Date of publication SEP-30, 2025, date of current version JUN-02, 2025.
www.computingonline.net / computing@computingonline.net

Print ISSN 1727-6209
Online ISSN 2312-5381
DOI 10.47839/ijc.24.3.4181

Double-Layer Encryption using Chemical Periodic Table and a Pseudo-random Number Generator

JOSE PAREDES-MALAGA, ROXANA FLORES-QUISPE, YUBER VELAZCO-PAREDES
Universidad Nacional de San Agustín de Arequipa
Email: jparedesma@unsa.edu.pe, rfloresqu@unsa.edu.pe, yvelazco@unsa.edu.pe

Corresponding author: Jose Paredes-Malaga (e-mail: jparedesma@unsa.edu.pe).

ABSTRACT The global coronavirus pandemic has led to an increase in information transmission. Many public and private institutions have adopted remote work, ranging from educational institutions to those dealing with national security, making it necessary to have information protection mechanisms. For example, in 2022, the Guacamaya hacker group exposed over 283,000 emails stolen from the Peruvian army and Joint Command of the Armed Forces. On the other hand, in recent years, encryption using scientific knowledge from fields such as physics, chemistry, and biology has been studied due to its high complexity to generate new ways to encrypt information. For that reason, this research proposes a new method based on the properties of chemical elements in the periodic table and color cryptography, which incorporates two levels of security: a pseudo-random number generator and character substitution by atomic number. The security level of the system has been demonstrated by the extensive key size and comparative analysis, which aligns with cryptographic principles, providing robust protection against unauthorized access.

KEYWORDS Double-Layer encryption; Periodic Table; Color-Based Cryptography; Encryption; Decryption; Pseudo-Random numbers.

I. INTRODUCTION

The continuous growth of valuable information transfer over the Internet has demonstrated that security is a vital issue [1]. The security of individuals' and institutions' data is becoming important for the transmission safety and reliability of various messages, documents, images, audio, etc. Due to the presence of cyber criminals [2]. Thus, data encryption is taking center stage as it is one of the ways to ensure the integrity and confidentiality of information, creating a security barrier to safeguard information from unauthorized access, using important cryptographic algorithms; which involve three important parts: the key programming algorithm (KSA), the encryption algorithm, and the decryption algorithm to recover the original data [4].

The purpose of KSA is to make the key so strong that it is not vulnerable to attacks, and computer hackers cannot find the original key. The encryption algorithm uses a key to transform the data and converts it into an unreadable format, with various cryptographic properties such as non-linearity, propagation criteria, correlation, and algebraic immunity. This process is called encryption.

However, the security of encryption depends on how vulnerable the key is to a cryptanalysis attack. In addition to KSA, random numbers can be used to make the key more robust and complex. The PRNG algorithm is the most common way to generate pseudo-random numbers [5]. This generates sets of numbers that resemble random series, but they don't become random because they can be predictable if the seed number and the used algorithm are known. This production is carried out iteratively, generating numbers sequentially. Common classes of these algorithms are linear congruential generators, lagged Fibonacci generators, linear feedback shift registers, and generalized feedback shift registers [6].

In addition, to increase security, multiple encryption is being used, which is the process of encrypting a message that has already been encrypted one or more times, either using the same algorithm or a different one. It is also known as cascade encryption or super encryption [7]. In other cases, it has been necessary to resort to joint encryption and data insertion (JEDI), which has received a lot of attention in recent years thanks to the features it offers to address current applications [8]. Also, some researchers have proposed to modify and invent new cryptographic algorithms from time to time to ensure the privacy of the information and, in this way, bring with it innovation networks and information security [11]. Sinha et al. [12] used one of the most valuable instruments of science, the periodic table, to encrypt information since it orders the elements by their atomic number and stores multiple properties of chemical elements, allowing interaction between one element and another.

For that reason, this article proposes a double-layer encryption using chemical periodic table and pseudo-random number generator, which generate a first key of letters and symbols based on RGB colors, and a second key will be generated with the elements of the periodic table and color encryption technique, where each atomic number of the periodic table is assigned a different color, and finally, an image file in BMP format to both keys is generated. In this paper, a practical approach has been developed to improve security using a two-level security approach and an innovative method for generating security keys. This approach integrates other fields of knowledge in cryptography, including chemistry, which have generated considerable interest in the research community for their innovation potential.

The rest of the paper is organized as follows: Section 2 presents the related work; Section 3 provides all the details of the proposed method; Section 4 displays the experimental results; and finally, Section 5 presents the conclusions of this paper.

II. RELATED WORK

In the last few years, multiple investigations have been conducted in cryptography using different methods to encrypt information. One of these ways is related to basic sciences such as physics, biology, and chemistry, proposing in this last cryptography directly on chemical substances.

Clair [13] proposed a method of encryption by adjusting the levels of carbon-13 in atoms within a molecule to generate a stable isotopically encoded signature that would be difficult to intercept due to the need for access to extraction protocols because sophisticated NMR instrumentation and deep knowledge in this field were required.

Another interesting advancement was proposed by S. Jain et al. [14], who used the principles of genetics to encrypt information in the form of DNA nucleotides (A, T, G, and C). The numerous combinations of these bases generate a high capacity for information storage in DNA chains, creating a new method to provide security to data in the form of DNA sequences by converting a table of 256 decimal numbers into their corresponding DNA sequences of length 4. This type of cryptography has been used to encrypt text, audio, and images.

Likewise, Arunpandian et. al. [15] introduced a novel symmetric encryption algorithm for securing unique identification numbers and biometric images. The approach involves utilizing existing unique numbers to generate secret keys through preprocessing and shuffling techniques. The secret key incorporates Aadhaar number manipulation and atomic symbols based on the periodic table. Additionally, biometric images undergo shuffling and pixel scrambling for enhanced security. Despite a reduced key space, the encryption scheme demonstrates effective authentication and verification, outperforming existing approaches in experimental results and ensuring robust security measures.

In the field of biology, M. Yamuna et al. [16] have presented a redesigned periodic table for encrypting drug information based on the standard periodic table properties. This innovative system aims to enhance the secure transmission of details related to drugs, whether based on their names or chemical formulas, addressing the imperative need for confidentiality in online communication within the drug discovery process.

