Eurasian Journal of Analytical Chemistry
ISSN: 1306-3057OPEN ACCESS 2018 13 (2):385-391

# Security Enhancement of Public key Cryptography through Randomize the Seed value

G. Deepa, Kayalvizhi R, Anitha P, Nithya N

Received 1 April 2018 ▪ Revised 10 May 2018 ▪ Accepted 24 May 2018

***Abstract:*** *Cryptography is the art of securing information by applying encryption and decryption on data to be transmitted which ensures that the original message can be understood only by the right person A Random Number Generator (RNG) may be a machine (or) physical device designed to get a sequence of numbers or symbols that lack pattern (i.e.) seem indiscriminately. Computational Intelligence (CI) is one of the popular approaches of Artificial Intelligence (AI). The purpose of CI is used to optimize the complex problems. Optimization is used role in optimizing the objective function. The optimization algorithms are mainly used to optimizing the numerical functions. Swarm Intelligence (SI), can be defined as the pointed behavior of intelligent swarms. SI mainly comes under evolutionary computing. Artificial Bee Colony (ABC) is one of the admired swarm intelligent approaches which are used for optimizing the numerical functions to find the best solution out of the solution space. Numerical function optimization plays an important. ABC is also known as population-based search procedure. Also, the original ABC algorithm combines both local search methods and global search methods that are being performed by the employed and onlooker bees for balancing the exploration and exploitation capacity. This paper proposes the concept of evolutionary algorithms, Artificial Bee Colony Algorithm (ABC). ABC focuses on only the best possible solution. The Random key is generated using ABC which produces a numeric key, it is important for a key to possess uncertainty for key force. The generated random key results shaped by this algorithm to be tested for serial test and run test. This method is observed to give quick and better performance results having sensible and possible implementation.*

***Index Terms****: Public-Key Cryptography (PKC), Evolutionary Algorithm, Optimization, Swarm Intelligence, Key Generation, Artificial Bee Colony (ABC).*

## INTRODUCTION

### Cryptography

The word cryptography is a general term that describes mathematics to encrypt and decrypt data. Cryptography enables to collect protected information are transmitting across unconfident networks. The meaning of plaintext is ordinary readable text in such a way is called encryption. Encrypting plaintext results in unreadable is called cipher text. The process of reversing cipher text to its original plaintext is called decryption. Cryptology is essentially based on arithmetic's involves transforming the letters that make up the message into a series of numbers (in the form of bits in computing because computers use the binary system), and then performing calculations.

G. Deepa, Kayalvizhi R, Anitha P, Nithya N
Assistant Professors, Department of Computer Applications, Dhanalakshmi Srinivasan College of arts and science for woman, (Autonomous) Perambalur.
E-mail:deepaasanmathi@gmail.com

The cryptography is split into 2 main classes, the primary one is classical cryptosystems secret writing algorithmic rule (also referred to as single-key or symmetric) that uses one key shared to encipher and decrypt a message. The second category is called asymmetric cryptosystem algorithm which uses two keys instead of one. One of the key is used to encrypt the message is called public key, the second is used to decrypt the message is called private key. The two keys are mathematically related.

## OBJECTIVE OF CRYPTOGRAPHY

The fundamental task and objective of cryptography is given into the following fig 1.

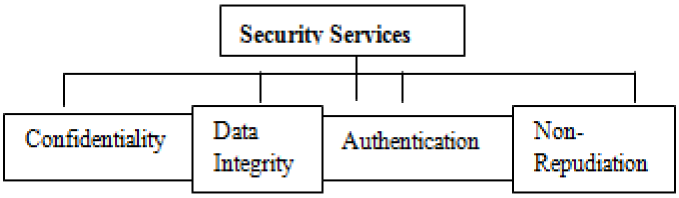


Figure 1: Security Services

**The Security Services of Cryptography is,**

Confidentiality: Unconstitutional revelation of contents.
Data veracity: Ensuring no variation to anticipated message.
Validation: Confirming uniqueness of sender.
Non-Repudiation: For proof of broadcast and rescue.

## RANDOM NUMBERS

Arbitrary number generators are just the modern application of randomness devices such as dice, shuffled cards, flipping coins and even drawing straws. On the other hand, generating “premium” random numbers generated is not so simple. Simulations of probabilistic events require random numbers.

Trippett implies to move toward with arbitrary statistics by selecting a card willy-nilly from a collection of cards by hand.

