

Pseudorandom Numbered Hybrid Crypto-Algorithm with Two Bit Crossover and Boundary Mutation

B. Reddaiah

Abstract: *In spite of all the advantages while using networks in any form, there are large numbers of possible security issues that are rising with networking. To sort the security issues network security is the action that is intended to safe guard the resources and integrity of network and data. At work stations there are filters, firewall to protect. But while data in transmission security services are needed and frequent change in methods are to be developed to counter threats. In this work different methods like pseudorandom generation and multiple genetic algorithms are used that resembles quite different in nature. This proposed hybrid algorithm can be used in small business applications where they are frequently hacked. Small organizations that cannot afford to build a strong security system can use such hybrid systems.*

Keywords: *Security attacks, Pseudorandom numbers, Encryption, Decryption, Crossover Function, Mutation.*

I. INTRODUCTION

NETWORK SECURITY

Securing the network is a hard task and the aim is to safeguard the usage of resources and network integrity and finally the data that travels through the network. This network security deals with physical resources and logical resources. A very good mechanism is needed across the network to manage the resources. The aim of the mechanisms that provides security is to deal with different types of threats and prevents them from damaging the network. With the wide use of network, securing it is becoming difficult as the attacks are increasing enormously and the nature of attacks is also not constant. As a whole the cost of cybercrimes is likely to increase up to \$2.1 trillion globally by the end of 2019. This estimation itself shows the importance of securing the network and it also specifies the attention required to put on network security.

A. Basic Attacks in Network Security

Due to the rapid advancement in the current internet and its related technologies and information system, is becoming the reason to connect either individually or as enterprise or as school or government department to Internet. In the same way for activities like social, personal and professional they depend on internet and its sources. This is giving more chance and reason for unauthorized and illegal activities by different

kinds of attacks thus destroying the resources in network. As internet is very important in all kinds, there may be people that will be always trying to disturb the services of internet. These people may damage the internet resources, disrupt privacy policies and may reduce internet services. Due to the regularity of attacks and diversity in current attacks and keeping in mind the future attacks and threats, providing security to the network has become a main issue in the field of computer networking. Attacks related to security are divided into two types. They are passive and active attacks. Passive is simply observing the transmission and attacks are traffic analysis, eavesdropping and monitoring [5], [6] & [7]. Active blocks the data stream and are like Interruption, Modification and fabrication [9], [10].

II. BACKGROUND STUDY

The essential application of networking features security comprising of detecting intruder, analyzing the traffic and monitoring the security in the network is discussed by Marin [1]. A framework for public key infrastructure that focuses on wireless networks is proposed by Wuzheng [2]. An innovative method has been proposed by Flauzac namely grid of security [4]. It is distributed security solution in a balanced collective method. Wu Kehe came up with a model to describe information security that is categorized into network business security, network security and data security [3].

III. SECURITY METHODS

In present scenario with the wide usage of networks and internet, exchange of secret data in a safe manner and through secure channel while travelling in network is foremost important for industry. Network security is a sequence of events and actions that defines the way of using security services through improved, strong and harmless channel that is developed and upheld in industry. In network while transmitting data, unauthorized people tends to access the data thus confidentiality, authentication and integrity are lost. To protect the data from unwanted access, data that is being transmitted through network has to be protected and safely transmitted. For secure transmission of information and other security services the most widely used tool is cryptography. Basically, the cryptography is based and utilizes mathematical concepts for encoding and decoding data that is to be transmitted. Strength of cryptosystem depends on the ciphers.

Revised Manuscript Received on February 04, 2020.

Reddaiah Buduri*, Yogi Vemana University, Kadapa, Andhra Pradesh, India. Email: b.reddaiah@yogivemanauniversity.ac.in



The process of developing secret code from original from is Cryptography. This science is about studying and developing protocols which may stop the unauthorized activities [8]. This research paper focuses on developing a hybrid system that is based on pseudorandom number generation, Crossover function and Mutation from Genetic algorithms. This group of functions may help in developing a complicated cryptosystem that is difficult to understand and break the system.

IV. PROPOSED SCHEME

In any kind of security system privacy, authentication, integrity, non-repudiation are the issues that are more significant. In this proposed hybrid system pseudorandom numbers and Genetic algorithms are used in developing the algorithm.

