Received: July 14, 2023. Revised: August 20, 2023.

*International Journal of*
Intelligent Engineering & Systems

http://www.inass.org/

# A Comparative Study of a Hybrid Approach Combining Caesar Cipher with Triple Pass Protocol and Krill Herd Optimization Algorithm (KHO)-Based Hybridization

**Liqaa Saadi Mezher[1]***  **Ayam Mohsen Abbass[1]**  **Basma Jumaa Saleh[1]**

*Department of Computer Engineering, College of Engineering, Mustansiryihya University, Baghdad, Iraq*
* Corresponding author's Email: iqa35@uomustansiriyah.edu.iq

**Abstract:** This paper introduces a novel approach to enhance data security through the combination of the caesar cipher with triple pass encryption, utilizing the Krill herd optimization algorithm. The proposed method aims to safeguard sensitive information during transmission and storage by leveraging the strengths of both encryption techniques and optimizing the generation of random keys. In this approach, the caesar cipher adds an extra layer of security by shifting each character in the plaintext by a fixed number of positions. The triple pass encryption further reinforces the encryption process by applying the caesar cipher three times, each with a different shift value. To evaluate the effectiveness of this combined approach, it is compared against the basic caesar cipher and basic triple pass protocol. The experimental results demonstrate superior performance of the proposed method in terms of minimal processing time, 100% accuracy, and zero errors when compared to these traditional techniques. The Krill herd algorithm plays a crucial role in generating random keys and determining the optimal shift values for both the caesar cipher and triple pass encryption. The effectiveness of this combined approach is compared to existing techniques, and the experimental results demonstrate superior performance in terms of minimal processing time, 100% accuracy, and zero errors. This promising solution holds potential for enhancing data security across various domains, as the Krill Herd-based key generation significantly improves the randomness of encryption keys, thereby increasing their resilience against cryptographic attacks.

**Keywords:** Cryptography, De-cryptography, Caesar cipher, Triple-pass protocol, Encryption, Decryption, Security, Substitution, Key, Frequency analysis, Krill herd optimization, Robustness.

## 1. Introduction

The exponential growth of internet communication has increased the demand for various types of cryptographic protocols to safeguard information transmitted over networks[1]. Various techniques, such as steganography, watermarking, and cryptography, can be applied to security. Cryptography is the technology of encoding information so that unauthorized parties cannot readily access it [2]. Encryption is one of the primary cryptography processes, performed on the sender's side. The second major process, decryption, is performed on the recipient's side to restore the original data form. These two procedures are the primary cryptographic operations [3]. Encryption techniques have been developed to protect sensitive information from unauthorized access. However, traditional encryption methods, such as the Caesar cipher, have inherent limitations and vulnerabilities due to their simplicity and ease of cracking. To address these challenges, researchers have explored integrating advanced and secure encryption algorithms [4].

Researchers, statisticians, and cryptologists have developed encryption algorithms, making them more complex and challenging to access to protect data in modern society. However, despite well-shielded data, there is always a possibility that third entities will decode the data. To mitigate this possibility, different encryption methodologies are introduced[5, 6]. A promising approach to enhancing data security is the combination of the Caesar cipher with the Triple Pass Protocol. The Triple Pass Protocol eliminates the need for the sender to transmit encryption keys to the receiver. Instead, each participant utilizes their own private key for text encryption and decryption, making it significantly more challenging for adversaries to compromise the security of the transmitted data. This protocol involves encapsulating a plain text message within three layers of encoding, with each stage utilizing a different offset key for encryption and decryption [7]. The model supports both upper and lower case letters and primarily applies to text files [8].

To further fortify the security and robustness of the encryption process, optimization algorithms such as Krill herd optimization (KHO) have been considered. KHO is a population-based optimization technique inspired by the collective behavior of krill herds. By incorporating KHO into the encryption process, the selection of encryption keys can be optimized to enhance randomness and cryptographic strength [9]. The KHO algorithm mimics the movement and interaction of krill individuals within a swarm, iteratively searching for optimal key combinations that enhance the security of the encryption algorithm.

The combined utilization of the Caesar cipher, triple pass protocol, and KHO-based key generation presents a comprehensive and advanced approach to data security. By encrypting a regular text message three times using this optimized model, the complexity of the encoded text is significantly increased, making it challenging to decipher the code and compromising the security of the data. While the Caesar cipher is one of the oldest encryption techniques, its simplicity and susceptibility to cracking have motivated the exploration of more secure alternatives [10, 11]. Efforts to enhance data safety have led to the development of various encryption algorithms. Protecting important data is crucial to prevent unauthorized access and potential harm to data owners. By combining Caesar encryption with the triple-pass protocol and incorporating KHO-based key generation algorithms, data can be more securely safeguarded, particularly for document files and text messages. This combination of encryption methodologies ensures the inclusion of the alphabet, numbers, and symbols, introducing greater confusion and complexity into the modified code development process [11, 12].

While newer encryption algorithms offer improved security, the Caesar cipher algorithm remains one of the fastest in terms of execution speed due to its simplicity. However, its vulnerability to cracking poses a significant concern. To enhance its safety features, this paper proposes the combination of the Caesar algorithm with the triple-pass protocol, fortified by the inclusion of KHO-based key generation [13]. This innovative approach aims to provide enhanced security and protection for data transmission and storage. The triple-pass protocol, initially introduced by scientist Adi Shamir in 1980, plays a pivotal role in this combined encryption scheme [14, 15]. The fundamental concept of the triple-pass protocol revolves around both the sender and receiver possessing their own private encryption and decryption keys. Each party independently uses their respective key to encode and decode the texts, eliminating the need for key exchange or distribution [16]. The protocol's name derives from the use of a three-way interchange during the initial protocol exchange, which serves to authenticate the sender and receiver [17].

In summary, this paper proposes an advanced encryption approach that combines the simplicity of the Caesar Cipher, the security of the triple-pass protocol, and the optimization capabilities of KHO-based key generation. By leveraging these techniques, data security can be significantly enhanced, ensuring the confidentiality and integrity of sensitive information in the digital landscape.

The study's key contributions can be summarized as follows:

1. Enhanced data security: By integrating the strengths of the Caesar cipher and triple pass protocol, the proposed approach provides an additional layer of security to the encryption process. The successive application of the Caesar cipher with different shift values in the triple pass encryption method adds complexity to the ciphertext, making it more resistant to attacks.
2. Optimal key generation: The Krill herd optimization algorithm is utilized to generate random and secure keys for the encryption process. KHO's ability to efficiently explore a large search space leads to the generation of highly randomized keys, enhancing the overall security and robustness of the encryption.
3. Superior performance: Experimental evaluations demonstrate superior performance of the combined approach compared to current techniques. The optimized approach exhibits minimal processing time, 100% accuracy in decryption, and zero errors, indicating the effectiveness of the integration of KHO in improving efficiency and precision.

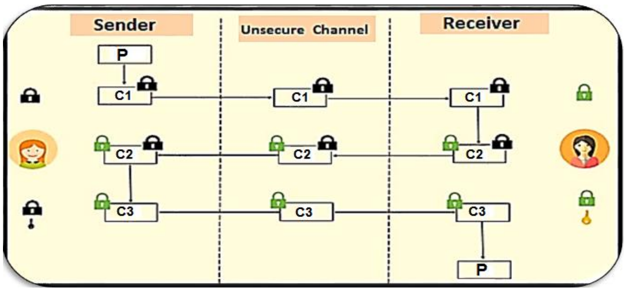

Figure. 1 The triple pass protocol's structure

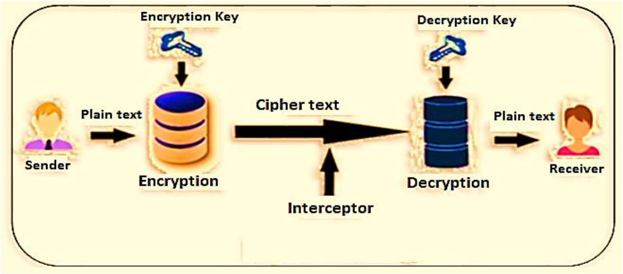

Figure. 2 Architecture of caser cipher classical

4. Resilience against cryptographic attacks: The utilization of KHO for key generation significantly enhances the randomness of the encryption keys, making them more resilient against cryptographic attacks, including brute-force and frequency analysis attacks.
5. Practical application: The study's findings underscore the potential of optimization algorithms, like KHO, in significantly enhancing the security and robustness of encryption methodologies. The optimized approach presents a promising solution for securing sensitive data in various domains, offering practical implications for real-world data security applications.
6. Exploration of optimization algorithms: The study highlights the impact of integrating KHO as an optimization algorithm for encryption. This opens up opportunities for further research and testing to explore additional optimization algorithms and evaluate their practical effectiveness in safeguarding data.