The result was robustly deviated, and notices the complexity in generating unpredictability by hand. Simulations of probabilistic events require random numbers. Such a use of arbitrary statistics, or any related numerical estimation based on random numbers, is called Monte Carlo methods.

**Characteristics of the Good Random numbers:**

o Decision making (e.g., coin flip).
o Generation of numerical test data.
o Generation of unique cryptographic keys.
o Search and optimization via random walks.
o Selection.
o Simulation.
For example, evaluate the following sequences of heads and tails generated by a fair coin
HTHTHTHTHTHTHTHTHTHT
HTHTTHHHTHTHHTTTTHTH

**Applications for Random Numbers**

- ✓ Arithmetical Sampling
- ✓ Cryptography
- ✓ Processor Programming
- ✓ Mathematical scrutiny
- ✓ Conclusion Making

## OPTIMIZATION

It is finding an efficient or uppermost possible performance under the given constraints, by maximizing favored factors and minimizing undesired ones. In assessment, maximization means trying to reach the peak or maximum result or outcome devoid of observe to charge or expenditure. Optimization is to finding "best available" values of some objective and type of differing types of objective functions and differing types of domains.

## LITERATURE REVIEW

There are many optimization algorithms based on environment-influenced concepts. Evolutionary algorithms (EA) and swarm optimization algorithms are two modules of environment-influenced algorithms. The word swarm intelligence (SI) is defined as the united behavior of broadcast and self-organized perception to reproduce the development of ordinary progress [1]. A basic GA consists of a random number generator, a robustness assessment method and heritable operators for imitation, alteration and intersects operations. Genetic algorithms (GA) and Differential Evolution (DE) algorithms are the illustration of Evolutionary algorithms.

The DE algorithm like heritable algorithm using the similar operators: Intersect alteration and collection. The DE algorithm has been planned to rise above the main shortcoming of pitiable local search facility of GA. The main distinction in constructing better solutions is that GA crossover while DE relies on variation operation. PSO is a population based stochastic optimization technique and well adapted to the optimization of non-linear function in multi-dimensional space.

In PSO, a population of particles starts to move in explore space by following the in progress optimum element and changing the point in order to find out the optima. The point refers to a possible solution of the function to be optimized and the evaluating the function by particle's position provides the fitness of that solution.

For optimizing multivariable numerical functions, Dervis Karaboga planned a bee swarm rule referred to as artificial bee colony algorithm in 2005 as a technical report for numerical optimization issues [5]. ABC is based on the show the way of bright hunt behavior of honey bees.

## PROBLEM DEFINITION

The concept of this proposal is to find a possible solution to generate random number with minimum cost and speed using the Bee Colony algorithm.

One of the key differences between ABC and other Swarm intelligence algorithms is about the feasible solutions of the algorithm. ABC has been applied to solve different kinds of problems which are considered as food sources and not individuals (honey bees).

However, in the algorithms such as PSO, the feasible solutions are supposed to be the swarm individuals. Amusingly, in the ABC algorithm the quality of clarification (fitness of a food resource) is calculated by means of the intention of function in a particular problem.

## ABC SYSTEM WORKS

In the ABC algorithm, the combined intellect pointed reproduction of artificial bee colony consists of three crucial mechanisms:

- Worked (In employment) bees
- Viewer (Onlookers) bees
- Scouts

In ABC algorithm, the location of a food resource represents a possible resolution to the optimization difficulty and the nectar amount of a food resource corresponds to the value of the connected clarification.

The quantity of the working bees or the looker-on bees is capable the quantity of result within the residents. At the most important step, the ABC generates an arbitrarily circulated first population Pop(C=0) of SN solutions (food resource positions), where SN denotes the size of working bees or onlooker bees. Each solution $x_i$ (i=1 1, 2. . . SN) is a D-dimensional vector. Here, D is the amount of optimization attributes.

After initialization, the population of the positions is thesis to frequent cycles, C=1, 2,. . ., of the explore processes of the working bees, the on looker bees and the scout bees. A utilized bee produces a variation on the position in her memory calculation on the native info (visual information) and tests the nectar measure (condition value) of the new supply (new resolution). If the nectar amount of the novel one is superior than that of the previous to one, the bee memorizes the new place and forgets the old one. If not the nectar keeps the point of the previous one in its recollection.

