Volume 1, Issue 1 (2018)
Article No. 1
PP 1-6

VIVA-TECH IJRI
ANNUAL RESEARCH JOURNAL

VIVA-TECH INTERNATIONAL JOURNAL FOR RESEARCH AND INNOVATION
ANNUAL RESEARCH JOURNAL
ISSN(ONLINE): 2581-7280

Advance Cipher Technique to Secure Email Contents

Tatwadarshi P. Nagarhalli[1]
[1](*Computer Engineering Department, VIVA Institute of Technology, India)*

Abstract: *Billions of emails are sent all over the world. Many a times these emails contain sensitive information. The email system providers do provide security for the emails sent. But if the authentication is compromised then the whole Pandora of sensitive information will be out in the open. So, the paper provides a system called as the 'Advance Cipher Technique (ACT)' to secure the contents of the emails before it is sent over the email. The paper proposes to secure the email contents by using substitution and permutation, with the fronts provided by the email systems acting as the keys.*
Keywords *– Advance Cipher Technique, Email Security, Data Security, Substitution Cipher, Permutation.*

1. INTRODUCTION

There are a total of about 7.5 Billion human souls in on the planet as on 30th June, 2017. Of this, about 3.9 Billion people use internet. That is, around 51.7% of the human population on earth use internet for some purpose or the other [1]. The purpose might be anything, form shopping to reading reviews to communication to socializing.

One of the important tasks for which the internet is used is communication through emails. Electronic Mails or emails are used universally by individuals, business or governments [2].

According to one estimate in 2015 2.6 Billion users were using emails for communication. And, this number is set to grow to 2.9 Billion by 2019 [3]. Also, about 205 Billion emails were sent/received, which is said to grow to about 246 Billion by 2019 [3]. Even the defence forces use emails for communication among themselves. Often these email services used by the defence forces are exclusive and secure. But there have been instances where the defence emails have also been leaked [4]. So securing the emails are of utmost importance.

The paper proposes a new why in which data can be secured with fonts as a key, before it is sent over an unsecured channels like emails.

2. SECURITY SYSTEM

There are two ways in which data can be secured cryptography and steganography. In cryptography the data which is to be secure is converted to some unreadable form with the help of some mathematical formulas [5]. Whereas, in steganography the data which is to be secured is embedded into some other medium like text, image, video and audio [6].

In cryptography the data to be secured also called as the plain text is converted to an unreadable from called as the cipher text with the help of a key, this process is called as the encryption. And at the receiver side the original message can be extracted from this cipher text with the help of a key. Fig. 1 shows the general process of encryption and decryption.

Volume 1, Issue 1 (2018)
Article No. 1
PP 1-6

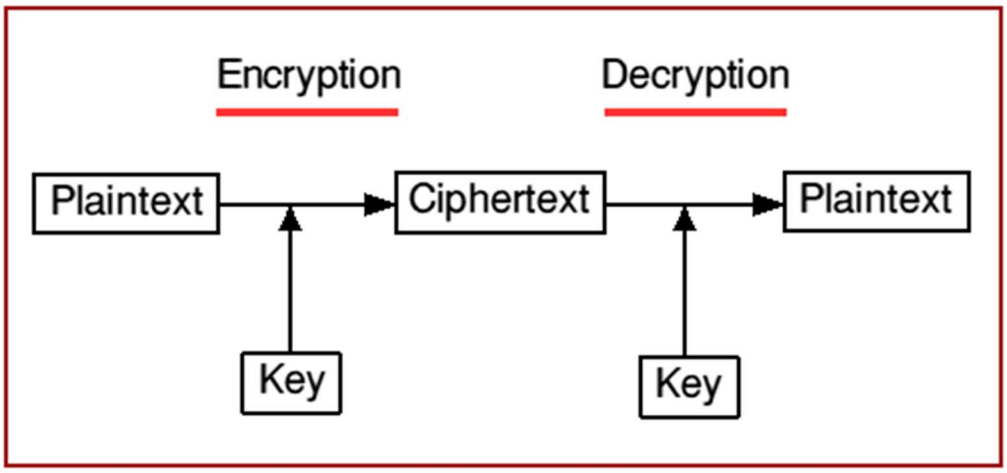

Fig. 1 Encryption and Decryption [7]

There are essentially two ways in which the plain text can be converted into cipher text. These two ways are stream cipher technique and block cipher technique. Fig. 2 shows the type of cryptography algorithms.

