ISSN (e): 2250 – 3005 || Volume, 08 || Issue, 6|| Jun – 2018 ||
International Journal of Computational Engineering Research (IJCER)

Enhanced Encryption Algorithm Based On Prime Number, DNA Sequence And PI Sequence

Sasipreetham Kottu[1], Vikas B[2]

[1] *B.Tech Student, Dept. of Computer Science and Engineering, GITAM Institute of Technology, GITAM, Visakhapatnam, India,*

[2] *Asst. Professor, Dept. of Computer Science and Engineering, GITAM Institute of Technology, GITAM, Visakhapatnam, India*

[*] *Corresponding Author: Sasipreetham Kottu*

ABSTRACT

In a World full of communications, it is essential to protect the data in order to ensure the privacy of the users. There is a lot of sensitive data present in the web and it needs to be protected. Conventional security methods like RSA,DES,AES algorithms and others are no longer sufficient enough to protect the data from any kind of potential abuse. Complex algorithms are required to encrypt the data which makes it difficult to break and ensures the security of data from theft by any third parties.We proposed an Enhanced Encryption Algorithm based on Prime number, DNA sequence and PI sequence which is used to encrypt the data in a more secured and complex manner. Our algorithm uses two different keys to produce the cipher text where one of them is generated with the help of a PI sequence which has nearly billions of digits with non repeating sequences and the other with a DNA sequence which has nearly 3.3 billion combinations. It produces different cipher text for the same plain text which confuses the hacker to achieve the original text and makes it near impossible to break it.

KEYWORDS: Cryptography, PI, DNA, Cipher Text, Plain Text, Key, Encryption, Decryption.

Date of Submission: 06-06-2018 Date of acceptance: 21-06-2018

I. INTRODUCTION

In today's Digital World, Communication plays a major part which involves exchange of data between devices by wired or wireless means [1]. As technology is emerging at a rapid rate, the amount of data in the internet is increasing at an exponential rate. As the data is increasing at an exponential rate, it also involves a lot of sensitive data which is not just limited to military applications, but it has also extended to all kinds of applications which are present in the web [2]. There is a rapid growth in data theft related crimes which involves a great deal for its security. This creates the need for securing the data by appropriate measures. These cyber crimes has enforced many Governments and other organizations to invest more in protection of their data and make it their primary concern which has forced them to upgrade to new encryption techniques as traditional cryptographic techniques are not sufficient enough to protect the sensitive data[3]. It is necessary to develop more complex and efficient encryption techniques to secure the data.

A. Cryptography

It is the process of generating cipher text from plain text with the help of a key where the cipher text generated is usually present in an incomprehensible format so that it is protected from any kind of unauthorized access. Key plays a major role in the level of encryption. The more complex the key and the encryption process, the more difficult it becomes to break the encrypted text. Cryptography is of two types

i. Symmetric Key Cryptography

As the name suggests, it is a kind of cryptography where a symmetric key is used i.e. same key is used for both encryption as well as decryption of a text [5]. Some of widely used and most common symmetric encryption techniques are AES, DES, 3- DES, and Blowfish.

- **DES**

Date Encryption Standard (DES) is one of the most famous and widely used algorithm which is adopted as Federal Information Processing Standard (FIPS PUB 46) by the National Institute of Standards and Technology (NIST)[14]. It is a block Cipher. It uses same key for both encryption and decryption. Its key consists of a length of 64-bit where 56 bits are used as key and the remaining 8 units are for error detection [13].

- **AES**

Advanced Encryption Standard is introduced to overcome the drawbacks present in DES. In 2001, NIST recommended to replace DES [14]. Its supports data of block length 128 bits and 3 types of combinations of key length of 128, 192 and 256 bits and the number of rounds for processing them is 10, 12, 14 respectively[3].

ii. Asymmetric Key Cryptography

As the name suggest, it is a kind of cryptography where an asymmetric key is used i.e. two different keys are used namely public key for encryption and a private key for decryption. It is also commonly known as public key cryptography. This is a irreversible cryptographic technique. RSA, El Gamal, Diffie-Hellman Key exchange, Digital Signature, Elliptical Curve Cryptography(ECC) are some of the most common and widely used asymmetric encryption algorithms[6][15].

