Public key cryptography by changing the seed value

R.Jothi, Dr.Anand, P.Anitha, S.Arthi

*Department of computer Applications, Dhanalakshmi Srinivasan College of Arts and Science for Women,,Perambalur , 621 212, Tamilnadu, , India.

Email: jothi47859@gmail.com *(Jothi R) Corresponding author: Jothi R*

Abstract: -Both encryption and decryption methods in cryptography ensure that only the intended receiver can decode a communication's message. Possible that a Random Number Generator (RNG) is a machine that creates random numbers or symbols. Computational Intelligence (CI) is one of the most prominent approaches to AI (AI). Complicated situations are the primary focus of CI. In order to get the desired outcome, optimization is essential. It is the numerical functions that are the major focus of the optimization procedures. Swarm intelligence is a term used to characterise a group of intelligent swarms (SI). Evolutionary computing is the primary focus of SIG. Swarm intelligence methods like Artificial Bee Colony may help you find the best answer in the solution space (ABC). The original ABC algorithm balances exploration and exploitation capabilities by using both local and global search approaches that are performed by the employed and observer bees. Artificial Bee Colony Algorithm (ABCA) is suggested in this research (ABC). Using ABC's method, just the best response is taken into account. The strength of a key is determined by its capacity to produce random numeric keys using ABC. For testing in a sequential and running context, this method creates random key results. Real-world results have been shown by applying this strategy, which is fast and effective.

***Index Terms**:* Public-Key Cryptography, Evolutionary Algorithm, Optimization,

1. INTRODUCTION

1.1CRYPTOGRAPHY

Using mathematics to encrypt and decrypt data is referred to as cryptography. Using cryptography, private information may be recovered from untrustworthy networks. Decryption is the process of defining plaintext as a kind of encryption. When plaintext is encrypted, the result is ciphertext, which is unreadable. Decryption is the process of converting encrypted text back to its original form [1]-[5].

A message is encoded using the binary system, which necessitates the application of mathematics to turn the characters into a series of numbers. In classical cryptosystems, a single common key is used to encrypt and decrypt a message (also known as single-key or symmetric). Asymmetric cryptosystems, on the other hand, use two keys instead of only one. Message decryption requires the private key and the public key that encrypts it [6]-[10].

OBJECTIVE

Fig. 1 shows the primary job and aim of cryptography. Confidentiality is the ability to keep one's private information private. Ensuring that the intended message is not tampered with. Proof of transmission and delivery: Non-Repudiation. Numbers that are completely unrelated to each other

Essentially like dice, shuffling cards, flipping coins and even drawing straws. It's difficult to generate "high-quality" random numbers manually. Random numbers are needed for simulations of probabilistic occurrences. It's difficult to generate "high-quality" random numbers manually. L.H.C. Trippett selects a random card from a set of numbered cards by hand to generate random numbers. He discovered that the outcome was wildly out of whack, and he realised how difficult it was to create randomization by hand.

As a result, he created the world's first publicly available random number table. It is necessary to use random numbers in order to simulate probabilistic occurrences. Any numerical calculations based on random numbers, such as Monte Carlo techniques, are used in this case.

What are the Good Random Numbers like?

o Making choices (e.g., coin flip).
It's necessary to generate numerical test results.
· Creation of cryptographic keys that are unique.
o Using random walks to find and optimise.
o The choice.
o Simulated.
It is likely that everyone has a basic understanding of what randomness is. Heads and tails obtained by a fair coin, for example, are seen in the following examples

HTHTHTHTHTHTHTHTHTHT
HTHTTHHHTHTHHTTTTHTH

Applications for Random Numbers

- ✓ Sampling for Statistics
- ✓ Cryptography
- ✓ Programming a computer
- ✓ Applied Numerical Methods
- ✓ When it comes to making decisions, Sampling for Statistics
- ✓ Cryptography
- ✓ Programming a computer
- ✓ Applied Numerical Methods
- ✓ When it comes to making decisions,

OPTIMIZATION

To maximise desired characteristics while limiting undesirable ones, one must identify the most cost-effective or best possible performance option within the given restrictions. In contrast, the term "maximisation" refers to the pursuit of the greatest possible result or outcome, regardless of the associated cost or expenditure. To discover "best available" values of some goal and type, optimization is to find the "best available" values for different kinds of objective functions and domains.