## 2. Third pass protocol (TPP) methods

Adi Shamir, a physicist, developed the three pass technique in 1980 [15, 16]. It is a category of procedures that enables the sender to send a secure encrypted message to the recipient, who can then decrypt it without the sender's key [17]. A current coding method is called three-pass. Each partner in a triple pass protocol has a private ciphering key and a private decoding key, which is its main idea [18]. The text's sender simply needs to convey the message to the recipient; the key, or important distributor, doesn't require distribution [17]. The goal of this work is to provide a method for ensuring text transmission security while using diverse algorithms without requiring key sharing between participants. Caesar cipher methods are used in the encryption and decryption processes. Results from the coding procedure are obtained as an encoded massage. As shown in Fig. 1 [18], the three-pass protocol process, the recipient of the text, and the Caesar cipher algorithm will all perform the encryption three times in succession. The recipient of the text and the sender will also perform the decryption three times in succession.

## 3. Caser cipher classical methods

This essay provides one of the more well-known replacement encryption techniques that has the same symmetry is the Caesar cipher [16]. The primary encryption algorithm, in which the same key is used for both encryption and decryption [19–21]. It relies on letters, employs a key, and the quantity of displacement is determined by the amount of encryption. Caesar's encryption method is based on the shift-by-n rule, which makes disassembling it so simple that a thorough search of the other 25 keys is comfortably possible, as depicted in Fig. 2 [22]. De facto, it is always crucial and required to investigate the promotion of this basic code. To improve security utilizing various encryption technologies, this work focuses on creating an improved model for Caesar encryption [23], where a message that has previously been encrypted once or more times is encrypted using the same or a different method. The new technique encrypts and decrypts a plain text communication three times, using different encryption and decryption keys at each stage [24].

The process of converting plaintext and the key into cipher text is known as encryption. The opposite of encryption is decryption. The Caesar cipher is a traditional cryptographic cipher [5]. A mono alphabetic cipher is the Caesar cipher. It is a substitution cipher that creates the cipher text by substituting a different letter for each one in the plaintext [25]. English characters are frequently encoded using the Caesar cipher. Cipher text is the result of English letters that have been encrypted. The frequency distribution of English letters can be used by the attacker to quickly decrypt the Caesar encryption, as shown in Table 1.

Using the supplied number of keys, each letter in plain text is converted using the Caesar cipher to produce an encrypted text. The secret key is also employed in this method's coding scheme and is set

Table 1. Number to alphabetical conversion

| A | B | C | D | E | F | G | H | I | J | K | L | M |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
| N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |

Table 2: Number to alphabetical conversion

| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| A | B | C | D | E | F | G | H | I | J | K | L | M |
| 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |
| N | O | P | Q | R | S | T | U | V | W | X | Y | Z |

up as a square matrix (range of rows equals range of columns), along with the usage of a mathematical Eq. (1).

$$C = (P + K) mod\ 26 \tag{1}$$

Each letter in the number-encoded text returns to the number of keys to decrypt the encryption, as shown in Table 2, and is then converted to plain text.

When decrypting a file, we employ the mathematical Eq. (2), the inverse of the key, and the output of the coding process.

$$P = (C - K)\ mod\ 26 \tag{2}$$

The science that examines methods to make data or messages safe includes encryption. technical data replacement-based encryption techniques [26]. Since encryption relies on mathematical formulae, ranging from simple to sophisticated algorithms, it may be used to address issues with data or information leaks. The traditional encryption, which uses a symmetric key, incorporates the caesarean encryption algorithm. Based on the findings of this study, it can be said that a Cesare coding technique can assist protect data to lessen data leakage. The science of encryption involves turning a communication that can be recognized or understood by a qualified person into a message that cannot be. Caesar's encryption is a highly traditional and fundamental message encoding technique [27]. The process of confirming plain text to cipher text (cipher) and cipher text to plain text (decoding), which MATLAB R2010a wants to execute more simply, must be tested using software testers to ascertain the logic. Procedure for encryption.

## 4. Krill herd algorithm

Krill herd (KH) is a heuristic optimization method that takes its inspiration from the social behaviour of krill. The KH algorithm is based on three key krill behaviours, which are as follows [18–21]:

1. Induced movement.
2. Foraging
3. Diffusion at random

The Lagrangian methodology adopted by the KH algorithm was as follows:

$$\frac{d\mathcal{X}_i}{d\text{ŧ}} = \text{Ŋ}_i + \text{Ƒ}_i + \text{Đ}_i \tag{3}$$

Where $\text{Ŋ}_i$ is the induced movement amongst other krill; $\text{Ƒ}_i$ is the foraging action; and $\text{Đ}_i$ is the diffusion at Random in the ith krill.

- The induced movement describes the collective behaviour of the herd's individuals to keep things tight. Here is the mathematical formula:

$$\text{Ŋ}_i(\text{ŧ} + 1) = \text{Ŋ}_{\text{ɱ}ax}\alpha_i + wn\,\text{Ŋ}_i(\text{ŧ}) \tag{4}$$

Where $\alpha_i = \alpha_i{}^{\text{Ŀ}ocal} + \alpha_i{}^{\text{Ʈ}arget}$ , $\text{Ŋ}_{\text{ɱ}ax}$ is the max-speed caused via induction, $wn$ represents the moment of inertia associated with the produced motion in [0, 1], $\text{Ŋ}_i(\text{ŧ})$ represents the final induced motion, $\alpha_i{}^{\text{Ŀ}ocal}$ is the neighbourhood’s contribution to the local effect, and $\alpha_i{}^{\text{Ʈ}arget}$ is the best krill's direction effect in that it points in the direction of the target. The formula for determining $\alpha_i{}^{\text{Ʈ}arget}$ is as follows:

$$\alpha_i{}^{\text{Ŀ}ocal} = \sum_{j=1}^{\mathcal{P}} \breve{\mathfrak{K}}_{i,j}\, \breve{\mathfrak{X}}_{i,j} \tag{5}$$

$$\breve{\mathfrak{X}}_{i,j} = \frac{X_j - X_i}{\|X_j - X_i\| + \varepsilon} \tag{6}$$

$$\breve{\mathfrak{K}}_{i,j} = \frac{K_i - K_j}{K_{worst} - K_{best}} \tag{7}$$

Where the maximum and worst fitness values among the krill individuals are denoted by $K_{best}$and $K_{worst}$, respectively; A krill's fitness, or its objective

Received: July 14, 2023. Revised: August 20, 2023.

function value, is denoted by its K index i; $K_j$ represents the fitness of the jth neighbor (j = 1, 2,..., $\mathcal{P}$); Where $X$ is the set of connected coordinates and $\mathcal{P}$ is the total number of adjacent points. To prevent singularities, add $\varepsilon$ a modest positive number to the base. Each individual krill has a specific fitness floor that corresponds to its target vector. To account for the influence of the most fit krill on the i-th krill, we use Eq. (5). To get to the global optimum, set it to this level, which is expressed a

$$\alpha_i{}^{Ʈarget} = Ḉ^{best}\check{\mathfrak{K}}_{i,best}\check{\mathfrak{X}}_{i,best} \tag{8}$$

Where, $Ḉ^{best}$ is the fitness-to-fitness effective coefficient of the best krill individual, i.e., the krill with index i. $\alpha_i{}^{Ʈarget}$ provides a definition for this coefficient. It should be more efficient than other krill individuals, like neighbours, and lead the solution to the global optimum. To be specific, the meaning of $Ḉ^{best}$ is as follows:

$$Ḉ^{best} = 2(ɍand + i/i^{max}) \tag{9}$$

Where " $ɍand$ " is a random number between 0 and 1 chosen to encourage curiosity, whereas $i$ represents the current iteration, $i^{max}$ is the maximum number of iterations that can be performed.

- The motion of foraging is defined by two primary operational characteristics. The first is the physical place where the meal is served, and the second is the patron's impression of the restaurant from past visits. For the i-th krill, this motion may be written as:

$$₣_i = V_₣\mathcal{B}_i + \ wf₣_i{}^{old} \tag{10}$$

Where

$$\mathcal{B}_i = \mathcal{B}_i{}^{food} + \mathcal{B}_i{}^{best} \tag{11}$$

And $V_₣$ is the foraging velocity, In the interval [0, 1], $wf$ represents the inertia mass of the foraging motion, an ancient $₣_i{}^{old}$ is the final foraging action, Attractive food is denoted by $\mathcal{B}_i{}^{food}$, and the best fitness result for the i-th krill up to this point is shown by $\mathcal{B}_i{}^{best}$. Based to data on foraging velocity, a total of 0.02 (ms-1). According to the krill's fitness distribution, which takes its cues from the concept of "center of mass," we may predict where the greatest concentration of food is virtually located. The formula for the iteratively changed center of the food is:

$$\mathfrak{K}^{food} = \frac{\sum_{i=1}^{S}\frac{1}{\mathfrak{K}_i}\mathfrak{K}_i}{\sum_{i=1}^{S}\frac{1}{\mathfrak{K}_i}} \tag{12}$$

Hence, the i-th krill's propensity to seek out food can be calculated as follows:

$$\mathcal{B}_i{}^{food} = Ḉ^{food}\check{\mathfrak{K}}_{i,food}\check{\mathfrak{X}}_{i,food} \tag{13}$$

Where $Ḉ^{food}$ represents the coefficient for food. Due to food's diminishing influence on krill herding with time, we can calculate its coefficient as:

$$Ḉ^{food} = 2(1 - i/i^{max}) \tag{14}$$

The following equation accounts for the influence of the i-th krill individual's optimal fitness:

$$\mathcal{B}_i{}^{best} = \check{\mathfrak{K}}_{i,best}\check{\mathfrak{X}}_{i,best} \tag{15}$$

Where $\check{\mathfrak{K}}_{i,best}$ represents the optimal location that the i-th krill has visited in the past.

