IOSR Journal of Computer Engineering (IOSRJCE)
ISSN: 2278-0661 Volume 1, Issue 5 (May-June 2012), PP 06-08
www.iosrjournals.org

Cryptography Using Genetic Algorithms (GAs)

Sonia Goyat
Student, M.Tech, Department of Computer Science and applications, Maharishi Dayanand University (MDU), Rohtak, India.

ABSTRACT: *Cryptography is essential for protecting information as the importance of security is increasing day by day with the advent of online transaction processing and e commerce. Public key cryptography is one of the most important types of cryptography. In public key cryptography the key has to be unique. There are two ways of key production, the first one is mathematical like AES, DES and the other one is based on the theory of natural selection. The work explores the different techniques of cryptography in order to prove that the natural selection based techniques are as good as the rigorous mathematical techniques. 12 papers and theses have been studied in order to reach the conclusion.*

Keywords: *Cryptography, Genetic Algorithms, Natural Selection, Public Key Cryptography, Vernam Ciphers*

I. INTRODUCTION

The mathematical or conventional methods like AES are extensively used as the key length is as large as 256 bits thus making the number of possible keys equal to 2^{256}. The complexity of the method is too high so the advantage wanes. The methods explored in the work use heuristic search algorithms like Genetic Algorithms (GAs) which are known to be robust. A new method has been proposed. The key produced by the method is shown to be non-repeating and thus making the cipher unbreakable as is already established. The paper relies on the randomness of GAs and their ability to make the population converge towards the desired point using a fitness function and combines it with the concept of feedback similar to that of neural networks .The technique has been implemented and the randomness of the population generated was calculated. The experiments carried out established the ability of GAs to produce a good random sample. If the key of the Vernam Cipher is selected from that sample then it is found to be better as compared to PRNG.

II. GENETIC ALGORITHMS

The Genetic Algorithms (GAs) are exploration algorithms based on the theory of natural selection with an inventive finesse of nature. The central idea of research on GAs has been robustness [6]. This class not only takes into accounts the efficiency but also efficiency [8]. The implications of robustness are the removal of costly resigns and higher level of variation.

The depiction of a natural population is done using, what is called chromosomes which are nothing but a set of numbers, generally binary [6]. Each number represents a cell and can be perceived as an affirmative or negative answer. For example, a chromosome 10110 if applied to knapsack problem can be assumed as selecting the first, third and fourth item from amongst a set of five items, as we have 1 at the first, third and fourth position. The initial population can be generated using any Pseudo Random Number Generator. Each chromosome is then assigned a fitness value [6], [9]. Based on this fitness value replication is done. Now generate a random number % 100. Let it be 63. Now Cumulative Frequency 63 lies in Chromosome some chromosome say x. Therefore, Chromosome x is replicated.

The above population is enhanced by using basic operations like crossover and mutation.

1.1 Crossover

Crossover operator has the significance as that of crossover in natural genetic process. In this operation two chromosomes are taken and a new is generated by taking some attributes of first chromosome and the rest from second chromosome. In GAs a crossover can be of following types [9], [10], [11]

1.1.1 Single Point Crossover: In this crossover, a random number is selected from 1 to n as the crossover point, where n being the number of chromosome. Any two chromosomes are taken and operator is applied.

1.1.2 Two Point Crossover: In this type of crossover, two crossover points are selected and the crossover operator is applied.

1.1.3 Uniform Crossover: In this type, bits are copied from both chromosomes uniformly.

1.2 Mutation

Mutation is a genetic operator used to maintain genetic diversity from one generation of population to the next. It is similar to biological mutation [9]. Mutation allows the algorithm to avoid local minima by preventing the population chromosomes from becoming too similar to each other [10]. GAs involves string-based modifications to the elements of a candidate solution. These include bit-reversal in bit-string GAs [6].

1.3 Selection

It is quantitative criterion based on fitness value to choose which chromosomes from population will go to reproduce. Intuitively the chromosome with more fitness value will be considered better and in order to implement proportionate random choice, Roulette wheel selection is used for selection [9], [11].

GAs are different from the other search processes owing to the fact that they work on coding of the parameter set and not on the parameters [12]. It is also general belief that GAs use payoff and not auxiliary knowledge. Moreover, determinism is not needed in GAs.

The initial population for GAs is generated by applying the following procedure [9], [10], [11].

Initial population is stored in a 2D array, let it be called init_pop[][].

```
for i = 0 to n
begin
    for j = 0 to m
    begin
        Generate a random number x modulo 100
        if(x <= 50) then init_pop[i][j] = 0
        else init_pop[i][j] = 1
    end
end
```

III. CRYPTOGRAPHY

Key generation in cryptography has been dealt with in many papers but the use of GA in the process has not as yet been explored. It is the most important part of encoding the data .A non repeating key guarantees better results and generates a code that is theoretically impossible to break .Some of the classical techniques used for generating unique keys are OTP and Pseudo random number generators. The work tries to explore use of non-conventional techniques in the process.

