Secure Text Conferencing System Using Multiple Layer Encryptions

Najmadin Wahid Boskany

Computer Science Department, Faculty of Science and Science Education, University of Sulaimani, Kurdistan Region- Iraq, Email: boskany@hotmail.com

Abstract:

The coding theory becomes increasingly important over the decades. There are some different works that have been dedicated to the problems of cryptography. In the present paper, the design and implementation of a secure text conferencing system have been proposed and implemented. Also explained how plaintext can be encrypted in three levels before sending it to the destination has been explained. Later, how ciphered text decrypted from destination side to its origin plaintext has been described.

Keywords: *Secure Text Conferencing, Plaintext, Cipher Text, Promiscuous Mode, Windows Sockets, Network Security, Client-Server Networks.*

Introduction

Text conferencing means exchanging text messages between two or more people logged into a particular instant messaging service. It is an interactive way because messages are sent immediately, whereas e-mail messages can be queued up in a mail server for seconds or minutes. The instant messaging text box is usually short and is designed for fast text interaction.

The purposes of using text conferencing may run from the intention of giving students space for purely exploratory exchange, along to the intention of providing a forum in which students could ask questions or seek feedback which might be largely fielded by teaching personnel. [1]

Question-fielding is one motive for cultivating a discussion forum. Another motive would be to facilitate the conduct of some particular course-relevant tasks. For example, it may be important for students to carry out a collaborative project. If so, then text conferencing may be regarded as a useful tool for coordinating the activity. Sometimes, such

coordination is used as a device to promote more active use of the medium. Perhaps the hope is that once familiarity is achieved through the need to coordinate for some project, then future less structured use will occur more readily. There remains the question of why any of these educational ambitions (question fielding, exploratory discussion, collaborative work, etc.) should be carried out through a text conference rather than through using more traditional formats. The "purpose" in this sense usually relates to some impossibility of gathering students for synchronous interaction. Evidently, the

asynchronicity of text conferencing allows a substitute form of discussion. [7].

Also there are other styles of text conferencing which is called chat, which owns more feature and flexibility. Chat is a form of synchronous textual communication between communities of users. These users converse in chat rooms (sometimes called channels), which are virtual locations for chatting on the Internet and private networks. These can be supported using, for example, tools for instant messaging, adding animation, attaching pictures, and Internet Relay Chat. Most chat room user interfaces follow a similar structure, with an abstract user interface; they include a window that lists the participants, a window that displays the history of typed messages, and a window for typing in a new message. Within the

message history's window, messages are displayed in the chronological order that they were received by the system, with new messages appearing at the bottom of the screen [12]. Chat conversations are widely used as text based communication tools. Chat mediums are one of the communication mediums which are used by people from all ages frequently. The importance of social and semantic inferences from chat mediums is increasing day by day with this much usage and extension of these mediums [13]

Although text conferencing and chat have the above advantages, we are often in a risk and we face problems if we do not care about securing our text conferences because sometimes special people sitting behind our networks and trying to access and log into our network sessions illegally. Their effort is for stealing information, by using some dedicated software and tools. Sometimes they change their Network Interface Card (NIC) setting into a special mode i.e.; Promiscuous Mode for this purpose. So we have to worry and think about how to design and use a system to protect our exchanged information from these persons by using some techniques like text ciphering [1].

Ciphering is a method for encrypting a message; i.e., for transforming the message into one that can not be easily read. In another meaning, it is the changing of texts or other data into a code that appears to be unreadable. The original message is called "plaintext" and the encrypted message is called a "cryptogram" or "cipher text." Cryptography is the study and art of sending and receiving secret messages [3, 8]. The cipher text message contains all the information of the plaintext message, but is not in a format readable by a human or computer without the proper mechanism to decrypt [2].

Text security and authenticity are very important in many applications. They are used in our daily life such as in text conferencing, banking, smart card, business discussion and insurance. To prevent unauthorized use to our text sessions or any transmitting process through communication mediums, the information should be securely encrypted. Encryption is often used to achieve data security, particularly when using a credit card to place orders for goods or other services on the different types of networks and Internet. Encrypted data is referred to as cipher text. [5, 6]

A substitution cipher is the one in which each letter of the plaintext is replaced by some other symbol. Usually the replacement symbols are themselves letters of the alphabet. Also many other types of ciphering exist like transposition and symmetric and asymmetric methods.

