IJSRA

International Journal of Science and Research Archive

eISSN: 2582-8185

Cross Ref DOI: 10.30574/ijsra

Journal homepage: https://ijsra.net/

(Review Article)

A novel package of key generation and integrity validation in symmetric key cryptography

Vinay S * and Kumar Siddamallappa U *

Department of studies in Computer Science, Davangere University, Davangere, India

International Journal of Science and Research Archive, 2023, 09(02), 997–1002

Publication history: Received on 08 June 2023; revised on 18 July 2023; accepted on 21 July 2023

Article DOI: https://doi.org/10.30574/ijsra.2023.9.2.0480

Abstract

In this paper we presents a new cryptography method on symmetric key Cryptography along with that it will ensure the integrity of the data during the transmission. Here encryption and decryption operation is performed on bit stream of data. It is suitable for any type of text files. This method of encryption is simple and powerful to secure data in network against passive attack like traffic analysis to provide data confidentiality. The Cryptography package deals with generating a simple encryption key by choosing a byte of data in the plaintext. By using that secure encryption key Plain text is converted to cipher text and in the destination Cipher text is converted to plain text by performing basic XOR and other operation. To ensure integrity of data available parity bit methods are applied.

Keywords: Encryption; Decryption; Block Cipher; Plain text; Cipher text; Bit stream; Parity bit; Integrity.

1. Introduction

The science of securing messages is called cryptography. Cryptanalysts will perform cryptanalysis and break the cipher text. The mathematical logic of cryptography and cryptanalysis is called as cryptology. Its practitioners are called as cryptologists, they are trained in mathematics. From past four decades, public academic research in cryptography and steganography has been increased. While classical cryptography techniques are being used by ordinary citizens [1].

The Encryption and the decryption are accomplished by using cryptographic methods parameterized by crypto keys .The original form of message that has to be sent is called as Plain Text denoted by *P* and message M. The data can be a stream of bits, text file, and stream of digital voice, video or image. In computer message (*M)* is simply a binary data. The encrypted data is called as the cipher text. (Denoted by *C*) and its a binary data, the size of this cipher text may be same size as *M* or it may be larger. The encryption function (*E*) operates on message (*M)* to produce Cipher text (*C)*. $E(M) = C$ *is the* Mathematical notation *,* The decryption function (*D)* operates on *Cipher text (C)* to produce Message *M*: Denoted as $D(C) = M$ *[2].*

A cryptographic algorithm is a Mathematical function used in encryption and decryption. The two types of cipher methods: Bit Stream method- where plain text is converted into cipher text by one bit at one time and another is Block Cipher method where plain text is divided into block of 8, 16, 32 or 64 bit block is and whole block converted at one time into cipher text. Stream ciphers convert plaintext to Cipher Text by one bit at a time. Many cipher methods are available , Substitution Cipher: Mono alphabetic Cipher, Vernam Cipher ,Transposition Cipher , Running key Cipher, etc. are the examples [3].There are two general categories for key-based Encryption: Symmetric Encryption which is also called Private key, where same key is used for both encryption and decryption. Asymmetric Encryption is one which uses two different keys - public key and private key. Public Key is used to encrypt the message, and private key used to decrypt it [3].Strength of the encryption depends on size of key. Increase in size of key increases the strength of

* Corresponding author: Vinay S. (Orcid Id: 0000-0002-2327-4915); Kumar Siddamallappa U. (Orcid Id: 0000-0002-1975-3868)

encryption. For an example if no. of bits is 32 then estimated time to crack the code is 8 min & if key size is 56 then it takes 285 years and 32 weeks.[2].

2. Methodology

Our new cryptography method consists of three concepts: Symmetric key Cryptography, Bit stream cipher method, Key Generation from Plain text and two dimensional parity bit method. We implements bit stream cipher method using XOR operation in slightly improved way. Here we select a byte in the plain text to generate Symmetric key which will be used in Cryptography process. This approach will provide two layer of security, Means that the key shared between the sender and the receiver is not the actual encryption/decryption key, it's just a numerical value that will be used for generating symmetric key. So, even if intruder knows the numerical key shared between two parties they are unaware of steps of generating the actual encryption/decryption key. Bit stream will be encrypted using XOR Logical operation with key and arranged in a matrix. Two dimensional parity bit method is applied to ensure integrity at the receiver side.