- **RSA**

RSA algorithm is named after its authors Ron Rivest, Adi Shamir and Leonard Adleman. It is the most widely used asymmetric algorithm. It uses two different keys. A public key for encryption and a private key for decryption. It is known for its high security and irreversibility i.e. it is nearly impossible to trace back the private key from public key[16].

B. PI

PI which is also known as Archimedes constant is generally termed as the ratio between the circumference and diameter of the circle. It is denoted with the Greek letter "π". PI being an irrational value, it is generally taken as 22/7 for easy calculations. Its decimal value is 3.1415926535897 and so on. It has an infinite sequence of digits where there is no repeating sequence even after computer scientists have calculated millions of digits. Due to its statistical randomness it can be used in encryption techniques for key generation [9].

C. DNA

Deoxyribonucleic Acid is a self replicating molecule i.e. it is a double stranded helical molecule which is present in nearly all living organisms. It carries some essential genetic information which is useful in classifying to which particular species it belongs to. DNA strands are made up of four bases namely Adenine (A), Thymine (T), Guanine (G), and Cytosine (C). It is important to note that Adenine combines with Thymine and Guanine with Cytosine only. Nearly 3 billion combinations of A-T & G-C are present in DNA Strand [2][10].

D. DNA Cryptography

DNA Cryptography is the art of protecting the data with the help of cryptographic techniques combined with DNA sequences. It is one of the most emerging technologies in the field of information security. Since DNA primarily consists of the nucleotide base A-T and G-C, it is the uniqueness in those sequences which makes it complex and hard to break it [7]. When data is encrypted in the form of DNA sequences it is hard to break it as it consists of nearly 3 billion combinations. DNA computing also supports parallel processing capability which is used in performing encryption and decryption of keys. DNA cryptography is more efficient in terms of space complexity as a DNA strand can store huge amounts of data with the help of its A-T and G-C combinations. It can nearly hold 10^8 tera bytes of data for every 1gm [8].

This paper is organized as follows: In section II, a brief description of related works is explained. In section III methodology of the algorithms is explained. In section IV, Key exchange techniques are discussed. In section V, the proposed algorithm is specified including a general example of the technique, with the Conclusion specified in Section VI.

II. RELATED WORK

Many researchers have done an extensive research on encryption techniques and proposed some new innovative techniques which are more efficient than the traditional encryption techniques like AES, DES etc. Techniques which are proposed from time to time they have grown to become more efficient that the predecessors. Apart from the being efficient they have also compromised some drawbacks which lead to new challenges as well.

Vikas et al. [2] have proposed a symmetric algorithm called A Novel DNA and PI based Key Generating Encryption Algorithm. This algorithm uses both PI and DNA sequence to generate the key which is used for encryption. As the PI sequence used in algorithm is picked from its infinite non repeating sequence and DNA sequence from nearly billions of its combinations, it is impossible to crack such a combination by the cryptanalyst. This makes the key very complex to crack it.

Aswin Achuthshankar and Aswathy Achuthshankar [3] have proposed A-S Algorithm which is very simple and efficient than traditional encryption techniques. This algorithm will take plain text as well as the key from the user. It will convert each letter of plaint text and key into ASCII code and then it will perform XOR operation between them. The obtained code is converted
back to equivalent characters which is nothing but cipher text. This algorithm is very simple which makes it efficient but at the same time it is also easy for a modern cryptanalyst to crack it as it contains only one major step.

Liu Tao and Wen Yudong [4] have proposed an Double Encryption Algorithm where it encrypts the data using DES algorithm to encrypt the data. Since the key generated in it is symmetric i.e same key is used for encryption and decryption and it is essential to protect it so, the authors have encrypted this key using RSA algorithm which is a asymmetric key which in turn produces a private key and public key. These keys and the encrypted data are transmitted through a covert channel.

