TEST Engineering & Management

January-February 2020
ISSN: 0193-4120 Page No. 15355 - 15360

Data Security using Efficient Cryptosystem

[1]U.Bhanu Prasanna[1]Dr.P.Sri Ram Chandra
Faculty of Engineering, Godavari Institute of Engineering and Technology (A),
Rajahmundry, Andhra Pradesh, INDIA.

Article Info
Volume 82
Page Number: 15355 – 15360
Publication Issue:
January-February 2020

Article History
Article Received*: 18 May 2019*
Revised*: 14 July 2019*
Accepted*: 22 December 2019*
Publication*: 28 February 2020*

Abstract:
Data is a tactical resource. Information transactions across the world have become inextricably interwoven. Providing security to that data is one of the primary aspects so as to protect from unauthorized disclosure and modification. A rigorous search made us to consider cryptography algorithms as the principle means of providing the data security. As numerous cryptographic algorithms exist but each of them has their own solid and frail focuses in terms of complexities. Keeping in mind the end goal to develop a low complex algorithm we have proposed a new symmetric stream cipher in this research article and named as "Random Prime Key - RPK" Algorithm. The strength of this algorithm has been analyzed over differential cryptanalysis and suitable criteria in order to ensure low complexity and high security.

Keywords: *Cryptography, Prime Number, Encryption ,Decryption, Data Security, Authentication.*

I. INTRODUCTION

The info or data transferring from transmitter to recipient with data auspices is becoming very tough nowadays. To overcome the data security problems the two most well-known techniques are encryption and decryption respectively. The encryption is such a process that is based upon converting normal text to unintelligible text and the same the other way around i.e changing or converting unintelligible text back to the correct message or normal text by utilizing the decryption method. We have proposed an efficacious cryptographic algorithm that is used for data protection. The intention is to overcome the data security problems by using a cryptographic algorithm for encryption and decryption, and also we use stream of symmetric keys for encryption and decryption methods.

1.1CRYPTOGRAPHY

Cryptography is a proficiency technique of ensuring security to data and communications through the utilization of codes so that only those persons for whom the information is allocated can understand it and process it. The prefix "crypt" refers to "hidden" and suffix grapy refers to "writing". In Cryptography the functional techniques which are used to defend data are attained from mathematical concepts and a set of rule-based calculations known as algorithms to convert the text that makes it tough to decipher it. These algorithms are used for cryptographic key generation, digitized signing, verification to secure data privacy, web browsing on the internet and to protect surreptitious trading such as credit and debit card.Where the cryptography plays a vital role ? Cryptography is the acquisition of using mathematics for encrypting and decrypting information, which refers to putting into or decrypting from a mathematical terminology. It is the cognitive operation of encrypting and decrypting the message. The encryption is a typical process of changing legible text to unreadable text in a similar way changing unreadable text back to legible text by using the decryption method.

1.2 CLASSIFICATION OF CRYPTOGRAPHY

SYMMETRIC KEY CRYPTOGRAPHY

It is an encryption scheme where the transmitter, as well as recipient of data, use a single mutual key to encrypt and decrypt textual data. Symmetric Key Systems are swifter and simplest but the trouble is that the transmitter and recipient have to interchange

January-February 2020
ISSN: 0193-4120 Page No. 15355 - 15360

key in a protected manner. The most familiar symmetric-key cryptographic system is the Data Encryption System(DES).

ASYMMETRIC KEY CRYPTOGRAPHY

Under this system, a Gallus of keys is used to encrypt and decrypt data. A public key is utilized for encryption and a private key is utilized for decryption. Public key and Private keys are dissimilar. Even if the public key is familiar to everyone the intended recipient can only decrypt it because he alone knows the private key.

1.3 ROLE OF NUMBER THEORY IN CRYPTOGRAPHY

Number theory plays a vital role in an encryption algorithm. Cryptography is the recitation of concealing information, converting secret data to unreadable texts. The common tools used in number theory are primes, divisors, congruencies, and Euler's 'ϕ ' function are used in cryptography for security.

PRIME NUMBER: The positive integer numbers which have divisors of 1 and itself are known to be prime numbers . Prime numbers are central to number theory. We need to make a note that '1' is prime, but is generally not of interest.

Example– 2,3,5,7,11 are prime 4,6,8,9,10 are not, List of prime numbers less than 100 is 2,3,5,7,11,13,17,19,23,29,31,37,41,43,47,53,59,61,67,71,73,79,83,89,97

2.LITERATURE SURVEY

P.Sri Ram Chandra ,G.Venkateswara Rao ,G.V.Swamy[1] have proposed a new symmetric cryptography algorithm Ultramodern Encryption Standard (UES) which uses prolic series number for generating set of keys, binary and gray code operations for encryption and decryption processes.