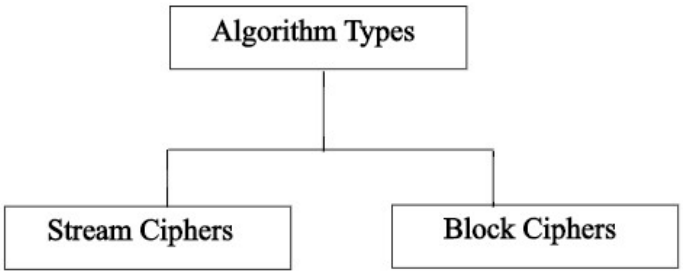

Fig. 2 Types of Cryptography Algorithms

The stream cipher transforms the plain text to cipher text one symbol at a time. Whereas the block cipher converts a group of symbols in the plain text to cipher text at a time [8]. Fig. 3 shows the block diagram of stream cipher. And, Fig. 4 shows the block diagram of Block cipher.

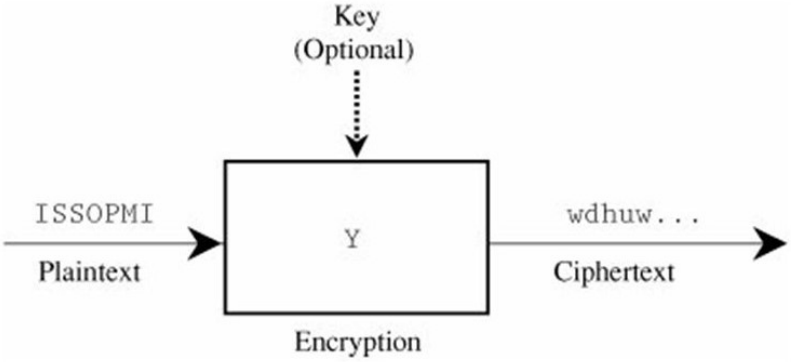

Fig. 3 Steam Cipher

Volume 1, Issue 1 (2018)
Article No. 1
PP 1-6

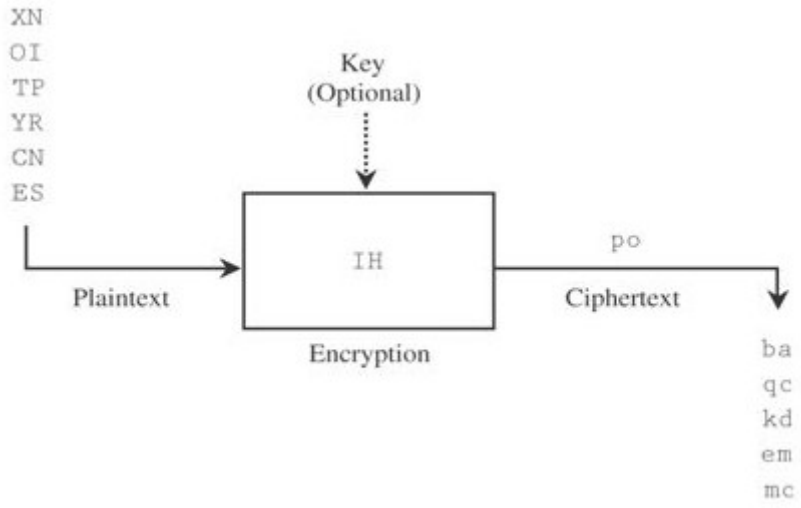

Fig. 4 Block Cipher

3. RELATED WORKS

As Tianlin Li et. al. [2] demonstrate, most of the email systems try to provide as much security as they can. In general, email systems like the Gmail secure the email data using the S/MIME. S/MIME stands for Secure/Multipurpose Internet Mail Extensions. S/MIME provides the following security services Authentication, Message integrity, Non-repudiation of origin (using digital signatures), Privacy and Data security (using encryption) [9].

