Doble grado de Informática y Matemáticas

Fundamentos de Redes

Definición e implementacin de un protocolo de aplicación

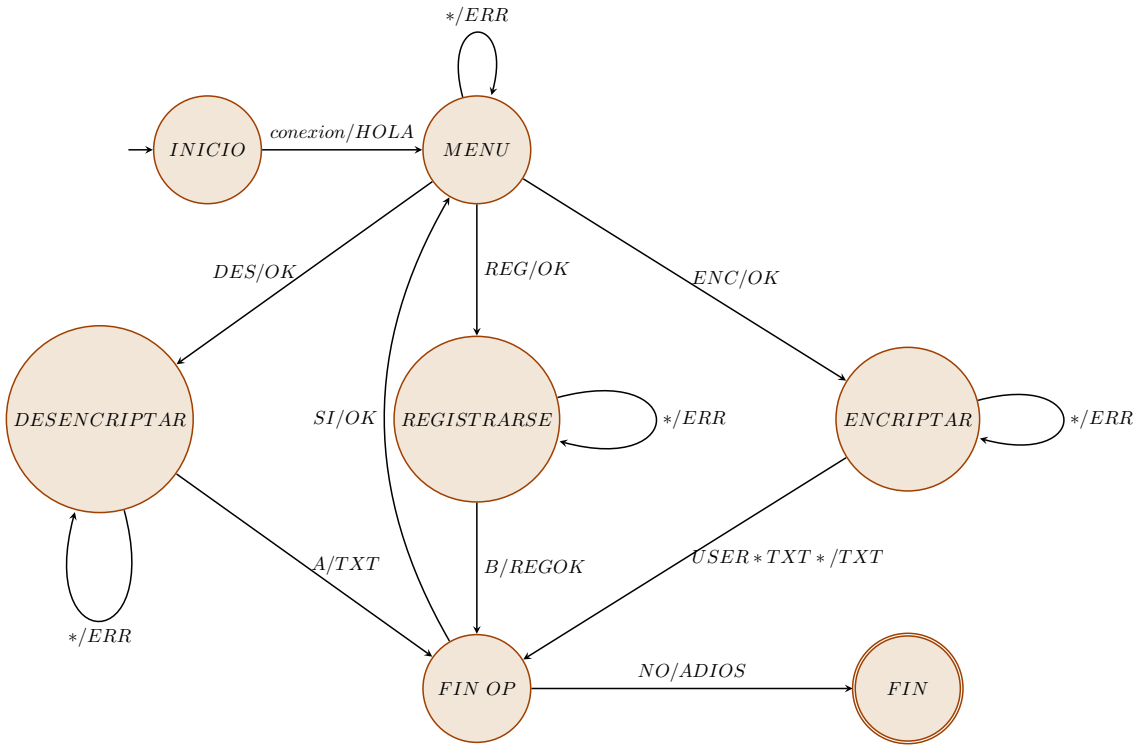
Johanna Capote Robayna
Guillermo Galindo Ortuo

1 Descripción de la aplicación, funcionalidad y actores que intervienen

Nuestro proyecto se basa en un encriptador y desencriptador de mensajes. En este caso hemos utilizado una estructura de cliente-servidor, en la que el cliente será el que desea encriptar o descriptar un mensaje mienteas que el servidor será el que se encargue de estas tareas. El servidor permite que que varios clientes se conecten cocurrentemente.
Basicamente, el sistema de encriptado funciona mediante claves publicas y privadas, a cada cliente que se registre en el servidor con un usuario y una contrasea se le asigna una clave pública y una clave privada. Cuando un cliente solicite encriptar un mensaje se pedirá el login del usuario destinatario, y este mensaje se cifrara con las claves del usuario registrado y se devolverá el mensaje encriptado. Y viceversa, si se quire desencriptar un mensaje, el cliente se identificara con su login y contrasea y adjuntará el mensaje encriptado que quiere desencriptar, acto seguido el servidor le devolvera el mensaje desencriptado.
Para este proyecto usaremos sockets TCP lo que nos garantiza un orden FIFO, importante para que los mensajes se transmitan correctamente, y además se garantiza que la comunicación entre el servidor y los clientes es fiable.

2 Diagrama de estados del servidor

El programa comienza en un estado de INICIO, el cliente realiza la conexión pasando así al MENU. En este caso, el cliente puede elegir entre 3 opciones: registrarse, encriptar o desencriptar. Para REGISTRARSE el servidor le pedirá un usuario y una clave, si el usuario es correcto el servidor devolverá un mensaje de "regok".Para ENCRIPTAR el cliente deberá introducir el usuario destinatario y el mensaje, devolviendo el servidor el texto encriptado. Y por último para DESENCRIPTAR el cliente debe introducir su usuario y contrasea y el texto a desencriptar, a lo que el servidor devuelve el mensaje desencriptado.
Si ocurre algún error, como introducir un usuario y una contrasea erronea, o una opción inexistente, el programa volverá a pedir estos datos. Y a la finalización de la operación elegida, se volverá otra vez al menu principal pudiendo el cliente as completar varios propositos.



Donde $A = USER * PASS * TXT *$ $B = USER * PASS *$

3 Mensajes que intervienen

Cdigo	Cuerpo	Descripcin
1001	HOLA	Conexin establecida correctamente
1002	DES	Peticin de desencriptacion
1003	ENC	Peticin de encriptacin
1004	REG	Peticin de registro
1005	OK	Opcin escogida correcta
1006	A	Mensaje con un texto a desencriptar y las credenciales del receptor
1007	TXT	Texto obtenido tras encriptar o desencriptar
1008	B	Credenciales para registrarse
1009	REGOK	Registro exitoso
1010	$USER*TXT*$	Texto a encriptar y usario destino
1011	SI	Seguir realizando operaciones
1012	ADIOS	Desconexin del programa

4 Evaluación de la aplicación

En este apartado se muestra un ejemplo de ejecución del programa.

```
Menu de opciones: (1)Registrarse (2)Encriptar (3)Desencriptar (-1)Salir
1
OK
Introduzca el login que quiere:
johanna
OK
Introduzca el password:
ajedrez
REGOK
Menu de opciones: (1)Registrarse (2)Encriptar (3)Desencriptar (-1)Salir
2
OK
Introduzca el usuario al que le quiere enviar el mensaje encriptado:
johanna
OK
Introduzca el mensaje que le quiere encriptar:
hola
O8T+slySeBSrF/6MZRze+qHs55TAIUyZUKyR4BZWoj3bHkb0RhwXR/Go06t9nax1qvNipk6uoyNzSJfr/Rxa5
Menu de opciones: (1)Registrarse (2)Encriptar (3)Desencriptar (-1)Salir
3
OK
Login:
johanna

Password:
ajedrez
OK
Introduzca el mensaje que le quiere desencriptar:
O8T+slySeBSrF/6MZRze+qHs55TAIUyZUKyR4BZWoj3bHkb0RhwXR/Go06t9nax1qvNipk6uoyNzSJfr/Rxa5
hola
Menu de opciones: (1)Registrarse (2)Encriptar (3)Desencriptar (-1)Salir
-1
-1
BUILD SUCCESSFUL (total time: 1 minute 17 seconds)
```

Como podemos observar un usuario se puede registrar, encriptar un mensaje y desencriptarlo sin ningún problema.