Genetic Algorithm for Cryptography: A Review

Ms. Pooja A. Bagane[#1], Dr. Kshama V. Kulhalli [#2]

#1 Assistant Professor, Sharad Institute of Technology College of Engineering, Yadrav, 9922007250 .

#2 Vice Principal & HOD of IT Dept, D.Y.Patil College of Engineering and Technology, Kolhapur, 9764997271 .

ABSTRACT

Cryptography is essential for protecting information as the importance of security is increasing day by day. Cryptology is the science and study of systems of Cryptology is the science and study of systems for secret communications. Genetic Algorithm (GA) is typically used to obtain solution for optimization and search problems. This paper presents application of GA in the field of cryptography. The goal of this paper to present review on genetic algorithm for cryptography with reference to metrics of the problem and evolutionary techniques used to solve the problem. This paper also presents review of genetic algorithms used for cryptography.

Key words: Cryptography, Ciphers, Genetic Algorithms.

Corresponding Author: Ms. Pooja A. Bagane

INTRODUCTION

Genetic algorithms (GA) are adaptive heuristic search algorithms based on the evolutionary ideas of natural selection and genetics which are based on the principle of Darwinian idea of survival of the fittest and natural genetics [1].Cryptanalysis is the process of attempting to recover the plaintext and /or key from a ciphertext. In the Brute Force attack the attacker tries every possible key on a piece of ciphertext until an intelligible translation into plaintext is obtained; it has the disadvantage of high computational complexity. In order to overcome this drawback, the optimization heuristics techniques like Genetic Algorithm (GA) are used [2]. The possibility of using a random type search to break a cipher is explored. The most focus of work is on the use of a GA to conduct a directed random search of a key space and to guess the key size.

The rest of the paper is organized as follows: In section 2 about Cryptography and Cryptanalysis. Section 3 discusses basic idea of Genetic Algorithms. Section 4 gives review of Genetic algorithm for Cryptography with respect to Ciphers attacked, metrics and heuristic techniques used. In Section 5 is review of genetic algorithmic approaches for Cryptography. Finally, in Section 6 we outline the conclusions of our study.

CRYPTOGRAPHY

Cryptography is the art of secret writing. More generally, people think of cryptography as the art of mangling information into apparent unintelligibility in a manner allowing a secret method of unmangling. The basic service provided by cryptography is the ability to send information between participants in a way that prevents others from reading it. It consists of two complementary fields of study: cryptography and cryptanalysis [3].

Traditional use of cryptography: A message in its original form is known as plaintext or cleartext. The mangled information is known as ciphertext. The process for producing ciphertext from plaintext is known as encryption. The reverse of encryption is called decryption.

plaintext
encryption
ciphertext
decryption
plaintext

While cryptographers invent clever secret codes, cryptanalysts attempt to break these codes. These two disciplines constantly try to keep ahead of each other. Ultimately, the success of the cryptographers rests on the Cryptographic systems tends to involve both an algorithm and a secret value. The secret value is known as the key. The reason for having a key in addition to an algorithm is that it is difficult to keep devising new algorithms that will allow reversible scrambling of information, and it is difficult to quickly explain a newly devised algorithm to the person with whom you'd like to start communicating securely. With a good cryptographic scheme it is perfectly OK to have everyone, including the bad guys (and the cryptanalysts) know the algorithm because knowledge of the algorithm without the key does not help.

Typically, the objective of attacking an encryption system is to recover the key in use rather than simply to recover the plaintext of a single ciphertext. Cryptanalytic attacks rely on the nature of algorithm plus perhaps some knowledge of the general characteristics of the plaintext or even some sample plaintext-ciphertext pairs. This type of attack exploits the characteristics of the algorithm to attempt to deduce a specific plaintext or to deduce the key being used.

In Brute-force Attack, the attacker tries every possible key on a piece of ciphertext until an intelligible translation into plaintext is obtained. On average, half of all possible keys must be tried to achieve success.

GENETIC ALGORITHM

Genetic Algorithms (GAs) are randomized yet structured search and optimization algorithms based on the evolutionary ideas of natural selection and genetics [1]. GAs simulates the survival of the fittest among individuals over consecutive generations for solving a problem. Each generation consists of a population of individuals. Each individual represents a point in a search space and a possible solution. The individuals in the population are then made to go through a process of evaluation through three operators. The basic GA procedure has following operation:

1. Initialization.

GAs usually generates the initial population of candidate solutions randomly according to a uniform distribution over all admissible solutions. However, the initial population can sometimes be biased using prior problem-specific knowledge or other optimization procedures.