- The physical diffusion is assumed that the krill's physical dispersal is a random process. This motion can be modelled using a maximum diffusion speed and a random direction vector. These are some possible ways to express it:

$$\mathcal{D}_i = \mathcal{D}^{max}\delta \tag{16}$$

Where $\mathcal{D}^{max}$ is the maximum diffusion rate, $\delta$ is the random directional variable, and x and y are uniformly distributed between -1 and 1. If you look at Eq. (16), you'll see that the physical diffusion is a random vector that doesn't decrease consistently as you increase the number of iterations. Following a geometric annealing schedule, this term gradually slows the random rate down over time as:

$$\mathcal{D}_i = \mathcal{D}^{max}(1 - i/i^{max})\ \delta \tag{17}$$

- Crossover operator is originally employed as a powerful tool for worldwide optimization [22]. There is a crossover probability, $C_r$, that governs the process, and there are two possible implementations of the crossover procedure: (1) logistic and (2) exponentially. Each of the d variables or parameters in the binomial system undergoes a crossover operation. Using a random number with a uniform distribution between 0 and 1, the mth component of $\mathfrak{X}_i$, $\mathfrak{X}_{i,m}$ is modified as follows:

$$\mathfrak{X}_{i,m} = \left\{\begin{matrix} \mathfrak{X}_{i,m} & rand_{i,m} < C_r \\ \mathfrak{X}_{r,m} & Else \end{matrix}\right\} \tag{18}$$

Where r ∈ {1, 2, . . ., i _ 1, i + 1, . . ., S}and $C_r = 0.2\breve{\mathfrak{K}}_{i,best}$.

- Mutation operator plays a crucial level in evolutionary algorithms. A mutation probability determines the rate of mutation ($M_u$). Here we employ an adaptive mutation approach expressed as:

$$\mathfrak{X}_{i,m} = \left\{\begin{matrix} \mathfrak{X}_{gbest,m} + \mu(\mathfrak{X}_{v,m} - \mathfrak{X}_{w,m}) & rand_{i,m} < M_u \\ \mathfrak{X}_{i,m} & Else \end{matrix}\right\} \tag{19}$$

Where $M_u = 0.05/\breve{\mathfrak{K}}_{i,best}$ and v, w ∈{1, 2, . . ., i _ 1, i + 1, . . ., S} and $\mu$ is a value in range 0 and 1. It ought to be mentioned in $\breve{\mathfrak{K}}_{i,best}$ the proposer is $\breve{\mathfrak{K}}_i$ _ $\breve{\mathfrak{K}}_{best}$.

- Motion Process: Motions often shift a krill's posture in a way that improves its fitness. There are two global and two local methods in the foraging movement and the motion generated By additional krill organisms. KH is an effective algorithm because of these functioning in tandem. Each of the above-mentioned effective factors ( $\breve{\mathfrak{K}}_i$ , $\breve{\mathfrak{K}}_{best}$ , $\breve{\mathfrak{K}}_{food}$ $\breve{\mathfrak{K}}_{i,best}$ has an attracting impact if its associated fitness value is greater than (less than) the objective of the i-th krill, and a repulsive effect otherwise. From these definitions, it is also apparent that an individual's fitness level has a direct bearing on how well they move krill. In the suggested strategy, the physical diffusion acts as a random search. The following equations describes the position vector of a single krill from time $t$ to time $t$ plus $\Delta t$, accounting for variations in the effective parameters of the motion throughout that period.

$$\mathfrak{X}_i(t + \Delta t) = \mathfrak{X}_i(t) + \Delta t \frac{d\mathfrak{X}_i}{dt} \tag{20}$$

$$\Delta t = C_t \sum_{j=1}^{NK} (B_j^U - B_j^L) \tag{21}$$

Where $B_j^L$ and $B_j^U$ are the minimum and maximum values for the j-th variable (j = 1, 2..., NK), and NK is the total number of variables. Consequently, the search space is revealed by the absolute value of their difference. Observational evidence suggests that $C_t$ has a fixed value between 0 and 2. It is also evident that the krill can search the environment with great precision at low $C_t$ values.

## 5. Methodology

The methodology is proposed in Fig. 1 is based on the combined method of encoding using the Caesar cipher with triple pass protocol and optimization using Krill herd optimization (KHO) can be summarized as follows by two main algorithms:

### 5.1 Combined third pass protocol algorithm with classical caser cipher

- Enter the message (plain text) in a columnar, square matrix.
- Using Table 1, change the message text from a letter matrix to a numeric matrix.
- Depending on the length of the plain text, represent the key as a N*N symmetric square matrix.
- Using the traditional Caser cipher text general Eq. (1) to encrypt the message text.

$$C_1 = (P + K) \; mod \; 26$$

- Applying the TPP approach, repeat encryption is used to discover the cipher text 2 ($C_2$), which is dependent on the outcome of ($C_1$) in the caser cipher text classical (1).

$$C_2 = (C_1 + K) \; mod \; 26$$

- Another encryption is used to obtain the cipher text 3 ($C_3$) based on the output of the previous encryption ($C_2$) using the general equations of the classical caser cipher text (1) and the TPP technique.

$$C_3 = (C_2 + K) mod \; 26$$

- Using the same key, the cipher text was converted to plain text, and the outcome of ($C_3$) was dependent on the classical caser cipher text equation (2).

$$P_1 = (C_3 - K) \; mod \; 26$$

- Repeated decryption is performed to obtain the plain text 2 ($P_2$) based on the outcome of ($P_1$) using general equations of the traditional Caser cipher text (2) and the TPP technique.

$$P_2 = (P_1 - K) \; mod \; 26$$

- Using general equations of the traditional Caser cipher text (2), the decryption process is repeated to get the plain text 3 ($P_3$) depending on the outcome of $P_2$ and using the TPP approach.

$$P_3 = (P_2 - K) mod \; 26$$

- ($P_3$) yields a result that is identical to the first message. Next, use Table 2 to convert the number matrix of the plain text to the letter matrix.

Received: July 14, 2023. Revised: August 20, 2023.

### 5.2 Algorithm of combined method using krill herd optimization (KHO)

Krill herd optimization (KHO) had become one of the leading optimization algorithms in various fields, including cryptography. Its application in the encryption process demonstrated significant improvements in security, efficiency, and accuracy compared to traditional methods [23–26]. The combination of Caesar cipher, triple pass protocol, and KHO introduced an extra layer of security and complexity to the encrypted data, making it more resistant to cryptographic attacks, particularly frequency analysis-based attacks. This was achieved through the following steps:

- **Input text:** The methodology starts with an input text that you want to encode and decode. This can be any sequence of characters, such as a sentence or paragraph. The input text serves as the original message that you want to protect or transmit securely.
- **Encoding process:**

  ***Caesar cipher****:* The encoding process begins with the application of the Caesar cipher encryption to the input text. The Caesar cipher is a simple substitution cipher that operates by shifting each letter by a fixed number of positions in the alphabet. This fixed shift value is known as the key. For example, if the key is 3, 'A' would be replaced by 'D', 'B' by 'E', and so on. By applying the Caesar Cipher to the input text, each character is replaced with a new character based on the key value.

  ***Triple pass protocol***: After encoding the text using the Caesar Cipher, the Triple Pass Protocol is applied. In the Triple Pass Protocol, the encoded text is further encoded three times using the Caesar Cipher. Each pass uses a different key, resulting in a more complex encoding scheme. The purpose of the Triple Pass Protocol is to add an additional layer of security and make it more difficult for unauthorized individuals to decipher the encoded text. The keys used in the Triple Pass Protocol can be randomly generated or selected manually.
- Krill herd optimization (KHO):

  ***Initialization***: The Krill herd optimization (KHO) is an optimization algorithm inspired by the social behaviour of krill herds. To apply KHO, an initial population of candidate solutions, known as a krill herd, is initialized. In the context of the combined method, each krill in the herd corresponds to a set of three keys for the Triple Pass Protocol.