The most important Points of the algorithm are as below:

1: Start the Population<br>
2: Reiterate

3: Position the working bees on their fare resources
4: Position the viewer bees on the fare resources depending on their nectar amounts
5: Send the scouts to the search area for discovering new fare sources
6: study the most effective fare supply found up to now
7: In anticipation of supplies are met.

## TESTING OF RANDOM NUMBER GENERATORS

Not unexpectedly, there are a lot of dissimilar tests for RNG's and the sequences they fabricate. These tests can be separated into two different groups: Pragmatic tests and Hypothetical test. Pragmatic tests are conducted on a series generated by a RNG; require no knowledge of how the RNG produces the series.

Hypothetical test, which are enhanced when they exist, in the sense that they have knowledge but the series does not essentially need to be generated. I focus mainly on the Pragmatic tests here.

### Run Test for Randomness

A run is a sequence of occurrences of a certain type preceded and followed by the occurrences of that alternate type or by no occurrences at all. The run take a look at may be a statistical method accustomed verifies whether or not the pattern of occurrences of 2 types of observations is set by a random method.

For huge sample, the z statistical reported by Run test is inaccurate for the runs changeable test. Let 'N' be the number of comments and let 'a' be the number of runs. The predictable number of runs in the run changeable test is

Mean ($\mu_a$) = $\frac{2N-1}{3}$
Variation ($\sigma^2{}_{a)}$ = $\frac{16N-29}{90}$
Critical Value $Z_0 = (a - \mu a) / \sigma a$

### Serial Test for Randomness

The center of attention of this experiment is the frequency of each and every intersection of m-bit pattern diagonally the whole series.

The reason of this take a look at is to see whether or not the quantity of phenomenon of the 2m m-bit intersection patterns is about constant as would be expected for a arbitrary series. Specifically, for $i_1,\cdots,i_m$ operation from side to side the set of all $2^m$ possible 0,1 vectors of duration m, let $v_{i1\cdots i_m}$denote the occurrence of the pattern $(i_1,\cdots,i_m)$ in the "circularized" string of bits $(f_1,\cdots,f_{n,}\ f_1,\cdots,f_{m-1})$

If the enumerated P-face value is <0.01, then bring to a close that the series is non-arbitrary. Or else, terminate that the series is arbiter.
Observed value=x1
Expected value=x2
Difference = (x1–x2)

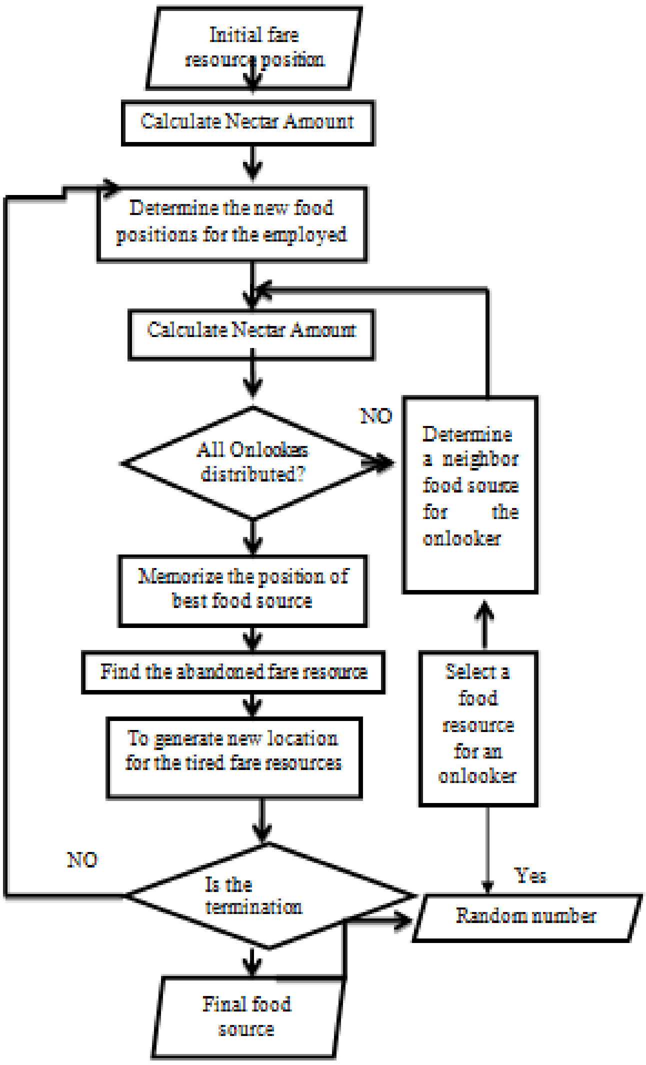
## ABC GENERATE RANDOM KEY

The Schema of the artificial bee colony algorithm is given. Introduction the working bees onto the fare resources and scheming their nectar amounts inserting the viewer bees onto the fare resources and scheming the nectar amounts and formative the survey bees and placing them onto the arbitrarily strong-minded fare resources. In the ABC, a fare resource location represents a feasible resolution to the quandary to be optimized. A set of fare resource positions are arbitrarily shaped and the ethics of the algorithm organize the attributes are assigned.