2.1. Sender side operations

2.1.1. Key Generation

In our new cipher method our algorithm takes P (plain text) as input and Pre negotiated key which directly represents the index value the character in plaintext which has to be used to generate symmetric key. This numerical integer value we denote as 'Nk'.which works as index value to select a byte of data in a plain text. In next step it reads the plaintext picks up the Nkth byte in the plain text(P) to generate a secure key. The selected byte from plain text(P) is converted it into its- 2's compliment. This converted byte becomes a Symmetric key for encryption/decryption. We call this key as secure secret key 'Ssk'.

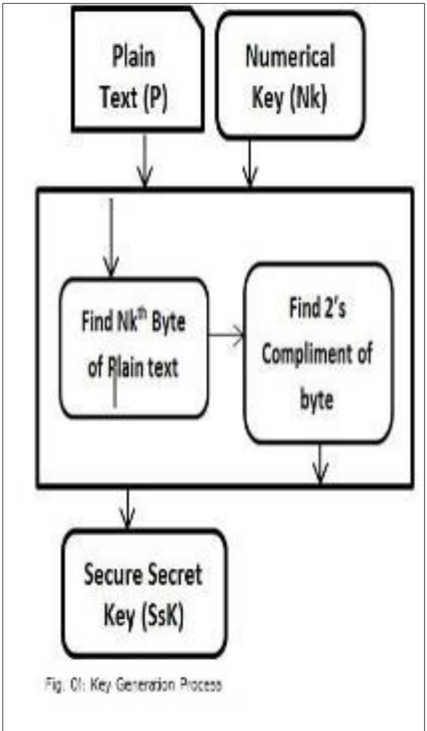
Plain Text (P)
Numerical Key (Nk)
Find Nkth Byte of Plain text
Find 2's Compliment of byte
Secure Secret Key (SsK)
Fig. 01: Key Generation Process

Figure 1 Key Generation Process

The numerical integer key (Nk) must be shared between communication parties directly or through a trusted third party by a secure electronic media. Here even if any intruder accesses this key during key exchange it is not so easy for them to decrypt cipher text, because they are not aware of the logic of generating Symmetric key which we call as Secure Secret Key (Ssk). So this will provides two level of security.

Fig. 1 shows the process of key generation.

Algorithm:

- Step 1: Read Plain text & Numerical Key.
- Step 2: Find Nkth byte in the plain text.
- Step 3: Find 2's Compliment of Nkth Byte. This will becalled as SsK(Secure Secret Key).
- Step 4: Forward this SsK key to Encryption algorithm.

2.1.2. Encryption

Encryption Algorithm comes to action after generating Secure Secret key –Ssk. Encryption Process consists of two Phases. In phase-1 XOR operation is performed between all bits of Plain Text and Secure Secret Key- Ssk, Here the bytes which are same as of Nkth byte in Plain Text are which is used for generating Secure Secret key are excluded from XOR Operation. In the Phase-2 the output of phase one is grouped in 7X7 array and then transposition is performed on both column and rows for Tk times. Here Tk =Nk and if Nk > 7 then Tk= Nk Mod 6. The result of Phase-2 is the Cipher text C.

Figure 2 shows the process of Encryption.

Algorithm:

- Step 1: Read Plain Text (P) & Secure Secret Key (SsK).
- Step 2: Perform XOR operation between each bit of P and SsK. (Except with Plaintext byte which is same as SsK).
- Step 3: Arrange bits in 7X7 arrays which are generated In the step -2.
- Step 4: Perform Transposition for 'Tk' times on both Row & Column level. Resultant will be the Cipher Text
- Step 5: Apply Two Dimensional Parity bit Method on each Array of Cipher text
- Step 6: Transmit this cipher text to destination.

