International Journal of
Emerging Research in Management &Technology
ISSN: 2278-9359 (Volume-5, Issue-5)

Research Article | **May 2016**

Cryptanalysis of Knapsack Cipher: A Survey

Moein Asgharnejad Tehran, Shabina Ghafir
Faculty of Engineering and Technology, Jamia Hamdard University,
New Delhi, India

Abstract—

The transformation of cipher text to plaintext is knows as cryptanalysis. The topic is the one of the most researched ones since 1932. As the problem is NP Hard, soft computing techniques provide a permanent means to reach an almost a great solution in limited time. It was shown that the knapsack based cryptosystem is highly insecure. The work paves way for the use of Knapsack Cipher in the witching field of cryptanalysis. As per the paper, the results are more efficient and convenient than Genetic Algorithms (GA).

Keywords— Knapsack, Cryptography, Cryptanalysis, Knapsack Cipher, Genetic Algorithm.

I. INTRODUCTION

Cryptography and Cryptanalysis have always enchanted the computing fraternity. In Cryptography, we convert the original information which is known as the plaintext, into the encrypted data, the cipher text. Encryption converts plaintext into cipher text, and decryption converts cipher text back to the plaintext [1]. On the other hand cryptanalysis is method of retrieving a plaintext from a cipher text [2]. The work reviews the available techniques of cryptanalysis of knapsack cipher. Knapsack cipher is deep-seated on Knapsack problem which is an NP complete problem. This spellbinding algorithm is worth exploring, owing to its uses in public key cryptography. A specified set of values m_1 up to m_n and a sum S. It is favourable to find the coefficient C_o up to C_i such that,

$$S=C_om_o+C_1m_1+\ldots\ldots+C_nm_n \text{ [3]} \qquad (1)$$

The values C_i can be 0 or 1 containing that the elements are selected in an outcome sets or not. In the cryptosystem the plaintext is equivalent to the number of items in a pile and cipher text would be a resultant sum.

An extensive literature review has been carried in order to determine various types of ciphers and to legitimatize the use of soft computing techniques for cryptanalysis. Primarily, the study actuate the three most prominent cryptosystem namely Merkle-Hellman, Diffie-Helman, Cryptosystem and Shamir's.

In 1976, Whitefield Diffie and Martin Hellman proposed the first public key exchange system over an insecure channel exploiting symmetric which is known as Diffie-Hellman Key Exchange [4]. In 1977, Rivest, Shamir and Adleman discovered a public key cryptosystem exploiting asymmetric algorithm [5]. Later in 1978, Merkle and Martin Hellman proposed a public key cryptosystem firmly-fixed on a Knapsack and Subset sum problem which in turn is NP complete [6].

The review paper has been organized as follows: Section 2 present background. Section 3 presents the literature review and Section 4 concludes. As stated earlier, the work analysis different techniques used in cryptanalysis of knapsack cipher.

II. BACKGROUND

Knapsack problem is one of the most significant problems in computer science. The problem finds its applications in various fields. In knapsack problem, vector `C' is to be determined, given vector `W' and sum `S' so that the equation is:

$$\sum C_i W_i = S \qquad (2)$$

It is a NP-complete problem since the solution is very difficult to find and once the solution is found, it is easy to verify. The density of knapsack problem is specified as under:

$$D=\frac{n}{\log_2 A}, \text{ where `A' is the maximum amongst } C_{i's} \text{ [7]} \qquad (3)$$

Merkle and Hellman proposed one of the most important analysis of knapsacks. In hatred of its being NP-complete, it can be broken by the technique proposed by Shamir [6]. It is interesting to note that there are plenty versions of knapsack problem, almost all of them were broken except one [8]. There are many attacks which are relying on low density of knapsack system; therefore it becomes necessary to analyse the minimum density which a given knapsack must have, so that it becomes hard to break it.

Shamir proposed a pioneering work to break knapsack. The attack was on Merkle-Hellman knapsack cryptosystem where in the sender chooses a super-increasing sequence in a way that any number in the sequence is greater than the sum of the number preceding it. We need two positive integer `W' and `P' such that $a_i=b_i W \bmod P$ and then choose one of the permutation of so formed array. Here super increasing sequence would act as the private key and a's would act as the public key. In the original system the value of n was 100. The message can be encrypted by grabbing an element from the message and multiply it with the corresponding elements with a_i, the receiver computes $M=C_iW^{-1} \bmod P$. since the value of `P' is greater than sum of the all b_i's, therefore

$$b_j \leq 2^{ni} \leq 1 \quad (4)$$

The low density attack on knapsack system is relying on the following premise.

If $N \geq \frac{1}{2}\sqrt{n}$, then the system can be broken easily if the density is less than 0.904.

Cryptanalysis of Hwang cryptosystem uses the following method. Here we compute a_i = b.W, and vector that requires to be find out is a subset of given D. The methodology uses the verity that the ability of regression using Neural Networks has already been established.

III. LITERATURE REVIEW

In order to place everything in the correct prospect, an immense literature review has been carried out. The review which has been done is to find out the existing techniques toward the topic and to find the gaps therein.

