International Journal of Pure and Applied Mathematics
Volume 119 No. 12 2018, 13317-13324
ISSN: 1314-3395 (on-line version)
url: http://www.ijpam.eu
Special Issue

ijpam.eu

A Modified Polybius Square Based Approach for Enhancing Data Security

G.Manikandan*, P.Rajendiran, R.Balakrishnan, S.Thangaselvan
School of Computing, SASTRA Deemed University, Thanjavur, India
*Corresponding Author

Abstract:

Digital communication is the prominent technique used by various organizations for information exchange. It replaces the traditional methods with the help of internet and its related technologies. There is a chance to retrieve the contents of the transmitted message from the unsecure communication medium. The biggest challenge is to deploy a suitable mechanism for secure communication. Cryptography plays a dominant role in the information security domain. This paper proposes a modified Polybius square based approach for efficient key generation. New key is obtained from the original key by performing three different operations on modified Polybius square namely Square ring rotation, Square reversal and Transpose. From the security analysis it can be inferred that the proposed approach generates an efficient key.

Index Terms —Security, Encryption, Decryption, Plain Text, Cipher Text, Key

INTRODUCTION:

In the modern world, every organization uses the internet as the primary communication medium. Internet provides a platform to exchange the information in a short span of time. Information security is one of the critical issues to be addressed in the communication system. Ensuring data security is the biggest challenge in the current digital world. Right from the age of Julius Caesar, various techniques have been used to defend the data from the intruders. To protect the private contents of the message from the unauthorized users, two most popular data hiding techniques namely cryptography and steganography are used.

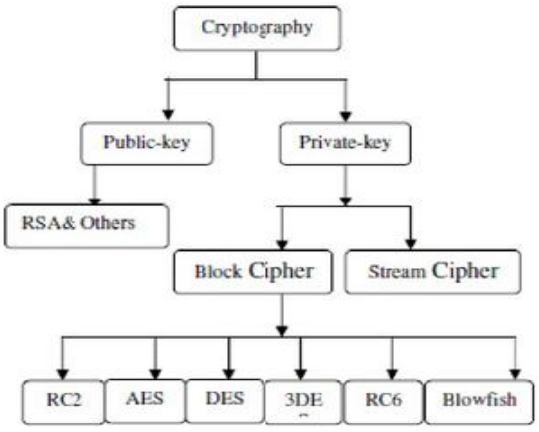

Figure.1 Classification of Cryptographic Techniques.

Steganography deals with message hiding. The basic objective of any steganographic algorithm is to hide a given message in another cover file like image, audio and video. The concept of "bit stuffing" is used by most steganographic algorithms to replace the selected bits in the cover file with the bits of the original message. The stego object created as part of the embedding process resembles exactly like an original object [13-24]. The advantage of this approach is that, the original message is embedded as it is, without any modification. The main disadvantage of this approach is that, it requires large cover files for the messages with larger size [25-37].

Fig.1 shows the Classification of various cryptographic techniques. Cryptography applies scrambling mechanism to convert the message into an unintelligible form. This scrambling process is done with the help of an algorithm and a key value. Based on the number of keys used the cryptographic algorithms were classified as symmetric key algorithm and asymmetric key algorithm. In the case of symmetric key algorithms, the same key is used by the communicating parties for the purpose of encryption and decryption. Two keys namely public key and private key is used in the asymmetric category. The message is encrypted using the receiver's public key and decrypted using the private key. From the above discussion it can be observed that the strength of the cryptographic algorithm relies on the keys used. In this paper, the proposed method focuses on the usage of modified Polybius square for generating an efficient key. The steps of the proposed method are explained in the next section.

PROPOSED SYSTEM

The data security is improved by using the proposed method. Initially, the key is obtained from the user and then modified using the modified Polybius square. The modified Polybius square used here is a 6x6 matrix consisting of the elements 'a' to 'z' and 0 to 9. To generate the new key, the content of the modified Polybius square is transformed in three different ways namely ring rotation, reversal of rows and transpose. The order of steps depends upon the sum of the ASCII values of the given key. Polybius square ring rotation is the process of rotating the given matrix layer by layer according to the sum of the ASCII values. The number of rotations of each ring is equal to the ASCII sum modulo length of the corresponding ring. Polybius square reversal of rows is the process of reversing each row of the given matrix. Transpose of the Polybius square is the process of transposing of the given Polybius matrix. AES algorithm is used for demonstration purpose. The execution time is computed using the original and the new key.