2. Selection.

Each GA iteration starts by selecting a set of promising solutions from the current population based on the quality of each solution. Selection operator equates the survival of the fittest.

3. Variation.

Once the set of promising solutions has been selected, new candidate solutions are created by applying recombination (crossover) and mutation to the promising solutions.

Crossover operator represents mating between individuals. Mutation introduces random modification. For example, if original streams are 10010011 and 11001110, then crossover result streams are 10011110 and 11000011. If original stream is 10010011, then mutation result is 10000111.

4. Replacement.

After applying crossover and mutation to the set of promising solutions, the population of new candidate solutions replaces the original one or its part, and the next iteration is executed (starting with selection) unless termination criteria are met.

LITERATURE REVIEW

This section gives the details about the Techniques used, metric considered and Ciphers attacked during previous research.

Description of Techniques

Many Evolutionary algorithms have been proposed in past for Cryptography. In this section, we discuss some of the existing Evolutionary algorithms used.

1. Genetic Algorithms

A genetic algorithm is any population based model that uses selection and recombination operators to generate new sample points in a search space. Genetic Algorithms (GAs) are randomized yet structured search and optimization algorithms based on the evolutionary ideas of natural selection and genetics [A1]. GAs simulates the survival of the fittest among individuals over consecutive generations for solving a problem. Each generation consists of a population of individuals. Each individual represents a point in a search space and a possible solution. Most of the researcher presents their work on GA for Cryptography in [2, 4-25]

2. Memetic Algorithm

Memetic algorithms (MA) is now widely used as a synergy of evolutionary or any population-based approach with separate individual learning or local improvement procedures for problem search also as Baldwinian evolutionary algorithms (EA), Lamarckian EAs, cultural algorithms, or genetic local search. In the context of complex optimization, many different instantiations of memetic algorithms have been reported across a wide range of application domains, in general, converging to high-quality solutions more efficiently than their conventional evolutionary counterparts. In [10], uses Memetic Algorithm as evolutionary algorithm.

3. Brute Force search algorithm

Brute force is a straightforward approach to solve a problem based on the problem's statement and definitions of the concepts involved. It is considered as one of the easiest approach to apply and is useful for solving small–size instances of a problem. In [11], researcher compared Brute Force Search Algorithm with Genetic Algorithm for Cryptography.

4. Tabu Search

Tabu search approach is one of the popular local search techniques based on neighborhood search algorithm. Fread Glover proposed tabu search in 1986. Tabu search can be directly applied to virtually any kind of optimization problem. Most of the problems are in the following form, where optimize means minimize or maximize [26].

$$\textit{Optimize } f(x)$$
$$\textit{Subject to } x \,\varepsilon\, X$$

The function f (x) may be linear, non-linear and even stochastic and the set X summarizes constraint on the vector of decision variable x. In [22, 23], uses Tabu Search for Cryptography.

Description of Ciphers

Most of the ciphers attacked are considered to be classical. In this section, we discuss some of the existing ciphers attacked in various environments as shown in table 1.

Ciphers attacked include:

- Monoalphabetic Substitution cipher:

This Cipher includes mapping the plaintext alphabet onto cipher text characters.

- Polyalphabetic Substitution cipher:

The simplest case consists of using different alphabets sequentially and repeatedly, so that the position of each plaintext character determines which mapping is applied to it. Under different alphabets, the same plaintext character is encrypted to different cipher text characters, making frequency analysis harder.

- Permutation cipher/Transposition cipher:

The permutation cipher is applied to blocks of characters while the columnar transposition cipher is applied to the entire text at once.

- Vernam cipher:

The Vernam cipher is a stream cipher defined on the alphabet A = {0, 1}. A binary message $m_1m_2 . . .m_t$ is operated on by a binary key string $k_1k_2 . . . k_t$ of the same length to produce a cipher text string $c_1c_2 . . . c_t$ where $c_i = m_i\ XOR\ k_i, 1 < = i < = t$ [4]. If the key string is randomly chosen and never used again, this cipher is called a one-time system or one-time pad.

