ASRAR AL-MUJAHIDEEN 2.0

Terr0r1st extras

> It is entirely up to you on how to establish communication between contacts without being obvious to the intelligence services that you are using this program.

In the previous issue, we discussed in-depth the main function of *Asrar al-Mujahideen 2.0*, namely its communication methods through the use of encryption. Here, we will be touching on some of the extra functions of the program that you can find useful. We will talk about encrypting and decrypting files on your computer. Afterwards, we will discuss the File Shredder process.

Before we start talking about that, it is important to note that getting caught from the intelligence services for using this program will most likely end you up in prison. So we have explained how to use the program, but it is entirely up to you on how to establish communication between contacts without being obvious to the intelligence services that you are using this program. It will take research and exploration on your part in order to devise a well-thought out plan to keep every identity safe.

1. Encrypt File

Let's say you have a Word Document on your computer that you don't want any prying eyes to see. You could just use the hidden feature available on the system or bury the file somewhere in some system file, but it's still possible that someone can find it if he searches hard enough. For law enforcement agencies however, finding files isn't much of an issue. They have programs exclusive to their departments that can seek out what they are looking for based on both the file name and its contents. In order to have some peace of mind, the encryption method would be the best alternative to take.

Towards the bottom of Figure 1.0, you will see a series of tabs. The first of them is 'Select File to Encrypt'. This is what we want. What will happen in this process of encryption is that a copy of your file will be made and converted into an unreadable format, leaving the original intact. In order to get rid of the original, place a check in 'Shred Out Original File' towards the bottom.

Next, click the yellow folder to the right to select your file. When you click open, you will see the path bar filled in. If not, try again.

Next, you will choose your Pub/Priv key and click the large red arrow. Then you will choose the one which will be able to see your encrypted file and click the large blue arrow.

Afterwards click 'Encrypt File' towards the top left of the menu. You should get a message saying that the file was encrypted successfully. You should then see a file that ends with .enc in the same place your original file is. If you get an error saying 'No mail box specified', then it means you haven't properly chosen either the Local or Remote User (i.e., the blue and red arrows).

2. Decrypt File

Decrypting the file you made is the same process as above. In the main window, you will click on the tab on the bottom 'Select File to Decrypt'. Click the yellow folder to select your file then click 'Decrypt File' at the top left in the menu. You will be asked for your password. Type it in and click OK. Once that's finished, depending on the size of the file, it will take some time to decrypt. You should then get a message saying that the file was decrypted successfully. In the same folder where your encrypted file is, a new folder will be automatically created called

'Decrypted'. In it you will find your file.

3. File Shredder

Many intelligence officers are able to find deleted files on a hard drive through the use of specially made programs. For instance, let's say a person deleted a file and formatted their computer. After a few years, the hard drive falls into the hands of the intelligence agency. Through their programs, there's a high possibility of them recovering that file. The *Asrar* program has a feature for permanently deleting your files, making it harder for the enemy to retrieve them.

Click on 'File Shredder' on the left menu.

From here, the process is simple. In Figure 1.3 you will see three columns. Starting from the left, the first column shows the root folders and disks of your computer. You will select the folder in which your file is located from here. Once you select the folder, the second column displays all the files in that folder. To delete the file, simply click on it, drag it into the third column and click the 'Shred Files' button towards the bottom.

There are many programs that can do the same. If you ever come across them, you will find options such as wiping three times over, seven times over and so on. This just means that the process of deletion will be repeated that many times. The more times it is wiped over, the safer is your hard drive from prying eyes. The minimum wipe times you should use is 7 times.

FIGURE 1.0

FIGURE 1.0: The first tab in the bottom panel will allow you to encrypt any file of your choosing.

FIGURE 1.1

FIGURE 1.1: Select your Pub/Priv key as the local user & then choose a remote user. Then click Encrypt File.

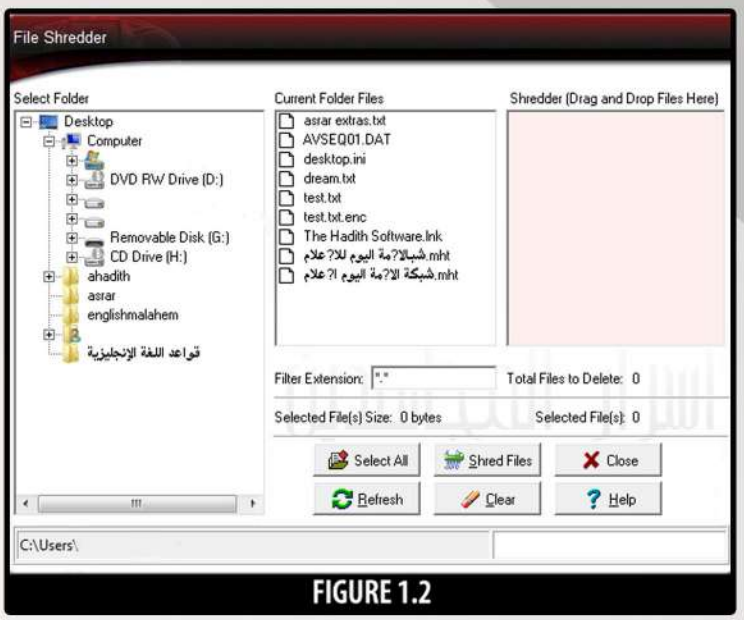

FIGURE 1.2

FIGURE 1.2: Choose the folder in which your file is located. Drag & drop from the second column to the third. Click Shred Files.