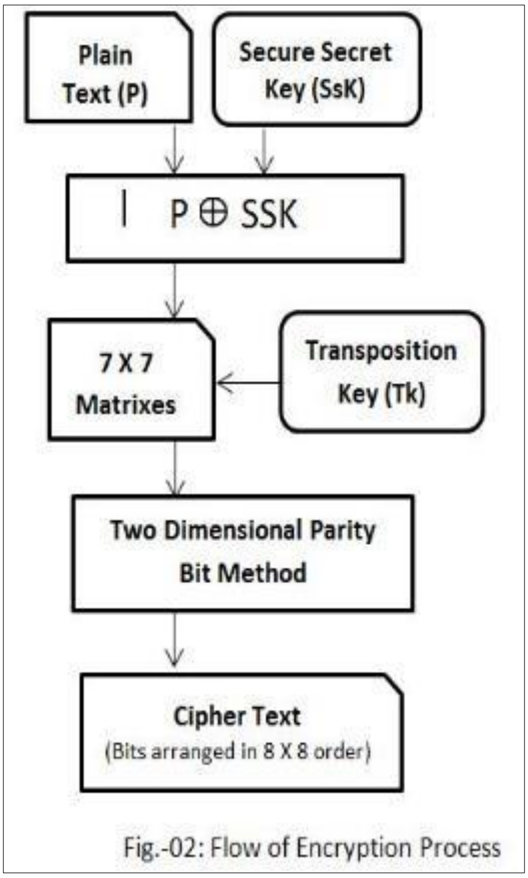
Plain Text (P)
Secure Secret Key (SsK)
| P ⊕ SSK
7 X 7 Matrixes
Transposition Key (Tk)
Two Dimensional Parity Bit Method
Cipher Text
(Bits arranged in 8 X 8 order)
Fig.-02: Flow of Encryption Process

Figure 2 The process of Encryption

List of Short forms:

- PLAIN TEXT - P,
- CIPHER TEXT - C,
- ENCRYPTION PROCESS -E
- NUMERICAL KEY- Nk
- SYMMETRIC KEY –SsK
- TRANSPOSITION KEY (Tk) = Nk
- Tk = Nk Mod 6 (if Nk > 7)

2.2. Receiver Side operations

2.2.1. Data integrity Validation

This process uses the logic of Two Dimensional Parity bit method. The Cipher text bit stream received from the sender will be grouped into 8X8 arrays and each row and column is examined for even number of 0's and 1's. if each row and column consists of even no of 1's and 0's then it will ensures that the data is not being modified by any intruder or by any technical errors during transmission. If it doesn't match the condition then, it will be considered that it will consider that the received data being modified or compromised with data integrity. Then the data will be discarded and intimated to sender about the action.

First phase in the figure-3: Receiver side operations will shows the working of integrity validation process.

Algorithm:

- Step 1: Receive Cipher text(C).
- Step 2: Arrange bit stream in 8X8 arrays.
- Step 3: Check for even No. of 0's and 1's on each Rowand Column of each array.
- Step 4: If step 3 result is true, then forward this bit streamto Decryption Process.
- Step 5: If step-3 results is false, then discard this bit stream and send notification to sender.

2.2.2. Key extraction

Here algorithm takes cipher text as input. In the first step it arranges the cipher text bit stream into 8x8 order Checks for the integrity violation by counting no. of one's and zero's as per the logic of Two Dimensional Parity Bit method. Then it will remove the parity bits. Then the bits are arranged in 7X7 arrays order. Transposition of array is performed using Nk key. In second step it reads the Cipher Text bit format and picks up the Nkth byte from the cipher text and generates the Ssk key by calculating its 2's compliment. Here the 'Nk' is the pre negotiated key between sender and receiver.

Second phase in the figure-3: Receiver side operations will shows the working of Key Extraction Process.

Algorithm

- Step 1: Remove 2D parity bits from 8x8 array's it willCreate 7x7 arrays.
- Step 2: Transpose these 7X7 arrays by shifting rows andarrays to' Tk' times.
- Step 3: Find the Nkth value in the cipher text and GenerateSsK key.

2.2.3. Decryption

This process is similar to the Encryption process. After generating Ssk a Secure Secret Key XOR operation will be performed between the bit stream of Cipher Text and Secure Secret Key- SsK, except the bytes which are same as the Nkth byte in Cipher Text.