The S/MIME does provide a credible amount of security. But the problems remains that what if the account passwords gets leaked or hacked, in such cases it is impossible to secure the email content. So, a system or a mechanism is required which can secure the data before it is sent via the email systems.

There have been systems which have been proposed to secure the email data. Apeksha Nemavarkar and Rajesh Kumar Chakrawarti [10] provide a multi-step email verification system. Whereas B. Suresh Kumar and V. P. Jagathy Raj [11] provide a system which encrypts the data according to the identity of the user. Paper [11] does work on the data level of the email contents but paper [10] propose a system which performs verification of the user and not on the data.

There have also been system which propose to secure the email data with the help of steganography like a system proposed by B. Veera Jyothi et. al. [12]. On the other hand Salvatore J. Stolfo et. al. [13] propose to secure the emails by studying the behavioural patterns and allowing the email to be read by only those who confirm with the behavioural patterns of the verified user.

Yogendra Kumar Jain and Pramod B. Gosavi [14] provide a system to not only encrypt the data but also to tries to compress the data. The cipher text key is defined from the receiver user id and the character is converted to cipher text with different key, also the key incremented every time by one. Even though the paper tries to ensure the security of the email data the key is easily identifiable.

M. Ferris [15] on the other hand talks about the security infrastructure that is required to secure an email system. The author does not talk about the contingency plan if the emails are compromised.

A. Malatras et. al. [16] reviews the outstanding privacy and security risks in email communications and describes a set of countermeasures, based on combinations of existing standards, which are capable of effectively mitigating the identified risks. Also, based on the analysis the authors propose a set of technical recommendations for email providers that needs to be followed to enhance security, whilst preserving the compatibility of the ecosystem.

W. Bai et. al. [17] observed that for the sake of usability many a times the security is compromised. So, they propose a system which tilt the trade-off between usability and security in favour of security. The paper talks about securing the email system and not much has been discussed about security of the data.

W. Bai et. al. [18] conduct a survey to find if people feel secure about the steps taken by the email system to secure their data. The survey finds out that most people so feel secure but as the authors put it, there has to be even more that could be done to secure the email contents.

So, in the current paper a system has been to secure the email data with the help of an Advance Cipher Technique with the help of the fonts available for email communication.

Volume 1, Issue 1 (2018)
Article No. 1
PP 1-6

4. PROPOSED SYSTEM

The paper proposes Advanced Cipher Technique using modified stream cipher system and fonts for securing email contents. For the sake of convenience Gmail has been used as email system on which the proposed system has been implemented.

The Gmail currently provides eleven fonts to choose from. These fonts include Sans Serif, Serif, Fixed Width, Wide, Narrow, Comic Sans MS, Garamond, Georgia, Tahoma, Trebuchet MS and Verdana. In the proposed system these font acts as a key to identifying the deciphering of the cipher text.

In the proposed system a message which is to be secured is grouped together containing five words each. For example for a secret message "India is on the verge of attacking XYZ nation"; the message contains 9 words, so two groups are formed. First group contains the words "India is on the verge"" and the second group contains the words "of attacking XYZ nation". The reason for grouping the complete sentence or paragraph into a groups of words containing five words is that the proposed system works at five words at a time.

In the proposed system encryption and decryption takes in two phases. During encryption in the first phase substitution cipher is applied and in the second phase permutation is carried out. Whereas permutation is carried out first phase for decryption.

For encryption, in the first phase once the group has been formed each word is encrypted to get a cipher text. The plain text is converted into cipher text with the help of substitution cipher. The key for this substitution cipher is different for each word in a group and is also different for each font.

The formula can be given as

$C = E(Ki)$

Where Ki for Gmail would be K1 to K11 (The number of Fonts)

Table 1 gives the Advance Cipher Technique – Substitution Box (ACT-S Box), with the keys for each fonts. For enhancing the security the ACT-S Box can changed from time to time as well.

