Chat que codifica la información por medio de play fair

Bárbara-Emma Sánchez-Rinza
Facultad de computación, Benemérita Universidad Autónoma de Puebla, México
brinza@hotmail.com

Carla Maritza Rojas Ramos
Facultad de computación, Benemérita Universidad Autónoma de Puebla

Resumen

El presente trabajo realizado se aplicó el algoritmo de plat fair a un chat, para la seguridad de la información, buscando un mecanismo de comunicación adecuado donde el paso de información sea seguro, el más fácil en cuanto a la programación y donde pueda ser mejor visualizado por cualquier usuario.

1. Introducción

La comunicación entre los seres humanos ha existido desde tiempos remotos desde la imprenta, el telégrafo, la televisión y entre otros inventos que creo el ser humano para comunicarse, pero uno que ha marcado una era en la tecnología en las comunicaciones ha sido la computadora y con ella la creación de múltiples software que ha facilitado la vida de las personas.

El chat a través de la computadora se volvió algo vital, ya que es un método de comunicación digital, en el cual dos o más personas a través de una computadora escriben mensajes y se envía a la persona deseada.

Pero no todo chat creado es confiable ya que se ha dado en la actualidad el robo de información, en la que "hackers" pueden leer y descargar conversaciones de los chats.

El robo de información es un peligro de la era actual y el cual se crean mecanismos de seguridad para que esto disminuya.

El chat se realizó a través de un socket orientado a conexión es que, para poder comunicarse entre ellos se necesita establecer una conexión, utilizando el protocoló TCP/IP para toda la conexión.

2.-Ejecución del servidor

Una vez ejecutado el servidor aparecerá una ventana como la siguiente (figura 1), donde se mostrara todas las acciones realizadas por los clientes con el fin de ver si todos los movimientos disponibles en el chat se realizaron de manera exitosa.

Figura 1**.** Interfaz del servidor

3.-Ejecución del programa cliente

Se abrirá una pantalla como se muestra en la figura 2, donde al oprimir el botón conectar, abrirá una ventana de diálogo, que pedirá la IP de donde fue levantado el servidor, figura 2. En caso de que el

servidor fue levantado en la misma maquina se puede dejar “localhost” o colocar “127.0.0.1”.

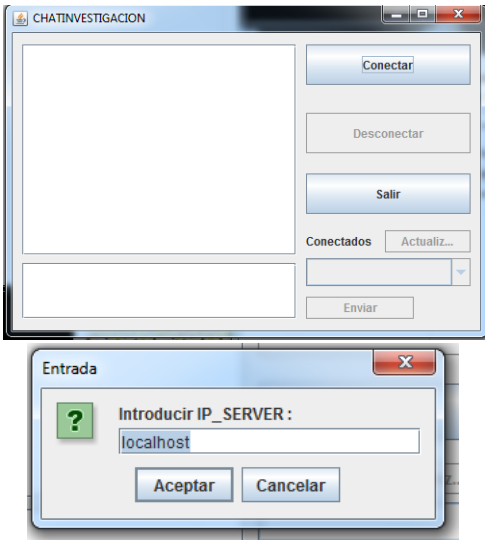

Figura 2.-Imagen de la interfaz del programa cliente y ventana de la IP

Una vez colocado la IP, el cliente se tratara de conectar al servidor, si no hubo ningún problema en la ventana del Servidor mostrara que un cliente se conectó y le asignara un número que lo identifica, en caso contrario la ventana cliente se quedara en espera hasta establecer conexión.

Para poder ver la lista de conectados al servidor solo debemos pulsar el botón Actualizar. Y se mostraran los clientes conectados identificados por un número, figura 3.

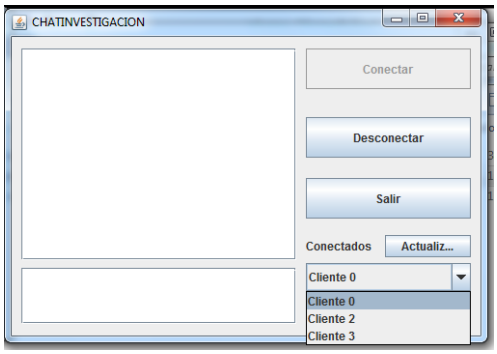

Figura 3**.** En la imagen se muestra los diferentes clientes que están conectados

Una vez seleccionado el cliente con el que queremos comunicarnos, podemos escribir un texto y al pulsar el botón enviar, se le hará llegar al cliente seleccionado. En el cuadro de diálogo mostrara toda la conversación que se haya tenido con el o los diferentes clientes con los que se haya hecho comunicación, como se muestra en la figura 4.

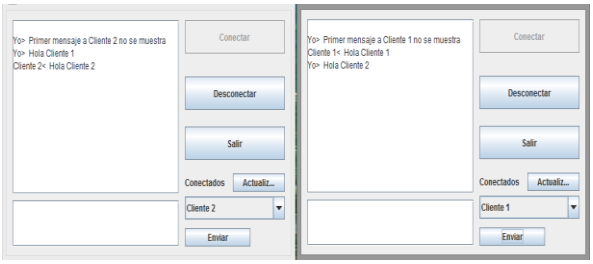

Figura 4. Imagen donde se ha hecho la conexión y se han mandado mensajes

El servidor solo mostrara el cliente que mando mensaje al igual de su destinatario. Para poder desconectare solo en necesario pulsar el botón *Desconectar* o simplemente salirse véase en la figura 5. Y por último, el servidor mostrara que cliente se ha retirado figura 6.