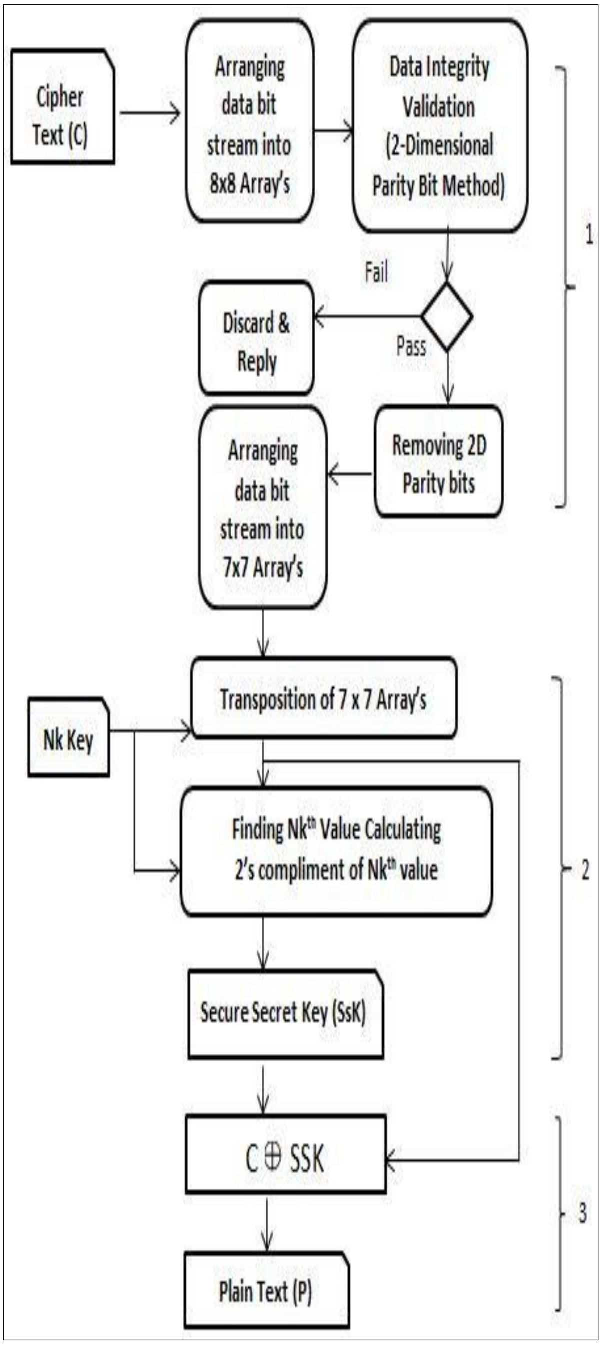
Cipher Text (C)
Arranging data bit stream into 8x8 Array's
Data Integrity Validation (2-Dimensional Parity Bit Method)
1
Fail
Discard & Reply
Pass
Removing 2D Parity bits
Arranging data bit stream into 7x7 Array's
Nk Key
Transposition of 7 x 7 Array's
Finding Nk^th Value Calculating 2's compliment of Nk^th value
2
Secure Secret Key (SsK)
C ⊕ SSK
3
Plain Text (P)

Figure 3 Receiver side operations

3. Conclusion

This new approach of cryptography package is best suitable for small institutions, organizations and offices for daily communication confidential and sensitive files of office. Important Documents can be encrypted by applying this method then it can be sent via e-mail fax or any electronic media. This new technique described in our paper might not be similar to well-known highly standardized security application but its simplicity proves that, it can be developed as application to satisfy the needs of data security in small organizations without need of purchasing expensive software in the market. As an opportunity to enhance this method the encryption key size can be increased and no. of basic operations like transposition and substitution can be increased. Existing efficient methods like diffe helman key exchange algorithm can be adopted to share the 'Nk'key which we used in this new algorithm.

