International Journal of Engineering & Technology, 7 (2) (2018) 880-883

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET
doi: 10.14419/ijet.v7i2.12315
Research paper

An integrated approach for enhancing data security

G. Manikandan [1] *, R. JeevaDharani [1], R.Maya [1]

[1] School of Computing, SASTRA Deemed University, Thanjavur, India
**Corresponding author E-mail: manikandan@it.sastra.edu*

Abstract

Information security is a key challenge in today's information era where a huge volume of data is being generated on the internet as a result of the online transaction. This data needs to be protected from the unauthorized users on the web. Cryptography is used to ensure the confidentiality and integrity of data in the virtual world. The strength of the cryptographic algorithm relies on the complexity involved in retrieving the original content from the unintelligible information. The system proposed in this paper focuses on the use of a different mechanism to increase complexity involved in the cryptanalysis. Different cryptographic techniques are used to create a modified plain text and modified key. The newly generated key is used to encrypt the modified plaintext to generate the ciphertext. From the security analysis, it is evident that the time taken for cryptanalysis by the proposed scheme is more when compared with the existing systems.

Keywords: *Key Strength; Security; Atbash Cipher; Rail Fence Cipher; Playfair Cipher; AES Algorithm.*

1. Introduction

Data security is the most important problem faced by the millions of users on the internet. The data must be hidden from intruders to ensure data security and it must be made available only to the authorized users. Cryptography is one of the most prevalent technique used in implementing various security requirements like availability and integrity. The principal objective of cryptography is to generate unintelligible information from the original data. Modern cryptographic algorithms make use of complex procedures to create a ciphertext.

A cryptographic system can be classified based on the use of an operation to generate a ciphertext and the keys used for this purpose. Cryptosystems are classified as symmetric key cryptosystem and public-key cryptosystem. In a symmetric key cryptosystem, the same key is used for encryption and decryption whereas in public-key cryptosystem two different keys namely public key is used for encryption and the private key is used for decryption.

Ideally, the requirement of the user is a cost-effective cryptographic algorithm with good performance. However, no such algorithm exists in reality but there are several cryptographic algorithms with a tradeoff between cost and performance.

The primary objective in designing an encryption algorithm is to translate an original message into a nonreadable text to ensure confidentiality during transmission over the network.

A large number of cryptographic algorithms have been developed which aims at providing better security over the other. Classification of various cryptographic techniques is shown in Fig.1. In this paper, the proposed method focuses on the integration of cryptographic techniques to generate the modified plain text and modified key.

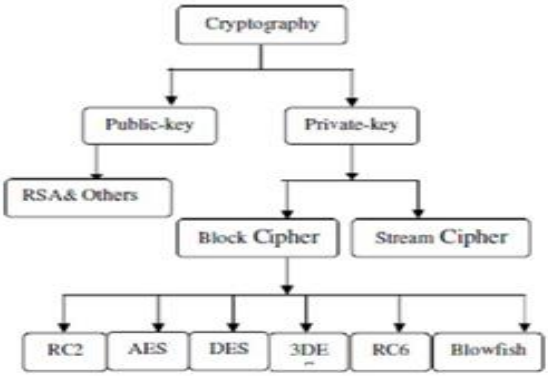


Fig. 1: Classification of Cryptographic Techniques.

2. Literature survey

Encryption algorithms namely, Blowfish, RC2, RC6, AES, DES, and 3DES were evaluated. These algorithms were compared using parameters such as Size of data blocks, Power Consumption, Key size, and speed. [3].

In order to increase the efficiency, the authors have proposed an architecture to perform transformation by integrating Mixcolumn and pre-process InvMixcolumn. [4].

A Hardware implementation of the AES was used for Encryption and Decryption. [5].

A framework containing four different modules namely Public key-Public key technique, Public key-Private key technique, Private Key-Public key technique and Private Key-Private key technique was used for data security. [6].

For a given decimal number Turing-machine is used to generate the equivalent binary number. This approach is used in cryptography to enhance the data security. [7].

