ISSN: 0974-6471, Vol. 10, No. (3) 2017, Pg. 580-584

Oriental Journal of Computer Science and Technology

Journal Website: www.computerscijournal.org

Linear Cryptanalysis of Substitution Ciphers Using Particle Swarm Optimization

Dr. G. RAJKUMAR

Assistant Professor Department of Computer Applications, N.M.S.S. Vellaichamy Nadar College, Madurai, Tamilnadu, India.

Abstract

Cryptanalysis is a standout amongst the most vital requesting zones of capable research in the request of the security. An approach of data security is Cryptography. Cryptanalysis is the investigation to break cryptography without the encryption key. Cryptanalysis is breaking or separating cipher text content into its identical plain-content without past data of the secret key or without knowing the real approach to unscramble the cipher text content. Particle Swarm Optimization (PSO) is a population based, self-versatile find improvement of optimization performance motivated by group performance of bird flocking or fish schooling. In this paper discussed with use of PSO in automated cryptanalysis of simple substitution ciphers. In this manner, encrypted data can be sent by any individual utilizing the general public key, yet the data can be decoded just by the holder of the secret key.

Article History

Received:19 September 2017
Accepted: 30 September 2017

Keywords

Cryptanalysis,
Particle Swarm Optimization,
Plain text,
Cipher Text.

Introduction

In cryptology procedure for ensuring the secrecy and authenticity of information are studied. Traditional symmetric and asymmetric methods are not suitable when the needed level of security is high. The two main branches of cryptology are cryptography and cryptanalysis. In cryptography, designs of such techniques are studied but for cryptanalysis, the defeating of such techniques is studied to pick up information or forging information that will be accepted as dependable. In cryptography, encryption is the process of renovating information referred to as plaintext. The outcome of the procedure is information which is, referred to as cipher text. The receptive data that is deposited and transmitted on the internet must protection from attackers. Cryptography algorithms are the key aspect of the security mechanisms used for data storage and uninterrupted network transmissions. Particle Swarm Optimization is a method which has a number of populations, motivated by social manners of birds and animals such as bee colonies. Population

CONTACT Dr. G. RAJKUMAR mdugrk@gmail.com Assistant Professor Department of Computer Applications, N.M.S.S. Vellaichamy Nadar College, Madurai, Tamilnadu, India.

To link to this article: http://dx.doi.org/10.13005/ojcst/10.03.04

consists of individual particles which jointly in a multidimensional travel around space for verdict the best explanation known as the global optimum.

Previous Works

In recent years, various investigations have been refined for cryptanalysis. This Section presents different research services finish in the field of cryptanalysis and Particle Swarm Optimization. Cryptanalysis, from the Greek kryptós, "covered up", and analýein, "to slacken", is the workmanship and study of breaking, i.e., interpreting cipher text content into its identical plaintext, selective of earlier information of the secret key.

Carrol and Martin[5] built up a specialist framework push toward to determine simple substitution ciphers utilizing handcoded heuristics. Mohamed Faisal and Youssef[6] manage research the utilization of PSO in modernized cryptanalysis of plain substitution cipher. Forsyth and Safavi-Naini[10] recast the issue as a combinatorial enhancement issue and displayed an assault on inconvenience free substitution cipher utilizing simulated annealing algorithm. Anjali and Surendra Kumar yadav[2] examine with a concise prologue to cryptography and fluffy developmental calculation systems.

Nalini and Raghavendra Rao[7] builds up the materialness of a consolidate of streamlining heuristics to cryptanalysis examines; one upheld on thermo factual persistency connected to mimicked tempering and the extra one in light of Particle swarm guideline. Spillman *et. al.,*[8] offered an assault on basic changeover cipher utilizing genetic algorithm. Jakobsen[9] started a fast calculation for the cryptanalysis of basic substitution figures in view of a technique where a preparatory key figure is refined amid various cycles.

Particle Swarm Optimization

Particle Swarm Optimization (PSO) is a computational system that streamlines a trouble by iteratively requesting to build up a hopeful arrangement with considers to given quantify of value. Swarm Intelligent is a kind of Artificial Intelligence in view of the conduct of animals living in gatherings and having some fitness to interrelate with another and with the environment in which they are incorporated. Each particle in the swarm performs in a circulated way by methods for the insight of its own and the gathering knowledge. PSO consolidates swarming practices exploratory in groups of feathered creatures, schools of fish, or swarms of honey bees and even human social conduct, from which the thought is appeared. Particle Swarm Optimization method depends on the examination of flying creature and fish rush development of practices while hunting down nourishment, the flying creature or either scattered or go together before they find where they can discover the nutrition. While the birds are scanning for nourishments starting with one place then onto the next place there is dependably a flying creature that can notice the sustenance exceptionally well and having the better sustenance benefit information's. They are transmitting the data exceptionally the great data whenever while looking through the sustenance starting with one place then onto the next place.

