

Manual de usuario

CP²-D

producto de “RSA Daniel Production”

Bienvenido a la aplicación CP²-D. Esta aplicación le permitirá mandar y recibir mensajes en una red local de manera muy segura y sin la necesidad de tener el contacto físico entre los usuarios.

Instalación

PASO 1:

Para empezar a usar CP²-D primero hay que instalar el programa “CP2-D-1.5.py” y colocarlo en una carpeta que será reservada para esta aplicación.

PASO 2:

En su red local (LAN / WLAN / CAN...) tiene que crear (si no existe) una carpeta compartida a la que tendrán acceso todos los usuarios de la red. En esta carpeta se van a colocar los mensajes enviados así como una lista de los usuarios de CP²-D de esa red (“Contactos.txt”) que hará las veces de una base de datos. Es muy importante que esta carpeta compartida no sea la misma en la que está situado el programa “CP2-D-1.5.py” ya que eso pondría en riesgo la seguridad de comunicación.

PASO 3:

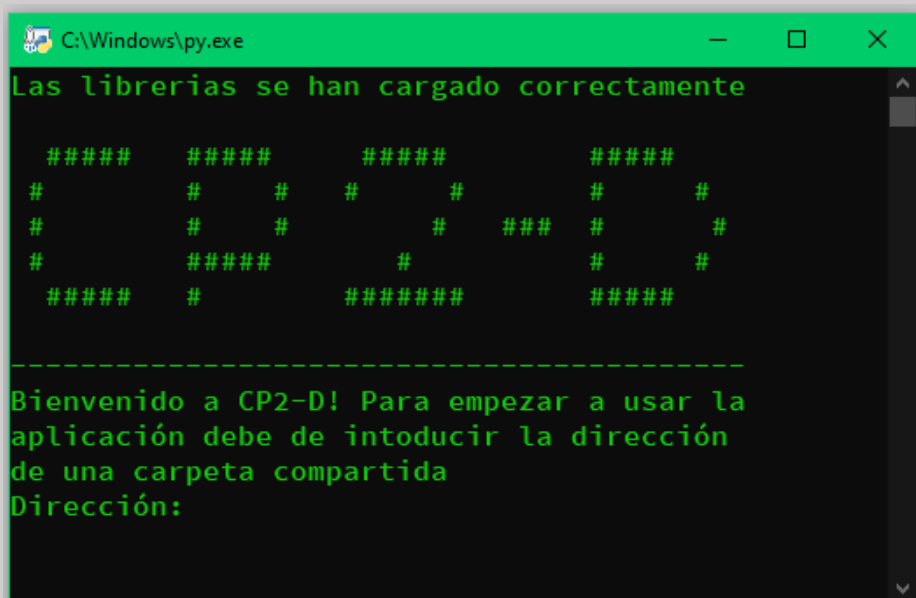
Para el correcto funcionamiento del programa es necesario tener instalado la última versión de Python. Además hay que instalar un módulo extra de Python. Esto se hace de la siguiente manera:

1. Se abre la consola de Windows (se hace pulsando WINDOWS + R y luego poniendo en la ventana abierta “cmd”)
2. En la consola se introduce el comando “`pip install gmpy2`” y se pulsa la tecla ENTER
3. Al finalizar el proceso tendrá el módulo necesario instalado

Este módulo es imprescindible para el proceso de cifrado y descifrado ya que permite elevar grandes números a grandes potencias en aritmética modular con tremenda velocidad y eficiencia.

Uso

Al terminar el proceso de instalación puede iniciar la aplicación (se abre al ejecutar el programa “CP2-D-1.5.py”). Al iniciar CP²-D se abre la siguiente ventana:



```
C:\Windows\py.exe
Las librerías se han cargado correctamente

#####
#           #           #           #           #
#           #           #           #           #
#           #####           #           #
##### #           #####           #####

-----
Bienvenido a CP2-D! Para empezar a usar la
aplicación debe de introducir la dirección
de una carpeta compartida
Dirección:
```

Al hacerlo por primera vez tendrá que introducir la dirección de la carpeta compartida, en la cual se creará la lista de contactos. Además se creará el archivo “shared_folder.bin” en la carpeta del programa (donde está “CP2-D-1.5.py”). En el caso de necesidad de cambiar la dirección de la carpeta que se usa como compartida debe de eliminar este archivo (“shared_folder.bin”), por lo cual el programa se lo volverá a preguntar una dirección nueva.

NOTA: Si en la parte superior de la ventana en vez de “Las librerías se han cargado correctamente”, pone “ERROR: La librería gmpy2 no ha podido ser cargada” es que no tiene descargado el modulo extra de Python (gmpy2) del PASO 3 del proceso de instalación.

El programa tiene tres opciones: para cifrar un mensaje, descifrar uno o cerrar la aplicación (terminar):

Al elegir la opción “*cifrar*” simplemente hay que seguir las instrucciones del programa y el mensaje cifrado se colocará en la carpeta compartida con el nombre “encrypted_message_5.bin”. El número marcado en azul cambia según el destinatario elegido. También hay que tener en cuenta que los mensajes se envían de forma anónima para que ninguno de los miembros de la red pueda vigilar las conversaciones mantenidas. Por lo cual se recomienda firmar los mensajes enviados especificando de quien son en el mismo mensaje (si quiere que el destinatario lo sepa).

Al elegir la opción “*descifrar*” por primera vez se iniciará el proceso de creación del usuario, por tanto se le pedirá su nombre que no debe contener espacios en si mismo ni tampoco coincidir con el nombre de otro usuario (en el caso de coincidencia el programa pedirá introducir otro nombre). El proceso de creación del usuario puede tardar un rato. Suelen ser 10-40 minutos (aunque puede variar según la potencia de su ordenador). Durante ese proceso no se recomienda cerrar el programa o apagar el equipo, ya que se perderá el progreso de creación de claves. Una vez creada la cuenta su nombre junto con el numero asignado y las claves públicas aparecerá en la lista de los contactos de la carpeta compartida. La creación de la cuenta se realiza solo una vez, pero si quiere crear otra cuenta hay que eliminar el archivo “private_key.bin” que estará en la misma carpeta que el programa. Entonces la cuenta con sus claves se eliminará sin posibilidad de recuperarla.

NOTA: En la carpeta del programa también van a aparecer varios ficheros tipo “encoded_message_... .bin”. Son ficheros temporales que se crean en el proceso de cifrado y descifrado y de los que se puede recuperar los mensajes que han sido enviados (aunque para ello se necesita otro software). También en el fichero “encoded_message.bin” estará guardado el último mensaje recibido.

Finalmente, para descifrar un mensaje destinado a su cuenta solamente tiene que elegir la opción “*descifrar*”.

Con esto ya puede usar la aplicación CP²-D de manera cómoda y efectiva. Si tiene alguna pregunta o problema, no dude en ponerse en contacto con nuestro equipo de soporte técnico.