Copyright © 2018 G. Manikandan et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

AES and Blowfish are two symmetric cryptographic algorithms used to enhance data security. Encryption and decryption are done with different file types. [8].
A new model integrating AES and DES was proposed for security enhancement [9]. As a result of more number of computations, this model provides better nonlinearity than the original AES.
Cryptography and Steganography are combined to achieve data security enhancement [10]. The original plain test is converted into ciphertext using a well defined cryptographic algorithm and the resultant ciphertext is embedded in an image. The stego image is sent to the receiver over a public network.
In [11], an integrated approach for encryption and decryption using Playfair cipher, Polybius square, and Blum-Blum sub generator techniques was proposed. The limitation of this work is that the continuous re-encryption results in increased complexity.
The concept of involutory matrices is used to generate the ciphertext(C) and plain text (P) using the formulas C = (AP+B) mod N and P = (A(C-B)) mod N, where A and B are the involutory matrices [12].
Manikandan et al. [13] have proposed a method to increase the key strength based on Huffman Tree approach and proved that their model increases the difficulty for the intruders to decipher the plain text.
An integrated approach to a hybrid model involving AES and DES is used [14]. As a result of more number of computations in the proposed model, the encryption and decryption process takes more time than their individual counterpart.
Cryptography and Steganography are combined to achieve data security enhancement [15]. The ciphertext is obtained from the original plaintext using cryptographic techniques and the resultant ciphertext is embedded in an image. The stego image is sent to the receiver over a public network. It is also proved that the PSNR value lies within the acceptable level for various data payload sizes.

3. Proposed system

The proposed system mainly focuses on the use of modified plain text and modified key. The AES algorithm is used for demonstrating the proposed system. The plain text is modified using Atbash cipher and the key is modified using the Rail fence cipher to create modified plain text and key. The modified plain text is again encrypted using Playfair Cipher. The output of Playfair cipher is given as input to the AES algorithm which generates the ciphertext using the modified key.

3.1. Encryption

The encryption technique follows the steps as shown in the flow diagram Fig.2. The key and the plaintext are modified separately and then given as input to the actual encryption process. The key is modified using Railfence Cipher and plaintext is modified using Atbash cipher. Encryption is done using Playfair cipher. The output is fed into AES algorithm to get the final ciphertext.

3.2. Decryption

The steps involved in the Decryption process of the proposed methodology follows the flow diagram shown in Fig.2. The ciphertext obtained as a result of encryption is fed into AES algorithm. The output generated by the AES is given to Playfair cipher that on further decryption gives the modified plaintext and modified the key. The original plaintext and key are obtained by decrypting the modified plaintext and modified key using Atbash Cipher and Railfence Cipher.

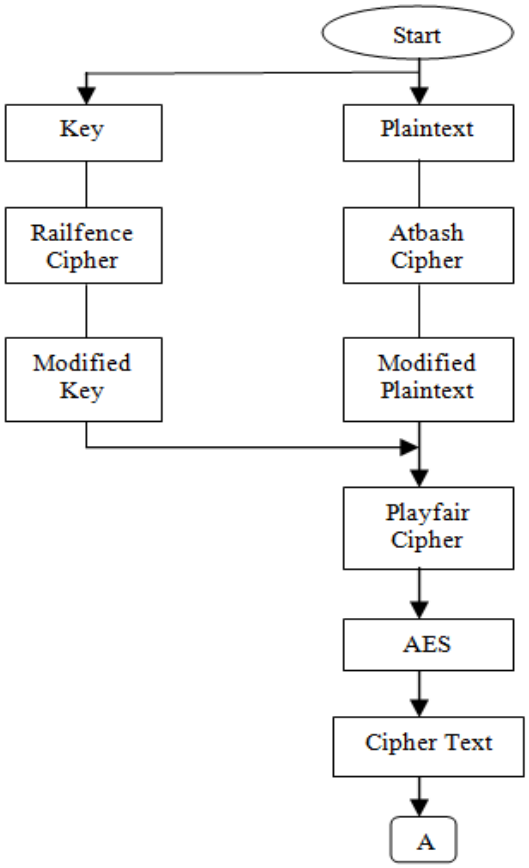


Fig. 2: Steps in the Encryption process.

