Abstract—With the advent of e-commerce, it has become extremely essential to tackle the sensitive issues of affording data security, especially in the ever-blooming open network environment of the modern era. The encrypting technologies of the time-honored cryptography are generally employed to shelter data safety extensively. The term ‘cryptography’ refers to the process of safeguarding the secret data against access by unscrupulous persons in scenarios where it is humanly impossible to furnish physical protection. It deals with the methods which convert the data between intelligible and unintelligible forms by encryption/decryption functions with the management of key(s). Nowadays cryptographic key management issues that arise due to the distributed nature of IT resources, as well the distributed nature of their control. Recently these issues are solved by optimization algorithms utilized in the cryptographic algorithms. The purpose of this paper is to give a survey of optimal cryptographic keys that can be developed with the help of optimization algorithms, and to address their merits to the real-world scenarios.

Keywords—Cryptography; Encryption; Decryption; Key Management; Optimization algorithm;

I. INTRODUCTION

Cryptography (also known as cryptology) is an art of achieving security by encoding messages to make them non-readable using different encryption algorithms so that only the intended user can see the original content [19-23].

The basic block diagram of a cryptosystem is given in figure 1. Cryptography prior to the modern age was effectively synonymous with encryption, the conversion of information from a readable state to apparent nonsense [24-28]. A cryptographic algorithm technically called as cipher, is a mathematical function used in the encryption and decryption process. A cryptographic algorithm works in association with a key to encrypt the message [1]. A cryptographic algorithm with all possible keys and protocols is known as a cryptosystem. Each security system must supply some security process that guarantees the secrecy of the system [29-32]. Some of the goals that can be achieved by cryptography are as follows: Authentication, Confidentiality, Access Control, Integrity, Non-repudiation, Availability and Accountability. In the cryptographic process encryption and decryption demands a key [33-36]. Some cryptosystems uses the same key together for encryption and decryption called as symmetric key or private key cryptography and asymmetric key or public key cryptography may use different keys together [2]. The mathematical optimization method, which is a best method to choose an element from a group of obtainable alternatives, is used in mathematics, computer science and operation research [37-42]. Simply, an optimization issue contains a set of maximum or minimum real functions from which selecting an input value from an acceptable value and calculating the value of the function [43-46]. Mostly, the optimization theory and methods are used in the field of applied mathematics [47-50]. The optimization method also includes finding the best accessible value of target function from a defined domain or variety of target functions from different type of domain [3]. The main purpose of optimization is to reduce the interval of a point multiplication that depends on the number of required cycles [51-55]. Especially, the replicated arithmetic obstructs are used to improve the parallelism for fundamental process. Most of the execution takes place on algorithm optimization or improved arithmetic architectures finds to be suitable for cryptographic operations [4].

II. SCOPE OF OPTIMIZATION PROBLEMS

In a standard point of view, the process of optimization can be described to find the best solution of the function from the
system within constraints [56]. This process needs the following components such as:

- The result of the function requires a minimized or maximized scalar quantitative process metrics and it is based on systems cost, yield, and profit.
- This converts the optimization issue into a group of equations and inequalities in order of constraints. These constraints are used to comprise a possible area which defines the limitations in process of the system [57].

The predictive model variables must fulfill the constraints. This can be achieved by multiple instances of variable values, guiding to a possible area that is established by a subspace of these variables. These subspaces are classified by a group of decision variables in many engineering issues that can be understood as degree of freedom in the process. Taxonomy of various bio inspired optimization algorithms [16] grouped by the area of inspirations as shown in figure 2.

![Taxonomy of various bio inspired optimization algorithms grouped by the area of inspiration](image-url)

**Evolution**

<table>
<thead>
<tr>
<th>Evolution Algorithms</th>
<th>GA</th>
<th>Genetic Algorithm</th>
</tr>
</thead>
<tbody>
<tr>
<td>GP</td>
<td></td>
<td>Genetic Programming</td>
</tr>
<tr>
<td>ES</td>
<td></td>
<td>Evolution Strategy</td>
</tr>
<tr>
<td>DE</td>
<td></td>
<td>Differential Evolution</td>
</tr>
<tr>
<td>PFA</td>
<td></td>
<td>Paddy Field Algorithm</td>
</tr>
</tbody>
</table>