Table 1 – Modified Polybius square

0	1	2	3	4	5
6	7	8	9	a	b
c	d	e	f	g	h
i	j	k	l	m	n
o	p	q	r	s	t
u	v	w	x	y	z

Table 2 – Polybius Square after row reversal

5	4	3	2	1	0
b	a	9	8	7	6
h	g	f	e	d	c
n	m	l	k	j	i
t	s	r	q	p	o
z	y	x	w	v	u

Table 3 – Polybius Square after Transpose

5	b	h	n	t	z
4	b	g	m	s	y
3	9	f	l	r	x
2	8	e	k	q	w
1	7	d	j	p	v
0	6	c	i	o	u

Table 4 – Polybius Square after ring rotation

y	x	w	v	u	o
z	p	j	d	7	i
t	q	k	e	8	c
n	r	l	f	9	6
h	s	m	g	a	0
b	5	4	3	2	1

After applying the steps in the proposed approach, a new Polybius square is obtained. The new key is computed by taking the position of characters in the key from the new Polybius square and retrieving the corresponding character in that position from the original Polybius square. For example, if the original key is 'abc' and the position occupied by the 'a' in the new matrix is (2,2) the element from the original matrix which is present in (2,2) is taken as the first letter of the new key. The similar process is followed for the entire key. Now the modified key is given to AES algorithm along with the plain text for encryption. For decryption, the receiver obtains the modified key by using the same process followed by the sender. This key is then used to obtain the plain text from the cipher text.

Let us assume key="sastra", the ASCII values of s=115,a=97,t=116,r=114 and totally the sum amounts to 654.So if we perform the modulo operation on the sum, then 654 modulo 6 would be equal to 0. So we have to perform the operations Polybius reversal of rows, Polybius square transpose and Polybius square ring rotation in the same order. The Table-1 shows Initial Polybius square. The result of the reversal of rows is in Table-2 and the result of ring rotation is in Table-3.Here in the process of ring rotation, the rotation of outermost ring is 14 (654%20=14), the second outermost ring rotation is 6 (654%12=6) and the inner ring is 2(654%4=2). The character 's' occupies the fifth row and second column (5,2) in the matrix as given in Table 4 so after completing all the operations, the character 's' is replaced with 'p' since Table-1 contains p in the fifth-row second column. Similarly, the letters 'a', 't' and 'r' are replaced by c and j respectively. Finally, 'sastra' will be modified into 'pspcjs'

SECURITY ANALYSIS:

In the proposed methodology the sender gives the plain text and the key to the AES for encryption. The key is then modified by using the modified Polybius square and the original text is encrypted using the modified key. The resultant cipher text is transmitted to the receiver. The receiver will get the encrypted text and he will decrypt the text by using the modified key.

The proposed scheme is implemented by using the Python programming language and the outcome is tested using a core i5 processor with 4GB RAM and windows 7 operating system. In the brute force attack, the analysis depends upon the key size .If we take the key size to be 256 bits then the time required to find the plaintext with one key value is 10^{-7} seconds.

So the time required for execution of the cipher with all possible keys will be

$$\frac{10^{76}\times 10^{-7}}{365\times 24\times 60\times 60} = 3.17\times\ 10^{61} \text{ years} \qquad 1.1$$

As the total set of possible keys is large in number it is impossible to break the cipher text. The relation between the original key and the modified key is given by

Modified key=C1 (C2 (C3 (Original key))) 1.2

Where, the operations C1, C2 and C3 can be in any order. In the above equation C1, C2, C3 represents Square ring rotation, Square reversal and Transpose.

CONCLUSION:

This paper introduces a different approach to increase the data security. To generate a modified key, the original key is modified by using a modified Polybius square algorithm. The resultant modified key is used for the encryption and decryption algorithm. From the security analysis section, it can be inferred that the time complexity for cracking the key is high. The intricacy involved in the new key generation mechanism makes it difficult for the intruder to get the modified key. In future, this approach can be extended with a different Polybius square size.

REFERENCES

[1] Chandan Kumar, Sandip Dutta, Soubik Chakraborthy , A Hybrid Polybius-Playfair Music Cipher, International Journal of Multimedia and Ubiquitous Engineering,2015. 8, pp.187-198.