Nature-inspired notions have influenced the development of several optimization methods. Swarm optimization techniques and evolutionary algorithms both draw inspiration from nature. Decentralized and self-organized swarms are referred to as swarm intelligence (SI) [2]. EA tries to replicate the process of natural evolution. Examples of EA include genetic algorithms (GA) and differential evolution (DE). A simple genetic algorithm (GA) comprises of a random number generator, a fitness assessment mechanism, and genetic operators for reproduction, mutation, and crossover.

The crossover, mutation, and selection operators of the DE algorithm are comparable to those of the genetic algorithm. The DE algorithm has been developed to address the fundamental drawback of GA's inability to do local searches. The fundamental difference between GA and DE is that GA uses crossover while DE depends on modification. Using mutation as a probe and choice operation, the rules guide the search to potential areas inside a search area.

Modeling social behaviour like bird flocking or fish schooling may be done using the PSO algorithm. In multi-dimensional space, PSO is a stochastic population-based optimization strategy that works well. Following the current best particle, a population of particles moves around the search space in attempt to locate the next best particle. Function optimization is based on the particle's location, and the particle's position serves as a potential solution to the function to be improved.

As a solution to the numerical optimization problem, Yang created an intelligent rule for honey bee colonies. Only a function with two variables can be optimised using VBA. An artificial bee colony algorithm (ABCA) was proposed by DervisKaraboga in 2005 as a technical report for numerical optimization concerns [5]. Honey bees' brilliant foraging activity served as the inspiration for ABC.

DEFINTION OF THE ISSUE

We want to provide a comprehensive (but not full) overview of advances and construct a Random Key for the original ABC, which is our primary goal in this thesis. In addition, ABC researchers have suggested possible future studies.

The ABC and other swarm intelligence algorithms vary greatly in terms of the number of possible solutions that may be generated by the algorithm.

Problems that are regarded food sources rather than persons have been solved with ABC (honey bees).

Swarm people are considered to be plausible solutions in algorithms such as PSO. In the ABC algorithm, the quality of clarity (the suitability of a food source) is assessed by comparing it to the issue it was designed to solve.

ABC SYSTEM WORKS

The artificial bee colony collective intellectpointed model in the ABC algorithm is made up of three key components. :

- Worked (Employed) bees
- Viewer (Onlooker)s bees
- Scouts

Nectar quantity is used to indicate how well an optimization problem's solution is based on a food source's location and the amount of nectar it contains.

The amount of bees in the population who are either working or just watching may tell us a lot about how many options there are in the population. Initial population P(C =0) of SN solutions (food source placements), where SN specifies the size of bees or onlookers employed by the ABC, is randomly distributed. Each xi (i=1, 2,.. SN) solution is a D-dimensional vector. There are a total of n optimization parameters, and D is the total number.

Search operations for employed bees, on-looker and scout bees are repeated in C=1,2,..., MCN cycles after initialization of population of positions.

To assess nectar quality and nectar amount, an experienced bee alters her memory based on what she sees (visual information) and what she experiences (sensory information) (new solution). New positions are memorised by bees when nectar concentrations are greater than those of previous ones. As a result of this, nectar retains the preceding nectar's place inside its memory.

The following are the algorithm's most critical steps:

1: Count the Number of People in the World

repeat step 2

In step three, put the worker bees on their food supply sources.

Place the bees on the food sources based on the nectar levels of the viewers (onlookers).

Send the scouts to look for new food sources in the search area.

