Development of Modified Polybius Technique for Data Security

Puneet Kumar
Research Scholar, Department of Electronics and Communication Engineering
Guru Nanak Dev University Regional Centre Gurdaspur, Punjab, India

Dr. Shashi B. Rana
Astt. Professor, Department of Electronics and Communication Engineering
Guru Nanak Dev University Regional Centre Gurdaspur, Punjab, India

Abstract- In present scenario sharing of information is increasing significantly. The information is being transmitted to different user and undergoes various passive and active attacks; therefore, the information security plays a challenging role in communication. Cryptography plays a vital role in secure wireless communication and provides an excellent solution to offer the necessary protection against the attacks. Polybius cipher is based on 5X5 matrix of letters constructed using numbers from 0 to 4. This existing Polybius contains alphabets only; therefore, 6X6 Polybius square has been proposed which includes both the alphabets and numbers leads to secured communication.

Keywords - Cryptography, Polybius cipher, hackers and attacks.

I. INTRODUCTION

Cryptography is the art of achieving security by encoding messages into the unreadable form. It not only protects the information but also helps in providing the authentication to the user. The original information and encrypted information are referred as plaintext and cipher text respectively [1]. The two types of process generally occurs known as encryption and decryption. During communication, the sender performs the encryption with the help of a shared secret key and the receiver performs the decryption. The basic cryptography model has been shown in the figure 1. Cryptographic has two categories: Symmetric cryptography (private key) and Asymmetric cryptography (public key) [1, 2]. Symmetric key algorithm is much faster to execute than the asymmetric key algorithm.

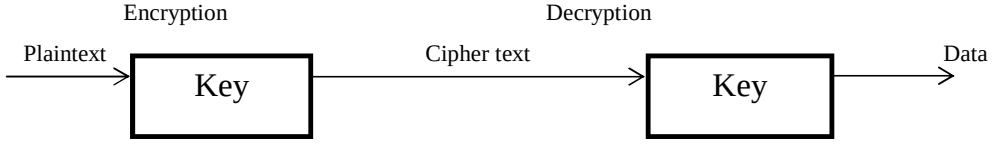

Figure 1: Basic Cryptography Model

II. LITERATURE SURVEY

This section involves the work done by the various researchers in the field of cryptography for data security.
Ahmet Dogan [3] et al. worked on analysing and comparing the AES architectures for their power Consumption and observed that AES has gained significant confidence for its security. They introduced low power AES[8]model which has gained more importance and performance oriented designs which will leads to reduced power consumption in FPGA (Field Programmable Gate Arrays). They also proposed most popular four architectures including; serial, outer pipeline, inner outer pipeline and one S-box only with all the different S-box realizations. Thus, they show its effectiveness by providing area, time and power dissipation. Kazuo Sakiyama [4] et al. proposed an information theoretic approach to optimal differential fault analysis. They worked on a comprehensive analysis of differential fault analysis (DFA) attacks on the advanced encryption standard (AES). They also presented a new DFA methodology to achieve the optimal DFA attack by deriving the amount of the leaked information for various fault models. Jinguang Han [5] et al. worked on identity based secure distributed data storage schemes. They proposed two new IBSDDS schemes in standard model, a) The first scheme is only secure against the chosen plaintext attacks (CPA), b) second scheme is secure against the chosen cipher text attacks (CCA). The owner has less control on his secret key than that in other public key encryption schemes. Aftab Alam [6] et al. proposed universal Playfair Cipher using MXN matrix. They

presented a security method which can be used for the both alphabets and numerals. The encryption and decryption of messages can be done with natural language with proper size of a matrix. Jin Li [7] et al. proposed a securely outsourcing attribute based encryption with check ability. Secure Outsourced ABE system supports both secure outsourced key issuing and decryption. It has been found that it takes more time than the original ABE system.

It is an Ancient Greek historical Polybius responsible for the sending the messages at the long distances, and invented a substitution cipher which is known as the Polybius square. The Polybius cipher uses the keywords such as Playfair Cipher, and is not much secure when used with the mixed alphabets. The pair of numeric and alphabets taken together forms a simple substitution. However, it is also useful in various ciphers such as Nihilist cipher, ADFGVX cipher and BIFID cipher[11]. The alphabets (26) are arranged in 5X5 matrix as shown in Table 1. The alphabets I and J are present in a unique cell and the choice of the alphabet can be done easily from the text meaning. In the Polybius square the number of letters reduced from 26 to 25 by considering I and J identical. The encryption consists of replacing each letter with the corresponding pair of numbers (the line and column crossing point) [12]. For instance, E is 04, M is 12 and O is 23. The existing Polybius square has been shown in the table 1. Where the letters are plaintext and the numbers are ciphertext. To decrypt a message one has to find the letter that intersects the specified row and column. For instance, 04 is E, 12 is M and 23 is O. Thus a Polybius substitution is generally used among cryptographers up to modern times and has been used for numerous ciphers.

	0	1	2	3	4
0	**A**	**B**	**C**	**D**	**E**
1	**F**	**G**	**H**	**I/J**	**K**
2	**L**	**M**	**N**	**O**	**P**
3	**Q**	**R**	**S**	**T**	**U**
4	**V**	**W**	**X**	**Y**	**Z**

Table 1: Existing Polybius Square

From the above section following observations have been drawn a) the letter I/J fall in a one cell and therefore, there is no provision for the numeric, and b) it does not have any key due to which it can be easily broken. Thus, these limitations overcome with the use of an extended Polybius Square in this it includes: a) key in order to provide more security, b) the size of square is increased which includes numeric, and c) the use alphabets I and J is separate.