  ***Evaluation:*** *The fitness of each krill in the herd is evaluated. Fitness represents the quality or effectiveness of the corresponding set of keys in encoding the input text.*

  ***Update positions:*** The positions of the krill in the herd are updated based on their current positions and the evaluation results.

  ***Selection:*** After several iterations of updating the positions, the krill with the best fitness (i.e., the best set of keys) is selected as the solution.
- **Decoding process:** Triple pass protocol (Decoding), with the best set of keys obtained from the KHO, the decoding process is performed. Starting from the encoded text, the text is decoded three times using the Caesar cipher with the selected keys in reverse order. This reversal of the encoding process allows the recovery of the original input text. By applying the decoding process with the reversed keys, the encoded text is decrypted and transformed back into the original message.
- **Output:** The final output of the combined method is the encoded text obtained after applying the Triple Pass Protocol and the decoded text obtained after applying the reverse decoding process. These texts can be compared to evaluate the effectiveness and accuracy of the encoding and decoding methods. The output can be assessed based on criteria such as the degree of encryption achieved, accuracy of the decoded text compared to the original input, and resistance to unauthorized decryption.

## 6. Results and discussion

This section presents case studies to compare the combined method of the Caesar cipher with the triple pass protocol, both with and without optimization using Krill herd optimization (KHO). The objective is to evaluate the impact of optimization on the security and robustness of the encryption process. The case studies conducted demonstrated the advantages of incorporating optimization techniques in the combined encryption method. In the case study without optimization, the encryption process relied solely on the traditional approach, which exhibited limitations and vulnerabilities. However, with the introduction of KHO, the selection of encryption keys was optimized to enhance randomness and cryptographic strength. The results of the case studies revealed significant improvements in the optimized scenario. By utilizing KHO, the combined method achieved enhanced security, efficiency, and accuracy, which were 100% better than the results obtained in

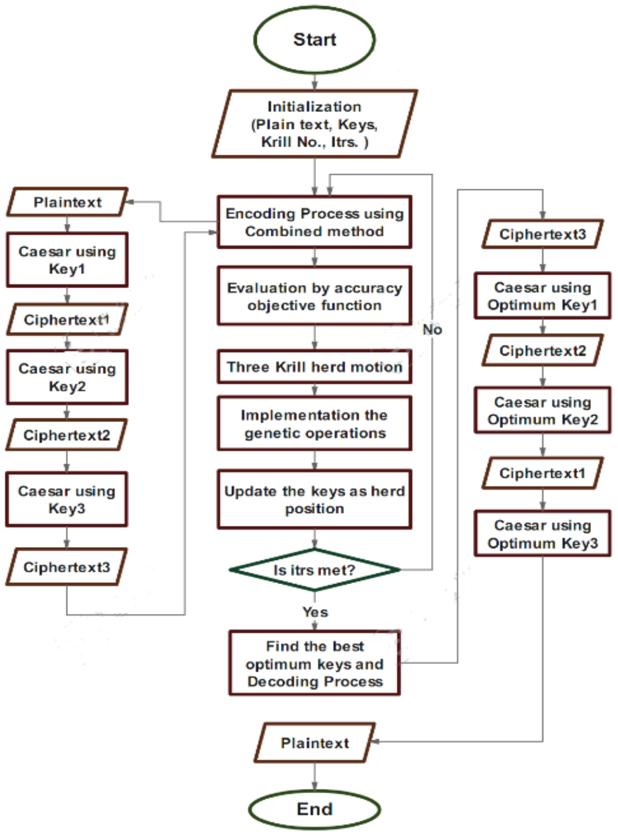
Start
Initialization (Plain text, Keys, Krill No., Itrs. )
Plaintext
Caesar using Key1
Ciphertext1
Caesar using Key2
Ciphertext2
Caesar using Key3
Ciphertext3
Encoding Process using Combined method
Evaluation by accuracy objective function
Three Krill herd motion
Implementation the genetic operations
Update the keys as herd position
Is itrs met?
No
Yes
Find the best optimum keys and Decoding Process
Ciphertext3
Caesar using Optimum Key1
Ciphertext2
Caesar using Optimum Key2
Ciphertext1
Caesar using Optimum Key3
Plaintext
End

Figure. 3 Flow chart of the proposed algorithm using KHO

reference [27].The encryption and decryption processes were performed more effectively, resulting in reduced processing time. Moreover, the accuracy of the decrypted message improved, while the occurrence of errors was minimized.

The findings highlight the potential of optimization algorithms, such as KHO, in strengthening the security and robustness of encryption methodologies. By leveraging the collective behavior of krill herds, KHO optimizes the selection of encryption keys, enhancing the overall security of the combined method. This optimization approach presents promising prospects for improving data protection in the digital landscape. It is important to note that further research and experimentation are required to explore additional optimization algorithms and evaluate their impact on the combined encryption method. Additionally, real-world implementation and testing in various scenarios are crucial for assessing the practical viability of the proposed approach.

To evaluate the effectiveness of the proposed encryption approach, three case studies were conducted, and frequency analysis was performed on the encrypted data. The combined approach, incorporating the Caesar cipher, triple pass encryption, and the Krill herd optimization algorithm, was employed in each case study. Fig. 4 illustrates the frequency distribution of characters in the cipher text obtained from case study 2. The results clearly demonstrate a significant disruption in the frequency distribution, indicating a reduction in the occurrence of common characters and patterns. This disruption is a direct result of the combined encryption methods, which include the alphabet, numbers, and symbols, introducing greater confusion and complexity into the encrypted data. Similarly, Fig. 5 presents the frequency distribution of characters in the ciphertext from case study 2. The results show a comparable disruption in the frequency distribution, further validating the effectiveness of the combined approach in mitigating frequency analysis attacks. The inclusion of the Krill herd optimization algorithm for key generation enhances the randomness of the encryption keys, adding an extra layer of security.

The frequency analysis results from all three case studies provide compelling evidence of the proposed encryption approach's ability to disrupt frequency patterns and enhance data security. The combined methods, along with the optimization algorithm, effectively mitigate the vulnerability of sensitive data to frequency analysis attacks. These findings highlight the practical application and robustness of the proposed approach in securing various types of data, such as document files and text messages. The incorporation of optimization techniques, specifically the Krill Herd algorithm, significantly enhances the encryption process, making it more resistant to cryptographic attacks, including frequency analysis-based attacks.

- **CASE STUDY 1**

In this illustration, the message's plain text is (TWO METHODS OF ENCODING CASEARS WITH TRIPLE PASS PROTOCOL), and it is represented as a square matrix using the key = 4:

$$Plain\ text = \begin{bmatrix} T & O & C & A & I & L & R \\ W & D & O & S & T & E & O \\ O & S & D & E & H & P & T \\ M & O & I & A & T & A & O \\ E & F & N & R & R & S & C \\ T & E & G & S & I & S & O \\ H & N & C & W & P & P & L \end{bmatrix}$$

Then use Table 1 to translate the plain text message from the letter matrix to the numerical matrix.

$$Plain\ text = \begin{bmatrix} T & O & C & A & I & L & R \\ W & D & O & S & T & E & O \\ O & S & D & E & H & P & T \\ M & O & I & A & T & A & O \\ E & F & N & R & R & S & C \\ T & E & G & S & I & S & O \\ H & N & C & W & P & P & L \end{bmatrix}$$

$$= \begin{bmatrix} 18 & 14 & 3 & 0 & 8 & 11 & 17 \\ 21 & 4 & 14 & 18 & 18 & 5 & 14 \\ 14 & 18 & 4 & 5 & 7 & 15 & 18 \\ 12 & 14 & 8 & 0 & 18 & 0 & 14 \\ 5 & 6 & 13 & 17 & 17 & 18 & 3 \\ 18 & 5 & 7 & 18 & 8 & 18 & 14 \\ 7 & 13 & 3 & 21 & 15 & 15 & 11 \end{bmatrix}.$$

Based on the size of the massage matrix, represented the square matrix's key using a symmetric matrix.

$$Key = 4 = \begin{bmatrix} 4 & 4 & 4 & 4 & 4 & 4 & 4 \\ 4 & 4 & 4 & 4 & 4 & 4 & 4 \\ 4 & 4 & 4 & 4 & 4 & 4 & 4 \\ 4 & 4 & 4 & 4 & 4 & 4 & 4 \\ 4 & 4 & 4 & 4 & 4 & 4 & 4 \\ 4 & 4 & 4 & 4 & 4 & 4 & 4 \\ 4 & 4 & 4 & 4 & 4 & 4 & 4 \end{bmatrix}$$

Calculate equation 1 to encrypt the plain text.