Unlike other previous techniques of text conferencing systems (i.e. clear text or plaintext based conferencing), in this paper the new technique which provides data encryption at three levels are proposed for designing secure text conferencing application. This system is designed on the basis of ciphering the exchanged texts between members of conference with strong encrypting, and it can be used between users and hosts in a network system or Internet. Since multiple cipher texts will be developed for one plain text, even if the user decrypts the message to plain text, s/he does not know how far s/he had guessed the message correctly. Moreover the cipher text will always be larger than the plain text. This encryption algorithm is based on the concept of poly alphabet cipher and character in the plain text which replaced by the use of a random sequence generator, which is an improvement over mono alphabetic technique. [4]

This proposed system has been designed by using Visual Basic for Applications (VBA) program language with some socket Application Programming Interface (API), which is it works under Windows operating system platforms.

The proposed Secure Text Conferencing System using multi layer encryption outline is depicted in figure (1.1).

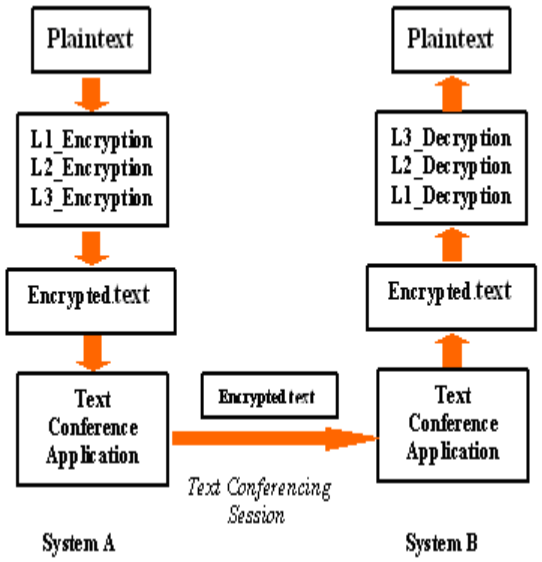

Fig 1.1: proposed Secure Text Conferencing System outline using multi layer encryption

The rest parts of this paper are organized as follows: In section 2, related work has been explained, In section 3, the proposed System Architecture has been illustrated; while in section 4 Encryption and Decryption algorithm have been explained. Then in section 5; Encryption and Decryption levels are illustrated by giving an example. System functional descriptions steps have been located in section 6. Finally, main conclusions and future works are summarized in section 7.

Related Works and Background :

In the last years, we have seen many text conferencing systems by using different efforts and approaches; they were concerned in developing applications which can operate on different platforms. These systems ranging from insecure systems (i.e.; plaintext based text conferencing), like **Anderson et al**'s system which have developed insecure text-based conferencing [9], and **Malhotra et al**'s system which have proposed a method to make a chat room using socket based on User Datagram Protocol (UDP) which enables the feature of acknowledgments after every message sent [11], and secured systems (i.e.; intelligent data encryption) like **Govindan et al's** system have developed a system which focuses on addressing vulnerability in data transmission over the Internet [10]. With compare to above approaches the proposed approach in this paper can be evaluated as good, user-friendly and has acceptable role in securing data during transmission.

System Architecture:

This system consists of two main parts. First one is designing client-server based application for text conferencing, while the second one is designing a three -level encryption technique for securing texts between computers that are integrated to the text conference system.

Below the design of the text conference application are illustrated in detail and the explanation of the encryption and decryption is located in the section 3.

The system architecture designed based on the client-server relationship, both sides must run the same text conference application. The proposed application depends on using windows socket for creating and controlling connection through the used medium of the network between computers. First, the server side application through its socket is in listening mode to the requests from clients for connection. Then, the client side through its socket must send request for creating connection with server via its IP address and port number. This process between client and server finally create text conferencing sessions. Figure 2.1 below illustrated how client and server create connections and they will start their session.