The papers have been selected in accordingly to the guidelines proposed by Kichenham [9]. The summary of the review are presented in the Table below. The table shows the techniques used in the work and the validation/verification used by the author(s):

Table 1 Literature Review

Ref.no.	Technique Used	Result
[10]	Binary Firefly Algorithm	As per the paper, the results are more effective than Genetic Algorithms (GA).
[11]	Binary Particle Swarm Optimization (PSO)	The paper states that for the sample taken, PSO are able to producing better results than GAs.
[12]	Differential Evolution Optimization	Here results have been compared with GA.
[13]	Mathematical computation	In this paper, the cryptosystem has been cracked using mathematic algorithms.
[14]	Two different congestion optimization techniques for cryptanalysis have been used.	As per the paper the samples taken for the verification and validation are adequate to prove the robustness of the proposed system.
[15]	A comprehensive review and history of knapsack-based cryptosystems and their possible cryptanalysis attacks.	The work primarily elucidate the following along with the basics. a) Integer programming approaches with focus on the polyhedral studies of convex hull of the integer set. b) Directions in exploiting integer programming in the cryptanalysis of knapsack ciphers.
[16]	This paper extent the knapsack based two-lock cryptosystem.	It has been shown that the knapsack based two-lock cryptosystem is extremely insecure.
[17]	The work shows a large class of diverse problems have a bi composite structure which makes it possible to solve them by using dissection.	The technique is a mixture of dissection and parallel collision search. The results obtained are fascinating.

IV. CONCLUSION

The survey shows the impact of Neural Network and Genetic algorithm in cryptanalysis of knapsack cipher where the security of original text is highly important. The GA algorithms are not stellar comparing to the other techniques used in cryptanalysis of knapsack chipper. It may be mentioned here that the above work is being extended to include different types of the said problem. The next phase of this project would use Diploid Genetic Algorithms (DGA), the review which has been already carried out. DGAs have been applied successfully to some of the NP Hard problems. The current problem could be reduced to a search problem and is hence a rival of the application of DGA.

ACKNOWLEDGMENT

The satisfaction that accompanies the successful completion of any task would be incomplete without the mention of people whose ceaseless cooperation made impossible, whose constant guidance and encouragement crown all efforts with success.

First and foremost we thank Mr. Harsh Bhasin Assistant Professor at Jamia Hamdard University for the guidance, inspiration and constructive suggestions that helped us in the course of this research paper.

Also we would like to use this opportunity to thank our family Mr. Mahmoud Asgharnejad and Mrs Maryam Salehi and my brother Mr. Mobin Tehrani for constant love and support.

REFERENCES

[1] Cormen, T.H.: Foundations of cryptography. *Algorithms unlocked.* London. MIT. 138--144 (2013)
[2] Schneier, B.: Foundations. *Applied Cryptography. Protocols. Algorithm and Source.* USA. Wiley. 16—17 (1996)
[3] Delman, B., I.: Genetic Algorithms in Cryptography. M.S thesis. Department of Computer and science. Rochester Institute of Technology. New York (2004)

[4] Diffie, W., Helman, M., I.: New directions in cryptography. *IEEE. Trans.Inform.Theory*. 644--654 (1976)
[5] Rivest, R.L., Shamir, A., Adleman, L.: A Method for obtaining digital signatures and public key cryptosystems. *Communication of the ACM*. 120--126 (1978)
[6] Merkle, R., Hellman, M.E.: Hiding information and signatures in trapdoor knapsacks. In *IEEE Trans.Inform.Theory*. 525--530 (1978)
[7] Odlyzko, A.M.: The rise and fall of knapsack cryptosystem. *Cryptology and Computational Number Theory*. (1990)
[8] Chor, B., Rivest, R.: A Knapsack-type public-key cryptosystem based on arithmetic. Finite fields. In IEEE Trans.Inform.Theory. 901--909 (1998)
[9] Kitchenham, B., Brerton, O.P., Budgen, D., Tuner, M., Bailey, J., Linkman, S.: Systematic literature reviews. Software engineering. A systematic literature review. *Elsevier*. 5--7 (2008)
[10] Palit, S., Sharma, S.N., Molla, M.A., Khanra, A.: A cryptanalytic attack on the knapsack cryptosystem using a binary firefly algorithm. 2nd *International Conference. Computer and Communication Technology*. Allahabad. 428--432 (2011)
[11] AbdulHalim, M.F., Attea, B.A., Hameed, S.M.: A binary particle swarm optimization for attacking knapsacks cipher algorithm. *International Conference. Computer and Communication Engineering*. Kuala-Lumpur. 77--81 (2008)
[12] Sinha, S.N., Palit, S., Molla, M.A., Khanra, A.: A cryptanalytic attack on knapsack cipher using differential evolution algorithm. Recent Advances in Intelligent Computational Systems. Trivandrum. 317--320 (2011)
[13] Raghuvamshi, A., Rao, P.V.: An effortless cryptanalytic attack on knapsack cipher. *International Conference of .Process Automation. Control and Computing*. Coimbatore. 1--6 (2011)
[14] Jain, A., Chaudhari, N.S.: Cryptanalytic results on knapsack cryptosystem using binary particle swarm optimization. *International Joint Conferences. SOCO'14-CISIS'14-ICEUTE'14*. Bilbao. 375--384 (2014)
[15] Mak-Hau, V.H., Batten, L.M.: The 0-1 knapsack polytype- A starting point for cryptanalysis of knapsack cipher?. *5th International Conference .ATIS*. Melbourne. 171--182 (2014)
[16] Zhang, B., Wu, H., Feng, D., Bao, F.: Cryptanalysis of knapsack based two-lock cryptosystem. *2nd Conference .ACNS*. Yellow mountains. 303--309 (2004)
[17] Dinur, I., Dunkelman, O., Keller, N., Shamir, A.: Efficient dissection of compose problems with applications to cryptanalysis, knapsacks, and combinatorial search problems. *32nd Anal Cryptology Conference*. CA. 375--384 (2012).