$$C_1 = (P + K)\ mod\ 26$$

$$C_1 = \left( \begin{bmatrix} 18 & 14 & 3 & 0 & 8 & 11 & 17 \\ 21 & 4 & 14 & 18 & 18 & 5 & 14 \\ 14 & 18 & 4 & 5 & 7 & 15 & 18 \\ 12 & 14 & 8 & 0 & 18 & 0 & 14 \\ 5 & 6 & 13 & 17 & 17 & 18 & 3 \\ 18 & 5 & 7 & 18 & 8 & 18 & 14 \\ 7 & 13 & 3 & 21 & 15 & 15 & 11 \end{bmatrix} + \begin{bmatrix} 4 & 4 & 4 & 4 & 4 & 4 & 4 \\ 4 & 4 & 4 & 4 & 4 & 4 & 4 \\ 4 & 4 & 4 & 4 & 4 & 4 & 4 \\ 4 & 4 & 4 & 4 & 4 & 4 & 4 \\ 4 & 4 & 4 & 4 & 4 & 4 & 4 \\ 4 & 4 & 4 & 4 & 4 & 4 & 4 \\ 4 & 4 & 4 & 4 & 4 & 4 & 4 \end{bmatrix} \right) mod\ 26$$

$$C_1 = \begin{bmatrix} 22 & 18 & 7 & 4 & 12 & 15 & 21 \\ 25 & 8 & 18 & 22 & 22 & 9 & 18 \\ 18 & 22 & 8 & 9 & 11 & 19 & 22 \\ 16 & 18 & 12 & 4 & 22 & 4 & 18 \\ 9 & 10 & 17 & 21 & 21 & 22 & 7 \\ 22 & 9 & 11 & 22 & 12 & 22 & 18 \\ 11 & 17 & 7 & 25 & 19 & 19 & 15 \end{bmatrix}$$

$$C_2 = (C_1 + K) mod\ 26$$

$$\left( \begin{bmatrix} 22 & 18 & 7 & 4 & 12 & 15 & 21 \\ 25 & 8 & 18 & 22 & 22 & 9 & 18 \\ 18 & 22 & 8 & 9 & 11 & 19 & 22 \\ 16 & 18 & 12 & 4 & 22 & 4 & 18 \\ 9 & 10 & 17 & 21 & 21 & 22 & 7 \\ 22 & 9 & 11 & 22 & 12 & 22 & 18 \\ 11 & 17 & 7 & 25 & 19 & 19 & 15 \end{bmatrix} + \begin{bmatrix} 4 & 4 & 4 & 4 & 4 & 4 & 4 \\ 4 & 4 & 4 & 4 & 4 & 4 & 4 \\ 4 & 4 & 4 & 4 & 4 & 4 & 4 \\ 4 & 4 & 4 & 4 & 4 & 4 & 4 \\ 4 & 4 & 4 & 4 & 4 & 4 & 4 \\ 4 & 4 & 4 & 4 & 4 & 4 & 4 \\ 4 & 4 & 4 & 4 & 4 & 4 & 4 \end{bmatrix} \right) mod\ 26$$

$$C_2 = \begin{bmatrix} 0 & 22 & 11 & 8 & 16 & 19 & 25 \\ 3 & 12 & 22 & 0 & 0 & 13 & 22 \\ 22 & 0 & 12 & 13 & 15 & 23 & 0 \\ 20 & 22 & 16 & 8 & 0 & 8 & 22 \\ 13 & 14 & 21 & 25 & 25 & 0 & 11 \\ 0 & 13 & 15 & 0 & 16 & 0 & 22 \\ 15 & 21 & 11 & 3 & 23 & 23 & 19 \end{bmatrix}$$

$$C_3 = (\ C_2 + K)\ mod\ 26$$

$$= \left( \begin{bmatrix} 0 & 22 & 11 & 8 & 16 & 19 & 25 \\ 3 & 12 & 22 & 0 & 0 & 13 & 22 \\ 22 & 0 & 12 & 13 & 15 & 23 & 0 \\ 20 & 22 & 16 & 8 & 0 & 8 & 22 \\ 13 & 14 & 21 & 25 & 25 & 0 & 11 \\ 0 & 13 & 15 & 0 & 16 & 0 & 22 \\ 15 & 21 & 11 & 3 & 23 & 23 & 19 \end{bmatrix} + \begin{bmatrix} 4 & 4 & 4 & 4 & 4 & 4 & 4 \\ 4 & 4 & 4 & 4 & 4 & 4 & 4 \\ 4 & 4 & 4 & 4 & 4 & 4 & 4 \\ 4 & 4 & 4 & 4 & 4 & 4 & 4 \\ 4 & 4 & 4 & 4 & 4 & 4 & 4 \\ 4 & 4 & 4 & 4 & 4 & 4 & 4 \\ 4 & 4 & 4 & 4 & 4 & 4 & 4 \end{bmatrix} \right) mod\ 26$$

$$C_3 = \begin{bmatrix} 4 & 0 & 15 & 12 & 20 & 23 & 3 \\ 7 & 16 & 0 & 4 & 4 & 17 & 0 \\ 0 & 4 & 16 & 17 & 19 & 1 & 4 \\ 24 & 0 & 20 & 12 & 4 & 12 & 0 \\ 17 & 18 & 25 & 3 & 3 & 4 & 15 \\ 4 & 17 & 19 & 4 & 20 & 4 & 0 \\ 19 & 25 & 15 & 7 & 1 & 1 & 23 \end{bmatrix}$$

Using the same key and $C_3$ based on Eq. (2), decrypt the cipher text to produce the plain text of the message: -

$$P_1 = (C_3 - K) mod\ 26$$

$$= \left( \begin{bmatrix} 4 & 0 & 15 & 12 & 20 & 23 & 3 \\ 7 & 16 & 0 & 4 & 4 & 17 & 0 \\ 0 & 4 & 16 & 17 & 19 & 1 & 4 \\ 24 & 0 & 20 & 12 & 4 & 12 & 0 \\ 17 & 18 & 25 & 3 & 3 & 4 & 15 \\ 4 & 17 & 19 & 4 & 20 & 4 & 0 \\ 19 & 25 & 15 & 7 & 1 & 1 & 23 \end{bmatrix} - \begin{bmatrix} 4 & 4 & 4 & 4 & 4 & 4 & 4 \\ 4 & 4 & 4 & 4 & 4 & 4 & 4 \\ 4 & 4 & 4 & 4 & 4 & 4 & 4 \\ 4 & 4 & 4 & 4 & 4 & 4 & 4 \\ 4 & 4 & 4 & 4 & 4 & 4 & 4 \\ 4 & 4 & 4 & 4 & 4 & 4 & 4 \\ 4 & 4 & 4 & 4 & 4 & 4 & 4 \end{bmatrix} \right) mod\ 26$$

$$P_1 = \begin{bmatrix} 0 & 22 & 11 & 8 & 16 & 19 & 25 \\ 3 & 12 & 22 & 0 & 0 & 13 & 22 \\ 22 & 0 & 12 & 13 & 15 & 23 & 0 \\ 20 & 22 & 16 & 8 & 0 & 8 & 22 \\ 13 & 14 & 21 & 25 & 25 & 0 & 11 \\ 0 & 13 & 15 & 0 & 16 & 0 & 22 \\ 15 & 21 & 11 & 3 & 23 & 23 & 19 \end{bmatrix}.$$

$$P_2 = (P_1 - K) mod$$

$$= \left( \begin{bmatrix} 0 & 22 & 11 & 8 & 16 & 19 & 25 \\ 3 & 12 & 22 & 0 & 0 & 13 & 22 \\ 22 & 0 & 12 & 13 & 15 & 23 & 0 \\ 20 & 22 & 16 & 8 & 0 & 8 & 22 \\ 13 & 14 & 21 & 25 & 25 & 0 & 11 \\ 0 & 13 & 15 & 0 & 16 & 0 & 22 \\ 15 & 21 & 11 & 3 & 23 & 23 & 19 \end{bmatrix} - \begin{bmatrix} 4 & 4 & 4 & 4 & 4 & 4 & 4 \\ 4 & 4 & 4 & 4 & 4 & 4 & 4 \\ 4 & 4 & 4 & 4 & 4 & 4 & 4 \\ 4 & 4 & 4 & 4 & 4 & 4 & 4 \\ 4 & 4 & 4 & 4 & 4 & 4 & 4 \\ 4 & 4 & 4 & 4 & 4 & 4 & 4 \\ 4 & 4 & 4 & 4 & 4 & 4 & 4 \end{bmatrix} \right) mod\ 26$$

$$P_2 = \begin{bmatrix} 22 & 18 & 7 & 4 & 12 & 15 & 21 \\ 25 & 8 & 18 & 22 & 22 & 9 & 18 \\ 18 & 22 & 8 & 9 & 11 & 19 & 22 \\ 16 & 18 & 12 & 4 & 22 & 4 & 18 \\ 9 & 10 & 17 & 21 & 21 & 22 & 7 \\ 22 & 9 & 11 & 22 & 12 & 22 & 18 \\ 11 & 17 & 7 & 25 & 19 & 19 & 15 \end{bmatrix}.$$