**Swarm Based**

<table>
<thead>
<tr>
<th>Natural River System</th>
<th>IWD</th>
<th>Intelligent Water Drops</th>
</tr>
</thead>
<tbody>
<tr>
<td>Human Immune System</td>
<td>AIS</td>
<td>Artificial Immune System</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Convergent Social Phenomenon in Animals</th>
<th>GSO</th>
<th>Group search optimizer</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>PSO</td>
<td>Particle Swarm Optimization</td>
</tr>
<tr>
<td></td>
<td>ACO</td>
<td>Ant Colony Optimization</td>
</tr>
<tr>
<td></td>
<td>FSA</td>
<td>Fish Swarm Algorithm</td>
</tr>
<tr>
<td></td>
<td>BFA</td>
<td>Bacterial Foraging Optimization Algorithm</td>
</tr>
<tr>
<td></td>
<td>FA</td>
<td>Firefly Algorithm</td>
</tr>
<tr>
<td></td>
<td>ABC</td>
<td>Artificial Bee Colony</td>
</tr>
<tr>
<td></td>
<td>SFLA</td>
<td>Shuffled Frog Leaping Algorithm</td>
</tr>
</tbody>
</table>

Fig. 2. Taxonomy of various bio inspired optimization algorithms grouped by the area of inspiration
III. OPTIMIZATION ALGORITHMS

Some important traditional and modern optimization algorithms are explained as follows [58-63].

A. Differential Evaluation (DE) Algorithm

DE is mainly used for multi-dimensional real-valued functions, but does not use the gradient of the issue being optimized. This denotes that DE does not possess any optimization issue, but requires classic optimization techniques such as gradient descent and quasi-newton techniques. DE can also be used for optimization issues such as non-continuous, noisy and change over time.

B. Genetic Algorithm (GA)

An algorithm is initiated with a collection of solutions (chromosomes) called population. One population’s solution can be used to create a new population. Solutions which are chosen to create new solutions (offspring) are chosen according to their fitness for reproduction and the most suited solution can be selected. In Genetic Algorithm, the fitness operation of the optimization method can be estimated by the chromosome in the hidden layer and neurons. The cross over is created depending on fitness value.

C. Cuckoo Search (CS) Algorithm

The Cuckoo Search algorithm is proposed by entrusting brood parasitism of many cuckoo species i.e., placing their eggs on the nest of host fledglings. The shades can be copied by those female parasitic cuckoos and through the example of host species’ eggs. For easiness, it is imagined that there is only one egg at once in a nest. The initial alignment can be interpreted by the accessible egg in the host nest. An egg placed by a cuckoo act as a guide to another alignment created by the strategy.

D. Ant Colony Optimization (ACO) Algorithm

The ACO algorithm is one of the most competent methods that indicate the main aspects of state transition rules and pheromone modernize devices. In each iteration, colonies of ants are sent to a particular place for solution. Each ant works steadily in their state transition rules. Suppose, if an ant completes a work, then the pheromone modernized begins to search another ant with similar strength. But it significantly reduces the opportunities and changes the search methodology [61].

E. Particle Swarm Optimization (PSO) Algorithm

The PSO strategy is engaged to differentiate the perfect solutions from the identified data limits that denote to obtain the perfect equation from the numerical model. The PSO is a population-based search algorithm which is initiated with unique population of randomly-produced solutions which are known as particles. In PSO strategy, the numbers of particles are initially prepared along with initiation of population size after this process updated with new solutions.

IV. CRYPTOGRAPHIC BASED OPTIMIZATION METHODS

In 2012, AartiSoni et al. recommended that the cryptography is crucial for ensuring data security with the increased online exchange handling [5]. The research exhibited that the Genetic Algorithm was employed to create a key with the help of a pseudo-irregular number generator. The Random number was created on the premise of current time of the framework. The quality of the way was kept to be great in spite of the entire strategy which is adequate. The authors symmetric key calculation which was utilized for scrambling the image was extremely secure technique for symmetric key encryption. Through the consequences, the effectiveness of strategy was expanded as far as the processing time got obliged and intricacy to assault the message.

K.Shankar et al. [6], proposed an efficient method of ECC based image encryption scheme with the aid of optimization technique using the Differential Evolution (DE) algorithm. In this method is used to improve the performance of an image encryption in ECC method, Differential Evaluation (DE) algorithm based optimization process is applied on the private key generation phase. The performance of the image is taken as a fitness value of the optimization process such as PSNR value that shows the efficiency of their method.

N. K. Sreelaja et al. proposed the method to encrypt binary image [7] using stream cipher and ant colony optimization technique for key generation. This method reduced the number of keys to be stored and distributed. The character code table is used to encode the keys and characters in the plain text. The result ensures this approach has the capability to encrypt binary images of various sizes.

The authors also proposed swarm intelligence approach [8] or otherwise termed as Ant Colony Optimization key Generation Algorithm (AKGA), for generating keys to encrypt the text message. In this method, stream cipher is used to encode the secret text and AKGA is used for generating keys. Here the keys are reduced and the results of the proposed framework ensure that it has the capability for encrypting original message of varying size.