In other research, Hammad et al. [17] creatively employed the periodic table by converting the Vigenere cipher and Caesar cipher methods into the names of chemical elements. This unique approach aims to enhance the security level of encryption, making it more resistant to cracking. By integrating the methods into the periodic table, the substitution of characters or letters is provided with a new layer of abstraction. Additionally, a steganography process is implemented, using the periodic table as a concealment method for messages or information. The utilization of the periodic table adds a novel dimension to cryptographic techniques, contributing to a more robust and intricate encryption process.

In addition, Sinha et al. [12] used a random ordering of elements in the periodic table, relating them to uppercase letters, numbers, and some symbols ("(", ")", "-", and (blank space)) to perform a cryptographic algorithm. They then encrypted each element with its properties, such as whether it is a noble gas, the group number, whether it is a metal or non-metal, and the group name of elements, such as alkali, alkaline earth, halogens, chalcogens, etc. In this way, a novel approach to dual-layer cryptography is proposed, employing multiplicative encryption in conjunction with the periodic table of elements using random-like encryption. The experiments and results show an alternative to conventional methods, as multiple encryption processes were executed.

On the other hand, Wang et al. [18] aimed to propose a secure and efficient color image encryption for heightened security, achieving improvements by incorporating chaos into image encryption. That is, they generated chaotic sequences that replaced and disseminated secret keys, thus reinforcing resilience against possible attacks. In our case, random numbers are used to achieve similar objectives.

From the above, it is evident that there is a search to achieve more complex encryption, since some researchers replaced the use of characters, numbers, and special symbols with colored blocks to improve the security of the encryption process. For example, Sharma's Color-based cryptographic algorithm [9] makes encryption more complex by using a wide range of colors, numbered in decillions, and covering a wide variety of shades.

Naik et al. [19] proposed a new method to replace each plain text character with a unique color block from the wide spectrum of available colors, making it resistant to common attacks such as it into a method resistant to common attacks such as Meet-in-the-Middle, Birthday, and Brute Force. This provides great security when encrypting data.

Johar et al. [10] used a key matrix to encrypt plaintext into blocks of color. The key matrix is transmitted for security using the RSA algorithm. The receiver decrypts the cipher text by substituting the color blocks with the corresponding plaintext characters. The maximum number of color combinations is 16777216, making it very exhausting for the computer criminal to try all these combinations. Hence, a brute force attack is unlikely.

Akre et al. [20] analyzed the security issues related to ATM PIN generation, authentication, and verification techniques with a new scheme that uses color cues and random challenges to improve PIN security.

The review of the related works shows that many of these rstudies are focused on different methods to encrypt the information, due to encryption playing an important role in improving data protection [3]. That is why this article proposes a new approach that combines color-based cryptography with the properties of chemical elements in the Periodic Table improving the security of the encryption process.

III. PROPOSED METHOD

In this research, a new encryption method is proposed using the information on the chemical elements of the periodic table. The proposed method encrypts any type of text and provides security at two levels, first using a pseudo-random number generator (PRNG) to assign a letter, number, or symbol to each chemical element, and then the atomic numbers of the periodic table are used for the second encryption. Furthermore, a new decryption method using color-based Cryptography to generate two image format keys is proposed too. Both encryption and decryption methods, with all their steps, are shown in Fig. 1.

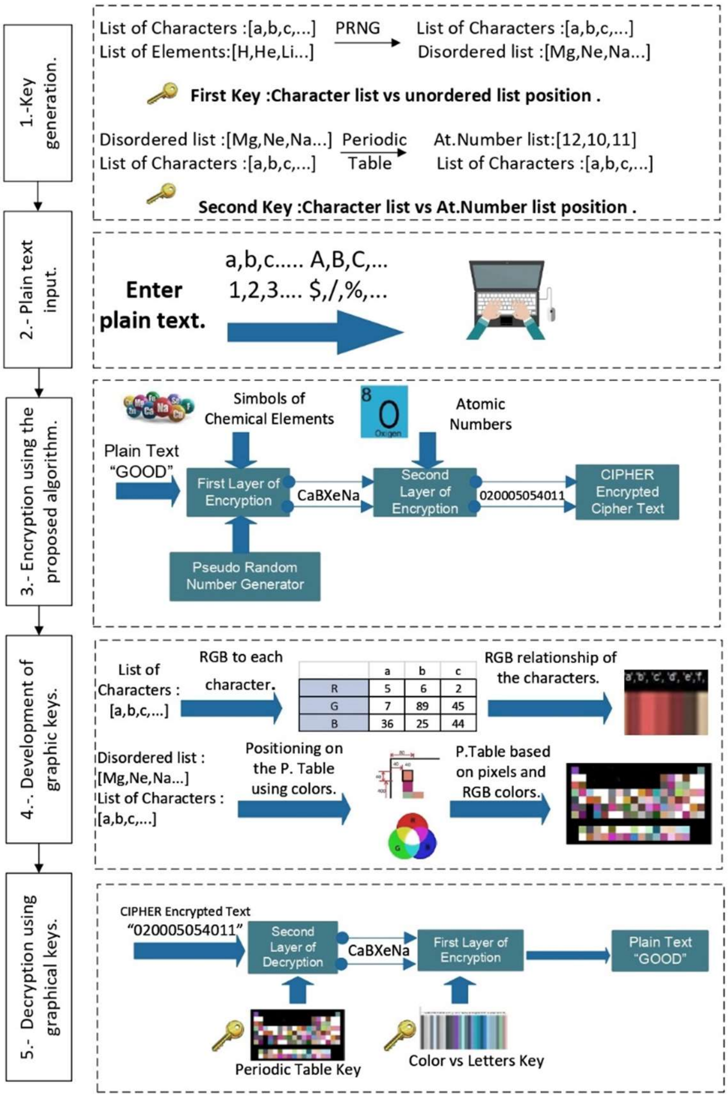
A. KEY GENERATION

A.1 USE OF THE PERIODIC TABLE AS A CODING TOOL

The proposed encryption method considers 118 elements of the chemical elements of the periodic table [10], and every structure has an atomic number, atomic symbol, and mass number [21].