If the novel nectar amount is privileged, then working bee is neglect the preceding quantity and remembers the new one. After the working bees inclusive their hunt, they come up to reverse into the swarm and split their in sequence regarding the nectar amounts of their resources with the viewer coming up on the tap area. All viewers consecutively establish a fare resource is with a likelihood based on their nectar amounts.

The bee colony has lookout their hives to prospect. They no need of hints to looking for fare. In the basics formula, if a resolution scheduled behalf of a fare resource cannot be improved.

A pre strong-minded number of trials, it means that the connected fare resource has been tired by the bees and the working bee of this fare resource becomes a survey. The point of the surplus fare resource is replaced with an arbitrarily shaped fare location. The number of trials for moving a fare deliver is sufficient the worth of "boundary," that is an essential supervision constraint of the fundamentals procedure. These Three steps are frequent in anticipation of the execution criteria are fulfilled.


Initial fare resource position
Calculate Nectar Amount
Determine the new food positions for the employed
Calculate Nectar Amount
All Onlookers distributed?
NO
Determine a neighbor food sourse for the onlooker
Memorize the position of best food source
Find the abandoned fare resource
Select a food resource for an onlooker
To generate new location for the tired fare resources
NO
Is the termination
Yes
Random number
Final food source

Flow Chart: Random Number Generation using ABC

## RESULT AND DISCUSSIONS

The proposed work's implementation established to show how the ABC algorithm urbanized is an appropriate contest for production of keys of elevated robustness for value. Rigorous testing was carried for keys generated intended to be performing standard statistical test.

The work has been implemented in JAVA platform and Run test and Serial test were accepted on the key bring out each repetition of the algorithm to make sure and generate arbitrary key.

### Serial Test

This test also known as scattering test. It was performed on samples of key generated.

Table I depicts the experiential values of the occurrences of consecutive 00,01,10,11, are initiate to be very close within the region of zero error percentage thus showing that the uninterrupted bits in keys are self-determining of each other.

### Run Test

The arbitrariness of key stream tested by run test. The designed run test value z was found a lesser amount of critical value of 1.96 as shown in table II. Therefore outcome overtake run test and it show the pure arbitrary allocation of at random generated key stream.

Table 1: Serial Test

| Total<br>No. of runs | Z = $(a - \mu a) / \sigma a$ |
|---|---|
| 16 | 0.29712133937748897 |
| 18 | 0.4907010389149647 |
| 16 | 0.356599506682666 |
| 19 | 0.6517520100116609 |
| 10 | 0.23620778599939485 |
| **Upper limit Z** | 0.6654559640190049 |
| **Z Vital (for alpha)** | **0.06** |
| **Z (critical)** | **1.95** |

Table 2: Run Test

| | **Observed (x1)** | **Expected (x2)=13/4** | **Difference=(X1-X2)** |
|---|---|---|---|
| **n00** | **1** | **3** | **-2** |
| **n01** | **4** | **3** | **1** |
| **n10** | **4** | **3** | **1** |
| **n11** | **4** | **3** | **1** |
| **Sum of Difference (D_SUM)** | | | **-1** |
| **Error Serial = abs (D_SUM)** | | | **1** |

## CONCLUSION

Artificial Bee Colony Algorithm (ABC) algorithm was residential based on fare resources of bees that performance of honey bees for solving optimization unconstrained and constrained harms. ABC is nature-inspired met heuristic that imitates the search behavior of bees.

ABC as a random technique is simple to implement, has fewer management parameters, and will simply be modify and hybridized with alternative meta heuristic algorithms.

ABC was proved to be favorable in assortment of the finest potential key from the amplification sphere of influence. The arithmetical tests results were accepted proving the success and efficiency of the united use ABC than other methods used for finding global optimum. Arbitrary Keys successfully passed Run and serial tests.

## 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.