Every Particle keeps pathway of its directions in the issue space which are related with the most outstanding arrangement it has finished up until this point. This assessment is known as the pbest. Another "best" assessment that is trailed by the particle swarm optimization agent is the best assessment, got so far by any particles in the neighbors of the molecule. This area is known as the lbest. At the point when a particle takes all the population as its topological neighbors, the best assessment is a worldwide best and is known as the gbest. The Particle swarm optimization idea comprises of, at each time step, shifting the speed of every particle toward its pbest and lbest areas.

Speeding up is weighted by an irregular period, with independent arbitrary numbers being shaped for quickening in the course of pbest and lbest areas. At the point when a particle gets branch of the population as its topological neighbors, the best assessment is a nearby best and additionally is called lbest.

After finding the two finest assessment each molecule modernized its speed ($V_{i,j}$) and position ($P_{i,j}$) towards its pbest and gbest positions,

Particle velocity update

$$(V_{i,j})=C_oV_{i,j}+c_1r_1\ (Ppbest_{i,j} - P_{i,j}) + c_2r_2(Pgbest_{i,j} - P_{i,j})$$

Particle Position Update

$$P_{i,j} = P_{i,j} + v_{i,j}$$

Where, $Ppbest_{i,j}$ and $Pgbest_{i,j}$ are the particle best and worldwide best position of the particles individually.

Proposed Work

Cryptography is the investigation and applies of encryption, the covering up of data. The resource of the word is gotten from the Greek words krypto and grafo, which mean covered up and to compose, correspondingly. At show, the word cryptography holds a double implying that to investigation of mathematics and computer science.

Plaintext is Original information, which is meaningful either by a person or by a PC. Though the cipher text content, which is disjointed, without the proper cipher to decode it. The method of encoding the plaintext into cipher text content is called Encryption and switch the way toward translating cipher text content to plaintext is called Decryption. The cryptanalysis is the entirety of a considerable measure of exceptionally propelled systems with a specific end goal to discover these keys.

A basic substitution cipher is a procedure of disguise that replaces each letter of a plaintext message with another letter. Here is the way to a basic substitution cipher:

The key provides the connection between a plaintext letter and its replacement cipher text letter. Using

Plain Text	A	B	C	D	E	F	G	H	I	J	K	L	M
Cipher Text	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

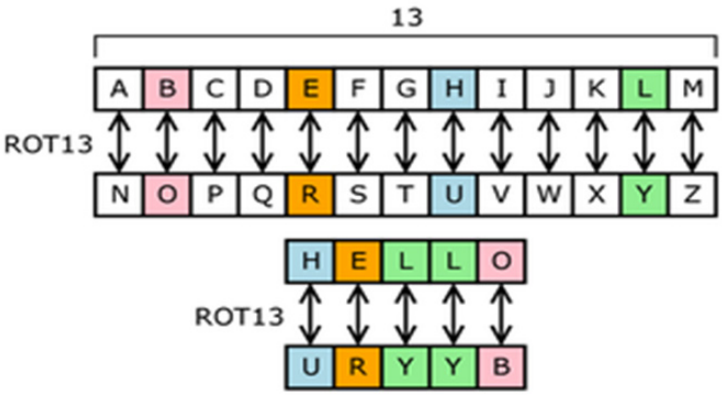

Fig. 1: Example of a Simple Substitution Cipher

this key, each plaintext letter 'A' would be substitute by cipher text 'N', letter 'B' would be substitute by cipher text 'O', letter 'L' by 'Y', etc. The above key was generated by randomly.

The swarm particles are joined with speed and also their area alongside by utilizing the cost reason and distinctive calculations the exceptional arrangement is registered in an exact time and phase. The proposed work discovers, PSO is a population based investigation calculation that connected more than a populace of people and bits of secret key enter utilized as a part of the Advanced Encryption Standard Algorithm to some level. As mentioned in the past returns a locale of the capacity space with most ideal arrangement. The population is known as the swarm and the individual substances are named as particles. The Proposed Work is executed in MATLAB. MATLAB gives the Particle Swarm Optimization tool which is utilized for the Optimization reason. The Particle Swarm Optimization method is connected on the AES (Advanced Encryption Standard).