- **Atomic Number:** The atomic number of an atom, representing the number of protons in its nucleus, defines the unique identity of each element. Distinct atomic numbers distinguish elements from one another; hence, atoms with distinct atomic numbers belong to different elements.
- **Mass Number:** The mass number is the number of neutrons in an atom of a specific element plus the number of protons in an atom of that element.
- **Atomic Symbol:** It represents chemical elements, for example, H for hydrogen, Cl for chlorine, and O for oxygen. Certain elements, reflecting their origin from languages other than English, may have less intuitive symbols. For instance, sodium is represented by the symbol Na, derived from the Latin word "Natrium," while Iron is denoted by Fe, originating from the Latin term "Ferrum", meaning iron. An example is shown in Fig. 2.

This information is used to represent each character in plaintext through chemical symbols, which are systematically organized based on their properties, among the most important of which is the atomic number. Besides these 118 elements, more than sufficient can cover the length of a message since plain text can be formed by 95 different characters, including letters, numbers, and symbols in the quantities shown in Table 1.


1.-Key generation.
List of Characters :[a,b,c,...]
List of Elements:[H,He,Li...]
PRNG
List of Characters :[a,b,c,...]
Disordered list :[Mg,Ne,Na...]
First Key :Character list vs unordered list position .
Disordered list :[Mg,Ne,Na...]
List of Characters :[a,b,c,...]
Periodic Table
At.Number list:[12,10,11]
List of Characters :[a,b,c,...]
Second Key :Character list vs At.Number list position .
2.- Plain text input.
Enter plain text.
a,b,c..... A,B,C,...
1,2,3.... $,/,%,...
3.- Encryption using the proposed algorithm.
Simbols of Chemical Elements
8
O
Oxigen
Atomic Numbers
Plain Text "GOOD"
First Layer of Encryption
CaBXeNa
Second Layer of Encryption
020005054011
CIPHER Encrypted Cipher Text
Pseudo Random Number Generator
4.-. Development of graphic keys.
List of Characters : [a,b,c,...]
RGB to each character.
RGB relationship of the characters.
'a','b', 'c', 'd', 'e','f',
Disordered list : [Mg,Ne,Na...]
List of Characters : [a,b,c,...]
Positioning on the P. Table using colors.
P.Table based on pixels and RGB colors.
5.- Decryption using graphical keys.
CIPHER Encrypted Text "020005054011"
Second Layer of Decryption
CaBXeNa
First Layer of Encryption
Plain Text "GOOD"
Periodic Table Key
Color vs Letters Key

	a	b	c
R	5	6	2
G	7	89	45
B	36	25	44

Figure 1. Proposed Cryptography method.

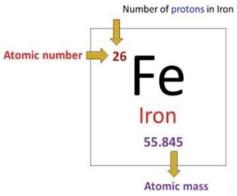


Figure 2. An example of a chemical symbol with atomic number and atomic mass

Table 1. Quantity and types of characters accepted in plain text

Type	Spaces	Letters	Numbers	Symbols	Total
Quantity	1	52	10	31	95

This set includes a variety of alphanumeric characters, punctuation symbols, and mathematical operators. The space character is also important for separating words and enhancing readability, which are essential for most basic writing and programming purposes.

Then the plain text is encrypted assigning characters based on an ordered distribution of the elements in the periodic table using their atomic number, which is increased from left to right and top to bottom as is shown in Fig. 3.

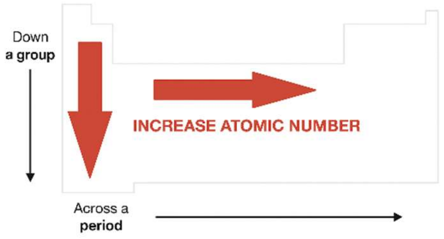


Figure 3. Increase of the atomic number in the periodic table

This distribution responds to the fact that the elements of the periodic table are grouped by energy levels in rows (periods) and chemical properties in columns (groups).

A.2 GENERATING THE FIRST KEY

Once the alphabet was defined, it was important to find a way to assign it to the elements of the periodic table to prevent intruders from discovering the secret message. It was decided to assign letters, numbers, and certain special characters at random to each chemical element, using the random shuffle function that swaps the position of each element with another element chosen at random from the 118 available elements.

This process is shown in Algorithm 1, where it is important that all random number generators (PRNGs) set a seed value. To achieve this, the processor time has been considered as the initiator. After that, the relationships between the newly ordered sequence of chemical elements and characters have been established.

Algorithm 1: Generating the first keys

```
Algorithm 1 Generating keys for a list of element symbols
and atomic numbers in comparison to a character list.
Require: $E_{[i]}$ =List of Chemical Elements, $C_{[i]}$ =List of
    Characters, $s$ = Seed Number,$E_{PRNG}$ = List of Chemical
    Elements Pseudo-randomly disordered.
Ensure: $s = srand(time)$
    $E_{PRNG} = randomshuffle(E_{[i]}, s)$
    for <i=0 to i<95> do
        <$E_{PRNG} \rightarrow C_{[i]}$>
    end for
    for <j=0 to j<118> do
        <$E_j \rightarrow j+1$>
    end for
```

A.3 GENERATING THE SECOND KEY

As atomic numbers are integers, they can be associated with the "+1" positions in an ordered list of chemical elements, starting with Hydrogen at position 0+1=1 and ending with Oganesson at 117+1=118 shown in Fig. 4. Then, by employing a simple conditional structure, the corresponding atomic number of the elements in the disordered list generated by a (PRNG) can be determined using the order list positions. This enables a list of each chemical symbol to be assigned to its atomic number, as shown in Algorithm 1.

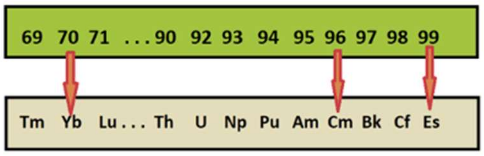
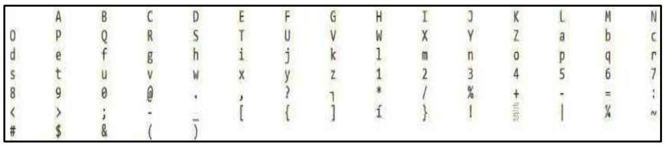


Figure 4. Position of elements as atomic numbers.