Table 1: ACT-S Box (Substitution) Keys for different font

	K_1	K_2	K_3	K_4	K_5	K_6	K_7	K_8	K_9	K_{10}	K_{11}
First Word	n	n-2	n-4	n+6	n+1	n+7	n+5	n+0	n+2	n-2	n+9
Second Word	n+2	n+3	n	n+4	n+9	n-1	n+7	n-3	n+5	n-5	n-3
Third Word	n+5	n+1	n+2	n+5	n-1	n-9	n-6	n	n+1	n-1	n-1
Fourth Word	n+1	n-6	n-2	n-5	n-3	n-5	n+9	n-4	n+9	n-9	n-8
Fifth Word	n+8	n-4	n-3	n-7	n+2	n+3	n+6	n-6	n+7	n-7	n+1

Where 'n' is the length of that particular word.

After the plain text is converted to cipher text with the help of the ACT-S Box, permutation is carried out as the second phase for encryption. Different set of permutation has been proposed for different fonts according to the ACT-P Box. So, the fonts carry the key as to how the substitution and permutation is to be carried out.

Table 2 provides an outline for permutation of the data. The table gives the Advance Cipher Technique – Permutation Box (ACT-P Box). The result received after applying ACT-S Box undergoes permutation with the help of the ACT-P Box. As with the ACT-S even the ACT-P Box can be updated from time to time to enhance the security of the system and keep the cracker guessing about the keys of the system.

Table 2: ACT-P Box (Permutation) for different fonts

	First Word shifted to position -	Second Word shifted to position -	Third Word shifted to position -	Fourth Word shifted to position -	Fifth Word shifted to position -
Sans Serif,	4	3	1	5	2
Serif	2	4	5	3	1
Fixed Width	3	5	4	2	1
Wide	5	3	1	2	4
Narrow	5	4	2	1	3
Comic Sans MS	2	5	1	3	4
Garamond	3	1	4	5	2

Georgia	4	5	2	1	3
Tahoma	5	3	4	2	1
Trebuchet MS	2	1	4	5	3
Verdana	4	5	1	5	2

For example:

If the secret message to be secured is “India is on attack mode”.

1. If the font ‘Sans Serif’ the cipher text would be
   a. By using ACT-S Box we will get
   nsinf mw vu haahjr yapq

   b. Applying ACT-P Box on the above cipher text for the font Sans Serif we will get
   vu yapq mw nsinf haahjr, this is the cipher text.

2. If the font ‘Fixed Width’ the cipher text would be
   a. By using ACT-S Box we will get
   joejb ku sr dwwdfn npef

   b. Applying ACT-P Box on the above cipher text for the font Sans Serif we will get
   npef dwwdfn joejb sr ku

So, it can be seen that with the change in the usage of font the cipher text undergoes a major change. Once the cipher text is formed it can be sent to the intended receiver in the font selected for encryption. Only the intended receiver who knows that the fonts act as a key and has the ACT system will be able to decrypt the message.

5. ANALYSIS AND ADVANTAGES

The proposed system has many advantages

1. A simple way to secure email content.

2. The system provide two layers of security. The first one is with the help of the ACT-S Box and the second layer is the permutation by using ACT-P Box.

3. With the change in the font the whole cipher text get changed. So, even the same message will produce a total of eleven different cipher text while using different Gmail fonts.

4. In the same secret message different keys are used to create cipher text. This enhances security. Also, scrambling of the words with the help of ACT-P Box makes it that much more difficult for the eves dropper to decode the message.

5. Keys are not sent at all through unsecured channels. This also enhances security.

6. For more security the ACT-S Box keys and ACT-P Box permutation positions can be changed from time to time.

7. Also, the implementation of temporal changes in the ACT-S Box and ACT-P Box will make the job of the cracker very, very difficult.

6. CONCLUSION

The paper identifies that even though email system provide security if the authentication step of the email systems is compromised the email content becomes available to all. This is undesirable. So, the paper provides a simple yet effective way in which the email contents or the data can be secured.

