World Journal of Research and Review (WJRR)
ISSN:2455-3956, Volume-4, Issue-4, April 2017 Pages 01-03

Chat Application with A Codified Information Traveling Option

Bárbara Emma Sánchez Rinza, Ruth Itzel Gutiérrez Castro, Emmanuel Félix Valenzuela

Abstract— **Cryptology is the science that involves the study of the various techniques to keep information secure. It is the science that deals with the theoretical problems related to the safety in the interchange, between a transmitter and a receptor, of codified information traveling in a communication channel [1].**
The project consist of building a software to cipher text messages using a variant on the Playfair cipher method, which is an algorithm used in cryptology. The variant consist on extend the allowed characters from Playfair to include every character on the ASCII code. In this case, a 16x16 matrix will be used, to be able to also include the extended characters. The project was developed in Matlab, a programming and design platform that is able to do matrix manipulation and calculation easily.
For the possible implementation, we're going to use a virtual application developed in Matlab using the TCP/IP protocol to send and receive encrypted messages.

Index Terms—**cryptology, playf air. Matlab, codifired**

I. Introduction

Playfair is a polygraphic substitution system that to each pair of letters from the text, corresponds another pair of letters in the encrypted text; to this end, the message is separated in pairs of letters and if there's, at the end, one letter alone, an 'X' is going to be introduced to make the final number of letters in the text even, which allows us to put it into the matrix and get a good arrangement.
This encryption method has some rules, which are:

- The message to encrypt has to be separated in pairs of letters. An 'X' is going to be introduced in case of repetition or, at the end, if the number of letters in the message is odd.
- If the two letters of the digraph are in the same row, but different column, each letter is displaced one column to the right to cypher them (If one of the letters is at the end of the row, the first letter of the row is replaced by the letter that was at the end of the row).
- If both letters of the digraph are in the same column, but different row, each letter is displaced one row down (If one the letters is at the end of the column, the first letter of the column is replaced by the letter that was at the end of the column).
- Letters in different lines and columns: the letters of the bigram make a "quadrilateral" and are replaced by the letters in the contrary vertices of the quadrilateral.

To look at an example with a 5x5 matrix, look at table 1
Message: hola barbara
Key word: buap
Pair separated message: HO LA BA RB AR AX

B	u	a	p	c
D	e	F	g	h
i/j	k	L	m	n
O	q	R	s	t
V	w	X	y	z

Table 1: 5x5 matrix

Encrypted message following the algorithm rules: DT FR UP OA FX FA

II. Project Development

Here we're going to make a detailed explanation of how the algorithm was developed. It is important to emphasize that this code is inside a Matlab's development interface (GUI), so a lot of the code for the interface is automatically generated.

A. *Message Cypher With The Playfair Algorithm*

The ciphering logic is going to be divided in the next six steps:

1. "Key reduce" step

   For this step we take the key word value with the objective to reduce the repeated characters in the key. To this end, first we convert every repeated character into null characters and then we eliminate those characters, reducing the matrix size. For example, if we have the word "chocolate" as key, at the end of this step we'll have the word "cholate" as key.

Barbara Emma Sanchez Rinza,Faculty of computer sciences, Benemerita Universidad Autonoma de Puebla, Puebla Pue. Mexico,
Ruth Itzel Gutiérrez Castro, Emmanuel Félix Valenzuela

2. "ASCII vector creation" step

   In this step, we transform a vector that goes from 0 to 255 into ASCII characters.

3. "Key vector + ASCII creation"

   In this step we put together the reduced key and the ASCII vector, after that the repeated characters are eliminated again. The size of the vector must be of 256 characters.

4. "Matrix creation" step

   In this step we convert the key vector + ASCII to a 16x16 matrix, where each matrix' element contains an ASCII character.

5. "Even size convertion of the message" step

   The Playfair method works with pairs of characters in the message we want to cypher, for that reason we have to extend the message if we have an odd number of characters; to this end, an X (or null character) is included at the end of the message if the number of characters is odd.

6. "Cypher rules application" step

   This is the last and longest step. Here we use the encryption rules to convert both characters of every pair of letters in the message.