A. Pseudo Random Number in Security

Pseudo Random Number theory is based on mathematical formulas. They are produced in sequences of random numbers. Pseudo random Number Generator (PRNG) algorithm can be developed, that can generate large quantity of numbers in a short time.

B. Role of Genetic Algorithms in Security

The genetic structure and behaviour of chromosomes is the likeness on which genetic algorithms are grounded. Among few optimization algorithms Genetic algorithms are the one that can give high quality solution and solve complex problems and search problems. They are grounded on the impression of natural selection and genetics. It is by modelling a shortened form genetic process. These algorithms are evolutionary ones that are adaptive heuristic search in nature and they are computational models built on the ideology of evolution and natural selection. Here the problem pertaining to a specific domain is transformed into a model by means of data structures that are identical to chromosomes. They are evolved by means of Selection, Crossover (Recombination) and Mutation operators.

A wide and broad range of applications can be made by using Genetic Algorithms. In applications that are related to security issues these algorithms are used to find the ideal solution to a particular problem and in general they are pretty straight forward in nature. But due to this nature they may be complex in utmost situations. As per the attributes of the problem, diverse places of respective chromosome are fixed as bits, characters or numbers. In solving and developing new systems parallel implementation of Genetic Algorithms can be used for effective results.

C. Applications of Genetic Algorithms

Genetic Algorithms are mostly used in optimization problems of several types and they are regularly used in diverse applications. They are used in solving problems related to optimization, illustrating economic models, training regular neural networks, good in solving parallel problems, tasks related to dense pixel matching in digital image processing, solving vehicle routing problems by soft time windows, multiple depots and a heterogeneous fleet, handling scheduling problems like time table problems, in machine learning, used to plot the track that a robot arm takes by moving from one point to other point, used in designing

aircrafts with different parameters and developing improved solutions, used to fix the structure of DNA by spectrometric data, provides decent methods for multimodal optimization for finding various best solutions and used to solve the travelling sales person problem by means of novel crossover and packing strategies.

D. Advantages of Genetic Algorithms

The strength of Genetic Algorithms in developing security systems is because they do not need copied information that might not be in existence for several real-world problems and they are more effective and quicker than old methods. These algorithms are very popular in parallel abilities, enhances continuous and discrete functions and also multi-objective problems. They are useful when the search space is actually big and when there exists large number of parameters that are included.

V. PROPOSED HYBRID SYSTEM

A. Encryption Process

Original text is transformed into scrambled text starting with generating pseudorandom number and then by using Single point crossover operator where two bits are considered, combined with boundary mutation operator as in Figure 1 and decoding as in Figure 2.

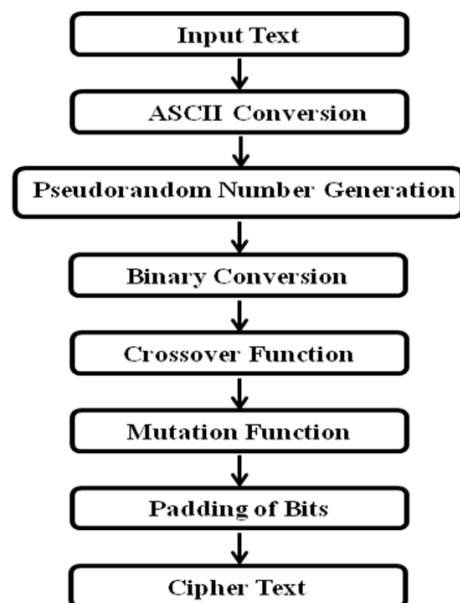


Fig. 1. Block Diagram of Encryption Process

B. Encryption Algorithm

Step 1: Start

Step 2: Read original text.

Step 3: Convert given input text into ASCII values.

Step 4: Generate Pseudorandom Number sequence for above ASCII values.

Step 5: Convert above pseudorandom numbers into binary form.

Step 6: Divide binary digits into two 15bits blocks. New binary blocks of 15bits are denoted as S1 and S2.