3.1 Vernam Ciphers:

In this process, the plaintext is converted into cipher text by XORing the binary plaintext with a binary key. The Cipher Text is transferred via a channel and when the receiver receives the cipher text and XORs it with the same key thus getting the plaintext again [2]. It has been proved that if the key, that is One Time Pad, is unique then the cipher text cannot be broken. m1 m2…..mt is operated on by a binary key string k1k2….kt of the same length to produce a cipher text string c1c2…..ct using Equation 1

$$ci = mi \oplus ki \, , \; 1 \leq i \leq t \qquad (1)$$

(Menezes,A.; van Oorschot ,P.(1997)). If the key string is randomly chosen and never used again, this cipher is called a one-time system or one-time pad.

GAs are adaptive heuristic search algorithms which are based on the Charles Darwin theory of survival of the fittest. The main idea behind these algorithms was to replicate the randomness of the nature. This required that the algorithm proposed should behave like a natural system. GAs emulate the nature to large extent .GAs produce a population in such a way that the trait which is popular ,that is, has higher fitness value is replicated more, as is done by the nature. This is also the fundamental concept behind evolution. So these algorithms are also referred as the evolutionary algorithms.

IV. PROPOSED WORK

The work proposes the use of GA in Cryptography. GAs have been successfully used in cryptography in many of the papers studied. In one of the works [2] around 400 keys were analyzed and no repetition was obtained therefore frequency test was not applied. The coefficient of autocorrelation was calculated for k = 1 to

k = 10. The result for k = 1 was 0.03, thus indicating a good random sample. Karl Pearson Coefficient of correlation has been calculated, also giving satisfactory data.
Randomness was ascertained by computing autocorrelations for data values at varying time lags. If random, such autocorrelations should be near zero for any and all time-lag separations. If non-random, then one or more of the autocorrelations will be significantly non-zero.

The work intends to propose a new technique and check it for its fitness by applying various tests.

V. CONCLUSION AND FUTURE SCOPE

The task is being carried out and simultaneously tested. The tests are being done using the Coefficient of autocorrelation as the principle factor in determining the randomness of the sample. It is a process based on heuristic selection therefore its strength can be evaluated against the current mechanism of producing keys based on Cellular Automata [4], Corpuscular theory [5] and ACO. Random Number Generation via Cellular Automata has been proposed in some paper [4]. The task therefore is to implement those works and compare the above work with a Cellular Random Number Generator. Corpuscular theory is a relatively new one. Its results are being asked for and when available will be compared with the above work.
PRNG is using ACO will be developed in the next phase.

REFERENCES

[1] ABDELSALAM ALMARIMI et al, A NEW APPROACH FOR DATA ENCRYPTION USING GENETIC ALGORITHMS, Published in: · Proceeding CERMA '10 Proceedings of the 2010 IEEE Electronics, Robotics and Automotive Mechanics Conference
[2] Harsh Bhasin, Nakul Arora, Reliability Infocom Technology and Optimization 2010, Conference Proceedings pages 226- 230.
[3] Bethany Delman, Genetic Algorithms in Cryptography, MS Thesis 2004.
[4] Cellular automata computations and secret key cryptography Franciszek Seredynski, Pascal Bouvry, Albert Y. Zomaya Parallel Computing May 2004, Elsiver
[5] Corpuscular Random Number Generator. Harsh Bhasin, IJIEE 2012, Vol.2 (2): 197-199 ISSN: 2010-3719.
[6] Modified Genetic Algorithms Based Solution to. *Subset Sum* Problem. *Harsh Bhasin* computergrad.com. Faridabad, India. Neha Singla, IJARAI Vol1 (1).
[7] Menezes, A., van Oorschot, P., & Vanstone, S. (1997). Handbook of Applied Cryptography Boca Raton: CRC Press
[8] Norman D. Jorstad, CRYPTOGRAPHIC ALGORITHM METRICS, January 1997
[9] H. Bhasin and S. Bhatia, "Application of Genetic Algorithms in Machine learning", IJCSIT, Vol. 2 (5), 2011.
[10] Pisinger D (1999). "Linear Time Algorithms for Knapsack Problems with Bounded Weights". Journal of Algorithms, Volume 33, Number 1, October 1999, pp. 1–14
[11] Harsh Bhasin, "Use of Genetic Algorithms for Finding Roots of. Algebraic Equations", IJCSIT, Vol. 2, Issue 4.
[12] S. Thrun, "Learning to Play the Game of Chess", In G. Tesauro, D. Touretzky, and T. Leen, editors, Advances in Neural Information Processing Systems(NIPS) 7, Cambridge, MA, 1995. MIT Press