The major highlights of this method is that, first it gives additional security for symmetric key by enforcing more than one step of procedure to generate it. The second advantage is concerned; it ensures integrity of data by adoption two dimensional parity bit methods, A well-known method in test the integrity of data. It builds confidence in between the communication parties in respect to data verification.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] "Crypto Matrix Symmetric Multilevel Cipher (CMSML)", Vinay S, Naveen Kumar P SISSN: 2320-9801 (IJIRCCE), Vol.5, Issue 2, April 2017.

[2] "A Plain Key Compliment XOR Cipher Method". Vinay S, Shivamurthaiah M,ISBN: 978-81-928203-0-9.

[3] S. Chatham, Jyotsna, J. Kumar, and A. Doegar, "Multiple layer Text security using Variable block size Cryptography and Image Steganography," in 3rd IEEE International Conference on Computational Intelligence and Communication Technology, 2017, pp. 1–7. https://doi.org/10.1109/CIACT.2017.7977303

[4] D. Seth, L. Ramanathan, and A. Pandey, "Security Enhancement: Combining Cryptography and Steganography," Int. J. Computer. Appl., vol. 9, no. 11, pp. 3–6, 2010.https://doi.org/10.5120/1433-1932

[5] S. Singh and A. Singh, "An Information Security Technique Using DES-RSA Hybrid and LSB," Int. J. Emerging. Technol. Computer. Appl. Sci., vol. 14, no. 355, pp. 187–192, 2013.

[6] "Edge Quick String Matching (EQ-SM)", Anusha jajur J, Vinay S, Shivamurthaiah M. ISBN: 978-81-207-97147.

[7] "CAL3Key Secure Key Exchange & Symmetric Encryption with Integrity Check (C3K-SE)." Vinay S, Shivamurthaiah M, ISBN: 978-81-207-97147.

[8] "A Plain Key Compliment XOR Cipher Method". Vinay S, Shivamurthaiah M,ISBN: 978-81-928203-0-9.

[9] "Private C-Multi key S Matrix Block Cipher". Vinay S, Shivamurthaiah M International Conference on Information & Communication Technology. May 5th - 6th 2014. ISBN: 978-81-926416-1-4.

[10] "Multi-Key XOR Cipher with Parity Check (MX-PC)". Vinay S, Shivamurthaiah M National Conference on Information Tech. for Sustainable Future (NCITSF'14)on 9th may 2014.

[11] S. Goel, S. Gupta, and N. Kaushik, "Image Steganography -- Least Significant Bit with Multiple Progressions," Proceedings of 3rd International Conference on Frontiers of Intelligent Computing- Theory and Applications (FICTA) 2014, 2015, pp. 105–112.

[12] Preneel, B. (2010, September). Cryptography for network security: failures, successes and challenges. International Conference on Mathematical Methods, Models and Arch. for Computer Network Security (pp. 36-54).Springer , Berlin , Heidelberg.

[13] Kumari, S. (2017). A research Paper on Cryptography Encryption and Compression Techniques. International Journal of Engineering And Computer Science, 6(4).

[14] Bhatia, P., & Sumbaly, R. (2014). Framework for wireless network security using quantum cryptography. arXiv preprint arXiv:1412.2495.

[15] Tayal, S., Gupta, N., Gupta, P., Goyal, D., & Goyal, M. (2017). A Review paper on Network Security and Cryptography. Advances in Computational Sciences and Technology, 10(5), 763- 770.

[16] Panda, M. (2014). Security in wireless sensor networks using cryptographic techniques. American Journal of Engineering Research (AJER), 3(01), 50-56.

[17] Dhamdhere Shubhangi, T., & Gumaste, S. V. Security in Wireless Sensor Network Using Cryptographic Techniques.

[18] Kumar, S. N. (2015). Review on network security and cryptography. International Transaction of Electrical and Computer Engineers System, 3(1), 1-11.

[19] Kaur, S., Kaur, R., & Raina, C. K. (2017). Review on Network Security and Cryptography.

[20] Duong, T., & Rizzo, J. (2011, May). Cryptography in the web: The case of cryptographic design flaws in asp. net. In Security and Privacy (SP), 2011 IEEE Symposium on (pp. 481- 489). IEEE.

[21] Stallings, W. (2006). Cryptography and Network Security, 4/E. Pearson Education India