Step 7: Apply two-bit crossover operator for parent blocks S1 and S2

- Step 8:** Apply boundary mutation operator for the resultant child blocks S11 and S22.
- Step 9:** Add S11 and S22 to form S1122.
- Step 10:** If given input text size is non-multiples of 4 or greater than 4 for every byte two multiples of dummy bits are to be added at end.
- Step 11:** Now divide S1122 into 8 bits blocks and convert the blocks into equivalent characters.
- Step 12:** The Resultant is the Cipher text
- Step 13:** Stop.

C. Decryption Process

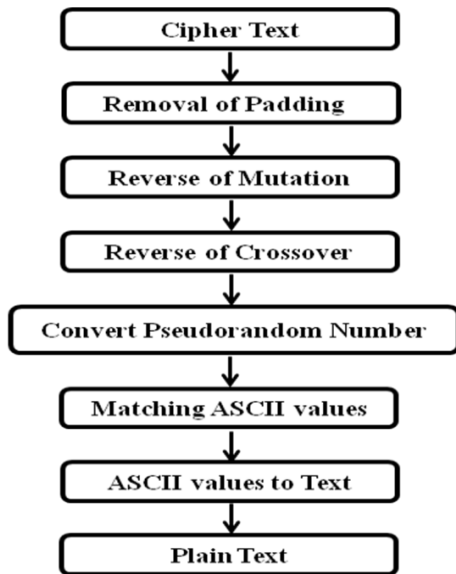


Fig. 2. Block Diagram of Decryption Process

D. Decryption Algorithm

- STEP1:** Start
- STEP2:** Read output of encryption algorithm.
- STEP3:** Convert the text into binary form.
- STEP4:** Remove padded bits at the end if added in encryption as described in step 10 of encryption.
- STEP5:** Apply boundary mutation operator for the above binary form and divide the result into S21 and S31 blocks.
- STEP6:** Then apply two-bit crossover operator for S21 and S31 blocks.
- STEP7:** After two bit crossing over divide S21 and S31 into S1, S2, S3 and S4 respectively.
- STEP8:** Now convert S1, S2, S3, and S4 blocks into pseudorandom numbers (Natural Numbers).
- STEP9:** Then compare pseudorandom numbers with ASCII values.
- STEP10:** Convert ASCII values into text and it is the original text that is decrypted.
- STEP10:** Stop

VI. RESULTS

Encoding results and decoding results are tabulated in Table I, II, III and IV for word ‘upesm’.

A. Encryption results

The word “upesm” is taken as example and processed through encryption algorithm. The outcome is tabulated in Table-I and in Table-II.

Table –I: Outcome of Encryption process

| Original Text | ASCII values | Pseudorandom Number Generation | Binary Conversion | Parents Creation |
|---------------|--------------|--------------------------------|-------------------|--|
| u | 117 | 58 | 111010 | S1=1110101110001110 S2=0101110011101110 |
| p | 112 | 56 | 111000 | |
| e | 101 | 50 | 110010 | |
| s | 115 | 57 | 111001 | |
| m | 109 | 54 | 110110 | |

Table-II: Outcome of Encryption process continued

| Applying Crossover | Applying Mutation | Total bits | Padding of bits | Converting into bytes (total bits/8) | Cipher text |
|-------------------------|-------------------------|--|--|--------------------------------------|-------------|
| S1= 0100101110001110 | S1= 1100101110101110 | S12= 1100101110101 10011111001100110 | S12= 11001011101011 0011111001100110(00) | 11001011 | Ě |
| S2= 1111110011101110 | S2= 0111110011001110 | | | 10101100 | ŕ |
| | | | | 11111001 | ù |
| | | | | 10011000 | ☒ |

For the Plain text ‘upesm’, after pseudorandom number generation and applying crossover and mutation genetic algorithms the cipher text derived is “Ě-ù☒”.

