Terr0r1st

How to use Asrar al-Mujahideen:
Sending & Receiving Encrypted Messages

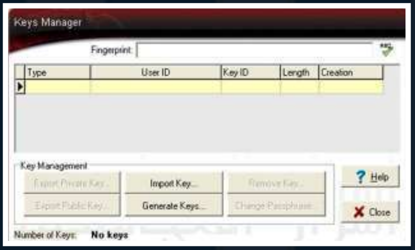
Sending an important message in the old days only required a piece of paper, a writing utensil, and a trustworthy messenger that knows the location of the party you need to reach. Today, this is still an effective method if such a messenger is available and can get around without anyone stopping him. However, for the most part, this method has slowly evaporated and is now replaced with the Internet. Its benefit is that if there is no messenger that exists, access to the other party is only a few clicks of a mouse button away. Its harm is that the spies are actively paying attention to the Emails, especially if you are an individual that is known to be jihādī-minded. So how does one go about sending important messages without it being noticed by the enemy? Following is one method and that is by using an encryption software.

One such software is a program created by our brothers called Asrar al-Mujahideen 2.0. Here, we will discuss how to use this program, how to create your key, how to send and receive the public key of the other party, and how to check if your version of the software is forfeited or not. There are many things you can do with this program besides sending and receiving encrypted messages; we will cover those aspects in later issue, *In Shā' Allāh*.

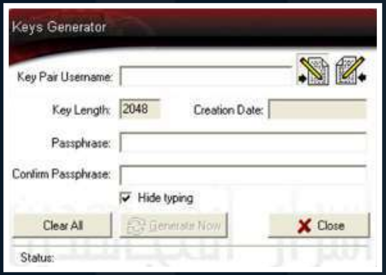
I. CREATING YOUR KEY

After you download Asrar and open the program, you will see the main interface as is:

The first thing you need to do is create a key for yourself. So go ahead and click on 'Keys Manager' on the left hand side menu. You will get a small pop-up menu looking like the image to the left. Go ahead and click on 'Generate Keys' towards the bottom. You will get a pop-up looking like the image on the right:



Number of Keys: No keys



Key Pair Username:

Key Length: 2048

Creation Date:

Passphrase:

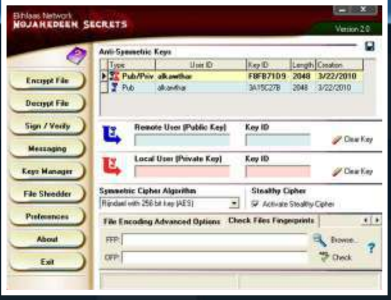
Confirm Passphrase:

☑ Hide typing

Status:

In the first field, you type in your username that you would like to use; it has to be at least 5 characters. If you would like to use Arabic, you just have to click on the button to the far right to change the language. Then for the passphrase, enter in a password that is easy for you to remember, but difficult for anyone to figure out; it has to be at least 8 characters. Afterwards, click on 'Generate Now' at the bottom. This will take some time to create, so be patient. Mines took 10 minutes, so don't be surprised if it's longer.

Afterwards, click 'Close'. Now you are back to the previous pop-up. Click on 'Import Key' and import both the public and private keys. When you do that, it should look like what I have below. When finished, click 'Close'.



Ekhlaas Network
MOJAHEDEEN SECRETS
Version 2.0

Anti-Symmetric Keys

Type	User ID	Key ID	Length	Creation
Pub/Priv	alkawthar	F8FB71D9	2048	3/22/2010
Pub	alkawthar	3A15C27B	2048	3/22/2010

Remote User (Public Key) Key ID

Local User (Private Key) Key ID

Symmetric Cipher Algorithm: Rijndael with 256 bit key (AES)

Stealthy Cipher: ☑ Activate Stealthy Cipher

File Encoding Advanced Options | Check Files Fingerprints

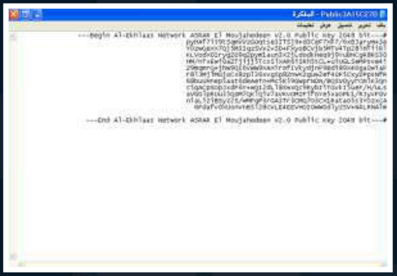
FFP:

OFP:

So now, under the Anti-Symmetric Keys, you should have both your keys listed. The first key is your private key; the second is your public. When you send your key to other people, you always send your public key and never the private one. This is because if they have the private key, they will be asked for your password.