The paper proposes an Advance Cipher Technique, where the fonts provided by the email systems, like Gmail, act as a key. The system provides two layers of security to secure the email contents. The first one is with the help of the ACT-S Box and the second layer is the permutation by using ACT-P Box.

By providing different keys for different words for the same font and scrambling of the encoded word

provides with an enhance security. Also, implementing temporal changes in ACT-S and ACT-P Boxes will further enhance the security. The proposed system can be seamlessly integrated into an email system for easy usage.

REFERENCES

[1] http://www.internetworldstats.com/stats.htm. Last Accessed on 10th September, 2017.

[2] T. Li, Mehta, and A. P. Yang, "Security Analysis of Email Systems", *IEEE 4th International Conference on Cyber Security and Cloud Computing*, 2017, pp. 91-96.

[3] The Radicati Group, Inc., "Email Statistics Report, 2015-2019", http://www.radicati.com/wp/wp-content/uploads/2015/02/Email-Statistics-Report-2015-2019-Executive-Summary.pdf.

[4] http://www.thejournal.ie/irish-defence-forces-hacking-team-2206527-Jul2015/, Last Accessed on 10th September, 2017.

[5] M. Pavan, S. Naganjaneyulu and C. Nagaraju, "A Survey on LSB Based Steganography Methods", *International Journal of Engineering and Computer Science, Vol.2, Issue 8*, August 2013.

[6] T. P. Nagarhalli and A. M. Save, "A Cross Lingual Approach for Hiding Hindi Text", *IEEE International Conference on Innovations in information Embedded and Communication Systems (ICIIECS)*, 2017, pp. 415-419.

[7] N. Queen, "Principles of modern cryptography", http://www.queen.clara.net/pgp/art6.html, Last Accessed on 10th September, 2017.

[8] C. P. Pfleeger and S. L. Pfleeger, *Security in Computing* (Fourth Edition, Pearson Education, 2017).

[9] https://en.wikipedia.org/wiki/S/MIME, Last Accessed on 10th September, 2017.

[10] A. Nemavarkar and R. K. Chakrawarti, "A uniform approach for multilevel email security using image authentication, compression, OTP & cryptography", *IEEE International Conference on Computer, Communication and Control (IC4)*, 2015.

[11] B. S. Kumar and V. P. J. Raj, "A Secure Email System Based on Identity Based Encryption", *IJWCNT, vol. 1, no. 1*, August-September 2012.

[12] B. V. Jyothi, S. M. Verma and C. U. Shanker, Implementation and Analysis of Email Messages Encryption and Image Steganography Schemes for Image Authentication and Verification, *IJCA Auguest*, 2014.

[13] S. J. Stolfo, Chia-Wei Hu, Wei-Jen Li, S. Hershkop, K. Wang and O. Nimeskern, "Combining Behavior Models to Secure Email Systems", *DARPA contract F*, pp. 30602-00-1-0603.

[14] Y. K. Jain and P. B. Gosavi, "Email Security Using Encrption and Compression", *IEEE International Conference on Computational Intelligence for Modelling Control & Automation*, 2008.

[15] M. Ferris, "New Email Security Infrastructure", *IEEE ACM SIGSAC New Security Paradigms Workshop*, 1994. Proceedings., 1994.

[16] A. Malatras, I. Coisel and I. Sanchez, "Technical recommendations for improving security of email communications", *IEEE 39th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), Opatija*, 2016, pp. 1381-1386.

[17] W. Bai, D. Kim, M. Namara, Y. Qian, P. G. Kelley and M. L. Mazurek, "Balancing Security and Usability in Encrypted Email", *IEEE Internet Computing*, *vol. 21, no. 3*, May-June 2017, pp. 30-38.

[18] W. Bai, D. Kim, N. Moses, Y. Qian, P. Gage Kelly and M. Mazurek, "Most of us trust our email provider": Balancing security and usability in encrypted email, in *IEEE Internet Computing*, *vol. PP, no. 99*, pp. 1-1.