Veeraragavan et al. [17] have proposed an Enhanced Encryption Algorithm which is an symmetric algorithm. It has two keys which are generated with the help of Key Generation Service. It initially converts the plain text into binary blocks and divides them based on a random prime generated based on their length and rotates the bits with the help of first key. Then the resultant of XOR operation performed between the second key and the rotated bits merged in sequential order eventually yields the cipher text. This algorithm makes the encryption process very complex and makes it impossible to break it.

Siddaramappa .V and Ramesh K.B [1] have proposed Cryptography and Bioinformatics techniques for Secure Information transmission over Insecure Channels where the authors have used DNA sequences in an innovative manner to encrypt the data. They have converted the input data into binary form and then into DNA sequence. Then a key value is taken from the server and complementary rules are applied for both of them followed by a XOR operation between the two. Then the resultant is converted to a DNA sequence and then to binary format which is the cipher text. This method converting into DNA sequence makes it harder for the cryptanalyst to break it as there are nearly billions of DNA sequences.

From the literature review it is clear that an innovative and efficient encryption technique is necessary for securing the data. This paper has proposed an Enhanced Encryption Algorithm based on Prime number, DNA Sequence and PI Sequence (EEA- PDP) which is a Symmetric algorithm. This algorithm is used to encrypt the users data as it needs to be secured from any kind of illegal usage [17]

III. METHODOLOGY

EEA-PDP is an encryption algorithm which is used to encrypt the users data. It is a symmetric encryption algorithm which uses the same key for both encryption and decryption. Keys of EEA-PDP are generated from DNA Sequence and PI Sequence. The DNA sequence is obtained from the National Centre for Biotechnology Information (NICB)[18]. The EEA-PDP algorithm uses these two keys along with a prime number for encryption and decryption of data.

I. Key Exchange

It is essential to pass the cipher text as well as the keys to the desired user after encryption. There is always a chance that a third party can spoof the network and steal the data. Though the data is in incomprehensible format the attacker can corrupt the data. So it is also essential to send the data over a secure channel. In order to tackle the secure transmission problem and prevent such kind of Man in the Middle Attacks (MIM Attack), Diffie-Hellman Key exchange algorithm can be used where it will generate the key on both sides rather than transmitting it [11]. It is an Asymmetric algorithm and is irreversible.

II. Proposed Algorithm

Our algorithm encrypts the data by taking it as input from the user. It first converts the data into ASCII code followed by its binary values. Then based on the length of the text, prime numbers are generated and a random prime number is picked out among it which is used to divide the binary blocks. A random sequence from PI is taken as Key-1 which is used in rotating the bits. After rotation, the bits are merged in sequential order and 2's complement is performed on them. A random DNA sequence is picked out and it is converted into binary form which will generate Key-2. Now, XOR operation is performed between the 2's Complemented bits and the DNA sequence. The resultant is divided into 8-bit binary blocks and then converted back to decimal form (ASCII code) and eventually the Cipher text is generated.

A. Encryption

Encryption is the process of generating cipher text from plaint text with help of an encryption algorithm and key to secure the data and transmit it through a insecure channel [12][13]. It is very essential in today's digital world to secure the data by means of encrypting it and protect it from any kind of malicious usage. In our algorithm the sender follows some certain steps to encrypt the data.

1. Start
2. Convert the Plain text to decimal number(ASCII Code)
3. Convert the ASCII Code to Binary Form
4. Calculate the total number of bits in plain text
5. Generate the Prime numbers between the 1 and length of the bits
6. Divide the Binary bits into Blocks based on prime number which is randomly chosen from the set of prime numbers in Step-5
7. Generate Key-1 by taking a random PI sequence
8. Rotate the binary bits in each block from left to right based on Key-1.
9. Merge the rotated binary bits in sequential order and perform 2's Complement on it
10. Generate the Key-2 by taking random DNA sequence and convert it to binary form(A=00, T=11, G=01, C=10)
11. Perform XOR Operation between Key-2 and output of Step-9
12. Divide the binary bits into 8-bit blocks
13. Convert the binary blocks into decimal number(ASCII Code)
14. Covert the ASCII Code to obtain Cipher Text
15. End

B. Decryption

Decryption can also termed as the reverse of encryption where it primarily deals with decrypting the encrypted text i.e. converting the cipher text into plain text with the help of a key and decryption algorithm. When we encrypt a particular data it is equally important to know how to decrypt it as well because it will be meaningless if we can't decrypt the encrypted data [12] [13]. In our algorithm the receiver receives the keys, prime number and encrypted data and follows certain steps to decrypt it.

