Global Scientific JOURNALS

GSJ: Volume 8, Issue 5, May 2020, Online: ISSN 2320-9186
www.globalscientificjournal.com

Key Generation Using Ant Colony Optimization Technique

1. *Paridhi Baliyan*

Galgotias College of Engineering and Technology
Greater Noida, India
paridhi.ab@gmail.com

2. *Prakhar Chandra*

Galgotias College of Engineering and Technology
Greater Noida, India
pcprakharchandra@gmail.com

3. *Sukriti Srivastava*

Galgotias College of Engineering and Technology
Greater Noida, India
sukriti.1998@rediffmail.com

4. *Dr. Inderpreet Kaur*

Associate Professor
Galgotias College of Engineering and Technology
Greater Noida, India
inderpreet.kaur@galgotiacollege.edu

Abstract*- Crytography is the procedure of fashioning the data to prevent the misusage of the very same. In this modernistic era of the wireless, it is monumental to ensure the secure delivery of the valued data which otherwise be subjected to contemptible intentions. The process of conversion of plaintext to cipher text is known as encryption and its vice-versa is known as decryption. Among the three types of cryptography techniques, viz., Asymmetric key, Symmetric-key and Hash Functions. A significant component of this contemporary technique is the key. This particular element is of utmost importance as this is what is made use of when encrypting or decrypting the coveted data. There are a myriad of techniques to administer encryption and effectuate keys like the RC4, Vernam Cipher, etc. However the approaches have some or the other in commodity. We operate on swarm intelligence where we endeavour to harness the metaheuristic of Ant Colony to generate keys for the encryption of the data. This whole methodology is based on the behaviour of the ants in their natural search of food. The bourne of wielding Ant Colony Optimization is to downscale the number of keys to be employed while encipherment when compared to the other techniques of cryptography in existence. ACO would warrant the generation of such keys that will be of utmost efficiency.

Keywords: Ant-Crypto, Ant Colony Optimization, Symmetric Encryption, Vernam Cipher, RC4 Cipher, Comparison of Optimization Techniques.

I. INTRODUCTION

Internet of this day and age has seen as explosive development due to its augmented usage these days. However the data is susceptible to eavesdropping which might expose the data to distasteful miscreants thereby threatening the privacy and integrity of the sender and the recipient. It is therefore enormously eminent that the date being conveyed from one point to the other is encrypted. There are three categories in which encryption can be subs sectioned. These are vide licit symmetric encryption, asymmetric encryption and hash functions. Here in this particular scenario we exercise the asymmetric type of encipherment particularly the RSA algorithm. The modus operandi of stream cipher each snippet of the plain text is inscribed with a certain bit of the key. Ant colony optimization (ACO) is a meta-heuristic that is inspired by intelligent behaviours of ants. This paper marks an endeavour to asphalt the path for better and effective approach for the formulation of the key stream. The paper is structured in the form of a comparison of the various key generation techniques and then concluding how the ACO approach is the best and most efficient of all. In this subjective survey of stream cipher techniques, Section II propounds the individual techniques which are and were employed for encryption cryptography and how key generation using ant colony optimization is a significant breakthrough. Furthermore, Section III canvasses the technique of ant colony optimization for the process of generation of keys which facilitate the encryption. Lastly Section IV concludes all the points discussed in this survey and then further charts out a route for the future scope of this technique. MANET is a type of network which can configure itself as well as change locations simultaneously. Ant colony optimization technique has a number of merits on which MANETS can successfully be harnessed.

II. COMPARISON BETWEEN DIFFERENT TECHNIQUES USED FOR GENERATING KEYS FOR ENCRYPTION

Following are the different methods of key generation and their comparison with our proposed method using ant colony optimization.

A. Vernam Cipher

Vernam Cipher method was considered by Pfleeber Charles [3] as a cipher which is perfect and a category of one-time pad cipher. The keys in this method are generated by the use a random stream generator. To decipher the image, the receiver requires a similar group of keys. The image is enciphered when long non repeating sequences are integrated with the bits that represent the binary image. The encrypted image is the result of the XOR operation performed on the bits representing the binary image with the conforming stream of arbitrary numerals. The generated keys in the particular approach described are of the same length as the text to ne encoded. This leads to one of the two disadvantages of Vernam Cipher. The drawback is that this particular method of key generation requires an unlimited quantity of keys depending on the plain text length. The array of such a considerable tally of arbitrary keys poses a problem. The second drawback of this otherwise stellar method of key generation is that if the arbitrary numeral progression is cracked then the keys used for encryption can be deciphered very with ease.

