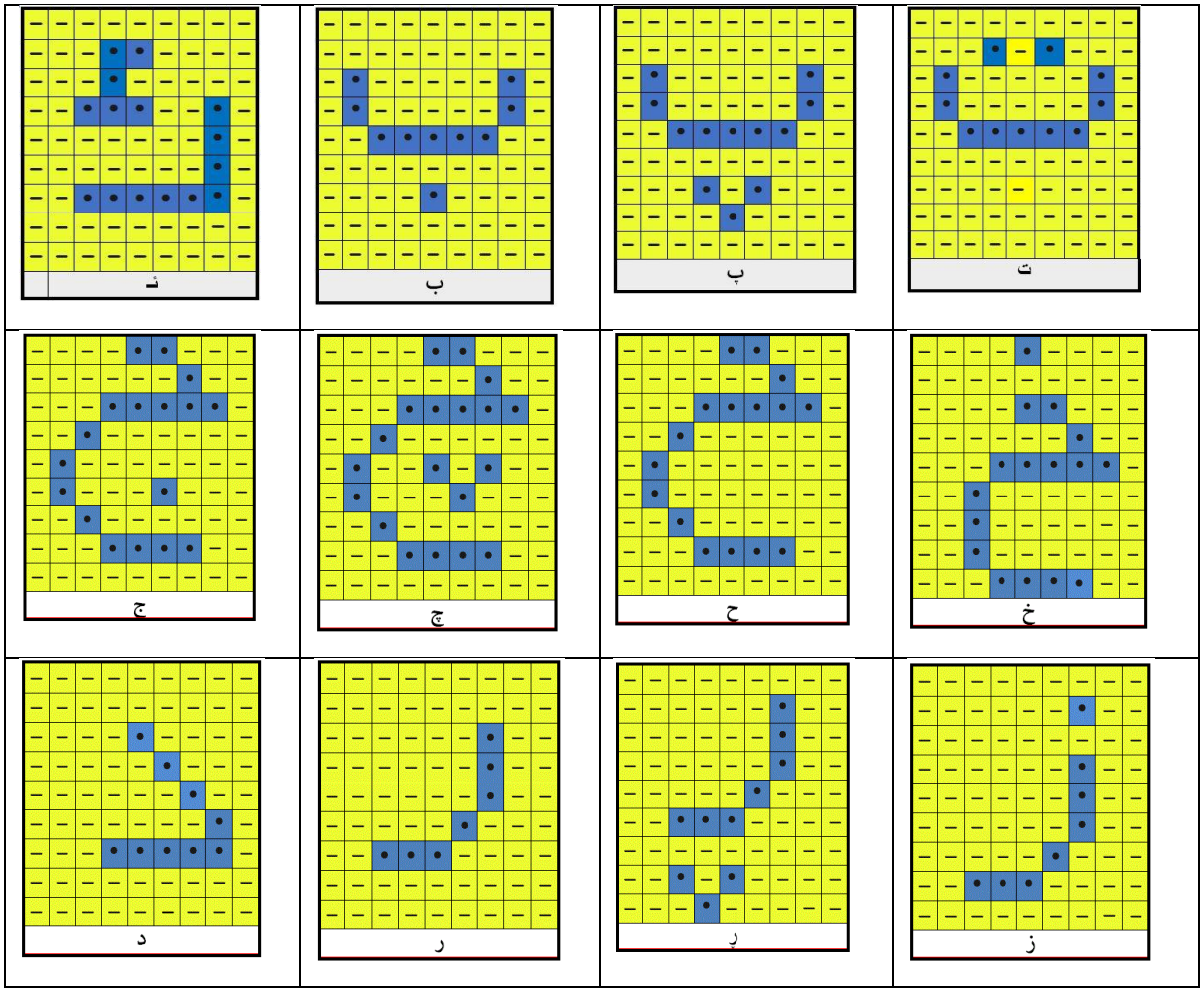
For setting up a concrete security model, firstly we test the letters in an Abacus James diagram in each diagram the symbol of bead ” ▯ “ is used to represent the position of $\boldsymbol{\gamma} -$ numbers in such a way that creates 36 upper case Kurdish letters (29 consonant letters and 7 vowels letters and there

, so the actual sum is 34 letters). It can also "ي، و" are two letters in common be noted that many of the letters are Arabic letters as well.