1. Start
2. Covert the Cipher Text to ASCII Code
3. Convert the ASCII Code to Binary form
4. Perform XOR Operation between the binary data and Key-2
5. Perform 2's Complement on the output of Step-4
6. Divide the binary bits obtained in Step-5 into blocks based on the prime number
7. Rotate the bits in each block from right to left based on Key-1
8. Merge the bits in Sequential order and divide the binary bits into 8-bit blocks
9. Convert the 8-bit blocks blocks into decimal number(ASCII Code)
10. Convert the ASCII Code to obtain Plain Text
11. End

C. Implementation

We will implement the above mentioned encryption and decryption algorithm with the help of an example

Encryption

Let us consider the following plain text from the user Plain Text: chat

1. The ASCII Code of Plain Text is [099, 104, 097, 116]
2. The Binary bits of the ASCII Code is [01100011, 01101000, 01100001, 01110100]
3. Calculating the total number of bits Number of Bytes=4
   Number of Bits= 32
4. The Prime numbers between 1 and length of plain text(in bits) Prime Number from 1 to 32(length in bits) : [2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31]
   Here, the Random Prime number (Block Size) chooses is 13
5. Dividing into Binary blocks of size 13(Random Prime Number chosen) Block-1: 01100011 01101
   Block-2: 000 01100001 01
   Block-3: 110100

6. The random PI sequence selected for the generation of Key-1 is 167. So, Key-1 : 167
7. Rotating the bits in each block by 167(Key-1) positions from left to right After Rotation
   Block-1: 1000110110101
   Block-2: 0011000010100
   Block-3: 101001
8. The rotated blocks after merging 10001101101010011000010100101001
9. Performing 2's Complement on the merged block 01110010010101100111101011010111
10. The random DNA sequence taken here is CTCAGCCC. Let us consider A=00, T=11, G=01, C=10 Binary form of CTCAGCCC = 1011100001101010
    Key-2: 1011100001101010
11. Performing XOR operation between the obtained output of Step-9 and Key-2(Step-10)
    01110010010101100111101011010111
    10111000011010101011100001101010

    11001010001111001100001010111101
12. Dividing the binary bits obtained in Step-11 into 8-bit binary blocks [11001010, 00111100, 11000010, 10111101]
13. Converting the Binary blocks into equivalent decimal numbers(ASCII Code) [202, 60, 194, 189]
14. Convert the ASCII Code to obtain Cipher Text Cipher Text : Ê<Â½

Decryption

Let us consider the following Cipher Text: Ê<Â½
Prime Number: 13
Key-1: 167
Key-2: 1011100001101010

1. The ASCII Code of Plain Text is [202, 60, 194, 189]
2. The Binary bits of the ASCII Code is [11001010, 00111100, 11000010, 10111101]
3. Merging the obtained Binary blocks 11001010001111001100001010111101
4. Performing XOR Operation between merged Binary block and Key-2.
   Key-2: 1011100001101010
   11001010001111001100001010111101
   10111000011010101011100001101010

   01110010010101100111101011010111
5. Computing 2's Complement on output obtained in Step-4 10001101101010011000010100101001
6. Dividing the computed 2's Complement into Binary blocks based on the prime number. Prime Number : 13
   Block-1: 1000110110101
   Block-2: 0011000010100
   Block-3: 101001
7. Rotating the binary bits in each block from right to left by 167(Key-1) positions Key-1 : 167
   After Rotation
   Block-1: 01100011 01101
   Block-2: 000 01100001 01
   Block-3: 110100
8. Merging the Binary blocks in sequential order and dividing them into 8-bit Binary blocks [01100011,01101000, 01100001, 01110100]
9. Converting the Binary blocks into equivalent decimal numbers(ASCII Code) [099, 104, 097, 116]
10. Converting the ASCII Code to obtain Plain Text Plain text : chat