Table1. Review of Ciphers Attacked

Ciphers	Monoalphabetic Substitution cipher	Polyalphabetic Substitution cipher	Permutation cipher	Transposition cipher	Vernam cipher
Reference No.	4,9,18,19,22	4,5,9,18,19	4,7,10,11,12,13,14,15, 17,20,21,23,24,25	4,6	2,4,16

Review of Metrics

In past different metrics are considered by researchers for Genetic Algorithm in Cryptography are summarized in table 2.

Table2. Metrics of Genetic Algorithm for Cryptography

Metrics	Time	Frequency Test	Gap Test	Key Size	Storage Space	Efficiency
Reference No.	4,6,8,10,13, 16,17,20,22	2,5,14,15	2,14,15	6,7,17	9	10,23
Metrics	Accuracy	Security	Feasibility	Throughput Rate	Confidentiality	
Reference No.	10	14,18,19,20, 25	21,25	21	24	

GENETIC ALGORITHM FOR CRYPTOGRAPHY- REVIEW

Genetic algorithm is proven to be one of the effective techniques for Cryptography. This section gives the details about the type of genetic algorithm, operators and chromosome representation used for cryptography summarized in table III to VII.

The four important types of genetic algorithms are simple genetic algorithm, steady-state genetic algorithm, incremental genetic algorithm, deme genetic algorithm [1]. In most of the paper that we have studied for Evolutionary Algorithms for Cryptography, simple genetic algorithm is used.

The number of possible representations is endless. Defining an appropriate representation is part of the art of using genetic algorithms (and at this point, it is still an art, not a science). Use a representation that is minimal but completely expressive [1]. There are different types of chromosome representation such as One Dimensional, Two Dimensional. One Dimensional chromosome representations used for Cryptography in most of the research.

Proper choice of selection, crossover and mutation operators plays very important role in performance of genetic algorithm. Roulette Wheel Selection Operator used mostly by researchers for Cryptography. Table 3 and 4 shows that standard crossover and mutation operators are working well for Cryptography as many researchers have used them.

Table3. Crossover Operator

Crossover Operator	One Point Crossover	Two Point Crossover	Uniform Crossover
Reference No.	3,6,9,12,13,14,15,18,23	15,17	5,7,15,16

Table4. Mutation Operator

Mutation Operator	Swapping	Reordering	Replacing	Bit Inversion	Reassignment
Reference No.	16	3	-	5,7,9,13,15,17,18,21	2,4,16

By observing table III and IV, we can say that most of the research used Single Point Crossover and Bit Inversion (Bit Flip) Mutation for better results.

This paper summarizes types of Cipher attacked and Metric considered in literature. Majority of the researchers are focused on Time and Security. For problems, like Cryptography, very few algorithms are able to generate the optimal solution. Even though problem can be solved by using exhaustive search, the time taken for generating the solution is very high. In this paper we have reviewed some of the evolutionary algorithm used to solve the problem. In future there is more scope for problem specific operators and hybridization.

CONCLUSION

This paper summarizes types of Cipher attacked and Metric considered in literature. Majority of the researchers are focused on Time and Security. For problems, like Cryptography, very few algorithms are able to generate the optimal solution. Even though problem can be solved by using exhaustive search, the time taken for generating the solution is very high. In this paper we have reviewed some of the evolutionary algorithm used to solve the problem. In future there is more scope for problem specific operators and hybridization.

REFERENCE

[1] Goldberg, D. E., Genetic Algorithms in Search, Optimization, and Machine Learning, Addison-Wesley, 1989.

[2] Farhat Ullah Khan, Surbhi Bhatia, A NOVEL APPROACH TO GENETIC ALGORITHM BASED CRYPTOGRAPHY, International Journal of Research in Computer Science, ISSN 2249-8265 Volume 2 Issue 3 pp. 7-10, 2012.

[3] Williams Stallings, Cryptography and Network security Principles and Practices, Pearson Education.

[4] Bethany Delman, Genetic Algorithms in Cryptography, Master's Thesis, July 2004.

[5] Ragheb Toemeh and Subbanagounder Arumugam, Applying Genetic Algorithms for Searching Key-Space of Polyalphabetic Substitution Ciphers, The International Arab Journal of Information Technology, Vol. 5, No. 1, January 2008.

[6] R. Toemeh, S. Arumugam, Breaking Transposition Cipher with Genetic Algorithm, ISSN 1392 – 1215, No. 7(79), 2007.