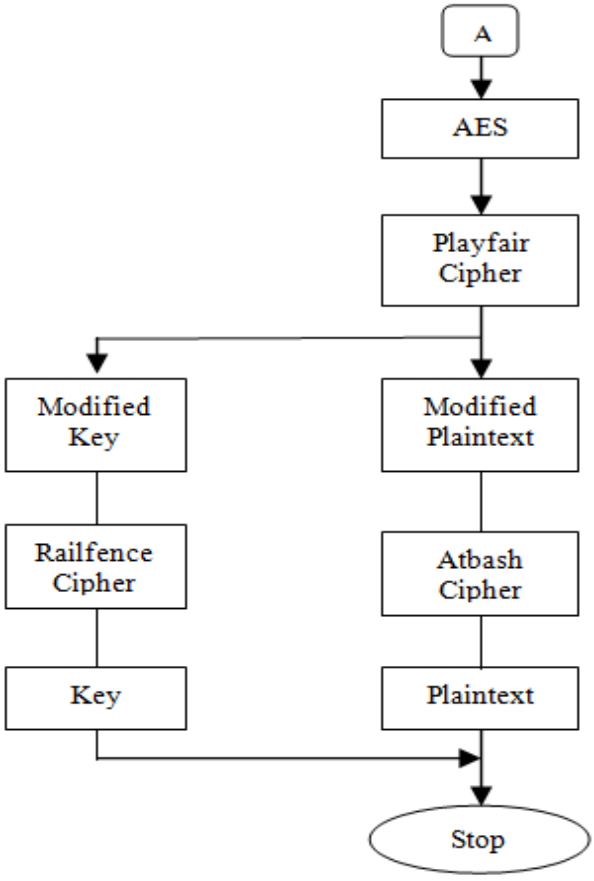


Fig. 3: Steps in the Decryption Process.

4. Case study

The proposed outlook is executed using Java programming language and the outcome is tested using a Corei3 processor with 4GB RAM with Windows 8 operating system. By the exploratory results, the encryption and decryption process with modified plain text and modified key involving Railfence Cipher, Atbash cipher and Playfair cipher methods will provide foremost results for effective data transmission and advancement in data security. The working of the proposed system is explained in the following steps:

1) Let the message be 'JEEVADHARANI' as shown in Fig.4

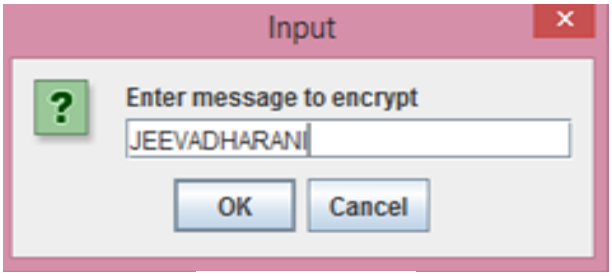


Fig. 4: Original Message.

2) The output obtained after applying the Playfair Cipher in Fig.5.

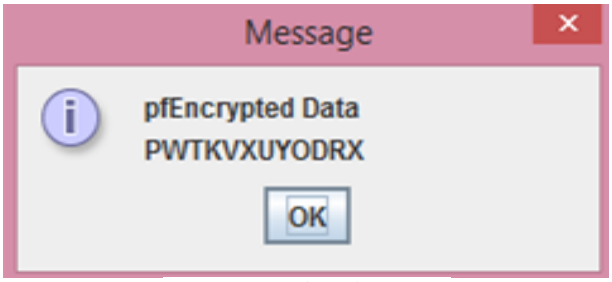


Fig. 5: Output of Playfair Cipher.

3) The output of the Playfair cipher is given as input to the AES algorithm and the ciphertext generated by this algorithm is shown in Fig.6.



Fig. 6: Cipher Text.

4) The output of each step in the decryption side to retrieve the original text from the Cipher text is shown in Fig. 7, Fig.8 and Fig.9

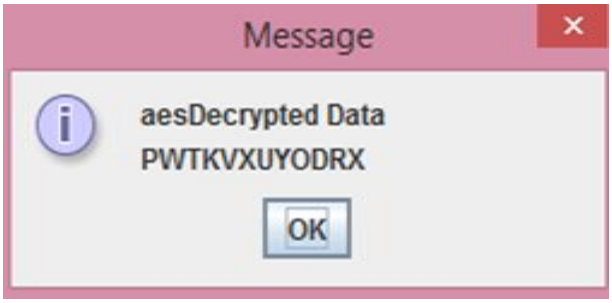


Fig. 7: Output of AES Algorithm.

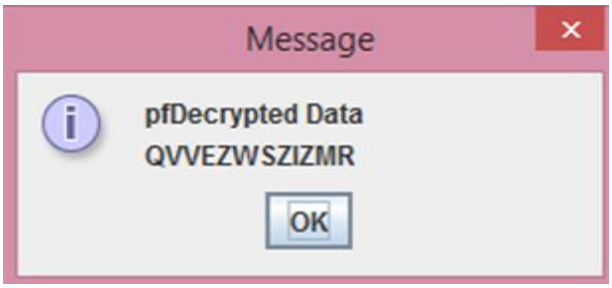


Fig. 8: Decryption Output of Playfair Cipher.