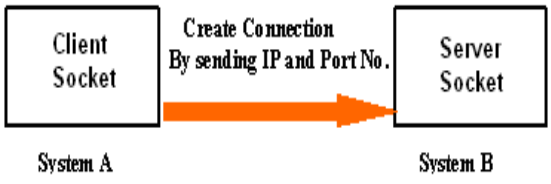

Fig 2.1: Client-Server Connection

Encryption and Decryption Algorithm

The proposed system has three levels of encryption and decryption on exchanged text messages. Below each level is described separately:

The first level encryption can be represented using modular arithmetic by first transforming the letters into numbers before sending it through the text conference system to the destination, according to the scheme:

A = 0, B = 1,....., Z = 25.

Encryption of a letter x by a shift n can be described mathematically as:

$$En1\ (x) = (x + n) \bmod 26$$

After the text messages are received by the destination side, the third level decryption is performed similarly.

$$Dn1\ (x) = (x - n) \bmod 26$$

(There are different definitions for modulo operation. In the above, the result is in the range 0...25. i.e., if x+n or x-n are not in the range 0...25, we have to subtract or add 26).

The replacement remains the same throughout the message, so the cipher at the first level is classed as a type of monoalphabetic substitution [1].

The second level encryption will make the text security stronger. It can also be represented by using modular arithmetic, by adding the random number to the encrypted text at the first level. The added random number can be generated randomly for each time.

$$En2\ (x) = [(x + n) \bmod 26] + RND(v)$$

After the text messages are received by the destination side the second decryption is performed by removing the random value (RND (v)) that is already come with the text for each character.

$$\mathbf{Dn2\ (x) = [(x - n) \bmod 26] - RND(v)}$$

After the text messages are received by the destination side, the second level decryption is performed by removing the random value for each character in order to be ready for the third level decryption.

In the same way the third level encryption can be represented by using modular arithmetic, by the transposition of each character with three random characters (as polyalphabetic or block substitution).

$$En3\ (x) = En2\ (x) \rightarrow \alpha\beta\delta$$

On the receiver side, after three levels of decryption are performed, the intended user can simply get the plaintext that is already sent from the sender.

$$Dn3\ (x) = \alpha\beta\delta \rightarrow Dn2\ (x)$$

One can see that after three levels of encryption (i.e. substitution, adding random value, and polyalphabetic transposition), the encrypted text will be much secured and it is hard for anybody to guess the encryption algorithm.

Probably the size of encrypted text can be noticed which is bigger than the origin text, but for short texts transmission (instant messaging), it does not matter**.**

Example

Below in this section a live example is presented using the proposed system, in order to be clearer for reader how to implement this system.

Encryption Levels:

Plaintext:
computer

First level encryption:
3 15 13 16 21 20 5 18

Second level encryption:
3.49 15.49 13.49 16.49 21.49 20.49 5.49 18.49

Third level encryption:
=#B2.&GPQ/w!<s^=#Baq@|pqGPQ/w!<s^=#Baq@2.&GPQ/w!<s^=#Baq@ml|GPQ/w!<s^=#B902aq@GPQ/w!<s^=#B902;&cGPQ/w!<s^=#B|pqGPQ/w!<s^=#Baq@>^sGPQ/w!<s^

Decryption Levels:

Cipher text:
=#B2.&GPQ/w!<s^=#Baq@|pqGPQ/w!<s^=#Baq@2.&GPQ/w!<s^=#Baq@ml|GPQ/w!<s^=#B902aq@GPQ/w!<s^=#B902;&cGPQ/w!<s^=#B|pqGPQ/w!<s^=#Baq@>^sGPQ/w!<s^

First level decryption:
3.49 15.49 13.49 16.49 21.49 20.49 5.49 18.49

Second level decryption:
3 15 13 16 21 20 5 18

Third level decryption (*Plaintext*):
computer

System Functional Description:

As illustrated before the application must be run on both sides from the client, connect button must be clicked by the user for the connection establishment. After connection has been established the application gives a message that alerts connection establishment between computers. Then the user can enter his/her texts and click the encrypt command button to encrypt the text before sending it to the network. Then the user clicks send to send encrypted text, as shown in the figure 5.1 (Secure Text Conferencing System User Interface) below. Also any ciphered text from the server side can be decrypted using decrypt command button, in order to be readable by the user.