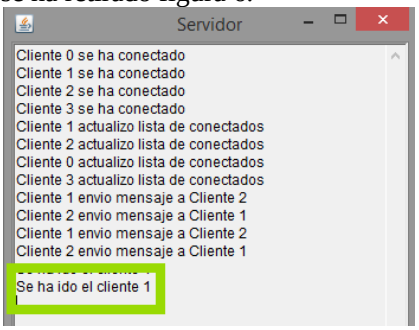

Figura 5**.** El servidor muestra todos los movimientos que se hicieron.

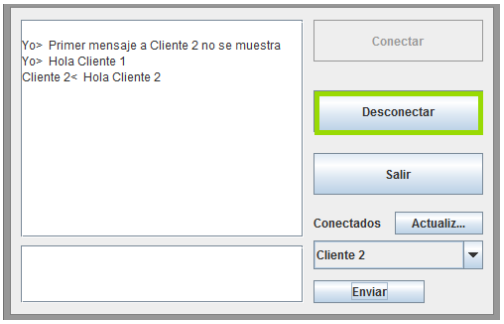

Figura 6**.** Imagen donde se muestran los botones de desconectarse y salir.

Sustitución poli alfabética: El criptograma del texto en claro puede ser diferente dependiendo de la clave que se utilice para cifrar, por lo que se dice que existen múltiples alfabetos de cifrado, de ahí el nombre de sustitución poli alfabética.

Se enfocó la investigación de dos algoritmos de diferente sustitución

4.- Cifrado Playfair

Para que este chat sea seguro se utiizo el cifrado de Playfair requiere que se construya una matriz de 16x16 en donde se coloca el alfabeto después de haber colocado una clave.

El método de cifrado trabaja con dos caracteres (bigrama) a la vez, por lo que el texto en claro se debe descomponer en parejas de dos caracteres. Cada una de las parejas de caracteres obtenidas después de la descomposición se sustituye por otra conforme a las siguientes reglas:

Para efectuar el cifrado se siguen las siguientes reglas:

1. Si el par de letras a cifrar están situadas en filas y columnas diferentes, se forma el rectángulo que tiene como vértices opuestos las dos letras. Las letras de los otros dos vértices forman el texto cifrado, ordenadas por filas de la misma forma que en el texto claro. Es decir que se pone antes en el texto cifrado la letra que se encuentra en la misma fila que la primera letra del texto claro. Por ejemplo, con la tabla anterior al par li le corresponde FA y al par zo le corresponde YB.
2. Si ambas letras se encuentran en la misma fila, se sustituyen por las que se encuentran en la misma fila a su derecha. Si alguna de ellas está en la última columna se sustituye por la letra de la misma fila en la primera columna. Por ejemplo ic se cifraría como TA y od como BN.
3. Igualmente, si están en la misma columna, se cifran mediante las letras que se encuentran justamente debajo de ellas. Si alguna está en la quinta fila, por la de la primera.

   No se pueden cifrar pares compuestos por letras iguales. La solución es procurar que no suceda esto por ejemplo introduciendo una letra con valor nulo entre las dos iguales. Si el número de letras a cifrar es impar, se le añade un nulo al final.

5.- Conclusiones

Después de a ver realizado el trabajo anterior, tanto el algoritmo de playfair como el chat, se concluye que es un buen mecanismo de comunicación los sockets y para el paso de mensajes a través de método de cifrado, los mensajes que se manden por medio de este algoritmos son más seguros.

Referencias:

[1] Sánchez, B. Bigurra, Diana. *et all*. ***De-Encryption of a text in Spanish using probability and statistics***. 18th International Conference on Electronics, Communications and Computers: isbn 07695 3120 2 march 2008.

[2] Sánchez, B. Cruz, S. ***Cesar decryption algorithm, but the method of frequency points in the Spanish language***. International Journal of Engineering and Innovative Technology, vol 3, issui 5 november 2013 issn 2277375

[3]Aceituno C. Vicente, ***Seguridad de lainformación***, First edition, EditorialLimusa,Mexico, 2006. ISBN 968-18-6856-0.

[4]Pino C. Gil, **Seguridad informática. Técnicas criptográfica,** First edition. Editorial Alfaomega, Mexico, 1997. ISBN 970-15-0328-7.

[5]Cole E., Krutz, R., Conley J. W., ***Network Security Bible***, Wiley, Indianapolis, IN, 2006. ISBN 0-7645-7397-7.

[6]Nestler V. J., Conklin W. A., White G. B., Hirsch M. P., ***Computer Security Lab Manual***, McGraw-Hill/Irwin, NY, 2006. ISBN 0-07-225508-0.

[7]Gómez V. Álvaro, ***Enciclopedia de la seguridad informática***, First edition, Editorial Alfaomega, Mexico, 2007. ISBN 978-970-15-1266-