Table 1: Comparison for AES, Proposed Algorithm, and DES

	AES	**Proposed Algorithm**	**DES**
Encryption time	4.08	3.6	2.00
Input Size(in bits)	12	12	12
Block Size	Fixed	Fixed	Variable

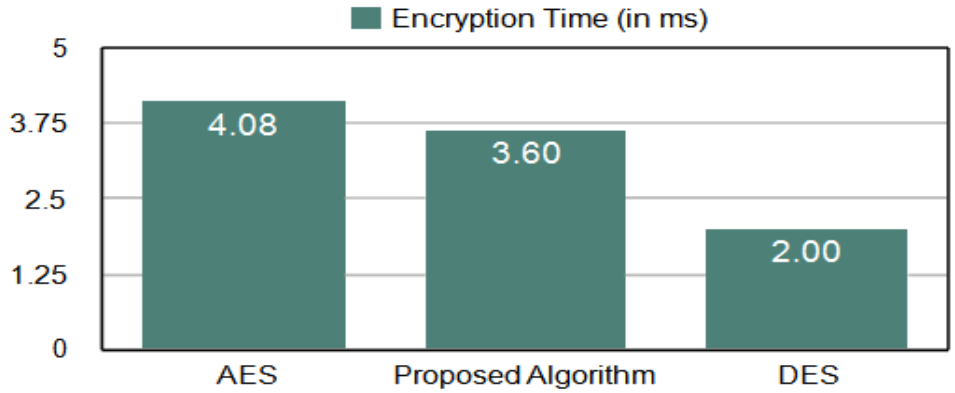

Figure 1: Comparison between various algorithms and the time taken for their encryption.

IV. CONCLUSION

In this paper we have reviewed various encryption techniques which are essential for securing the data. In order to protect the privacy of the users we need advanced encryption techniques which are complex than the traditional techniques. In this paper we have proposed an encryption algorithm namely, Enhanced Encryption Algorithm based on Prime number, DNA Sequence and PI Sequence. In every encryption technique, Key is the essential part and it needs to be larger and complex to break it. Considering the billions of combinations of DNA Sequences and a non repeating infinite sequence of PI values, we have used them to generate the Key in our algorithm. This makes the Key hard to break it and ensures the security of data. Notably our algorithm produces different cipher text for same plain text which confuses the cryptanalyst and makes it hard to break it. As shown in the results our algorithm is efficient than the powerful AES and is more complex than most of the traditional techniques.

REFERENCES

[1]. Siddaramappa .V, Ramesh K.B., "Cryptography and Bioinformatics techniques for Secure Information transmission over Insecure Channels" In the Proceedings of the 2015 International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT), Davangere, India, pp.137-139, 2015.

[2]. Vikas B., Akshay A.K., Thanneeru S.P.M., Raghuram U.M.V., Bhargav K.S. (2018) A Novel DNA- and PI-Based Key Generating Encryption Algorithm. In: Bhateja V., Nguyen B., Nguyen N., Satapathy S., Le DN. (eds) Information Systems Design and Intelligent Applications. Advances in Intelligent Systems and Computing, vol 672. Springer, Singapore.

[3]. Aswin Achuthshankar, Aswathy Achuthshankar, "A novel symmetric cryptography algorithm for fast and secure encryption" In the Proceedings of the 2015 IEEE 9th International Conference on Intelligent Systems and Control (ISCO), Coimbatore, India, pp.1-6, 2015.

[4]. Tao Liu, Yudong Wen, "Application of Double Encryption Algorithm in Covert Channel transmission", In the Proceedings of the 2018 International Conference on Intelligent Transportation, Big Data & Smart City (ICITBS), pp.210-213, 2018.

[5]. Jaime Raigoza, Kapil Jituri, "Evaluating Performance of Symmetric Encryption Algorithms", In the Proceeding of the 2016 International Conference on Computational Science and Computational Intelligence (CSCI), pp.1378-1379, 2016.