B. PLAIN TEXT INPUT

According to Cole [22], "plain text" refers to any type of data in its original, readable, and unencrypted form. Examples of plain text include text documents, images, and executables. It is crucial to note that plain text exclusively denotes unencrypted data. In the presented algorithm, only text processing is currently supported, and the input is supplied by the message sender. This input can be entered either directly through the keyboard or via a “txt” or “csv” file, with the message capable of containing up to 95 letters, numbers, or symbols, including white spaces, which are shown in Fig. 5.



	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	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	1	2	3	4	5	6	7
8	9	0	@	.	,	?	¬	*	/	%	+	-	=	:
<	>	;	-	_	[	{	]	¡	}	!	[illegible]	|	¥	~
#	$	&	(	)										

Figure 5. Letters, numbers, or symbols supported by the plaintext.

C. ENCRYPTION USING THE PROPOSED ALGORITHM

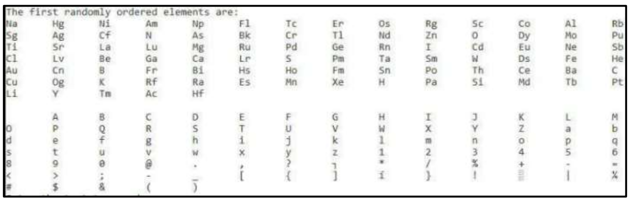
The algorithm begins with the first encryption layer over the plain text, where each letter of the text is compared with each of the characters using the first key "character list vs unordered list positions of chemical elements" (Encryption using PRNG) obtaining a sequence of chemical symbols which is shown in the Algorithm 2. After that, one of the fundamental properties of the periodic table is utilized: the atomic number. Each symbol is replaced by its corresponding atomic number. Finally, this sequence of atomic numbers is equivalent to the plain text, constituting the encrypted cipher text that will be sent to the message recipient.

Algorithm 2: Encryption using keys

```
Algorithm 2 Encryption using the keys
Require: $E_{[i]}$ = List of Chemical Elements, $C_{[i]}$ = List of
    Characters, $t$ = Plain text, $e_1$ = Encrypted Text.
Ensure: $T$ = strlength($t$), $cnt = 0$
    for $i = 0$ to $T$ do
        for $j = 0$ to 95 do
            if $t_{[}i] == C_{[}j]$ then
                $e_1[cnt++]$ = $E[j]$
            end if
        end for
    end for
        $cnt = 0$
    for $i = 0$ to $T$ do
        for $j = 0$ to 118 do
            if $e_1$[i] == $E_{PRNG}$[j] then
                $e_2[cnt++]$ = $j + 1$
            end if
        end for
    end for
```

C.2 COMPREHENSIVE ILLUSTRATION OF ENCRYPTION ALGORITHM EXECUTION

An example can be seen in Fig. 6, which shows a list of chemical elements with their assigned characters (letters, numbers, or symbols). Also, for each new text, a new list will be generated.



```
The first randomly ordered elements are:
Na    Hg    Ni    Am    Np    Fl    Tc    Er    Os    Rg    Sc    Co    Al    Rb
Sg    Ag    Cf    N     As    Bk    Cr    Tl    Nd    Zn    O     Dy    Mo    Pu
Ti    Sr    La    Lu    Mg    Ru    Pd    Ge    Rn    I     Cd    Eu    Ne    Sb
Cl    Lv    Be    Ga    Ca    Lr    S     Pm    Ta    Sm    W     Ds    Fe    He
Au    Cn    B     Fr    Bi    Hs    Ho    Fm    Sn    Po    Th    Ce    Ba    C
Cu    Og    K     Rf    Ra    Es    Mn    Xe    H     Pa    Si    Md    Tb    Pt
Li    Y     Tm    Ac    Hf

      A     B     C     D     E     F     G     H     I     J     K     L     M
O     P     Q     R     S     T     U     V     W     X     Y     Z     a     b
d     e     f     g     h     i     j     k     l     m     n     o     p     q
s     t     u     v     w     x     y     z     1     2     3     4     5     6
8     9     0     @     .     ,     ?     ¬     *     /     %     +     -     =
<     >     ;     -     _     [     {     ]     ¡     }     !     ░     |     %
#     $     &     (     )
```

Figure 6. The chemical elements with their assigned characters

As an example, the text CARLOS was processed with the first and second encryption layers (generated as shown in Fig. 6), In the first layer, each character was mapped to a chemical symbol based on its positional index in a predefined list—for instance, the letter C (position 3) was associated with the element Neon (position 3). Subsequently, in the second layer, each chemical symbol was replaced by its corresponding atomic number (e.g., Ne → 10), obtaining the code 102021010304. See Fig. 7.

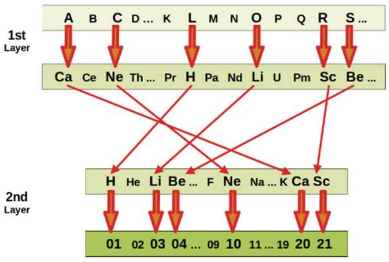

A B C D ... K L M N O P Q R S ...
1st Layer
Ca Ce Ne Th ... Pr H Pa Nd Li U Pm Sc Be ...
H He Li Be ... F Ne Na ... K Ca Sc
2nd Layer
01 02 03 04 ... 09 10 11 ... 19 20 21

Figure 7. First and second encryption layers for the plain text input "CARLOS"

D. DEVELOPMENT OF GRAPHIC KEYS

The use of the periodic table for encryption in the previous step has produced interesting results, but a robust implementation requires enhanced security to meet cryptography standards and protect information effectively. Thus, the public patterns of the periodic table could make it susceptible to dictionary attacks, compromising cryptography security. For that reason, the proposed method has been complemented for the decryption stage with color cryptography to leverage the graphical properties of the periodic table without compromising information security.

To generate the image format keys, a bitmap was used to delimit a certain number of rectangular blocks, and then a color was assigned to each block.

Fig. 8 shows how the periodic table was scaled in rectangles of 40 x 40 pixels, where each one of the 118 elements was located according to the atomic numbers of the chemical elements.

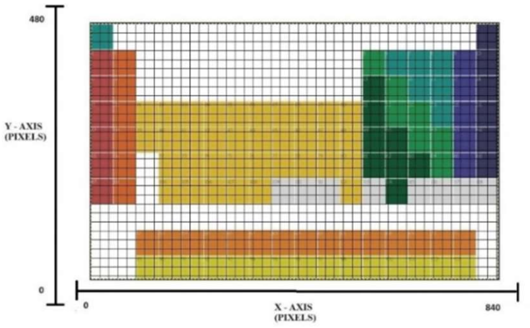


Figure 8. Scaling the elements of the periodic table in 40 x 40 rectangular blocks for each chemical element.