In another work authors also proposed particle swarm optimization, or otherwise termed as PKGA (Particle swarm optimization Key Generation Algorithm) for generating keys to encrypt original text message [9]. In this method, stream cipher is used to encode the secret text and PKGA is used for generating keys. In this method, keys are reduced to be stored and distributed when compared with vernam cipher. The result of this framework ensures that it has adequate encryption of varying size of original message. When PKGA is compared with AKGA (Ant colony optimization Key Generation Algorithm), the encryption process time is lesser in the former than the latter.

Genetic Algorithm is used by P. Saveetha et al. for reducing the computational complexity of the cryptanalysis [10]. Encoding process on the stream cipher using the GA with pseudo random series method consumed lesser memory.
and time when compared with the existing Fast Discrete Fourier Spectra approach on stream cipher.

The concept of utilizing Genetic Algorithm and RSA in modified approach is introduced by Abdel-karim S.O. Hassan et al. [11]. This method combines both symmetrical (using Genetic optimization) and asymmetrical (using RSA) method to ensure that make the key very complex to reinforce resistance to cryptanalysis. The first operation is symmetrical using GIC to generate the key from plaintext followed by the second operation of the new ciphering technique which is performed by RSA algorithm.

Threshold recovering algorithm for key management was developed by Xuanwu Zhou et al. [12]. In this method, encryption was done on private keys which are from KGC and then shared to aplier group. The threshold reconstruction of private keys provided protection for the secrecy of private key parameters and also aplier identity. In order to make the key management scheme effective, improved authenticated encryption scheme is presented.

K-Shankar et al. [13] proposed RGB-Based Secure Share Creation in Visual Cryptography Using Optimal Elliptic Curve Cryptography Technique. In this methods shares of the secret image in visual cryptography process are created by using the multiple shares creation method with ECC. The shares are separately encrypted and decrypted by means of the encryption and decryption technique in line with ECC. In the decryption process we generate the private key by using the cuckoo search optimization technique and for evaluating the performance of the optimization by using the peak signal to noise ratio (PSNR).

V.S.ShankarSriram et al. [14] have developed a scheme for scalar multiplication. In this scheme, the Encryption process involves two stages of Modular Multiplication. So, the time required to compute the keys is less and timing-based attacks on the key will be difficult. This scheme can be deployed in Mobile and other wireless devices.

In the method proposed by AartiSoni et al., AES algorithm is used for encrypting and decrypting digital images [15] and GA is used for key generation process. The Key length, for which the test is carried out, is 128 bit long. Longer key sequence will also work but time constraint doesn’t permit to check. The time taken to generate key for 300 iteration, with 10 new population each time, 10 crossover and mutation operations each iteration, is 75.382 seconds.

In 2014, Sindhuja et al. proposed the Genetic Algorithm (GA)-based symmetric key cryptosystem for encryption and decryption [15]. The basic content and the client information (key) were distorted into content matrix and key network separately. Additive matrices were produced by including the content matrix and key network. Linear substitution capacities were connected in the additive matrix to create the transitional figure. At that point, the GA capacities (hybrid and change) were connected to the transitional cipher to deliver the last cipher content. It was accomplished that the symmetric key substitution strategy was utilized to guarantee the secrecy in systems, which was linked and actualized with the assistance of genetic capacities to furnish including security.

J.SaiGeetha et al. proposed Artificial Bee Colony Random Number Generator [18], also called as ABCRNG which is fit to all public key cryptosystem to increase the strength of key as well as its security. It is proved through statistical tests that ABC is more efficient than other methods. Randomness of Random numbers is produced in large volumes which are evaluated by run test (Up and Down, above and below mean) method.

V. CONCLUSION

The survey has been investigated over many research papers based on optimization algorithm applied in the cryptographic algorithms. Each authors proposed some of the optimization algorithm is used to optimize the key values in particular cryptographic algorithm. Each method is unique in its own way, which have their own advantages and disadvantages. Based on existing research works the optimization algorithms are used to optimize the key values in complex cryptographic methods like ECC, RSA etc still remain significantly challenging tasks for the research community.

REFERENCES


Mohamed Elhoseny, Noura Metawa and Aboul Ella Hassanien, An automated information system to ensure quality in higher education institutions, Proceedings of 12th International Computer Engineering Conference (ICENCO), IEEE, 2016, pp, 196 - 201, https://doi.org/10.1109/ICENCO.2016.7826468


Mohamed Elhoseny, Noura Metawa and Aboul Ella Hassanien, An automated information system to ensure quality in higher education institutions, Proceedings of 12th International Computer Engineering Conference (ICENCO), IEEE, 2016, pp, 196 - 201, https://doi.org/10.1109/ICENCO.2016.7826468