P.Sri Ram Chandra ,G.Venkateswara Rao ,G.V.Swamy[2] have proposed a new symmetricblock cipher named Modular Encryption Algorithm which uses tri-modular matrix for its key generation and M-box is also used, a set of operations on a matrix, Permutations and Substitutions are performed for its encryption and decryption.

Vikas.B and Sasipreetham [3] have proposed an symmetric algorithm called A Novel DNA and PI-based Key Generating Encryption Algorithm. This algorithm uses both PI and DNA sequences to generate the key which is utilized for encryption. As the PI sequence used in the algorithm is sorted from its infinite non-repeating sequence and DNA sequence from nearly billions of the combinations which exist, it is highly impossible to trace such a combination by the cryptanalyst.Thangarasu.N and Arul Lawrence Selvakumar [4] have proposed a hill cipher algorithm that uses a key matrix for encryption. The main aim is to reduce the tedious complexity by avoiding the inverse of matrix at decryption time.

Anjali Patil and RajeshwariGoudar[5],[11] have proposed asymmetric key encryption algorithms such as DES, Triple DES, AES, Blowfish and asymmetric key encryption algorithms such as RSA, D-H, etc. Symmetric key encryption enhances vital security than asymmetric key encryption.Monika Agrawal and Pradeep mishra[6] ,[12]have proposed asymmetric key encryption algorithms such as DES, TRIPLE DES, AES, and Blowfish. Encryption algorithms indicate the supremacy of the Blowfish algorithm over DES, AES and Triple DES based on key size and security.Manali Vaidya, VaibhavBansod, MangeshManwar [7] have proposed a technique to encrypt the data using a key based upon Armstrong numbers. Central server system is utilized to protect intended Authentication between users. Two-way security is given to key as well as information. S.PavithraDeepa and S.Kannimuthu [8],[13] have proposed a technique that provides keen security with an increment in the key length of the Armstrong number. Utilization of three sets of keys named colors, an additional set of key values and Armstrong number wisely the data is transmitted securely and accessed only by authorized persons.S.Belose, M.Malekar, G.Dharmawat [9],[14]

January-February 2020
ISSN: 0193-4120 Page No. 15355 - 15360

have proposed a technique to encrypt the data using a key involving Armstrong numbers. Central server system is used to provide security which ensures over Authentication between users. Two-way security is given to key as well as information.

3.METHODOLOGY

RPK algorithm is an encryption algorithm which is used to encrypt the user's data. It is a symmetric encryption algorithm which uses the same key for both encryption and decryption.Keys of RPK are generated from a random prime sequence with the specified range.

3.1 KEY GENERATION AND EXCHANGE

It has been a practice to use the key in any cryptosystem, in this cryptographic algorithm the suitable prime number is selected as a key "K" where $1 \leq K \leq 13$. In order to use a symmetric cryptographic algorithm, it is necessary that the keys to be exchanged between the two parties where the encryption and decryption takes place. As the cipher we proposed is of symmetric kind, both sender and receiver will need to have a copy of the same key.

3.2 PROPOSED ENCRYPTION ALGORITHM

Encryption is the process of using an algorithm to transform the information as unreadable to avoid unauthorized access. This cryptographic method protects different kinds of sensitive data by encoding and transforming information into cipher text.

The following steps are depicted as encryption.

1. Consider the plaintext and write its corresponding ASCII value
2. Represent the above ASCII value in Binary Form
3. Count the total number of bits in above binary number
4. Divide the Binary bits into "K" number of chunks. (K is key selected as mentioned in key generation)
5. Represent the K value in its binary from and let it be P
6. Select the first bit in every chunk and consider it as Q
7. The resultant R is given as $R=P \oplus R$
8. Replace the first bit in each and every chunk with R and rotate the binary bits from left to right by one bit
9. Merge the rotated binary bits in sequential order and divide in to chunk of 8 bits
10. Convert the above 8 bit binary chunks into corresponding ASCII Code and write the ASCII character which is our resultant Ciphertext.

3.3 PROPOSED DECRYPTION ALGORITHM

The conversion of encrypted data into its original form is called Decryption. It is generally a reverse process of encryption. It decodes the encrypted information so that an authorized user can only decrypt the data because decryption requires a secret key or password.

1. Consider the Ciphertext and write its corresponding ASCII value
2. Represent the above ASCII value in Binary Form
3. Merge all the binary bits in sequential order
4. Divide the binary bits obtained in above step into chunks based on the key "K"
5. Rotate the bits in each chunk from right to left by one bit.
6. Represent the K value in its binary from and let it be P
7. Select the first bit in every chunk that is Q
8. Perform XOR operation between P and Q, assume result as $R=P \oplus Q$
9. Replace first bit in each and every chunk with the resultant R and merge the bits in Sequential order
10. Divide the binary bits into chunk of 8-bits and Convert the above 8 bit binary chunks into corresponding ASCII Code and write the ASCII character which is our resultant Cipher text.