Fig. 9 shows an example of the element "Hydrogen"; on the X axis it goes from pixel 40 to 80 and on the Y axis it goes from pixel 400 to 440.

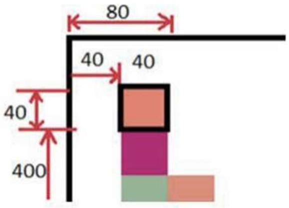


Figure 9. Location of the Hydrogen element

Algorithm 3 shows the calculation of the key in the form of a Periodic Table, where each square in the periodic table is associated with a character. Since there are more chemical elements than characters, the elements not assigned to a character will be colored white. Of the 118 elements, only 95 of them have been used.

Algorithm 3: Development of graphic keys.

```
**Algorithm 3** Development of graphic keys.
$P(x_1, x_2, y_1, y_2, r, g, b, name)$ = Paint class that depends on two values of X and Y, RGB values, and the name of the chemical element., $E_o$ = List of Chemical Elements ordered by the Periodic Table, $E_{PRNG}$ = List of Chemical Elements Pseudo-randomly disordered, $Tp$ = Object of the Paint class.

for $< i = 0$ to $i < 118 >$ do
    $Tp_i.setName(E_o[i])$
    $Tp_i.setCoord(x_1, x_2, y_1, y_2)$
    $Tp_i.setAtoNumb(i + 1)$

    for $< i = 0$ to $i < 118 >$ do
        string $ChElem = Tp_i.getName$
        for $< j = 0$ to $j < 95 >$ do
            if $ChElem = E_{PRNG}[j]$ then
                $Tp_i$.setRGB$(r(j), g(j), b(j))$
            else
                $Tp_i$.setRGB$(r(255), g(255), b(255))$
            end if
        end for
    end for
```

In addition, another graphic key is generated as a barcode, where each strip will be associated with a character. Fig. 10 shows an example of the barcode.

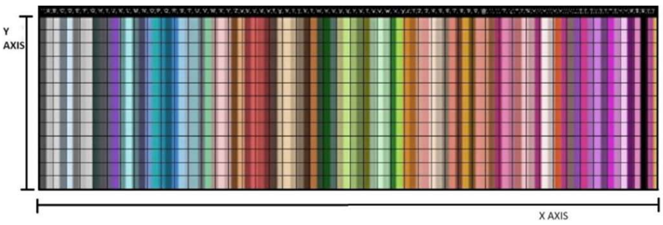


Figure 10. Color barcode

To avoid the repetition of colors, Table 2 shows the RBG components which were chosen randomly, and assigned to the 95 characters without repetition, then using the Color Barcode the "Color Periodic Table" was generated which is shown in Fig. 11. And, for each execution these will be related to different chemical elements chosen randomly.

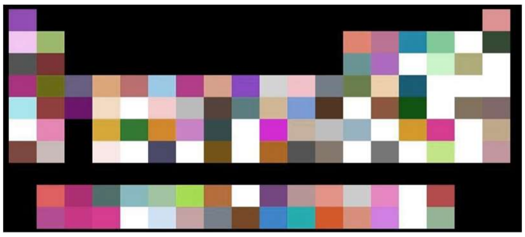


Figure 11. Color periodic table with color key

Table 2: RGB colors and characters versus chemical elements in different executions.

Paramete r	First Execution	Second Execution	nth Execution
R	84	84	84
G	100	100	100
B	37	37	37
Character	“ ”	“ ”	“ ”
Element Symbols	Pa	Ag	O

Thus, for each stage, a relationship between the characters defined in the alphabet with their respective chemical symbols and atomic numbers has been established.

The periodic table key establishes a relationship between the atomic number, the chemical symbol of the element, and the color. Then the barcode key will establish a correlation between color and characters. Finally, with both graphic keys is possible to encrypt and decrypt the message.

E. DECRYPTION USING GRAPHICAL KEYS

The process to decrypt the encrypted message is shown in Fig. 12, where the two graphical keys are used.

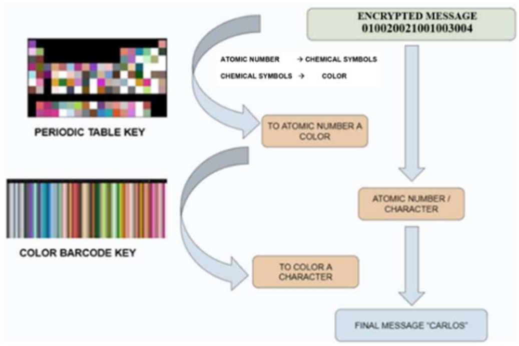


Figure 12. Using two graphical keys to decrypt the messages.

These two keys will be sent with the cipher text. Based on the encrypted message 010020021001003004 obtained in Section C.2, each chemical element is identified by extracting a sequence of three digits at a time, as illustrated in Fig. 13. Then, using the graphical key provided in Fig. 11, each three-digit code is mapped to its corresponding chemical element color. This color is subsequently decoded using the second graphical key shown in Fig. 10, completing the decryption process. This methodology is exemplified in Fig. 14, which illustrates the decoding steps for each character in the example word CARLOS.

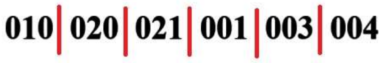


Figure 13. Extraction of atomic numbers from the encrypted text.

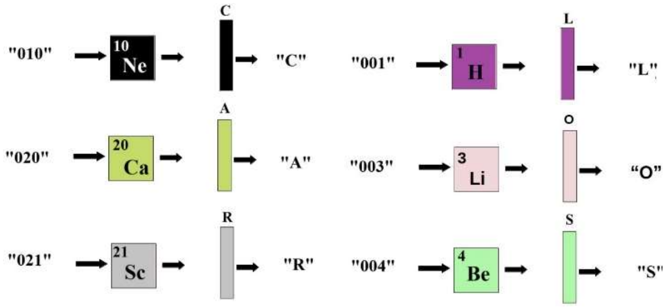


Figure 14. Decryption using the graphical keys.