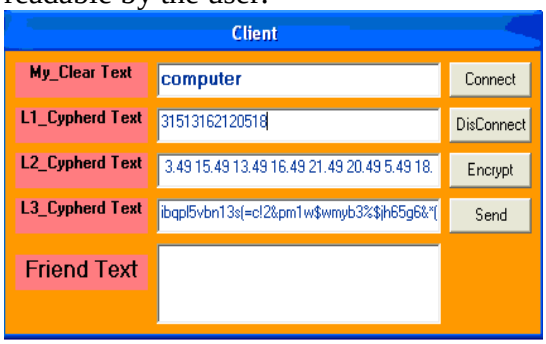

Fig 5.1: Secure Text Conferencing System User Interface

Conclusions and Future Work:

By using the presented system, we can say that it is difficult to decipher the texts that are transferred by this application, because three different levels of encryption (i.e.; substitution, adding random value, and polyalphabetic transposition) are used, and cannot be guessed by an intruder or at least s/he needs much time and special effort.

With comparison to other works that are exists in this field, this work can be classified as a good one, because it can be beneficial in network security field, thus the algorithm provides sufficient security against crypto analysis at a relatively low computational overhead. While other approaches that are used are at very good level but they may be more costly, complex, need more time to implement or need more requirements like coding or hardware.

Thus the computational overhead is very low. It is almost impossible to extract the original information in the proposed method even if the algorithm is known. In this block cipher algorithms, the plain text is converted into a cipher text after a number of levels, which makes the computational more complex.

References

[1] A.Chandra Sekhar, K.R. Sudha, and Prasad Reddy P V G D," Data Encryption technique using Random number generator", IEEE, **2007**.

[2] Holger kruse and Amar Mukherjee , "DATA COMPRESSION USING TEXT ENCRYPTION", 1068-0314, IEEE**, 1997**.

[3] Aamer Nadeem, Dr M. Younus Javed, "A Performance Comparison of Data Encryption Algorithms, IEEE, **2005**.

[4] Liakot Ali, Nurul Amziah Md Yunus, Haslina Jaafar, Rahman Wagiran, Evanna Low "Implementation of Triple Data Encryption Algorithm Using VHDL" ICSE2004, Proc. **2004**, Kuala Lumpur, Malaysia.

[5] Subbarao V. Wunnava and Ernesto Rassi;"Data Encryption Performance and Evaluation Schemes", Proceedings IEEE Southeastcon **2002**.

[6] A; Ammar, A. El Sherbini, I. Ashour, M. Shiple, "Random Data Encryption Algorithm (RDEA)", Twenty Second National Radio Science Conference (NRSC **2010**) March 15-17,2005, CaikEgypt.

[7] Zon-Yin Shae1, Dinesh Garg2 , Rajarshi Bhose2, Ritabrata Mukherjee3, Sinem Güven1, Gopal Pingali "Efficient Internet Chat Services for Help Desk Agents" **2007** IEEE International Conference on Services Computing (SCC 2007).

[8] Behrouz A. Forouzan, "Data Communication and Networking" fourth edition, ISBN: 978-0-07-296775-3, **2007**

[9] Dr. V.K. Govindan and B.S. Shajee mohan, "AN INTELLIGENT TEXT DATA ENCRYPTION AND COMPRESSION FOR HIGH SPEED AND SECURE DATA TRANSMISSION OVER INTERNET", **2004.**

[10] Lynn Anderson and Kathy McCarthy, **"**Text-based Conferencing Features vs. functionality", ERR-ODL journal, Vol. 6, No. 3, **2005**

[11] Malhotra, A., Sharma, V., Gandhi, P. And Purohit, N., "UDP based chat application" Journal: **2010** 2nd International Conference on Computer Engineering and Technology Year: **2010** Volume: 6 Pages: V6-374-V6-377 Provider: IEEE Publisher: IEEE DOI: 10.1109/ICCET.2010.5486192.

[12] David C. Uthus, David W. Aha, "Multiparticipant chat analysis: A survey",NRC/NRL Postdoctoral Fellow, Washington, DC 20375, United States, Navy Center for Applied Research in Artificial Intelligence, Naval Research Laboratory (Code 5514); Washington, DC 20375, United States, **2013**.

[13] Özcan Özyurt *, Cemal Köse, "Chat mining: Automatically determination of chat conversations", topic in Turkish text based chat mediums, Karadeniz Technical University, Department of Computer Engineering, Faculty of Engineering, 61080 Trabzon, Turkey, **2010**.