[2] Dr.V.Vaithiyanathan, G.Manikandan, G.Krishnan. A Novel Approach to the Performance and Security Enhancement Using Blowfish Algorithm. International Journal of Advanced Research in Computer Science. 2010. 1; pp.451-454.

[3] Dr.N.Sairam, G.Manikandan, G.Krishnan. A Novel Approach for Data Security Enhancement Using Multi Level Encryption Scheme. International Journal of Computer Science andInformation Technologies. 2011. 2; pp.469-473.

[4] G.Manikandan, R.Manikandan, P.Rajendiran, G.Krishnan, G.Sundarganesh. An Integrated Block and Stream Cipher Approach for Key Enhancement. Journal of Theoretical and applied information Technology. 2011. 28; pp.83-87.

[5] G.Manikandan, G.Krishnan, Dr.N.Sairam. A Unified Block and Stream Cipher Based File Encryption. Journal of Global Research in Computer Science. 2011. 2; pp.53-57.

[6] G.Manikandan, M.Kamarasan, P.Rajendiran, R.Manikandan. A Hybrid Approach for Security Enhancement by modified Crypto- Stegno scheme in European. Journal of Scientific Research. 2011.60; pp.224 – 230.

[7] G.Manikandan, P.Rajendiran, K.Chakarapani, G.Krishnan, G.SundarGanesh. A Modified Crypto Scheme for Enhancing Data Security. Journal of Theoretical and applied information Technology. 2012. 35; pp.149-154.

[8] G.Manikandan, N.Sairam, M.Kamarasan. A New Approach for Improving Data Security Using Iterative Blowfish Algorithm. Journal of Applied Sciences, Engineering and Technology. 2012.4; pp.603-607.

[9] G.Manikandan, N.Sairam, M.Kamarasan. A Hybrid Approach for Security Enhancement by Compressed Crypto-Stegno Scheme. Journal of Applied Sciences, Engineering and Technology. 2012. 4; pp.608-614.

[10] S.Karthikeyan, N.Sairam, G.Manikandan, J.Sivaguru. AParallel Approach for Improving Data Security. Journal of Theoretical and Applied Information Technology. 2012. 39; pp. 119-125.

[11] S.Karthikeyan, N.Sairam, G.Manikandan. A New Approach for Enhancing Data Security Using Parallel Processing. Advances in Natural and Applied Sciences. 2012. 6; pp.696-703.

[12] G.Manikandan,R.DalhousePrabu, P.SravanKumar, M.SudhakarRaj, S. Venkatakrishnan. Rendering A Fortify Key to Enhance the Security of Cryptographic Algorithms. International Journal of Applied Engineering Research. 2014. 9; pp.1987-1955.

[13] Logesh, R., Subramaniyaswamy, V., Vijayakumar, V., Gao, X. Z., & Indragandhi, V. (2017). A hybrid quantum-induced swarm intelligence clustering for the urban trip recommendation in smart city. Future Generation Computer Systems, 83, 653-673.

[14] Subramaniyaswamy, V., & Logesh, R. (2017). Adaptive KNN based Recommender System through Mining of User Preferences. Wireless Personal Communications, 97(2), 2229-2247.

[15] Logesh, R., & Subramaniyaswamy, V. (2017). A Reliable Point of Interest Recommendation based on Trust Relevancy between Users. Wireless Personal Communications, 97(2), 2751-2780.

[16] Logesh, R., & Subramaniyaswamy, V. (2017). Learning Recency and Inferring Associations in Location Based Social Network for Emotion Induced Point-of-Interest Recommendation. Journal of Information Science & Engineering, 33(6), 1629–1647.

[17] Subramaniyaswamy, V., Logesh, R., Abejith, M., Umasankar, S., & Umamakeswari, A. (2017). Sentiment Analysis of Tweets for Estimating Criticality and Security of Events. Journal of Organizational and End User Computing (JOEUC), 29(4), 51-71.

[18] Indragandhi, V., Logesh, R., Subramaniyaswamy, V., Vijayakumar, V., Siarry, P., & Uden, L. (2018). Multi-objective optimization and energy management in renewable based AC/DC microgrid. Computers & Electrical Engineering.

[19] Subramaniyaswamy, V., Manogaran, G., Logesh, R., Vijayakumar, V., Chilamkurti, N., Malathi, D., & Senthilselvan, N. (2018). An ontology-driven personalized food recommendation in IoT-based healthcare system. The Journal of Supercomputing, 1-33.