We take the value of the number e is nine with the same numbers of row's. Get the general Abacus James diagram and then select the location of $\gamma -$ numbers on it, to get the appropriate shape for each character of the thirty six Kurdish letters. We found the appropriate design for each character, so that each letter appears appropriately and clearly, as follows:

Table 2.1.

Consonants Kurdish Letters



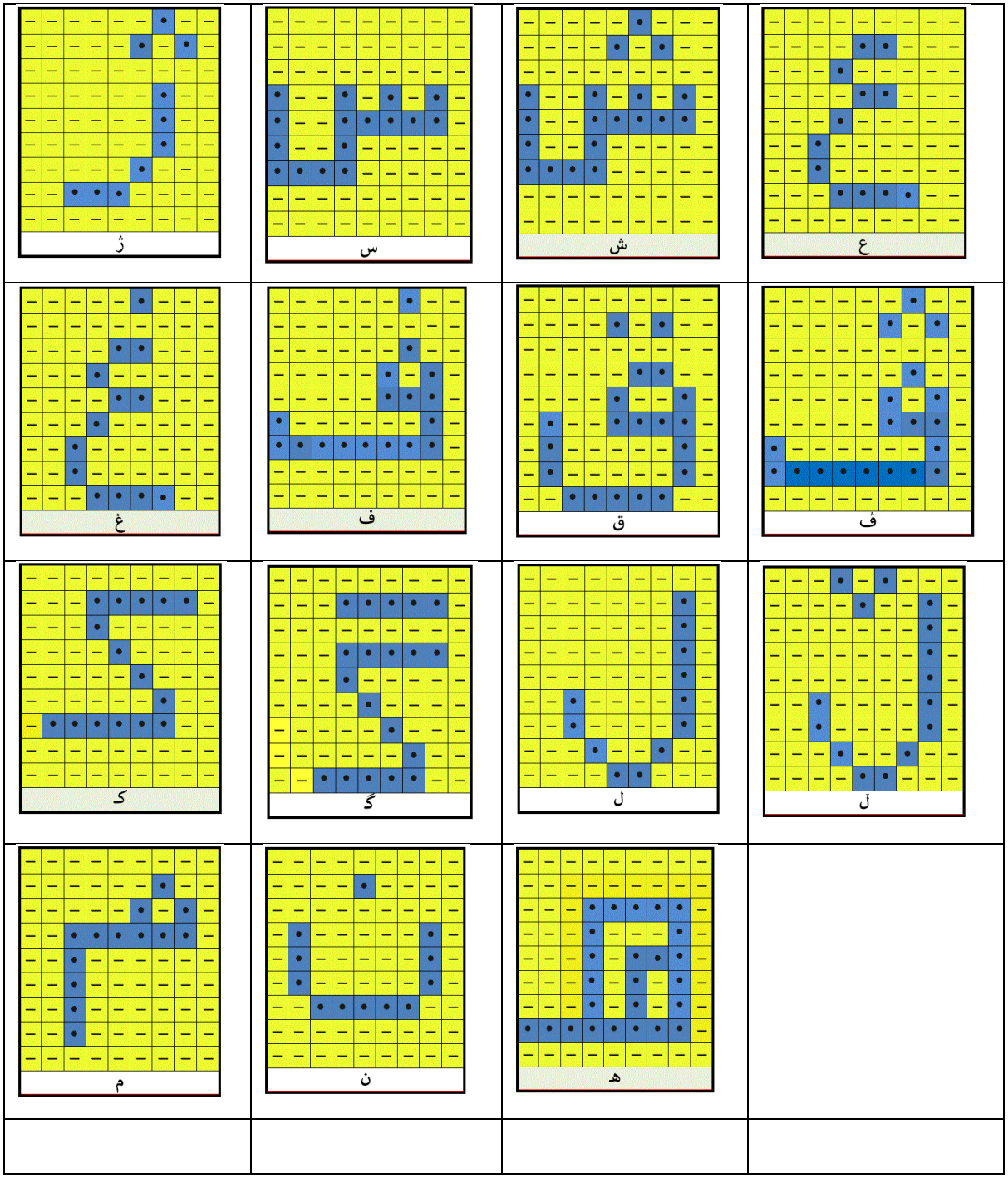
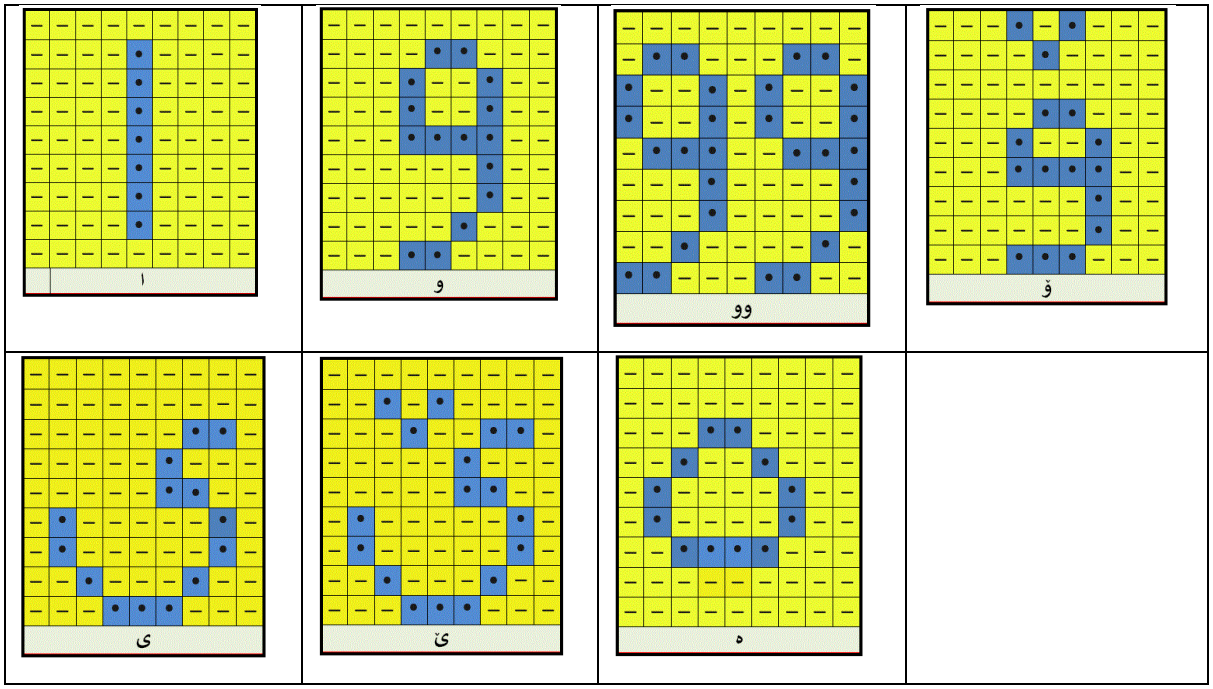