However in key generation using ant colony optimization, generation of keys is grounded on the character arrangement in the plain text. Although the keys appear like a stream of random arbitrary numbers, a completely random number generator is neither possible nor is manipulated for the process of key generation. This prevents any third unwanted party to fathom the code. A significantly fewer tally of keys are engendered using a predetermined value and the keys in the keystream. A mutated character code table is used for enciphering the plain text and keys in the keystream. This character code table is an efficacious method capable of producing fully potent keys which can withstand heavy tampering and still not crack.

B. Stream Cipher Cryptosystem

This innovative for encrypting binary images was first proposed by Martin del Ray. In this specific methodology of key generation, a stream cipher cryptosystem is utilized whose cryptographic secure pseudorandom bit generator is a cross breed boolean cellular machine. Moreover, to encrypt only the plain image to be encoded, Huffman coding is used. The disadvantage is that the confidential key of the cryptosystem is formed by 256 cells, which have to be sent to the receiver. The characteristic vector has 256 cells is distributed to the receiver. This in layman term means that the keys can be formed if pseudo random generator if cracked.

In the key generation using ant colony optimization technique, the key generation is based on the of character distribution in the plain text. In comparison a fewer number of keys are used because the keys are procured using the keys already present in the keystream. Moreover the keys are not in any endangerment of being cracked because absolute random number generator is not invoked.

C. RC4 Stream Cipher

RC4 stream Cipher is also called key pooled stream cipher. This method is used for transmission of multimedia files with security in the wireless mobile network. In this, a pseudo random stream of keys is produced by initializing a stable table with 1-256 bytes by swapping the elements in the 256 byte state table. The plain text is XORed with these set of keys to produce the encrypted text. The number of keys to be stored is less in comparison to Vernam Cipher. The drawbacks include that this stream cipher method is susceptible to the state table’s analytic attacks. There is a weak key amongst every 256 keys. These keys can be found by cryptanalysis and it can be discovered if the generated bytes are firmly and securely linked with the bytes of the key.

The technique of key generation using ant colony optimization ensures that the keys are not decrypted. The keys are encrypted using a mutated character code table. This character code table is an efficacious method capable of producing fully potent keys which can withstand heavy tampering and still not crack.

D. Fast and Secure stream Cipher

Proposed by Biham and Seberry, fast and secure stream cipher is both fast and secure. It is based on a primitive methodology called Rolling arrays. This method includes variable rotations and permutations and combinations. One of the very impressive qualities of fast and secure cipher is that it is exceptionally faster than RC4. The disadvantage of this impressive method is that for the initial permutation, an aggregate count of 256 keys have to be collected. The keystream which is generated is not reliant on the plain text to be encrypted. Furthermore the plain text is not enciphered. When we generate keys using ant colony optimization, the key generation is based on the character distribution in the plain text. A significantly fewer tally of keys are generated using a predetermined value and the keys in the keystream.

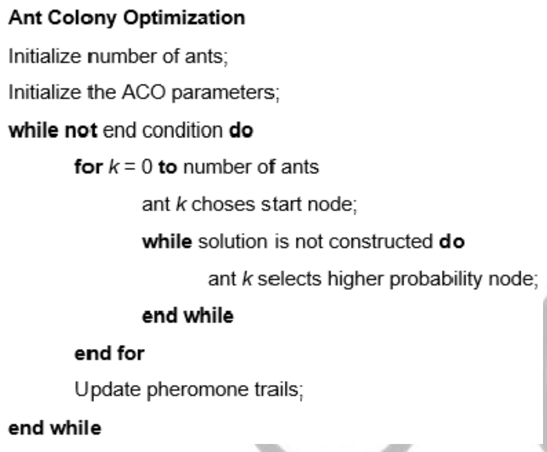
III. Ant Colony Optimization Technique

A. Ant Based Model

After all the disadvantages of different methods of enciphering texts in cryptography, a method that overcomes these disadvantages was needed. In this key generation method [7] we use ant colony-based approach to create and configure the key stream for plain text encryption. The motivation behind utilizing an ACO approach [4] is that a key stream for encryption is chosen on the basis of character circulation in plain text. A changed character code table as portrayed in Vernam Cipher is utilized for encoding of characters in the keystream which is happening in the plain text. As in the case of stream cipher the keys are to be circulated. This methodology decreases the quantity of keys. Consequently it gives a quicker and secure cryptography.