For the decryption algorithm the resulted cipher text of encryption process “Ě-ù☒” is considered for decryption

B. Decryption

Table-III: Outcome of Decryption process

| Cipher Text | Binary Conversion | Removing of Padding bits | Creating Parents | Applying Mutation | Applying Crossover |
|-------------|-------------------|---------------------------------------|-----------------------------|-----------------------------|-----------------------------|
| È | 11001011 | 11001011101011 00111110010011 0 | S21= 1100101110101 10 | S21= 01001011100 0110 | S21= 11101011100 0110 |
| ¬ | 10101100 | | | | |
| ò | 11111001 | | S31= 0111110011001 10 | S31= 11111100111 0110 | S31= 01011100111 0110 |
| ☒ | 10011000 | | | | |

Table-IV: Outcome of Decryption process continued

| Total bits | Dividing bits into 6-bit blocks (total bits/6) | Converting blocks into digits | Generate ASCII Values for Pseudorandom Numbers | Generating Cipher Text from ASCII values |
|--|--|-------------------------------|--|--|
| S23= 11101011 10001100 10111001 110110 | S1=111010 | 111010=58 | 58= 117 | u |
| | S2=111000 | 111000 =56 | 56= 112 | p |
| | S3=110010 | 110010 =50 | 50= 101 | e |
| | S4=111001 | 111001 =57 | 57= 101 | s |
| | S5=110110 | 110110 =54 | 54= 109 | m |

With the Cipher text “È-ò☒” when decrypted the plain text “upesm” is generated and is shown in Table-III and Table-IV.

VII. ADVANTAGES OF PROPOSED ALGORITHM

The major benefit of this proposed mechanism is that it will be executed by taking very less time as it is based on pseudorandom numbers. The other advantage is that the output that is generated by the encryption algorithm called cipher text is mainly in the form of symbols and special characters, but not the scrambled text always like in other algorithms. This makes the hackers think twice whether it is the cipher text or not to go for decoding the text. Because of this also the time taken by the hackers to decode increases. As this algorithm is developed by using more than one genetic algorithm it is very difficult to understand the structure of the algorithm which also consumes time of hackers while understanding the structure.

VIII. CONCLUSION

In the process of building cryptographic algorithms different functions and operators are used to increase security and to provide better security. In this work pseudorandom numbers are generated that helps in performing calculations with good speed and with less integer arithmetic instructions. This helps the algorithms to take less time for execution. This algorithm is developed by using more than one genetic algorithm, that strengthens the structure. In this proposed algorithm two-bit crossover is used for generating child characters. Along with Crossover, Mutation is also used that can preserve and diverse. In this Boundary mutation is used that is suitable for integers and float values.

REFERENCES

1. Marin, G.A. (2005), “Network Security Basics”, In security & privacy, IEEE, Issue 6, Vol. 3, pp. 68-72, 2005.
2. Wuzheng Tan, Maojiang Yang, Feng Ye, Wei Ren, “A security framework for wireless network based on public key infrastructure”, In Proc. Of Computing, Communication, Control and Management, 2009, CCCM 2009, Vol. 2, pp. 567 -570, 2009.
3. Wu Kehe, Zhang Tong, Li Wei, Ma Gang, “Security Model Based on Network Business Security”, In Proc. Of Int. Conf. on Computer

Technology and Development, 2009., ICCTD’09, Vol. 1, pp. 577 – 580, 2009.

4. Flauzac. O, Nolot. F, Rabat. C, Steffemel. L. A, “Grid of Security: A New Approach of the Network Security”, In Proc. Of Int. Conf. on Network and System Security, 2009. NSS’09, pp. 67 – 72, 2009.
5. Neha Khandelwal, Prabhakar. M, Kuldeep Sharma, “An Overview of Security Problems in MANET”.
6. Anupam Joshi and Wenjia Li, “Security Issues in Mobile Ad Hoc Networks – A Survey”.
7. Ali Ghaffari, “Vulnerability and Security of Mobile Ad Hoc Networks”.
8. Shyam Nandan Kumar, “Technique for Security of Multimedia using Neural Networks”, IJRETM-2014-02-05-020, Vol. 02, Issue. 05, pp. 1-7, Sep-2014.
9. MattCurtin, Introduction to Network Security, found at http://www.cs.cornell.edu/Courses/cs519/2003sp/slides/15_securitybasics.pdf, March 1997.
10. Stallings. W (2006), Cryptography and Network Security, Fourth Edition, Prentice Hall.

AUTHORS PROFILE



B. Reddaiah, completed his Ph.D from Acharya Nagarjuna University, Guntur. His research areas are Software Engineering, Security and Image Processing. He is working in Department of Computer Applications, Yogivemana University.