B. Decipher Playfair Algorithm

To do the decipher, we use the inverse of the encryption rules, reutilizing the matrix we used on the ciphering.

III. The Interface

For the interface (look at figure 1) every button and the text box "Clave" were built. We're going to explain the function of every element of the interface.

Both applications have practically the same structure, the only difference is in the beginning of each application with the buttons "Abrir Servidor" and "Conectar".

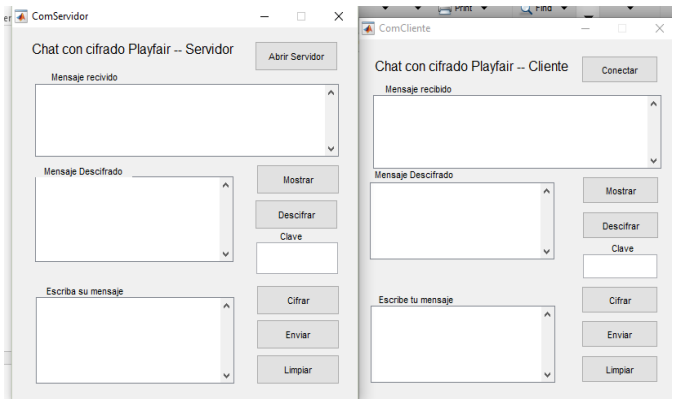

Figure 1: Chat graphic interface

➢ "Open Server" button
  ○ With this button, the TCP/IP protocol is opened to allow the communication. At the time the connection with another interface is completed, it shows a welcome message and sends an identical one to the other interface. Said message is eliminated after two seconds.

➢ "Connect" button
  ○ If a server looking for a client is found, pressing this button will create a communication between this interface and the server. At the time of the connection, a welcome message sent from the server will be shown. This message will also be eliminated after two seconds.

➢ "Send" buttons
  ○ This buttons look for the text in a text box and send it to the other interface.

➢ "Show" buttons
  ○ Here the sent (by the other interface) message is accepted and is shown in the screen.

"Key" text box

Here we have the playfair cipher. We put i here with the intention that, when the key is changed, the ciphering will be different. Here is found the code up to the matrix generation step.

➢ "Cipher" buttons
  ○ Apply the encryption rules to the message to be sent.

➢ "Decipher" buttons
  ○ Apply the deciphering rules (inverse to the encryption rules) to the received text box and shows them in a second text box.

➢ "Clean" buttons
  ○ This buttons erase the text written by the user in every text box to be filled again with new text.

To send simple messages, it is as simple as writing them in the last text box and press the "send" button (look at figure 2). This is useful because not every message that we send require the added security, that's why the chat has the two options to send either encrypted or normal messages.

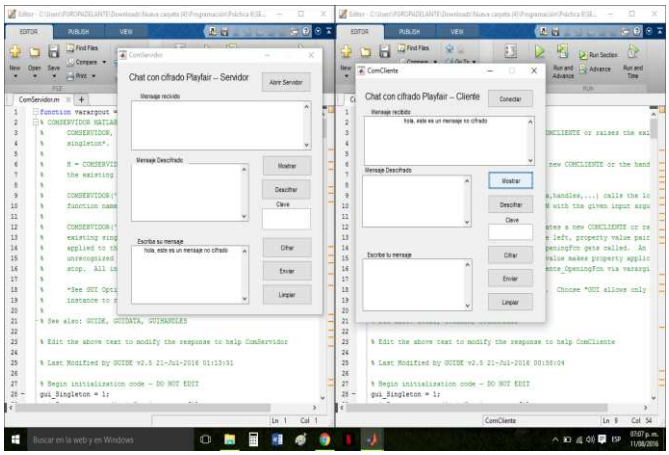

Figure 2: Screenshot where the unmodified text is shown both by the sender and the receiver

The message must be accepted from the other window to

receive it, to this end, the "Show" button on the first text box must be pressed, as observed in the figure 2. But if we want to cipher the information, this chat allow us to send encrypted messages, to that end, we write the message in the box and, after that, we press the button "Cipher", this can be appreciated in figure 3.