[20] Arunkumar, S., Subramaniyaswamy, V., & Logesh, R. (2018). Hybrid Transform based Adaptive Steganography Scheme using Support Vector Machine for Cloud Storage. Cluster Computing.

[21] Indragandhi, V., Subramaniyaswamy, V., & Logesh, R. (2017). Resources, configurations, and soft computing techniques for power management and control of PV/wind hybrid system. Renewable and Sustainable Energy Reviews, 69, 129-143.

[22] Ravi, L., & Vairavasundaram, S. (2016). A collaborative location based travel recommendation system through enhanced rating prediction for the group of users. Computational intelligence and neuroscience, 2016, Article ID: 1291358.

[23] Logesh, R., Subramaniyaswamy, V., Malathi, D., Senthilselvan, N., Sasikumar, A., & Saravanan, P. (2017). Dynamic particle swarm optimization for personalized recommender system based on electroencephalography feedback. Biomedical Research, 28(13), 5646-5650.

[24] Arunkumar, S., Subramaniyaswamy, V., Karthikeyan, B., Saravanan, P., & Logesh, R. (2018). Meta-data based secret image sharing application for different sized biomedical images. Biomedical Research,29.

[25] Vairavasundaram, S., Varadharajan, V., Vairavasundaram, I., & Ravi, L. (2015). Data mining-based tag recommendation system: an overview. Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery, 5(3), 87-112.

[26] Logesh, R., Subramaniyaswamy, V., & Vijayakumar, V. (2018). A personalised travel recommender system utilising social network profile and accurate GPS data. Electronic Government, an International Journal, 14(1), 90-113.

[27] Vijayakumar, V., Subramaniyaswamy, V., Logesh, R., & Sivapathi, A. (2018). Effective Knowledge Based Recommeder System for Tailored Multiple Point of Interest Recommendation. International Journal of Web Portals.

[28] Subramaniyaswamy, V., Logesh, R., & Indragandhi, V. (2018). Intelligent sports commentary recommendation system for individual cricket players. International Journal of Advanced Intelligence Paradigms, 10(1-2), 103-117.

[29] Indragandhi, V., Subramaniyaswamy, V., & Logesh, R. (2017). Topological review and analysis of DC-DC boost converters. Journal of Engineering Science and Technology, 12 (6), 1541–1567.

[30] Saravanan, P., Arunkumar, S., Subramaniyaswamy, V., & Logesh, R. (2017). Enhanced web caching using bloom filter for local area networks. International Journal of Mechanical Engineering and Technology, 8(8), 211-217.

[31] Arunkumar, S., Subramaniyaswamy, V., Devika, R., & Logesh, R. (2017). Generating visually meaningful encrypted image using image splitting technique. International Journal of Mechanical Engineering and Technology, 8(8), 361–368.

[32] Subramaniyaswamy, V., Logesh, R., Chandrashekhar, M., Challa, A., & Vijayakumar, V. (2017). A personalised movie recommendation system based on collaborative filtering. International Journal of High Performance Computing and Networking, 10(1-2), 54-63.

[33] Senthilselvan, N., Udaya Sree, N., Medini, T., Subhakari Mounika, G., Subramaniyaswamy, V., Sivaramakrishnan, N., & Logesh, R. (2017). Keyword-aware recommender system based on user demographic attributes. International Journal of Mechanical Engineering and Technology, 8(8), 1466-1476.

[34] Subramaniyaswamy, V., Logesh, R., Vijayakumar, V., & Indragandhi, V. (2015). Automated Message Filtering System in Online Social Network. Procedia Computer Science, 50, 466-475.

[35] Subramaniyaswamy, V., Vijayakumar, V., Logesh, R., & Indragandhi, V. (2015). Unstructured data analysis on big data using map reduce. Procedia Computer Science, 50, 456-465.

[36] Subramaniyaswamy, V., Vijayakumar, V., Logesh, R., & Indragandhi, V. (2015). Intelligent travel recommendation system by mining attributes from community contributed photos. Procedia Computer Science, 50, 447-455.

[37] Vairavasundaram, S., & Logesh, R. (2017). Applying Semantic Relations for Automatic Topic Ontology Construction. Developments and Trends in Intelligent Technologies and Smart Systems, 48.