III. PROPOSED SCHEME

The proposed Polybius Square uses the 6X6 matrix rather 5X5 matrix. The proposed matrix consists of both the alphabets and numerals filled without repetition from the left to right and thus, help in providing the secure information [11, 12]. The arrangements of numerals have been done in the ascending order from 0 to 9.

	0	1	2	3	4	5
0	**A**	**B**	**C**	**D**	**Y**	**4**
1	**E**	**F**	**G**	**H**	**Z**	**5**
2	**I**	**J**	**K**	**L**	**0**	**6**
3	**M**	**N**	**O**	**P**	**1**	**7**
4	**Q**	**R**	**S**	**T**	**2**	**8**
5	**U**	**V**	**W**	**X**	**3**	**9**

Table 2: Proposed Polybius Square

The user could efficiently encode alphabets and numerals. Thus, the plaintext consists of the Username, Identity, PAN number, Driving License and Date of birth etc. both in alphabets as well as in numbers. Thus, it can be easily encrypted using the proposed scheme. Similarly, one can also decode it into the original form consisting of alphabets and numbers.

For encryption, first we have to look at the intersection of any row and column (with row number given first and column number given second) as the representation of the alphabet or numerals. Let us take an Example: ENCRYPT2345 is the message which is to be encoded then decoded in the original message.

Plaintext	E	N	C	R	Y	P	T	2	3	4	5
Position	1	2	3	4	5	6	7	8	9	10	11
Ciphertext	10	31	02	41	04	33	43	44	54	05	15

Table 3: Encryption using Proposed Polybius square

As it clear form the Table 3, the plaintext which is an original text encrypted into the ciphertext with some codes and cannot be determined by the hacker. The Plaintext is ENCRYPT2345 and the Ciphertext is 10310241043343445405 15 in form of codes. Thus, encryption of message is done.
Now to decrypt the message back to the original text the representation of the rows and columns is done. This can be seen in the Table 4.

Ciphertext	10	31	02	41	04	33	43	44	54	05	15
Position	1	2	3	4	5	6	7	8	9	10	11
Plaintext	E	N	C	R	Y	P	T	2	3	4	5

Table 4: Proposed Polybius Square Decryption

IV. CONCLUSION AND FUTURE SCOPE

The extended Polybius square have been discussed which consist of both the alphabets and numerals. In the existing Polybius square there was the use of only alphabets not the numerals and can be hacked by the attacker easily. In proposed scheme, an attacker may not know the contents of a data transfer but could see that a message transfer occurred. In proposed scheme numerals are added in order to make the information more secure. Further, this proposed work can be extended with the AES encryption technique. Work can be extended if mathematical or soft computational tools such as fuzzy or neural networks are used to evaluate for processing speed and power computational values.

REFERENCES

[1] Ajay Kakkar, Dr.M L Singh, Dr. P.K. Bansal,"Efficient Key Mechanisms in Multinode Network for Secured Data Transmission", International Journal of Engineering Science and Technology, vol. 2, Issue 5, 2010, pp.787-795.
[2] Bruce Schneier, "Applied Cryptography", John Wiley & Sons, Second Edition, January 1996.
[3] Ahmet Dogan, S. Berna Ors, Gokay Saldamli, "Analyzing and Comparing the AES Architectures for their Power Consumption", Springer Computer Science, pp.263–271, 2011.
[4] K. Sakiyama, Yang Li, Mitsugu Iwamoto, and Kazuo Ohta, "Information-Theoretic Approach to Optimal Differential Fault Analysis", IEEE Transactions On Information Forensics and Security, Vol. 7, No. 1, .pp.109-120 February 2012.
[5] Jinguang Han, "Identity-Based Secure Distributed Data Storage Schemes", IEEE Transactions on computers, Vol. 63, No.4, .pp. 941-953, April 2014.
[6] Aftab Alam, Sehat Ullah, Ishtiaq Wahid, & Shah Khalid, "Universal Playfair Cipher Using MXN Matrix", International Journal of Advance Computer Science, Vol. 1,No.3,pp. 113-117, September 2011.
[7] Jin Li, Xinyi Huang, Jingwei Li, Xiaofeng Chen, and Yang Xiang, "Securely Outsourcing Attribute-Based Encryption with Checkability", IEEE Transaction on parallel and distributed systems, vol. 25, no. 8, .pp. 2201-2210, August 2014.
[8] "Advanced Encryption Standard (AES)", Federal Information Processing Standards Publication 197, November 26, 2001
[9] Julia Juremi, Ramlan Mahmod, Salasiah Sulaiman, Jazrin Ramli, "Enhancing Advanced Encryption Standard S-Box Generation Based on Round Key", International Journal of Cyber-Security and Digital Forensics (IJCSDF), .pp. 183-188, 2012.
[10] Chaitali Haldankar, Sonia Kuwelka, "Implementation of AES And Blowfish Algorithm", International Journal of Research in Engineering and Technology, vol-3, .pp.143-146, May 2014.
[11] Krawetz, N. 2007 Introduction to Network Security. Charles River Media.
[12] Forouzan, B. A. 2010 TCP/IP Protocol Suite. McGrawHill.