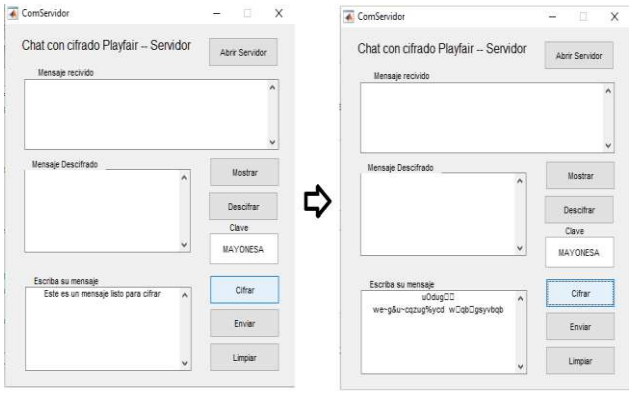

Figure 3: Encrypted Text

To cipher the messages, it must be written both a key, in the little text box on the right of the interface, and a message; after that, the "Cipher" button must be pressed and this will send the encrypted message to the receiver as shown in figure 4.

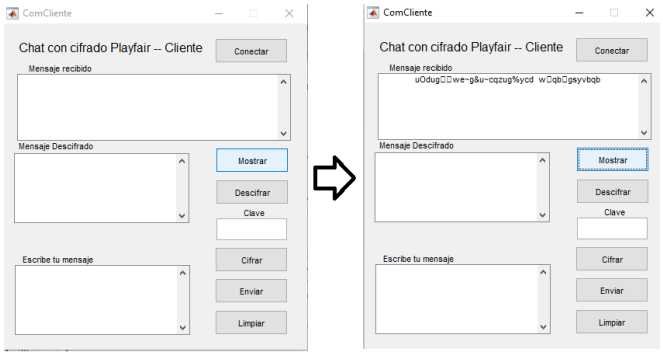

Figure 4: Encrypted text shown in the screen of the receiver

To decipher the encrypted message, the "Decipher" button must be pressed after the message is shown in the box. The deciphered message will be shown in the text box in the middle, as we can see in figure 5.

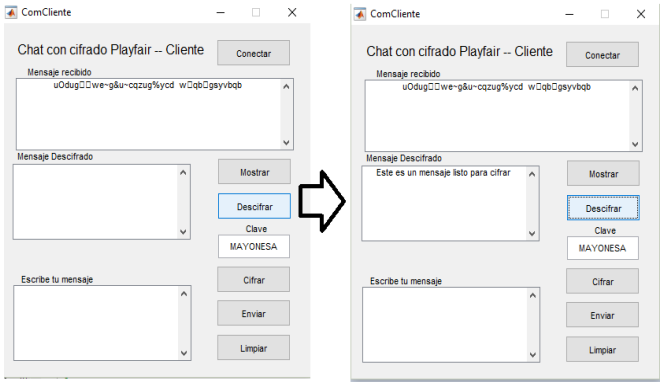

Figure 5: Deciphering of the message by the application

IV. CONCLUSION

The work successfully achieves the communication between the applications using the TCP/IP protocols with the objective to send and receive both encrypted and normal messages.

The encryption was realized using a variant of the Playfair algorithm that results very helpful in the message hiding.

As the chat works flawlessly in the computer, the next step is to apply it successfully on mobile devices.

REFERENCES

[1] Barbara Emma Sanchez Rinza, *Security system for sending voice signals hiding information using steganography using Matlab, IJEIT, volummen 6 issue 5, November 2016*

[2] Barbara Emma Sanchez Rinza, *Cesar descryption by the method of frequency points in the Spanish language , IJEIT, volummen 3 issue 5, November 2013*

[3] Barbara Emma Sanchez Rinza, *security system for sending information containing hidden voice data by steganography (siove) using matlab , IJEIT, volummen 5 issue 1, November 2015*

Bárbara Emma Sánchez Rinza Bachelor in Physics, Master Degree in Optics, Doctor's Degree in Optics. She has written 43 chapters of books, 33 national and international articles, 120 memoirs. She has participated in 104 conferences in different forums. She has directed 27 Bachelor Thesis and 6 Master Thesis.