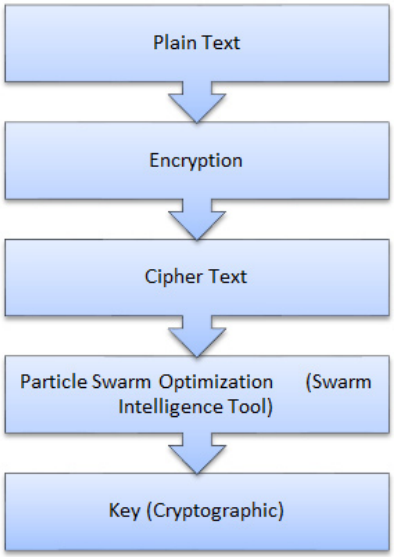

Fig. 2: Proposed Work

Conclusion

Particle Swarm Optimization presents an exceptionally predominant instrument intended for the cryptanalysis of plain substitution ciphers by assets of a cipher simply attack. Particle Swarm Intelligence upheld Cryptanalysis gives a finest and the upgraded clarification. A narrative approach has been utilized for Linear Cryptanalysis of Advanced Encryption Standards (AES) Algorithm utilizing Particle Swarm Optimization. PSO is all around coordinated for assaulting the ciphers. The fitness function work utilized as a part of this system guarantees the efficient arrangement. Improving the Particle Swarm Optimization by vary the parameters and its esteems to yield better outcome for the Linear Cryptanalysis of AES.

References

1 A. Ruba, Dr. G. Rajkumar and Dr. K. Parimala, "Biometrics based cryptographic key generation using Finger print", International *Journal of Computer Engineering and Research Trends*, Volume **4**, Issue 6, pp. 259 – 262, June 2017.

2 Anjali and Surendra Kumar Yadav, "Swarm Intelligence and Evolutionary computation based cryptography and cryptanalysis of 4-round DES algorithm", International *Journal of Advanced Research in Computer Engineering and Technology*, Volume **3**, Issue 5, May 2014.

3 Dr. G. Rajkumar, Dr. K. Parimala and A. Ruba, "An Innovative approach to Genetic Algorithm based Cryptography", *International Journal of Computer Science"*, Volume **5**, Issue 1, No 9,2017, pp. 1199 – 1202.

4 G.Rajkumar, "Evaluating Software Estimation Methods Using Particle Swarm Optimization", International Conference on Social Media for Service Sector at Fatima College, Madurai. ISBN NO.: 978–1–63315-205–2.

5 J. Carrol and S. Martin, "The automated cryptanalysis of substitution ciphers," *Cryptologia*, vol.**10**(4), pp.193–209, 1986.

6 Mohammad Faisal and M. Youssef, "Cryptanalysis of simple substitution ciphers using particle swarm optimization", IEEE Congress on Evolutionary computation, July 16 – 21, 2006.

7 Nalini and Raghavendra Rao, "Cryptanalysis of block ciphers via improvised Particle Swarm Optimization and Extended Simulated Annealing Techniques", *International Journal of Network Security*, Vol. **6**, No. 3, pp. 342 – 353, May 2008.

8 R. Spillman, M. Janssen, B. Nelson and M.

Kepner, "Use of a genetic algorithm in the cryptanalysis of simple substitution ciphers," *Cryptologia*, vol.**17**(1), pp.31–44, 1993.

9 Thomas Jakobsen, "A fast method for cryptanalysis of substitution ciphers," *The Cryptologia Journal*, pp. 265-274, July 1995.

10 W. S. Forsyth and R. Safavi-Naini, "Automated cryptanalysis of substitution ciphers," *Cryptologia*, vol.**17**(4), pp.407–418, 1993.

11 Dr. Salim Ali Abbas and et al., "Cryptanalysis of Stream cipher cryptosystem based on soft computing techniques", *IOSR Journal of Computer engineering*, Vol **19**, Issue 1, pp. 78 – 84.

12 Morteza and Mahdieh, "Automated Cryptanalysis of Transposition ciphers using Cuckoo Search Algorithm", *International journal of Computer Science and Mobile Computing"*, Volume **4**, issue 1, January 2014, pg: 140 – 149.