[7] Dr. Poornima G. Naik, Girish R. Naik, Asymmetric Key Encryption using Genetic Algorithm, International Journal of Latest Trends in Engineering and Technology (IJLTET), Vol. 3 Issue 3 January 2014.

[8] Dr. Dilbag Singh, Pooja Rani, Dr. Rajesh Kumar, To Design a Genetic Algorithm for Cryptography to Enhance the Security, International Journal of Innovations in Engineering and Technology (IJIET), Vol 2 Issue 2, April 2013.

[9] Nalini N., Dr. G. Raghavendra, A New Encryption and Decryption Algorithm combining the features of Genetic Algorithm (GA) and Cryptography, 2000.

[10] Poonam Garg, A Comparison between Memetic algorithm and Genetic algorithm for the cryptanalysis of Simplified Data Encryption Standard algorithm, International Journal of Network Security & Its Applications (IJNSA), Vol.1, No 1, April 2009.

[11] Lavkush Sharma, Bhupendra Kumar Pathak & Ramgopal Sharma, Breaking of Simplified Data Encryption Standard Using Genetic Algorithm, Global Journal of Computer Science and Technology, Volume 12 Issue 5, March 2012.

[12] Nicole Bilić, Solving Cryptographic Primitives Optimization Problem Using Evolutionary Computation Algorithms, Thesis, Zagreb, June 2014

[13] Sonia Goyat, Cryptography Using Genetic Algorithms (GAs), IOSR Journal of Computer Engineering (IOSRJCE) ISSN: 2278-0661 Volume 1, Issue 5, PP 06-08, May-June 2012.

[14] Swati Mishra, Siddharth Bali, Public Key Cryptography Using Genetic Algorithm, International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-2, Issue-2, May 2013.

[15] Sonia Goyat, Genetic Key Generation for Public Key Cryptography, International Journal of Soft Computing and Engineering (IJSCE), ISSN: 2231-2307, Volume-2, Issue-3, July 2012.

[16] Girish Patel, Genetic Algorithm for Cryptanalysis, Seminar report, 2008.

[17] Suvajit Dutta, Tanumay Das, Sharad Jash, Debasish Patra, Dr.Pranam Paul, A Cryptography Algorithm Using the Operations of Genetic Algorithm & Pseudo Random Sequence Generating Functions, International Journal of Advances in Computer Science and Technology, Volume 3, No.5, May 2014.

[18] ALI JASSIM MOHAMED ALI, Randomly Encryption Using Genetic Algorithm, International Journal of Application or Innovation in Engineering & Management (IJAIEM), Volume 2, Issue 8, August 2013.

[19] Sindhuja K , Pramela Devi S, A Symmetric Key Encryption Technique Using Genetic Algorithm, International Journal of Computer Science and Information Technologies (IJCSIT), Vol. 5 (1), 414-416, 2014.

[20] Vimalathithan.R, Dr.M.L.Valarmathi, “Cryptanalysis of S-DES using Genetic Algorithm”, International Journal of Recent Trends in Engineering, Vol 2, No. 4, November 2009.

[21] Anil Kumar, M. K. Ghose, “Information Security using Genetic Algorithm and Chaos”, 2007.

[22] A. K. Verma, Mayank Dave and R. C. Joshi, Genetic Algorithm and Tabu Search Attack on the Mono-Alphabetic Substitution Cipher in Adhoc Networks, Journal of Computer Science 3 (3): pp. 134-137, 2007.

[23] S. Picek, M. Golub, On Evolutionary Computation Methods in Cryptography, 2011.

[24] Jia-Shiang Chen, Yu-Bin Chen, Pei-feng Hsu, Nghia Nguyen-Huu, and Yu-Lung Lo, Cryptographic scheme using genetic algorithm and optical responses of periodic structures, OPTICS EXPRESS, Vol. 19, No. 9, April 2011.

[25] Gove Nitinkumar Rajendra, Bedi Rajneesh kaur, A New Approach for Data Encryption Using Genetic Algorithms and Brain Mu Waves, International Journal Of Scientific And Engineering Research Volume 2, Issue 5, May-2011.

[26] Glover, F., Laguna, M. and Mart, R., Handbook of Approximation Algorithms and Metaheuristics, Taylor & Francis Group (2007).