The complete process is summarized and shown in Fig. 15.

IV. EXPERIMENTAL RESULT

A. DESCRIPTION OF ENHANCING SECURITY WITH A COMPLEX RGB AND CHEMICAL ELEMENT-BASED KEY.

The article introduces an innovative encryption technique that securely encrypts text on two levels using the periodic table. It employs a pseudo-random number generator to associate characters with chemical elements. Additionally, it proposes a color-based encryption/decryption method, generating image-format keys. This robust methodology ensures a high level of security, making the vulnerability process more challenging. The approach combines elements of confusion and diffusion, aligning with cryptographic security principles established by Claude Shannon [23].

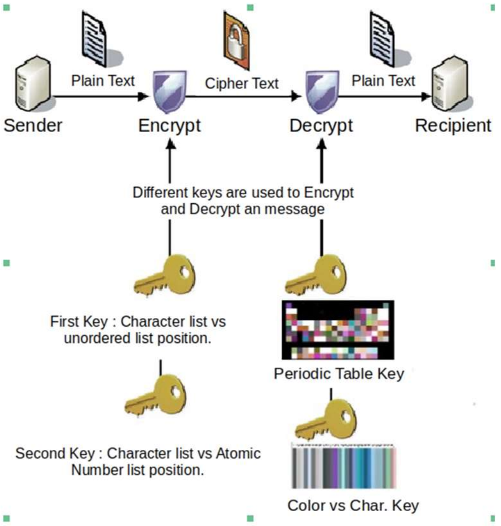

Plain Text
Cipher Text
Plain Text
Sender
Encrypt
Decrypt
Recipient
Different keys are used to Encrypt and Decrypt an message
First Key : Character list vs unordered list position.
Periodic Table Key
Second Key : Character list vs Atomic Number list position.
Color vs Char. Key

Figure 15. Cryptography between a sender and a receiver.

This generation of pseudo-random numbers associated with the chemical elements is produced every time a new message is to be encrypted. Therefore, the security of the proposed method is based on the use of a One-Time Password (OTP), which is temporarily valid only once. Its use is similar to specialized devices that are continuously updated to improve security against theft, reuse, and authentication systems, and online security. Also, with the increase in keys, the time taken to break the system increases, and the brute force attack also requires more time to break, and according to Kirchhoff's law, the security of the cryptosystem depends on the privacy of the key combinations and randomization [4].

To determine the security level of the proposed method, taking into account the proposal of Babu et al. [25], which involves RGB colors, represented in the 3 channels with values from 0 to 255 is possible to calculate the key size. Then, for our case, for each one of the 118 elements in the three channels with values from 0 to 255, see Fig. 16, the key size is 90270. This calculation was made using equation [eq1].

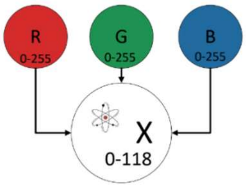


Figure 16. RGB and Chemical Element-Based Key

$$KeySize = 3 * 255 * 118 . \qquad (1)$$
$$KeySize = 90270$$

In addition, according to Verma et al. [24], (Table 3) presents a comparative analysis of brute-force attack resistance among existing algorithms as a function of key size expansion.

As the key size increases, the theoretical resistance against brute-force attacks grows exponentially, expanding the effective keyspace. For each key, for the purpose of comparing methods, we assume that the required time is one microsecond, which is [eq2]. The average number of trials in a brute-force attack is $2^{(\text{No. Keys } - \ 1)}$ because the correct key is statistically expected to be found after searching half the key space [30].

$$T_{\text{years}} = \frac{2^{\text{key\_size} - 1} \times \text{time\_per\_attempt}\ (\mu s) \times 10^{-6}}{\text{seconds\_per\_year}} \qquad (2)$$

In general, a larger key size provides more security, as it makes it more difficult for an attacker to break the encryption because the time computation required to break the cipher also increases [24].

Table 3. Comparative analysis of key size with existing algorithms

Algorithm	Ks (BITS)	No. Keys	Time 1 μs (Yrs.)	Security Level	O( )
DES	56	7.20×10^{16}	1142.47	Low	**O(n)**
AES	128	3.40×10^{38}	5.39×10^{24}	Standard	**O(n)**
Verma et al. [24]	9081	2.10×10^{2950}	3.00×10^{2953}	High	-
Proposed method	90270	1.90×10^{27174}	3.00×10^{27167}	Ultra-High	**O(n)**

We also analyze the computational complexity of the proposed algorithms (Table 3). The total time complexity is O(n) (linear), dominated by the encryption step (Algorithm 2), while key generation (Algorithm 1) and graphic key processing (Algorithm 3) run in O(1) (constant time). Notably, this complexity matches widely adopted standards such as AES and DES [31], ensuring competitive efficiency in practical implementations.

B. CRYPTOGRAPHIC STRENGTH EVALUATION OF THE ALGORITHM BASED ON PSEUDORANDOM NUMBER GENERATION

Another measure to verify the robustness of encryption [27], which evaluates the quality of the pseudorandom number generator (PRNG), can be obtained through an exhaustive analysis of the cipher's statistical characteristics of the random numbers produced. For this purpose, the NIST statistical test suite has been used [28]. This suite was developed by the National Institute of Standards and Technology, and it includes various evaluations designed to detect deviations from theoretical random distributions in binary sequences. Key tests, such as the Frequency Test, Runs Test, and Linear Complexity Test, analyze bit distribution, sequence runs, and the complexity of the sequences, respectively. Additionally, other tests evaluate uniformity and predictability, with the goal of determining whether the generators produce sequences that behave in a truly random and unpredictable manner. The evaluation process involves performing over 180 different statistical tests. In the encryption process, we employ a random shuffle function that swaps the position of each element with another. For the NIST STS test, this function is used to generate a binary string of 1 million bits.