6: research the most efficient food supply discovered to date

Until the conditions are satisfied

TESTING OF RANDOM NUMBER GENERATORS

Many different tests are available to determine the randomness of RNGs and the sequences they generate. It is possible to categorise these tests into two groups: empirical and theoretical. A random number generator (RNG) generates a sequence that may be tested empirically, without any knowledge of how the RNG generates the sequence. Rather than relying on actual sequence generation, theoretical tests rely on knowledge of the RNG structure and are thus preferable when they are available. In this post, I'll be focusing mostly on empirical testing.

Runs consist of a series of occurrences of one kind, followed by occurrences of another type, or by no occurrences at all. A statistical procedure known as the run test may be used to determine whether or not a random process is responsible for the pattern of occurrences of two different categories of data.

Runtest's z statistic for the runs up-and-down test is wrong for a small sample. Let N be the total number of observations and a be the total number of runs that were made. Running up and down the stairs will need an average of

Mean(μ_a)= $\frac{2N-1}{3}$

Variance (σ^2_a) = $\frac{16N-29}{90}$

Critical Value Z_0 = $(a - \mu a) / \sigma a$

Randomness is tested through a series of tests.

Each and every overlapping m-bit pattern in the whole sequence is being tested for frequency in this test.

The goal of this investigation is to determine whether or not the 2m m-bit overlapping patterns occur as often as predicted in a random sequence.

When going over all 2m possible 0,1 vectors of length m, the frequency of the (i1,,im) pattern in the "circularised" string of bits (fn, f1,,fm-1) may be expressed as vi1im.

Consider that the sequence is not random if the estimated P-value is less than or equal to 0.01. Alternatively, it is reasonable to infer that the sequence is non-deterministic.

This is the value that was actually measured.

x2 is the expected result.

(x1–x2) is the difference.

ABC GENERATE RANDOM KEY

As seen in Figure 4, the method for creating an artificial bee colony works as follows. Worked (employed) bees and nectar quantities are placed on the food sources while observers are placed and nectar amounts are calculated. Scout bees are then placed on random food sources and nectar amounts are calculated. It is possible to solve the optimization issue in the ABC by placing the food supply in the best possible place. Algorithm control parameters are allocated to a random set of food source sites.

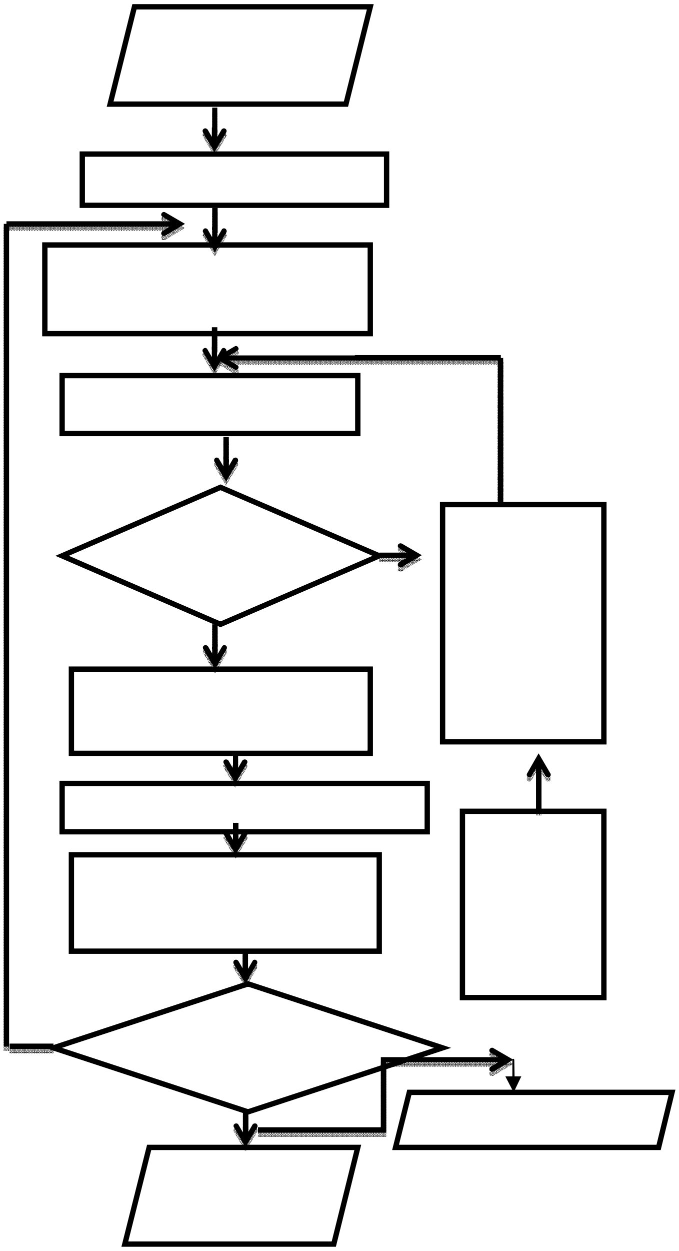
Employed bees forget about the previous nectar quantity if it is greater than the current one. When the hired bees have finished their search, they return to the hive and notify the observers waiting in the dancing area about the nectar quantities from various sources. A food source's chance is determined by the nectar quantities of all observers.