Table 2.2.

Vowels Kurdish Letters



Remark 2.1:

Arabic letters are distinguished by their difference in whether they are at the beginning, interior, or end of the word, but the general form known by them remains preserved. To reduce the use of diagrams, the word will be written on the origin of the letters, ignoring their location, whether it is at the beginning, at the end, or interior the word. This is also what is defined by the remaining letters of the Kurdish letters.

Now, Table 2.3, gives each Kurdish letter a symbol that can be found through partition theory based on James's diagram (Tables 2.1 and 2.2)

Table 2.3. The partition of Kurdish letters

Letters	Partition	Letters	Partition
ئـ	47^6,44,36,28,26^3,19,1$2^2$	غ	67^4,58,50,43,37^2,28,21^2,5
ا	62,54,46,38,29,21,13	ف	45^8,44,38,37^3,31,30,23,6
ب	49,34^5,31,26,24,19	ڤ	52^8,51,45,44^3,38,37,30,14,13,6

پ	56,49,48,34^{5},31,26,26,19	ق	59^{5},56,51,49,44,42^{4},40,38,36,30^{2},14,13
ت	32^{5},29,24,22,17,13,12	ک	51^{7},49,44,42,34,26,24^{3},21,18,14,12^{2}
ج	53^{4},44,39,36,28,21,18^{5},13,4^{2}	گ	57^{6},54,49,46,42,38,29,25^{5},12^{5}
چ	54^{4},42,37,34,31,30,28,21,18^{5},13,4^{2}	ل	66^{2},60,58,54,50,47,43,40,32,24,16
ح	54^{4},45,36,28,21,18^{5},13,4^{2}	ڵ	63^{2},57,55,51,47,44,40,37,29,21,13,11,4,3
خ	63^{4},54,46,38,35^{5},30,21^{2},4	م	53,45,37,29,26,6,23,22,15
د	53^{5},49,40,31,22	ن	49,5,46,41,39,34,32,27,13
ر	52^{3},47,40,32,24	ه	48^{4},44,40,37,33,29,27,21^{2}
ڕ	66,59,58,43^{3},38,31,23,15	ھ	46^{8},45,44,43,39,38,37,33^{3},32,28,25,21^{5}
ز	60^{3},55,48,40,32,15	و	62^{2},56,49,41,33^{4},28,26,21,19,3^{2}
ژ	58^{3},53,46,38,30,14,13,6	وو	50^{2},47^{2},46,42,40,36,33,29,26^{3},24^{3},23,22,21,19^{2},17,16,14,13^{2},10^{2}
س	43^{4},38,36,34^{5},32,31,30,29,27	ۆ	62^{3},57,49,41^{4},36,34,28^{2},11,4,3
ش	39^{4},34,32,31^{5},29,28,27,26,24,13,12,5	ی	64^{3},59,56,53,48,46,41,38^{2}30,24^{2}
ع	58^{4},49,41,34,28^{2},19,13^{2}	ێ	61^{3},56,53,50,45,43,38,35^{2},27,21^{2},19,12,11

3. Application of Encryption and Decryption of the Sentences in the Kurdish

In this paragraph, two examples will be given. The first is to encode a sentence of the Kurdish language into a sequence whose elements are made up of partitions and the second example will be to decrypt a sequence into a sentence in the Kurdish language.

Example 3.1: In this example, a sentence in the Kurdish language will be given and it will be encoded into a sequence of numbers whose elements are positive natural numbers, including them raised to powers (the elements of which we get from *e*-Abacus diagram in partition theory). It is an encoded sentence that can be sent to the requested party. The sentence **welcome to Iraqi Kurdistan** in Kurdish means "**بەخێربێن بۆ کوردستانی عێراق**", this sentence is equivalent in partition theory is

,44,40,37,33,29,27,21^2;63^4,54,46,38,35^5,30,21^2,4;61^3,56,48^4(49,34^5,31,26,24,19;
53,50,45,43,38,35^2,27,21^2,19,12,11;52^3,47,40,32,24;49,34^5,31,26,24,19;61^3,56,5
3,50,45,43,38,35^2,27,21^2,19,12,11;49,5,46,41,39,34,32,27,13;∅;49,34^5,31,26,24,
19;62^3,57,49,41^4,36,34,28^2,11,4,3; ∅;51^7,49,44,42,34,26,24^3,21,18,14,12^2;62^2,56,
49,41,33^4,28,26,21,19,13^2;52^3,47,40,32,24;53^5,49,40,31,22;43^4,38,36,34^5,32,31,
30,29,27;32^5,29,24,22,17,13,12;62,54,46,38,29,21,13;49,5,46,41,39,34,32,27,13
;64^3,59,56,53,48,46,41,$38^2$30,24^2; ∅;58^4,49,41,34,28^2,19,13^2;61^3,56,53,50,45,43,3
8,35^2,27,21^2,19,12,11;52^3,47,40,32,24;62,54,46,38,29,21,13;59^5,56,51,49,44,42^4
,40,38,36,30^2,14,13).

Example 3.2: In this example, we will be given a sequence of numbers whose elements are positive natural numbers and some of which are raised to powers, and what is required is to find the text that matches it by returning

each part of the sequence to its corresponding part based on the tables generated from *e*-Abacus diagram. Take the sequence:

(51^{7},49,44,42,34,26,24^{3},21,18,14,12^{2};62^{2},56,49,41,33^{4},28,26,21,19,13^{2};66^{2},60,58,54,50,47,43,40,32,24,16;64^{3},59,56,53,48,46,41,38^{2}30,24^{2};58^{3},53,46,38,30,14,13,6; Ø;60^{3},55,48,40,32,15;62,54,46,38,29,21,13;49,5,46,41,39,34,32,27,13;43^{4},38,36,34^{5},32,31,30,29,27;32^{5},29,24,22,17,13,12;;53,45,37,29,26,6,23,22,15;62,54,46,38,29,21,13;32^{5},29,24,22,17,13,12;53,45,37,29,26,6,23,22,15;62,54,46,38,29,21,13;32^{5},29,24,22,17,13,12;64^{3},59,56,53,48,46,41,38^{2}30,24^{2};51^{7},49,44,42,34,26,24^{3},21,18,14,12^{2}).