Table 4. Test Result Distribution by Passing Rates for Binary Strings

Passing Test (%)	100	90	80	<70	Average
N.-Binary sequence					
1	182	3	2	1	99.10
2	180	5	1	2	98.94
3	182	2	2	2	98.99
4	182	2	2	2	98.99
5	185	0	1	2	99.20
6	180	4	3	1	98.94
7	182	4	1	1	99.15
8	180	5	2	1	98.99
9	184	2	1	1	98.56
10	184	1	1	2	99.52

After that, ten resulting sequences were evaluated with the NIST STS (Table 4). Many of the tests showed a successfully result, with an average success rate exceeding 98%. For these tests, each value "1 or 100%" is the probability that a perfect random number generator would have produced a sequence less random than the sequence tested [29]. These results obtained show a comprehensive assessment of the sequence's randomness, offering valuable insights into the cryptographic robustness of our proposed method. Finally, we can conclude that our proposed algorithm has demonstrated a high level of cryptographic robustness for practical use.

C. EVALUATION OF THE PROPOSED METHOD USING FIVE DATASETS.

As well as in the research developed by Kyaw Zin et. al. [26], our proposed method has been validated with five data sets that work with both numerical and textual information, and show incremental scaling in size with longer encryption times. See Table 5. These datasets are commonly regarded as benchmarks for assessing storage and encryption methodologies, and they change in size.

The first and second datasets work with short plaintexts. The first is about the latest census in Perú, conducted in October of 2017. The census population was 31,237,385 inhabitants. The second dataset is about the three most spoken languages in South America, which were chosen. The results in both datasets demonstrated a fast and accurate encryption and decryption of our proposed algorithm.

Furthermore, the results from the third dataset illustrate the algorithm's capability to effectively encrypted and decrypted a straightforward sentence. The most noteworthy challenges are encountered in the fourth and fifth datasets. The fourth dataset encompasses the Geographic Code, Department, Capital, and Land Area (km²) of Perú's Regions, which is stored in a tabular format within a CSV file. Successfully encrypting both text and numbers from this dataset was particularly demanding.

The fifth data set comprises the full text of the Universal Declaration of Human Rights. Our proposed method was rigorously tested on this long text of 8959 characters, and fully achieved complete recovery of the encrypted text.

Table 5. Comparison with five datasets using our proposed method

ID	Datasets Designated for Implementation via the Proposed Method	Nº. of characters	Encryption Time (s.)	Text length / Accuracy	
1	"31.237.385" *Source: https://www.inei.gob.pe/media/MenuRecursivo/publicaciones_digitales/Est/Lib1539/cap01.pdf.*	10	0.416	↑	100 %
2	"Spanish-Portuguese-Quechua" *Source: https://en.wikipedia.org/wiki/Languages_of_South_America.*	26	0.497	↑	100 %
3	"Classes at the university will start at 7:00 AM for the 2023 B period."	27	0.552	↑ ↑	100 %
4	"Geographic Code, Department, Capital, and Land Area (km^2) of Peru's Administrative Regions" *Source: https://www.sport-histoire.fr/es/Geografia/Lista_departamentos_regiones_Peru.php.*	610	2.295	↑ ↑ ↑	100 %
5	"Complete Text of the Universal Declaration of Human Rights" *Source: https://www.ohchr.org/sites/default/files/UDHR/Documents/UDHR_Translations/eng.pdf.*	8959	16.494	↑ ↑ ↑ ↑ ↑	100 %

V. CONCLUSIONS

This research proposes an innovative modification to cryptography previously performed through the periodic table Sinha et al. [12], as well as the use of color and location-based encryption on the table of chemical elements for obtaining cryptographic keys. Enhancing the security level of the encrypted text is achieved by employing graphical keys. This innovative approach not only provides an additional layer of security but also adds a sophisticated element to the encryption process. By incorporating graphical keys, the intricacy of the cryptographic system is heightened, offering a multi-dimensional security framework. This not only aligns with advanced encryption principles but also introduces an aesthetically sophisticated aspect to the overall security paradigm. In future work, the applications could be extended to encrypt images, tables, audio, etc., to increase the scope of this work.

References

[1] Y. Velazco-Paredes, et al., "Relevance feedback through the generation of trees for image retrieval based on multitexton histogram," *Proceedings of the 2011 IEEE 30th International Conference of the Chilean Computer Science Society*, November 2011, pp. 1-7, https://doi.org/10.1109/SCCC.2011.1.

[2] K. D. Patel et al., "Image encryption using different techniques: A review," *International Journal of Emerging Technology and Advanced Engineering*, vol. 1, no. 1, pp. 30–34, 2011. https://api.semanticscholar.org/CorpusID:16076104.

[3] M. Ruelas Quenaya, A.A. Villa-Herrera, S. F. Chambi Ytusaca, J. E. Yauri Ituccayasi, Y. Velazco-Paredes, R. Flores-Quispe, "Image encryption using an image pattern based on advanced encryption standard," *Proceedings of the 2021 IEEE Colombian Conference on Communications and Computing (COLCOM)*, Cali, Colombia, 2021, pp. 1-6. https://doi.org/10.1109/COLCOM52710.2021.9486298.

[4] A. Saini, A. Tsokanos, & R. Kirner, "Quantum randomness in cryptography – A survey of cryptosystems, RNG-based ciphers, and QRNGs," *Information*, vol. 13, issue 8, 358, 2022. https://doi.org/10.3390/info13080358.

[5] M. Peyravian, S. M. Matyas, A. Roginsky, & N. Zunic, "Generating user-based cryptographic keys and random numbers," *Computers & Security*, vol. 18, issue 7, pp. 619–626. https://doi.org/10.1016/S0167-4048(99)82040-9.

[6] J. Ezhilarasi, et al., "Efficiency and area reduction for a PRNG framework based on Well method," *International Journal for Scientific Research and Development*, vol. 3, issue 2, pp. 2476-2482, 2015. https://api.semanticscholar.org/CorpusID:55679202.

[7] W. Stallings, *Cryptography and Network Security: Principles and Practice*, eighth edition, Global edition, Pearson, 2023, Ch.1, Ch.2, Ch.7. [Online]. Available at: https://books.google.com.pe/books?id=zjbZzgEACAAJ.

[8] R. Ito, et al., "Encryption and data insertion technique using region division and histogram manipulation," *Proceedings of the 2018 Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA ASC)*, 2018, pp. 1118-1121. https://doi.org/10.23919/APSIPA.2018.8659671.

[9] D. Sharma, R. Prasad, G. Bedi, A. Dad, "Colour based cryptography," *International Journal of Engineering Research & Technology (IJERT)*, vol. 5, 2018. https://api.semanticscholar.org/CorpusID:155649006.