During the search for food, honey bee colonies have explorers that don't require any help from the colony's scouts.

Using the fundamental formula, if a food source solution cannot be improved

Table I: Serial Test

by a pre determined number of trials, it means Bees have exhausted their food supply, thus one of their workers is now a scout for the next location. The deleted food source is replaced with a randomly generated food location. The "limit" component of the fundamental formula is satisfied by the number of trials for emotional food supply. Once the termination conditions have been met, these three procedures are repeated until they do is shown in figure 1.



Flow Chart 1: Random Number Generation using ABC

RESULT AND DISCUSSIONS

The suggested work's implementation demonstrates how the ABC method created is a good match for the production of keys with a greater grade of fit. There were rigorous tests carried out on the keys created for use in regular statistical testing. JAVA platform has been used to implement the work, and the key created each iteration of the algorithm was run and serially tested in order to guarantee a random key was generated[11-20].

SERIAL TEST

Samples of produced keys were subjected to an equi distribution test known as a serial test.

Keys are independent of each other, as shown in Table I by the fact that the observed values of successive 00,01,10,11 are fairly near with an error percentage of around zero.

PERFORM THE TESTS:

Run tests were used to verify the randomness of the key stream. According to table II, the computed run test value, z, was determined to be less than the critical value of 1.96 A random key stream was created, and the results passed a run test, showing a random distribution.

CONCLUSION

For tackling optimization, unconstrained, and constrained problems, the Artificial Bee Colony Algorithm (ABC) was created based on honey bee foraging behaviour. Nature-inspired metaheuristic ABC mimics bees' search activity.

Random techniques like ABC are easy to implement, have fewer management parameters, and can be easily modified and hybridised with other meta heuristic algorithms.

ABC was shown to be helpful in narrowing down the key domain to the best potential key. The results of the statistical tests show that the combined usage of ABC is more effective and efficient than other approaches for reaching the global optimum. Random Keys passed both the Run and Serial tests with flying colours.

REFERENCE

[1] P. J. Angeline, J. B. Pollack and G.M. Saunders, An evolutionary algorithm that constructs recurrent neural networks. Neural Networks in IEEE Transactions on, 5(1), 1994, 54-65.

[2] J. Kennedy and R. Eberhart, Particle swarm optimization, in Proceedings of IEEE International Conference on neural networks, 4, 1995, 1942–1948.

[3] E. Bonabeau, M. Dorgio, and G. Theraulaz, Swarm intelligence: from neural network to artificial intelligence, NY: oxford university press, New York, 1999.

[4] X.S. Yang, Engineering optimization via nature inspired virtual bee algorithms, springer-verlaggmbh, 2005,317.

[5] D. Karaboga. An idea based on honey bee swarm for numerical optimization. Techn.Rep. TR06, Erciyes Univ. Press, Erciyes, 2005.