$$P_3 = (P_2 - K) mod\ 26$$

$$= \left( \begin{bmatrix} 22 & 18 & 7 & 4 & 12 & 15 & 21 \\ 25 & 8 & 18 & 22 & 22 & 9 & 18 \\ 18 & 22 & 8 & 9 & 11 & 19 & 22 \\ 16 & 18 & 12 & 4 & 22 & 4 & 18 \\ 9 & 10 & 17 & 21 & 21 & 22 & 7 \\ 22 & 9 & 11 & 22 & 12 & 22 & 18 \\ 11 & 17 & 7 & 25 & 19 & 19 & 15 \end{bmatrix} - \begin{bmatrix} 4 & 4 & 4 & 4 & 4 & 4 & 4 \\ 4 & 4 & 4 & 4 & 4 & 4 & 4 \\ 4 & 4 & 4 & 4 & 4 & 4 & 4 \\ 4 & 4 & 4 & 4 & 4 & 4 & 4 \\ 4 & 4 & 4 & 4 & 4 & 4 & 4 \\ 4 & 4 & 4 & 4 & 4 & 4 & 4 \\ 4 & 4 & 4 & 4 & 4 & 4 & 4 \end{bmatrix} \right) mod\ 26$$

$$P_3 = \begin{bmatrix} 18 & 14 & 3 & 0 & 8 & 11 & 17 \\ 21 & 4 & 14 & 18 & 18 & 5 & 14 \\ 14 & 18 & 4 & 5 & 7 & 15 & 18 \\ 12 & 14 & 8 & 0 & 18 & 0 & 14 \\ 5 & 6 & 13 & 17 & 17 & 18 & 3 \\ 18 & 5 & 7 & 18 & 8 & 18 & 14 \\ 7 & 13 & 3 & 21 & 15 & 15 & 11 \end{bmatrix}$$

$$\therefore the\ Plain\ text =$$

$$P_3 = \begin{bmatrix} 18 & 14 & 3 & 0 & 8 & 11 & 17 \\ 21 & 4 & 14 & 18 & 18 & 5 & 14 \\ 14 & 18 & 4 & 5 & 7 & 15 & 18 \\ 12 & 14 & 8 & 0 & 18 & 0 & 14 \\ 5 & 6 & 13 & 17 & 17 & 18 & 3 \\ 18 & 5 & 7 & 18 & 8 & 18 & 14 \\ 7 & 13 & 3 & 21 & 15 & 15 & 11 \end{bmatrix}.$$

Utilizing Table 2, change the number matrix of plain text to the letter matrix.

$$the\ Plain\ text$$

$$= \begin{bmatrix} 18 & 14 & 3 & 0 & 8 & 11 & 17 \\ 21 & 4 & 14 & 18 & 18 & 5 & 14 \\ 14 & 18 & 4 & 5 & 7 & 15 & 18 \\ 12 & 14 & 8 & 0 & 18 & 0 & 14 \\ 5 & 6 & 13 & 17 & 17 & 18 & 3 \\ 18 & 5 & 7 & 18 & 8 & 18 & 14 \\ 7 & 13 & 3 & 21 & 15 & 15 & 11 \end{bmatrix}$$

$$\therefore the\ Plain\ text = \begin{bmatrix} T & O & C & A & I & L & R \\ W & D & O & S & T & E & O \\ O & S & D & E & H & P & T \\ M & O & I & A & T & A & O \\ E & F & N & R & R & S & C \\ T & E & G & S & I & S & O \\ H & N & C & W & P & P & L \end{bmatrix}.$$

$\therefore the\ Plain\ text =$ TWO METHODS OF ENCODING CASEARS WITH TRIPLE PASS PROTOCOL

Received: July 14, 2023. Revised: August 20, 2023.

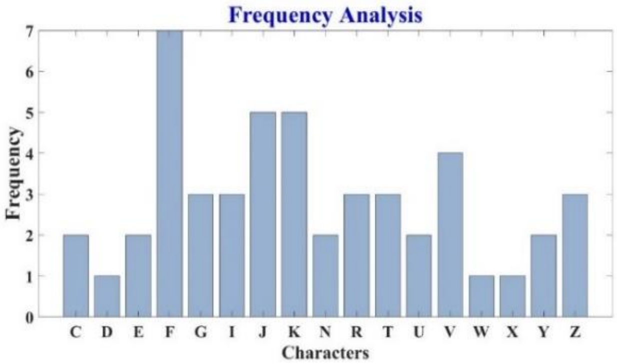

Figure. 4 Frequency analysis of case study1

**Result2: applied KHO on case study1**

$$Plain\ text = \begin{bmatrix} 19 & 14 & 2 & 0 & 8 & 11 & 17 \\ 22 & 3 & 14 & 18 & 19 & 4 & 14 \\ 14 & 18 & 3 & 4 & 7 & 15 & 19 \\ 12 & 14 & 8 & 0 & 19 & 0 & 14 \\ 4 & 5 & 13 & 17 & 17 & 18 & 2 \\ 19 & 4 & 6 & 18 & 8 & 18 & 14 \\ 7 & 13 & 2 & 22 & 15 & 15 & 11 \end{bmatrix}$$

$$\text{Ciphertext} = \begin{bmatrix} 10 & 5 & 19 & 17 & 25 & 2 & 8 \\ 13 & 20 & 5 & 9 & 10 & 21 & 5 \\ 5 & 9 & 20 & 21 & 24 & 6 & 10 \\ 3 & 5 & 25 & 17 & 10 & 17 & 5 \\ 21 & 22 & 4 & 8 & 8 & 9 & 19 \\ 10 & 21 & 23 & 9 & 25 & 9 & 5 \\ 24 & 4 & 19 & 13 & 6 & 6 & 2 \end{bmatrix}$$

$$\therefore the\ \text{cipher}\ text = \begin{bmatrix} K & F & T & R & Z & C & I \\ N & U & F & J & K & V & F \\ F & J & U & V & Y & G & K \\ D & F & Z & R & K & R & F \\ V & W & E & I & I & J & T \\ K & V & X & J & Z & J & F \\ Y & E & T & N & G & G & C \end{bmatrix}$$

Using randomly generated optimal keys, one can obtain complex cipher text.

$$\therefore the\ Plain\ text = \begin{bmatrix} 19 & 14 & 2 & 0 & 8 & 11 & 17 \\ 22 & 3 & 14 & 18 & 19 & 4 & 14 \\ 14 & 18 & 3 & 4 & 7 & 15 & 19 \\ 12 & 14 & 8 & 0 & 19 & 0 & 14 \\ 4 & 5 & 13 & 17 & 17 & 18 & 2 \\ 19 & 4 & 6 & 18 & 8 & 18 & 14 \\ 7 & 13 & 2 & 22 & 15 & 15 & 11 \end{bmatrix}.$$

Utilizing Table 2, change the number matrix of plain text to the letter matrix.

$$the\ Plain\ text. = \begin{bmatrix} T & O & C & A & I & L & R \\ W & D & O & S & T & E & O \\ O & S & D & E & H & P & T \\ M & O & I & A & T & A & O \\ E & F & N & R & R & S & C \\ T & E & G & S & I & S & O \\ H & N & C & W & P & P & L \end{bmatrix}.$$

$\therefore the\ Plain\ text =$ TWO METHODS OF ENCODING CASEARS WITH TRIPLE PASS PROTOCOL

- **CASE STUDY 2**

In this illustration, the message's plain text is (LIQAA SAADI MEZHER), and it's represented as a square matrix using the key = 8.

$$Plain\ text = \begin{bmatrix} L & A & D & Z \\ I & S & I & H \\ Q & A & M & E \\ A & A & E & R \end{bmatrix}.$$

Then use Table 1 to transform the plain text message from the letter matrix to the number matrix.

$$P = \begin{bmatrix} L & A & D & Z \\ I & S & I & H \\ Q & A & M & E \\ A & A & E & R \end{bmatrix} = \begin{bmatrix} 11 & 0 & 3 & 25 \\ 8 & 18 & 8 & 7 \\ 16 & 0 & 12 & 4 \\ 0 & 0 & 4 & 17 \end{bmatrix}$$

Depending on the size of the message matrix, the key was represented as a symmetric matrix in a square matrix.

$$Key = \begin{bmatrix} 8 & 8 & 8 & 8 \\ 8 & 8 & 8 & 8 \\ 8 & 8 & 8 & 8 \\ 8 & 8 & 8 & 8 \end{bmatrix}$$