3.4 IMPLEMENTATION OF CRYPTOGRAPHY ALGORITHM

Here we will implement an example with the help of above mentioned proposed encryption and decryption algorithms. Assuming that the random key is K=13

January-February 2020
ISSN: 0193-4120 Page No. 15355 - 15360

1) 3.4.1 ENCRYPTION

- Let us consider the following plain text from the user
- Plain Text: BHANU
- The ASCII Code(decimal numbers) of Plain Text is [66,72,65,78,85]
- The Binary bits of the ASCII Code is [01000010, 01001000, 01000001, 01001110,01010101]
- Calculating the total number of bits Number of Bytes=5 oNumber of Bits= 40
- K=13, the Random Prime number
- Dividing into Binary chunks of size 13

Chunk-1: Chunk-2: 0000100000101
.00001001001
Chunk-3: Chunk-4: 1
)11100101010

- convert the selected key K=13 into binary number (P = 1101)
  - Select the first decimal number in every chunk that is Q =0001
  - Performing XOR operation between P and Q that is R = 1100
  - Now replace the first decimals in every chunk with R then

Chunk-1: 0100001001001 Chunk-2: 0000100000101
Chunk-3: 0011100101010 Chunk-4: 1

  - Merging the Binary Chunks in sequential order and dividing them into 8-bit Binary Chunks [01000010, 01001000, 01000001, 01001110,01010101]
  - Converting the Binary Chunks into equivalent decimal numbers(ASCII Code) [66, 72, 65, 78, 85]
  - Converting the ASCII Code to obtain Plain Text Plain text : BHANU

II. SHANNON'S PROPERTY IN PROPOSED CRYPTOGRAPHIC ALGORITHM

Claude Shannon had proposed two properties namely "Confusion" and "Diffusion" in one of his reports "A Mathematical Theory of Cryptography". He suggested that any proposed cryptographic algorithm has to satisfy the properties mentioned. The detailed explanation and suitable justification of the above properties are depicted below. The algorithm ought to fulfil the Diffusion - Strict Plaintext Avalanche Criterion – SPAC i.e., with a fixed key and a minor change in the plaintext should result the huge changes in the cipher content The algorithm ought to fulfil the Confusion - Strict Key Avalanche Criterion – SKAC i.e., with a fixed plaintext and a minor change in the key should result the noteworthy changes in the cipher content

A. RESULTS AND DISCUSSIONS OF SPAC AND SKAC

The results depicted in tables 1 and 2 are evident that the proposed RPK is strictly following SPAC and SKAC respectively. Here in these results a noteworthy Avalanche Effect of minimum 65% has been observed in-order to ensure the security.

Table 1: Effect of SPAC-Diffusion

SPAC: Fixed Key and Changed Plaintext Fixed Key value K=13		
Case: 01	Plaintext (56 bits)	01000101010100110100010101011010000101001001
	Ciphertext (56 bits)	10001010101001101000011101101000000101010010010
	Number of bits changed	37
Case: 02	Plaintext (56 bits)	01000001010010110101001101001000010101000100000101010010001000001
	Ciphertext (56 bits)	10000010100101101010011011010000100000101010010010010011
	Number of bits changed	33
Case: 03	Plaintext (40 bits)	0101001101000001010001110100000010101

TEST Engineering & Management

January-February 2020
ISSN: 0193-4120 Page No. 15355 - 15360

		0010
	Ciphertext (40 bits)	101001101000 101010001110 110000101010 0101
	Number of bits changed	25
Case: 04	Plaintext (48 bits)	010100110100 100101001110 010001000100 100001010101
	Ciphertext (48 bits)	110100110100 110101001110 010001000100 100001010101
	Number of bits changed	29
Case: 05	Plaintext (56 bits)	010100110100 000101001110 010001000100 010101000101 0101000
	Ciphertext (56 bits)	101001101000 010100111001 100100010001 010100010101 0110001
	Number of bits changed	33
Case: 06	Plaintext (64 bits)	010100000101 001001000001 010100110100 000101001110 010011100100 0001
	Ciphertext (64 bits)	101000001010 010010000010 111001101000 001010011100 100111001000 0010
	Number of bits changed	35

III. COMPLEXITY ANALYSIS OF THE PROPOSED ALGORITHM

The time complexity nature of an algorithm implies the aggregate sum of time taken by it to run as a capacity thinking about the length of the input as 'n'. Big Oh is the most regularly utilized asymptotic documentation to speak to the time complexity nature of an algorithm, which prohibits the coefficients and lower order terms.For instance if the time taken by a different series of steps are $O(n^3)$,$O(n^2)$,$O(n)$, at that point the asymptotic time complexity is given as $O(n^3)$ which could be upper bound among all the three. Thus by observing the time complexities of the individual steps in proposed algorithm, the upper bound and lower bound of the complexity are given as O(N log N) and O(1) respectively.