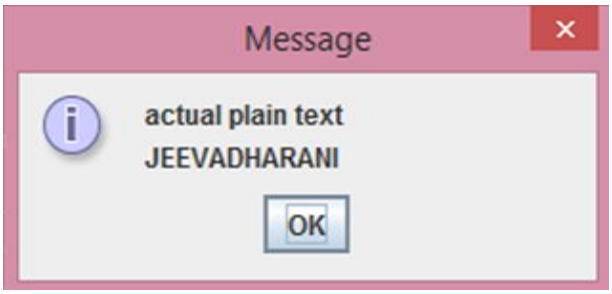


Fig. 9: Retrieved Plaintext.

5. Conclusion

This paper uses an integrated approach for data security enhancement. The novelty of the system is that the original plaintext is modified using Atbash Cipher and the key is modified using Railfence Cipher. The modified plain text and the modified key are fed as input to the AES algorithm. The encrypted ciphertext is the input to Decryption algorithm to obtain the modified plain text and modified key. Similarly, the modified plaintext is converted into plain text by decrypting it using Atbash cipher and original key is obtained by decrypting it using Railfence cipher.This approach can be extended in future with different cryptographic algorithms for generating the modified plain text and modified key.

References

[1] William Stallings, Cryptography, and Network Security, Wiley, 1995.
[2] Bruce Schiner, Applied Cryptography, John Wiley, 1996.
[3] SachinSharma, JeevanSingh, Bisht, "Performance Analysis of Data Encryption Algorithms", International Journal of Scientific Research in Network Security and Communication, pp.1-5, 2015.
[4] Yu-Jung Huang, Yang-Shih Lin, Kuang-Yu Hung, Kuo-Chen Lin, "Efficient Implementation of AES IP", IEEE Asia Pacific Conference on Circuits and Systems, 2006 https://doi.org/10.1109/APCCAS.2006.342467.
[5] Subashri T, Aruna chalam R, Gokul Vinoth Kumar B, Vaidehi V, "Pipelining Architecture of AES Encryption and Key Generation with Search-Based Memory", International Conference on Network Security and Applications. Pp.224-31, 2010.
[6] Natasha Saini, Nitin Pandey, Ajeet Pal Singh, "Enhancement of Security Using Cryptographic Techniques", 4th International Conference on Reliability, Infocom Technologies and Optimization 2015 https://doi.org/10.1109/ICRITO.2015.7359224.
[7] Himanshu Tripathi, Bramah Hazela Data, "Security Enhancement Through Number System", Second International Conference on Computational Intelligence & Communication Technology,pp.632-37, 2016.
[8] Shaikh Ammarah P, Vikas Kaul and S K Narayankhedkar," Security Enhancement Algorithm for Data Transmission using Elliptic Curve Diffie - Hellman Key Exchange", International Conference & workshop on Advanced Computing, pp 10-16, 2014.
[9] Jigar Chauhan, Neekhil Dedhia, Bhagyashri Kulkarni," Enhancing Data Security by using Hybrid Cryptographic Algorithm", International Journal of Engineering Science and Innovative Technology, pp.221-28, 2013.
[10] T. M. Sadikot, Dr. D. G. Kamdar," Data Security Enhancement with Crystography – A Combination of Cryptography and Ste-

ganography", International Journal of DARSHAN Institute on Engineering Research & Emerging Technologies, pp.1-6, 2015.
[11] Chandan Kumar, Sandip Dutta, Soubhik Chakraborty, "A Hybrid Polybius-Playfair Music Cipher", International Journal of Multimedia and Ubiquitous Engineering,pp.187-98, 2015.
[12] Aruna Varanasi, V.U.K.Sastry, and S.Udaya Kumar, "A Modern advanced hill cipher involving a pair of keys, modular arithmetic addition, and substitution", Journal of Global Research in Computer Science, pp.52-57, 2011.
[13] G.Manikandan, S.PrasannaVenkatesan, S.Srividhya, Nooka Saikumar, "Generating Strong Keys Using Modified Huffman Tree Approach", IEEE International Conference on Circuit, Power and Computing Technologies, 2016.
[14] D. Lin, P. Dunphy, P. Olivier, J. Yan, "Graphical Passwords & Qualitative Spatial Relations", Proceedings of the 3rd Symposium, On Usable Privacy and Security, Pittsburgh, USA, pp. 161-62, 2007. https://doi.org/10.1145/1280680.1280708.
[15] Manhas, Jatinder, "Initial framework for website design and development", International Journal of Information Technology, pp.363-75. 2017.