[6] R.S. Rao, SVL Narasimham, and M. Ramalingaraju.Optimization of distribution network configuration for loss reduction using artificial bee colony algorithm.International Journal of Electrical Power and Energy Systems Engineering, 1(2), 2008, 116-122.

[7] A. Singh. An artificial bee colony algorithm for the leaf-constrained minimum spanning tree problem.Applied Soft Computing, 9(2), 2009, 625–631.

[8] D. Karaboga and B. Akay. A comparative study of artificial bee colony algorithm. Applied Mathematics and Computation, 214(1), 2009, 108–132.

[9] D. Karaboga and B. Akay. Artificial bee colony (ABC) algorithm on training artificial neural networks.In Signal Processing and Communications Applications, SIU 2007. IEEE 15th, 2007, 1–4.

[10] C. Chidambaram and H.S. Lopes.A new approach for template matching in digital images using an artificial bee colony algorithm.In Nature & Biologically Inspired Computing IEEE, 2009.146–151.

[11] Remya, R. R., Samrot, A. V., Kumar, S. S., Mohanavel, V., Karthick, A., Chinnaiyan, V. K., ... & Muhibbullah, M. (2022). Bioactive Potential of Brown Algae. Adsorption Science & Technology, 2022.

[12] Remya, R. R., Julius, A., Suman, T. Y., Mohanavel, V., Karthick, A., Pazhanimuthu, C., ... & Muhibbullah, M. (2022). Role of Nanoparticles in Biodegradation and Their Importance in Environmental and Biomedical Applications. Journal of Nanomaterials, 2022.

[13] Madavan, R., Saroja, S., Karthick, A., Murugesan, S., Mohanavel, V., Velmurugan, P., ... & Sivakumar, S. (2022). Performance analysis of mixed vegetable oil as an alternative for transformer insulation oil. Biomass Conversion and Biorefinery, 1-6.

[14] Mohanavel, V., Ravichandran, M., Anandakrishnan, V., Pramanik, A., Meignanamoorthy, M., Karthick, A., & Muhibbullah, M. (2021). Mechanical properties of titanium diboride particles reinforced aluminum alloy matrix composites: a comprehensive review. Advances in Materials Science and Engineering, 2021.

[15] Raja, T., Ravi, S., Karthick, A., Afzal, A., Saleh, B., Arunkumar, M., ... & Prasath, S. (2021). Comparative Study of Mechanical Properties and Thermal Stability on Banyan/Ramie Fiber-Reinforced Hybrid Polymer Composite. Advances in Materials Science and Engineering, 2021.

[16] Gurusamy, P., Sathish, T., Mohanavel, V., Karthick, A., Ravichandran, M., Nasif, O., ... & Prasath, S. (2021). Finite element analysis of temperature distribution and stress behavior of squeeze pressure composites. Advances in Materials Science and Engineering, 2021.

[17] Dharmaraj, R., Karthick, A., Arunvivek, G. K., Gopikumar, S., Mohanavel, V., Ravichandran, M., & Bharani, M. (2021). Novel approach to handling microfiber-rich dye effluent for sustainable water conservation. Advances in Civil Engineering, 2021.

[18] Aravindh, M., Sathish, S., Prabhu, L., Raj, R. R., Bharani, M., Patil, P. P., ... & Luque, R. (2022). Effect of various factors on plant fibre-reinforced composites with nanofillers and its industrial applications: a critical review. Journal of Nanomaterials, 2022.

[19] Uthirasamy, R., Chinnaiyan, V. K., Vishnukumar, S., Karthick, A., Mohanavel, V., Subramaniam, U., & Muhibbullah, M. (2022). Design of boosted multilevel DC-DC converter for solar photovoltaic system. International Journal of Photoenergy, 2022.

[20] Chandrika, V. S., Thalib, M. M., Karthick, A., Sathyamurthy, R., Manokar, A. M., Subramaniam, U., & Stalin, B. (2021). Performance assessment of free standing and building integrated grid connected photovoltaic system for southern part of India. Building Services Engineering Research and Technology, 42(2), 237-248.