If we decode the above sequence and compare it with the resulting tables from *e*-Abacus diagram, then the sentence is ‘‘كوليژ زانست- ماتماتيك’’.

Finally, it is possible to create a program in any system based on the sequences that correspond to the letters obtained from the *e*-Abacus diagram through the use of many algorithms, such as symmetric-key encryption or asymmetric-key encryption that encode the letters into sequences and vice versa.

4. Conclusions:

In the current century and the world's development, encryption is not foolproof, and there are still vulnerabilities that cybercriminals can exploit. Therefore, it is necessary to keep updating encryption techniques and algorithms to stay ahead of cyber threats. One of the important methods is choosing a language that only a few master, as well as using scientific concepts that only specialists in data analysis master. Therefore, this paper

was based on conversational language (**Kurdish**) in addition to the use of the e- Abacus diagram in partition theory. As for creating and developing an algorithm, it is one of the things mentioned in the world of software and developing special codes according to what the programmer requires.

References

1. Mathas A. ; (1999). Iwahori-Hecke Algebras and Schur Algebras of the Symmetric Group, University of Sydney, NSW, Australia, 15. http://doi.org/10.1090/ulect/015/02
2. James G. D. ; (1978). Some combinatorial results involving Young diagrams. Mathematical Proceeding of the Cambridge Philosophical Society, 83, 1-10. https://doi.org/10.1017/S0305004100054220
3. Eman E. M., Haslinda I., Ammar S. M. and Nazihah A. ; (2015). Embedding chain movement in James diagram for partitioning β-numbers. AIP Conference Proc 1691 (040019): 1-7. https://doi.org/10.1063/1.4937069
4. Hadil H. S. and Ammar S. M.; (2017). Syriac Letters and James diagram (A) Int. J. of Enhanced Research in Science, Technology Engineering 6 (12): 53-62. https://www.erpublications.com/uploaded_files/download/hadil-h-sami-prof-dr-ammar-s-mahmood-iraq_FYaXD.pdf
5. Awreng B. M. and Ammar S. M. ; (2019). SecretText by e-abacus Diagram II. Iraqi J. of Science, 60(3):638-646. https://doi.org/10.24996/ijs.2019.60.3.22

6. Awreng B. M. and Ammar S. M. ; (2019). SecretWord by e-abacus Diagram I. Iraqi J. of Science, 60(4):840-846. https://doi.org/10.24996/ijs.2019.60.4.17
7. Ahmed M. A. and Ammar S. A.; (2020). The Graph of e-Abacus Diagram. WSEAS TRANSACTIONS on MATHEMATICS, 19, 486-497. https://doi.org/10.37394/23206.2020.19.52
8. Hanan S. M. and Nadia A. A.; (2021). Splitting the e-Abacus Diagram in the Partition Theory. Iraqi J. of Science, 62(10):3648-3655. https://doi.org/10.24996/ijs.2021.62.10.23
9. Hiba R. H. and Ammar S. M. ; (2022). Inclusion Mapping and Partition Theory. 3rd International Conference on Mathematics and Applied Science. Journal of Physics: Conference Series 2322: 1-10. https://doi.org/10.1088/1742-6596/2322/1/012027
10. Ammar S. M. ; (2023). On GCYD-Method In e-Abacus Diagram. Iraqi J. of Science, 64(7):3452-3457. https://doi.org/10.24996/ijs.2023.64.7.26
11. Ammar S. M. and Jwan K. K. ; (2024). Adding Rows in Main e-Abacus Diagrams. Iraqi J. of Science, 65(2):841-852. https://doi.org/10.24996/ijs.2024.65.2.21
12. George E. A.; (1998). The Theory of Partitions. Cambridge University Press- Mathematics .
13. Burce B. ; (2017). Theory of Partition (Lectures Notes). University of Illinois.

Victor K. (2017).The Partition Method for a Power Series Expansion: Theory and Applications. University of Melbourne, Nikki Levy.