B. Key Generation Using Ant Colony Optimization Method

Ant Colony Optimization for key generation is imaginative calculation proposed to create the keystream with exceptionally made sure about encryption. As the ants in this reality come together so as to get the food in a most ideal manner to such an extent that they need to do less work. Ant agents bunch move towards the food by dropping pheromone. This pheromone dropped by the ant agent bunch on the way which they have voyage, fills in as a correspondence channel between different ants. The pheromone deposition done by the early sets of ant agent bunch is represented by gathering of characters which don't have any replication, and thus it represents the keystream. In an ant bunch every ant agent does the pheromone dropping which represents the keystream. Later an energy value is determined for each pheromone dropping. Energy value is determined by tallying the number of characters in the keystream present in the plain text divided by the length of keystream. For getting an exact value ant agents sets a limit. By setting an edge we guarantee that at least threshold percentage of characters are present in keystream which signifies pheromone testimony by the ant agents. Doing this it would empower the enciphering of characters in the keystream consequently the security of the framework as given by different strategies explained above. The purpose behind accepting a threshold is that the measure of threshold portion in the keystream will be encoded by mutated character code table also, the left portion of the characters in the keystream are encoded utilizing their respective ASCII values. Along these lines this will help in forestalling the unfortunate outsider from distinguishing the characters encoded and subsequently upgrade the security in cryptography.



```
Ant Colony Optimization
Initialize number of ants;
Initialize the ACO parameters;
while not end condition do
    for k = 0 to number of ants
        ant k choses start node;
        while solution is not constructed do
            ant k selects higher probability node;
        end while
    end for
    Update pheromone trails;
end while
```

Fig1. Ant Colony Optimization Algorithm

C. Applications of Ant Colony Optimization Technique

- Routing in telecommunication networks
- Travelling salesman problem
- Graph colouring
- Scheduling
- Constraint satisfaction

IV. Conclusion and Future Scope

Encryption is an imperative issue in today's communication day and age since essential data is carried out over the wireless interface, and is more exposed to fraud and swindling. Ant Colony Optimization Key Generation Algorithm is a swarm intelligence based approach used for generating keystream from the characters of plain text which is to be encrypted. Subsequently it gives a superior, ultra-productive, satisfactory and streamlined method for encryption and it additionally beats the disadvantages of the current stream cipher strategies, for example, Vernam figure, RC4, Fast and secure cipher figure, Key pooled RC4.

MANET is a short form for Mobile Ad Hoc Network. It is a kind of system which can arrange itself just as change locations all the while. In this arrangement of system, remote associations are included as they are portable in nature. Ant Colony Optimization Technique has many all-around established and ensured qualities because of which they can be abundantly utilized in MANETS. When the reverse ant original path returns, the local model of the network state and the local routing table are updated. This gives a rudimentary worldview to the importance of Ant Colony Optimization Algorithm improvement calculations to MANET.

REFERENCES

[1] M. Dorigo and L.M. Gambardella. Ant Colony system: A cooperative learning approach to then travelling salesman problem.
[2] Swarm intelligence based key generation for stream cipher N. K. Sreelaja and G. A. Vijayalakshmi Pai.
[3] A Survey on Cryptography using Optimization algorithms in WSNs Swapna B. Sasi and N. Sivanandam
[4] Charles P, Shari LP, Security in Computing. 3rd ed. Prentice
[5] RC4 Encryption Algorithm. www.vocal.com/RC4.pdf,2003.
[6] Biham E, Seberry J. Py (Roo): a fast and secure stream cipher. *Research Online*, 2005.
[7]Santosa, Budi, Metoda Metaheuristik,

Konsep dan Implementasi, Guna Widya, Surabaya,Indonesia, 2011.