[10] P. Johar, S. Easo, K. K. Johar, "A Novel Approach to Substitution 'Play Color Cipher'", *International Journal of Next Generation Computer Applications*, vol. 4, issue 1, 2017. https://ijngca.com/CurrentIssues.html.

[11] R. Babu Kallam, S. Udaya Kumar, A. Vinaya Babu, "A new framework for scalable secure block cipher generation using color substitution and permutation on characters, numbers, images and diagrams," *International Journal of Computer Applications*, vol. 20, issue 5, pp. 37-42, 2011. https://doi.org/10.5120/2427-3259.

[12] A. Sinha, & A. Bhadani, "Double layer cryptography using multiplicative cipher and chemical periodic table," *Indian Journal of Data Communication and Networking (IJDCN)*, vol. 1, issue 2, 2021. https://doi.org/10.35940/ijdcn.B5008.041221.

[13] J. Clair, "Encoding matter with regiospecific 12 C/ 13 C isotopic labels," *Chemical Communications*, issue 21, 2018. https://doi.org/10.1039/C8CC00080H.

[14] S. Jain, & V. Bhatnagar, "A novel DNA sequence dictionary method for securing data in DNA using spiral approach and framework of DNA cryptography," *Proceedings of the 2014 International Conference on Advances in Engineering & Technology Research (ICAETR-2014)*, Unnao, India, 2014, pp. 1-5. https://doi.org/10.1109/ICAETR.2014.7012924.

[15] S. Arunpandian, S.S. Dhenakaran, "A novel key and image concealing with static-dynamic pattern using modified periodic table", *Journal of Information Security and Applications*, vol. 63, 2021. https://doi.org/10.1016/j.jisa.2021.103019.

[16] M. Yamuna, V. K. P. K., "Chemical formula encryption using 7-bit periodic table," *International Journal of PharmTech Research*, vol. 6, no. 3, pp 990-995, 2014. https://sphinxsai.com/2014/phvolpt3/2/(990-995)Jul-Aug14.pdf.

[17] R. Hammad, et al., "Implementation of combined steganography and cryptography Vigenere cipher, Caesar cipher, and converting periodic tables for securing secret message," *Journal of Physics: Conference Series*, vol. 2279, no. 1, p. 012006, 2022. https://doi.org/10.1088/1742-6596/2279/1/012006.

[18] X.-Y. Wang, Y.-Q. Zhang, X.-M. Bao, "A colour image encryption scheme using permutation-substitution based on chaos," *Entropy*, vol. 17, issue 6, pp. 3877-3897, 2015. https://doi.org/10.3390/e17063877.

[19] M. Naik, et al., "Color cryptography using substitution method," *International Research Journal of Engineering and Technology (IRJET)*, vol. 03, issue 3, pp. 941-944, 2016. https://api.semanticscholar.org/CorpusID:267830148.

[20] S. Akre and A. Sonawane, "Color cipher scheme based ATM pin generation and verification," *Proceedings of the 2020 Fourth International Conference on Inventive Systems and Control (ICISC)*, Coimbatore, India, 2020, pp. 1-4. https://doi.org/10.1109/ICISC47916.2020.9171058.

[21] S. Arunpandian, and S. S. Dhenakaran, "A novel key and image concealing with static-dynamic pattern using modified periodic table," *Journal of Information Security and Applications,* vol. 63, p. 103019, 2021. https://doi.org/10.1016/j.jisa.2021.103019.

[22] E. Cole, R. L. Krutz, & J. W. Conley, *Network Security Bible* (2nd ed). Indianapolis, IN: Wiley, 2009, Ch.5. [Online]. Available at: https://www.google.com.pe/books/edition/Network_Security_Bible_2Nd_Ed/bSN0CgAAQBAJ?hl=qu.

[23] C. Shannon, *A Mathematical Theory of Cryptography*, 1945, 92 p. https://evervault.com/papers/shannon.

[24] A. Verma, and G. Anjali, "Design and development of algorithm using chemical cryptography," *Procedia Computer Science*, vol. 58, pp. 643-48, 2015. https://doi.org/10.1016/j.procs.2015.08.083.

[25] K. Ravindra Babu, et al., "A block cipher generation using color substitution," *International Journal of Computer Applications*, vol. 1, no. 28, pp. 30-32, 2010. https://doi.org/10.5120/515-832.

[26] P. P. Zin, et al., "CryptoChem for encoding and storing information using chemical structures," *Chemistry*, 2020. https://doi.org/10.26434/chemrxiv.12921593.v1.

[27] S. Ostapov, B. Diakonenko, M. Fylypiuk, K. Hazdiuk, L. Shumyliak, O. Tarnovetska, "Symmetrical cryptosystems based on cellular automata," *International Journal of Computing*, vol. 22, issue 1, pp. 15–20, 2023. https://doi.org/10.47839/ijc.22.1.2874.

[28] L. E. Bassham, et al. "A statistical test suite for random and pseudorandom number generators for cryptographic applications," *NIST,* 16 Sept. 2010. https://doi.org/10.6028/NIST.SP.800-22r1a.

[29] NIST Statistical Test Suite. [Online]. Available at: https://csrc.nist.gov/projects/random-bitgeneration/documentation-and-software.

[30] D. P. Duplys, D. R. Schmitz, *TLS Cryptography In-Depth: Explore the Intricacies of Modern Cryptography and the Inner Workings of TLS.* 2024, Alemania: Packt Publishing.

[31] *Securing the Digital Realm: Advances in Hardware and Software Security, Communication, and Forensics*, CRC Press, USA, 2025.

JOSE PAREDES-MALAGA Current Computer Science student with a Master's in Chemistry. Research interests focus on applying chemical principles to computer science areas, particularly to enhance information security in remote communications.

ROXANA FLORES-QUISPE PhD in Computer Science, Professor and Researcher at the National University of San Agustín of Arequipa (Peru), specializing in artificial intelligence, machine learning, image processing, and cryptography. She has extensive teaching experience at various universities in the southern region.

YUBER VELAZCO-PAREDES PhD. in Computer Science from the National University of San Agustín of Arequipa (Peru), and Master in Informatic from the Pontifical Catholic University of Peru. He has taught at many universities in the country, with scientific publications at national and international conferences..