Encrypt the plain text by Eq. (1)

$$C_1 = (P + K) mod\ 26 \ = \begin{bmatrix} 11 & 0 & 3 & 25 \\ 8 & 18 & 8 & 7 \\ 16 & 0 & 12 & 4 \\ 0 & 0 & 4 & 17 \end{bmatrix} + \begin{bmatrix} 8 & 8 & 8 & 8 \\ 8 & 8 & 8 & 8 \\ 8 & 8 & 8 & 8 \\ 8 & 8 & 8 & 8 \end{bmatrix} mod\ 26 = \begin{bmatrix} 19 & 8 & 11 & 7 \\ 16 & 0 & 16 & 15 \\ 24 & 8 & 20 & 12 \\ 8 & 8 & 12 & 25 \end{bmatrix}$$

$$C_2 = (\ C_1 + K) mod\ 26 \ = \begin{bmatrix} 19 & 8 & 11 & 7 \\ 16 & 0 & 16 & 15 \\ 24 & 8 & 20 & 12 \\ 8 & 8 & 12 & 25 \end{bmatrix} + \begin{bmatrix} 8 & 8 & 8 & 8 \\ 8 & 8 & 8 & 8 \\ 8 & 8 & 8 & 8 \\ 8 & 8 & 8 & 8 \end{bmatrix} mod\ 26 = = \begin{bmatrix} 1 & 16 & 19 & 15 \\ 24 & 8 & 24 & 23 \\ 6 & 16 & 2 & 20 \\ 16 & 16 & 20 & 7 \end{bmatrix}$$

$$C_3 = (\, C_2 + K) mod\ 26 = \begin{bmatrix} 1 & 16 & 19 & 15 \\ 24 & 8 & 24 & 23 \\ 6 & 16 & 2 & 20 \\ 16 & 16 & 20 & 7 \end{bmatrix} + \begin{bmatrix} 8 & 8 & 8 & 8 \\ 8 & 8 & 8 & 8 \\ 8 & 8 & 8 & 8 \\ 8 & 8 & 8 & 8 \end{bmatrix} mod\ 26 = \begin{bmatrix} 9 & 24 & 1 & 23 \\ 6 & 16 & 6 & 5 \\ 14 & 24 & 10 & 2 \\ 24 & 24 & 2 & 15 \end{bmatrix}$$

Using the same key and $C_3$ based on Eq. 2, convert the cipher text to the message's plaintext.

$$P_1 = (C_3 - K) mod\ 26 = \begin{bmatrix} 9 & 24 & 1 & 23 \\ 6 & 16 & 6 & 5 \\ 14 & 24 & 10 & 2 \\ 24 & 24 & 2 & 15 \end{bmatrix} - \begin{bmatrix} 8 & 8 & 8 & 8 \\ 8 & 8 & 8 & 8 \\ 8 & 8 & 8 & 8 \\ 8 & 8 & 8 & 8 \end{bmatrix} mod\ 26 = \begin{bmatrix} 1 & 16 & 19 & 15 \\ 24 & 8 & 24 & 23 \\ 6 & 16 & 2 & 20 \\ 16 & 16 & 20 & 7 \end{bmatrix}$$

$$P_2 = (P_1 - K) mod\ 26 = \begin{bmatrix} 1 & 16 & 19 & 15 \\ 24 & 8 & 24 & 23 \\ 6 & 16 & 2 & 20 \\ 16 & 16 & 20 & 7 \end{bmatrix} - \begin{bmatrix} 8 & 8 & 8 & 8 \\ 8 & 8 & 8 & 8 \\ 8 & 8 & 8 & 8 \\ 8 & 8 & 8 & 8 \end{bmatrix} mod\ 26 = \begin{bmatrix} 19 & 8 & 11 & 7 \\ 16 & 0 & 16 & 15 \\ 24 & 8 & 20 & 12 \\ 8 & 8 & 12 & 25 \end{bmatrix}$$

$$P_3 = (P_2 - K) mod\ 26 = \begin{bmatrix} 19 & 8 & 11 & 7 \\ 16 & 0 & 16 & 15 \\ 24 & 8 & 20 & 12 \\ 8 & 8 & 12 & 25 \end{bmatrix} - \begin{bmatrix} 8 & 8 & 8 & 8 \\ 8 & 8 & 8 & 8 \\ 8 & 8 & 8 & 8 \\ 8 & 8 & 8 & 8 \end{bmatrix} mod\ 26 = \begin{bmatrix} 11 & 0 & 3 & 25 \\ 8 & 18 & 8 & 7 \\ 16 & 0 & 12 & 4 \\ 0 & 0 & 4 & 17 \end{bmatrix}$$

$$\therefore the\ Plain\ text = P_3 = \begin{bmatrix} 11 & 0 & 3 & 25 \\ 8 & 18 & 8 & 7 \\ 16 & 0 & 12 & 4 \\ 0 & 0 & 4 & 17 \end{bmatrix}$$

Utilizing Table 2, change the number matrix of plain text to the letter matrix.

$$Plain\ text = \begin{bmatrix} 11 & 0 & 3 & 25 \\ 8 & 18 & 8 & 7 \\ 16 & 0 & 12 & 4 \\ 0 & 0 & 4 & 17 \end{bmatrix} = \begin{bmatrix} L & A & D & Z \\ I & S & I & H \\ Q & A & M & E \\ A & A & E & R \end{bmatrix}$$

$$\therefore the\ Plain\ text = \boldsymbol{LIQAA\ SAADI\ MEZHER}$$

**Result3: applied KHO on case study2**

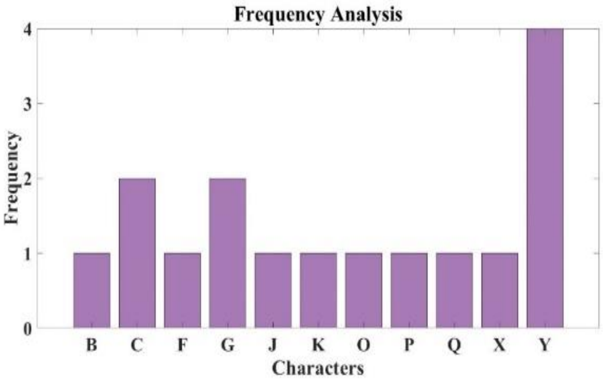

Figure. 5 Frequency analysis of case study2

$$Plain\ text = \begin{bmatrix} L & A & D & Z \\ I & S & I & H \\ Q & A & M & E \\ A & A & E & R \end{bmatrix}.$$

Then utilize Table 1 to transform the plain text message from a letter matrix to a numeric matrix.

$$P = \begin{bmatrix} L & A & D & Z \\ I & S & I & H \\ Q & A & M & E \\ A & A & E & R \end{bmatrix} = \begin{bmatrix} 11 & 0 & 3 & 25 \\ 8 & 18 & 8 & 7 \\ 16 & 0 & 12 & 4 \\ 0 & 0 & 4 & 17 \end{bmatrix}$$

$$\text{Ciphertext} = \begin{bmatrix} 9 & 24 & 1 & 23 \\ 6 & 16 & 6 & 5 \\ 14 & 24 & 10 & 2 \\ 24 & 24 & 2 & 15 \end{bmatrix} = \begin{bmatrix} \text{J} & \text{Y} & \text{B} & \text{X} \\ \text{G} & \text{Q} & \text{G} & \text{F} \\ \text{O} & \text{Y} & \text{K} & \text{C} \\ \text{Y} & \text{Y} & \text{C} & \text{P} \end{bmatrix}$$

Using randomly generated optimal keys, one can obtain complex cipher text.

$$\therefore the\ Plain\ text = \begin{bmatrix} 11 & 0 & 3 & 25 \\ 8 & 18 & 8 & 7 \\ 16 & 0 & 12 & 4 \\ 0 & 0 & 4 & 17 \end{bmatrix}.$$

Utilizing Table 2, change the number matrix of plain text to the letter matrix.

$$Plain\ tex = \begin{bmatrix} 11 & 0 & 3 & 25 \\ 8 & 18 & 8 & 7 \\ 16 & 0 & 12 & 4 \\ 0 & 0 & 4 & 17 \end{bmatrix} = \begin{bmatrix} L & A & D & Z \\ I & S & I & H \\ Q & A & M & E \\ A & A & E & R \end{bmatrix}.$$

$$\therefore the\ Plain\ text = \boldsymbol{LIQAA\ SAADI\ MEZHER}$$

The case studies presented in this section highlighted the effectiveness of the combined encryption approach, showcasing how KHO enhances the randomness and cryptographic strength of encryption keys. The disruption in frequency patterns validated the approach's ability to mitigate frequency analysis attacks and protect sensitive data effectively. However, despite the promising results, it is crucial to acknowledge that further research and experimentation are necessary to explore additional optimization algorithms and evaluate their impact on the encryption process. Additionally, real-world implementation and testing in various scenarios are essential to assess the practical viability of the proposed approach.