Table 2: Effect of SKAC-Confusion

SKAC: Fixed Plain Text and Changed Key Fixed Plaintext "BHANU"		
Case: 01	Key	2
	Ciphertext	10000001100001 00100000101000 110110101110
	Number of bits changed	23
Case: 02	Key	3
	Ciphertext	10000000100100 10100000101001 100010111010
	Number of bits changed	24
Case: 03	Key	5
	Ciphertext	01000010010010 00010000010100 111001010101
	Number of bits changed	24
Case: 04	Key	7
	Ciphertext	10000100100100 00100000101001 110010001010
	Number of bits changed	23
Case: 05	Key	11
	Ciphertext	10000100101100 00100001101001 110000101010
	Number of bits changed	25
Case: 06	Key	13

January-February 2020
ISSN: 0193-4120 Page No. 15355 - 15360

	Ciphertext	10000100100110 00100000101101 110010101000
	Number of bits changed	21

IV. CONCLUSIONS AND FUTURE SCOPE

Data security is a chief aspect in current era of technological transactions. It has become a healthy practice of securing the data. In order to develop a low complex algorithm we proposed an algorithm in this research paper. The results depicted are evident that the Shannon's property holds good in this algorithm. The strength of this algorithm is analyzed over differential cryptanalysis ensuring that SPAC and SKAC are satisfied. Further the cryptosystem can be upgraded by altering the key range and utilizing some tangled activities in the encryption and decoding.

REFERENCES

1. P.Sri Ram Chandra,G.Venkateswara, G.V.Swamy, 'Ultramodern Encryption Standard Cryptosystem Using Prolic Series for secure data transmission'' ,International Journal of Latest Engineering Research and Applications(IJLERA)ISSN 2455-7137 Volume_02,Issue 11,November-2017,pp-29-35.
2. P. Sri Ram Chandra, G. Venkateswara, G .V.Swamy, "Modular Encryption Algorithm for Secure Data Transmission ", Int .J. Sc.Res. in Network security and Communication ,ISSN:2321-3256,volume 6,Issue-1,February 2018.
3. Visas 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.
4. Thangarasu.N, Arul Lawrence selvakumar,"Encryption Using Lester Hill Cipher Algorithm", international journal of innovation research in advanced engineering(IJIRAE) issue 12,vol 2(December 2015) .
5. Anjali patil, RajeshwariGoudar, "A Comparative Survey ofSymmetricEncryption Techniques for Wireless Devices", international journal of scientific and technology research volunteers 2,issue 8,pp.2058-2062, July 2013.
6. Monika Agrawal, Pradeep mishra,"A Comparative Survey on Symmetric key Encryption Techniques", international journal of engineering and technology(IJET)vol-4,no5,pp.877 -882,may 2012
7. Mrunali Vaidya, VaibhavBansod, MangeshManwar, "A Review On Cryptography Using Armstrong Numbers and Colors", international journal of computer science and mobile computing, vol. 3 issue. 10,october 2014,pg.926-931.
8. S.PavithraDeepa,S. Kannimuthu, V. Keerthika., "Security Using Colors and Armstrong Numbers", Proceedings of the National Conference on Innovations in Emerging Technology, 17 & 18 February, 2011.pp.157-160.
9. S. BELOSE ,M.MALEKAR, G.DHARMAWAT, "Data Security Using Armstrong Numbers", Interrnational journal of Emerging technology and engineering, vol 2 , issue 4,april 2012.
10. Michael Sipser , Introduction to the theory of Computation (Second Edition)
11. Estharakula, Suresh, and JMSV Ravi Kumar. "EBPH-MAC: Emergency Based Priority Hybrid Medium Access Control for Mobility Aware Cooperative WSN's In Indoor Industrial Monitoring." International Journal of Research 5.12 (2018): 1456-1465.
12. ESTHARAKULA S, KUMAR DJ. SECRBAC: Secure Data In The Clouds. International Journal of Research. 2018 May 1;5(15):95-106.
13. Kumar JM, Reddy MB, SreeRam N, Kumar IR. Reverse Engineering A Generic Software Exploration Environment Is Made Of Object Oriented Frame Work And Set Of Customizable Tools. International Journal of Advanced Research in Computer Science. 2011 Sep 1;2(5).
14. Kumar, J. M. S. V., et al. "System Testability Assessment and testing with Micro architectures." International Journal of Advanced Research in Computer Science 2.6 (2011).