[6]. Tutubalin Pavel Innokentievich, Mokshin Vladimir Vasilevich, "The Evaluation of the Cryptographic Strength of Asymmetric Encryption Algorithms ", In the Proceeding of the 2017 Second Russia and Pacific Conference on Computer Technology and Applications (RPC), pp.180-183, 2017.

[7]. Partha Sarathi Goswami, Tamal Chakraborty, Harekrishna Chatterjee, "A Novel Encryption Technique Using DNA Encoding and Single Qubit Rotations", International Journal of Computer Sciences and Engineering, Vol.6, Issue.3, pp.364-369, 2018.

[8]. Tausif Anwar, Abhishek Kumar, Sanchita Paul, "DNA Cryptography Based on Symmetric Key Exchange", International Journal of Engineering and Technology (IJET), Vol.7, No.3, pp.938-950, Jun-July 2015.

[9]. PI, https://en.wikipedia.org/wiki/Pi

[10]. Watson, J.D., Crick, F.H.C., "A Structure for De-oxy Ribose Nucleic Acid ",Nature,vol.25(1953),pp.737-738.

[11]. Whitfield Diffie, Martin Hellman.:New Directions in Cryptography. IEEE Transactions On Information Theory Vol IT-22, pp. 644-654, November 1976.

[12]. Monika Agrawal, Pradeep Mishra, "A Comparative Survey on Symmetric Key Encryption Techniques", International Journal of Engineering and Technology (IJET), Vol.4, No.5, pp.877-882, May 2012.

[13]. Anjali Patil, Rajeshwari Goudar, "A Comparative Survey Of Symmetric Encryption Techniques For Wireless Devices", International Journal Of Scientific & Technology Research Vol.2, Issue.8, pp.61-65, August 2013.

[14]. Gurpreet Singh, Supriya Kinger, "Integrating AES, DES, and 3-DES Encryption Algorithms for Enhanced Data Security", International Journal of Scientific & Engineering Research, Vol.4, Issue.7, pp.2058-2062, July 2013.

[15]. Jitendra Singh Laser, Viny Jain, "A Comparative Survey of Various Cryptographic Techniques", International Research Journal of Engineering and Technology (IRJET), Vol.03, Issue.03, pp.163-171 March 2016.

[16]. Sourabh Chandra, Smita Paira, Sk Safikul Alam, Goutam Sanyal, "A comparative survey of Symmetric and Asymmetric Key Cryptography", In the Proceedings of the 2014 International Conference on Electronics, Communication and Computational Engineering (ICECCE), pp.83-93, 2014.

[17]. N.Veeraragavan, L.Arockiam, S.S. Manikandasaran, "Enhanced Encryption Algorithm (EEA) for Protecting Users' Credentials in Public Cloud", In the Proceedings of the 2017 International Conference on Algorithms, Methodology, Models and Applications in Emerging Technologies (ICAMMAET), pp.1-6, 2017.

[18]. National Centre for Biotechnology Information, http://www.ncbi.nlm.nih.gov/

Authors Profile

Mr. Sasipreetham Kottu is currently pursuing his Bachelors degree from Department of Computer Science and Engineering, from GITAM Deemed to be University, Visakhapatnam, India since 2015. He is a member of ACM since 2016. His main research work focuses on Cryptography Algorithms, Network Security, and Data Mining based education.

Mr. Vikas B pursued Bachelor of Technology and Master of Technology from JNTUH, Hyderabad in year 2010 and 2012 respectively. He is currently pursuing Ph.D. and currently working as Assistant Professor in Department of Computer Science and Engineering, GITAM Deemed to be University, Visakhapatnam since 2014. He is a member of IEEE & IEEE computer society since 2012. He has published 6 research papers in reputed international journals and conferences including Springer and are available online. His main research work focuses on Deep Learning, Bioinformatics, Cryptography Algorithms, Network Security, Machine Learning, Data Mining, IoT and Computational Intelligence based education. He has 7 years of teaching experience and 2 years of Research Experience.

Sasipreetham Kottu." Enhanced Encryption Algorithm Based On Prime Number, DNA Sequence And PI Sequence." International Journal of Computational Engineering Research (IJCER), vol. 08, no. 06, 2018, pp. 26-32.