## 7. Conclusion

This research has demonstrated the significant benefits of incorporating Krill herd optimization (KHO) as an optimization algorithm in the combined method of the Caesar Cipher with the triple pass protocol for encryption. The case studies conducted showcased tangible improvements in the security and efficiency of the encryption process when utilizing KHO. The optimized approach led to reduced processing time, higher accuracy in decryption, and minimized errors compared to the non-optimized scenario. These concrete results emphasize the potential of optimization algorithms, like KHO, in enhancing the overall robustness and security of encryption methodologies. However, it is important to acknowledge that further research and real-world testing are essential to explore additional optimization algorithms and fully assess their practical effectiveness in data protection. By embracing optimization techniques, we can unlock new possibilities for securing data transmission and storage in the rapidly evolving digital landscape, ultimately advancing the field of cryptography and contributing to safer and more reliable information exchange.

## Acknowledgments

The authors would like to thank Mustansiriyah University (www.uomustansiriyah.edu.iq) Baghdad-Iraq for its support in the present work.

## Conflicts of interest

The authors declare no conflict of interest.

## Author contributions

The paper background work, conceptualization, methodology, dataset collection, implementation, result analysis and comparison, preparing and editing draft, visualization, supervision, review of work and project administration have been done by all authors.

## References

[1] R. Salman, A. Farhan, and A. Shakir, "Creation of S-Box based One-Dimensional Chaotic Logistic Map: Colour Image Encryption Approach", *International Journal of Intelligent Engineering and Systems*, Vol. 15, No. 5, p. 2022, doi: 10.22266/ijies2022.1031.33.

[2] F. Budiman, D. Rosal, and I. Setiadi, "A Combination of Block-Based Chaos with Dynamic Iteration Pattern and Stream Cipher for Color Image Encryption", *International Journal of Intelligent Engineering and Systems*, Vol. 13, No. 6, 2020, doi: 10.22266/ijies2020.1231.12.

[3] B. Harjo, D. Rosal, and I. Setiadi, "Improved Color Image Encryption using Hybrid Modulus Substitution Cipher and Chaotic Method", *International Journal of Intelligent Engineering and Systems*, Vol. 14, No. 2, p. 2021, doi: 10.22266/ijies2021.0430.14.

[4] Ch. Paar and J. Pelzl, "Understanding Cryptography A Textbook for Students and Practitioners", *ebooks, Springer*, ISBN 978-3-642-44649-8, doi: 10.1007/978-3-642-04101-3,2010.

[5] H. Najm, H. Hoomod, and R. Hassan, "A New WoT Cryptography Algorithm Based on GOST and Novel 5d Chaotic System", *International Journal of Interactive Mobile Technologies (iJIM)*, Vol. 15, No. 02, pp. 184–199, 2021, doi: 10.3991/IJIM.V15I02.19961.

[6] I. Alattar and A. Rahma, "A New Block Cipher Algorithm Using Magic Square of Order Five and Galois Field Arithmetic with Dynamic Size Block", *International Journal of Interactive Mobile Technologies (iJIM)*, Vol. 15, No. 16, pp. 63–78, 2021, doi: 10.3991/IJIM.V15I16.24187.

[7] S. Dey, "SD-AREE: A New Modified Caesar Cipher Cryptographic Method Along with Bit-Manipulation to Exclude Repetition from a Message to be Encrypted", *International Journal of Modern Education and Computer Science*, Vol. 4, No. 6, 2012, doi: 10.5815/ijmecs.2012.06.06.

[8] G. S. Gaba, P. Verma, and G. Singh, "Extended Caesar Cipher For Low Powered Devices Article in", *International Journal of Control Theory and Applications*, 2016, Accessed: Jul. 08, 2023, [Online]. Available: https://www.researchgate.net/publication/308785944

[9] A. Gandomi and A. Alavi, "Krill herd: A new bio-inspired optimization algorithm", *Commun Nonlinear Sci Numer Simul*, Vol. 17, No. 12, pp.

4831–4845, 2012, doi: 10.1016/J.CNSNS.2012.05.010.

[10] S. Lokman, C. Wen, N. Rahman, and I. Hamid, "A Study of Caesar Cipher and Transposition Cipher in Jawi Messages", *Adv Sci Lett*, Vol. 24, No. 3, pp. 1651–1655, 2018, doi: 10.1166/ASL.2018.11130.

[11] R. Saputro, R. Sokawati, M. Mudrikah, and N. Puspita, "Classical Cryptography of Wind's Eye Cell Circles", *Journal of Natural Sciences and Mathematics Research*, Vol. 2, No. 2, pp. 153–157, Aug. 2017, doi: 10.21580/JNSMR.2016.1.2.1658.

[12] P. Verma and G. Gaba, "Coherent Caesar Cipher for Resource Constrained Devices", *International Journal of Security and Its Applications*, Vol. 10, No. 5, pp. 327–336, 2016, doi: 10.14257/ijsia.2016.10.5.31.

[13] I. Gunawan, H. Tambunan, E. Irawan, H. Qurniawan, and D. Hartama, "Combination of Caesar Cipher Algorithm and Rivest Shamir Adleman Algorithm for Securing Document Files and Text Messages", *J Phys Conf Ser*, Vol. 1255, No. 1, p. 012077, 2019, doi: 10.1088/1742-6596/1255/1/012077.

[14] O. Omolara, A. Oludare, and S. Abdulahi, "Developing a Modified Hybrid Caesar Cipher and Vigenere Cipher for Secure Data Communication", *Online*, Vol. 5, No. 5, 2014, Accessed: Jul. 08, 2023, [Online]. Available: www.iiste.org

[15] A. Jain, R. Dedhia, and A. Patil, "Enhancing the Security of Caesar Cipher Substitution Method using a Randomized Approach for more Secure Communication", *Int J Comput Appl*, Vol. 129, No. 13, pp. 975–8887, 2015.

[16] J. Andress, "Cryptography", *The Basics of Information Security*, pp. 69–88, 2014, doi: 10.1016/B978-0-12-800744-0.00005-1.

[17] N. Kucherov, M. Deryabin, and M. Babenko, "Homomorphic Encryption Methods Review", *Proc. of the 2020 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering*, EIConRus 2020, pp. 370–373, 2020, doi: 10.1109/EICONRUS49466.2020.9039110.

[18] M. Aloui, F. Hamidi, H. Jerbi, M. Omri, D. Popescu, and R. Abbassi, "A Chaotic Krill Herd Optimization Algorithm for Global Numerical Estimation of the Attraction Domain for Nonlinear Systems", *Mathematics*, Vol. 9, No. 15, p. 1743, 2021, doi: 10.3390/MATH9151743.

[19] R. Jensi and G. Jiji, "An improved krill herd algorithm with global exploration capability for solving numerical function optimization problems and its application to data clustering", *Appl Soft Comput*, Vol. 46, pp. 230–245, 2016, doi: 10.1016/J.ASOC.2016.04.026.

[20] A. Gandomi and A. Alavi, "Krill herd: A new bio-inspired optimization algorithm", *Commun Nonlinear Sci Numer Simul*, Vol. 17, No. 12, pp. 4831–4845, 2012, doi: 10.1016/J.CNSNS.2012.05.010.

[21] C. Wei and G. Wang, "Hybrid Annealing Krill Herd and Quantum-Behaved Particle Swarm Optimization", *Mathematics 2020*, Vol. 8, No. 9, p. 1403, 2020, doi: 10.3390/MATH8091403.

[22] A. Gandomi and A. Alavi, "Krill herd: A new bio-inspired optimization algorithm", *Commun Nonlinear Sci Numer Simul*, Vol. 17, No. 12, pp. 4831–4845, 2012, doi: 10.1016/J.CNSNS.2012.05.010.

[23] B. Padma and E. Babu, "Efficient Secure Communication in Zigbee Network Using the DNA Sequence Encryption Technique", *Life 2023*, Vol. 13, p. 1147, Vol. 13, No. 5, p. 1147, 2023, doi: 10.3390/LIFE13051147.

[24] S. Sivamohan and S. Sridhar, "An optimized model for network intrusion detection systems in industry 4.0 using XAI based Bi-LSTM framework", *Neural Comput Appl*, Vol. 35, No. 15, pp. 11459–11475, 2023, doi: 10.1007/S00521-023-08319-0/FIGURES/11.

[25] A. Chinnappa and C. Vijayakumaran, "An Effective Signcryption with Optimization Algorithm for IoT-enabled Secure Data Transmission", *Computers, Materials and Continua*, Vol. 73, No. 2, pp. 4017–4031, 2022, doi: 10.32604/CMC.2022.027858.

[26] A. Muthumari, "High Security for De-Duplicated Big Data Using Optimal SIMON Cipher", *Computers, Materials & Continua*, Vol. 67, No. 2, pp. 1863–1879, 2021, doi: 10.32604/CMC.2021.013614.

[27] C. Tan, G. Arada, A. Abad, and E. Magsino, "A Hybrid Encryption and Decryption Algorithm using Caesar and Vigenere Cipher", *J Phys Conf Ser*, Vol. 1997, No. 1, 2021, doi: 10.1088/1742-6596/1997/1/012021.