II. IMPORTING YOUR ASSOCIATE'S KEY

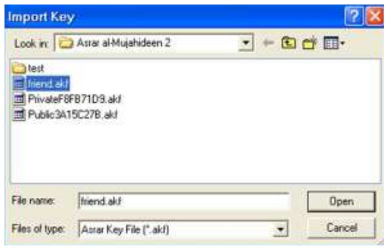
The next step is to import your associate's public key in order to communicate with him. But before we do that, we need to know how to export a key (pretending that you are the friend) and how to send that key. Click on 'Keys Manager' and click 'Export Public Key'. Here, you will notice that your Public Key is readily available from before, sitting in the folder that has the Asrar program. If you save, it's just going to overwrite the same file, so click 'Cancel'. Now access the folder that has your Asrar program and open your Public key using notepad. You will get the image to the left:



المفكرة - Public3A15C27B

```
----Begin Al-Ekhlaas Network ASRAR El Moujahedeen V2.0 Public Key 2048 bit----
[illegible]
----End Al-Ekhlaas Network ASRAR El Moujahedeen V2.0 Public Key 2048 bit----
```

The code sitting in the middle of the two lines is the public key. What you do is copy the entire page, and send that to your associate via any communication method you use such as Email. So now let's pretend that you already sent it over Email and your associate accesses that Email and sees the code. What does he do with it? He needs to first open notepad, and copy and paste the entire code. Save the file (the name doesn't matter) and close it. Then rename the file extension; notepad ends with .txt so we need to change it to .akf by right click, choosing rename and changing the extension. If you are unable to change the extension, then you need to access your folder options in any open window and uncheck 'hide extensions for known file types' [Tools - Folder Options - View]. Once you change it to .akf, go back to the Asrar program and import that public key by clicking 'Keys Manager' and 'Import Key'. Choose the file and click 'Open' to import it. Once imported, click close.



Import Key

Look in: Asrar al-Mujahideen 2

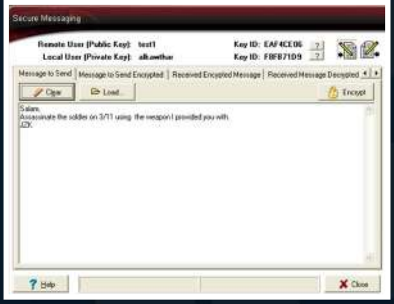
test
friend.akf
PrivateF8FB71D9.akf
Public3A15C27B.akf

File name: friend.akf

Files of type: Asrar Key File (*.akf)

III. ENCRYPTING THE MESSAGE

Now that you have your and your associate's key ready, it's time to send a message to him. On the main interface of Asrar, click on your private key (under 'Type', it starts with 'Pub/Priv') and then click the red arrow to the left of 'Local User (Private Key)' towards the middle. You will do this every single time you want to send a message to someone. Then click on your associate's public key and click the blue arrow to the left of 'Remote User (Public Key)'. You are clicking this because you want to send the message to this individual. If you make a mistake, you can always click 'Clear Key' to the right.



Secure Messaging

Remote User (Public Key): test1 Key ID: EAF4CE06

Local User (Private Key): alkawthar Key ID: F8FB71D9

Message to Send | Message to Send Encrypted | Received Encrypted Message | Received Message Decrypted

Salam,
Assassinate the soldier on 3/11 using the weapon I provided you with.
JZK

Now click on 'Messaging' on the menu bar. Here, you will see a variety of options. For now, we will stick to the tabs entitled, 'Message to Send' and 'Received Encrypted Message'. In the 'Message to Send', write a short message for your friend. If you want to change between Arabic and English, you can click on the buttons on the top right.

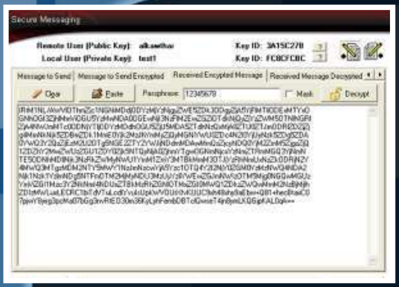
Once finished, click 'Encrypt'. The next step is to send the code between the two lines to your associate through a method that you both agreed upon. Make sure to only send the code in between and not the 'Begin' and 'End' lines since if the authorities or any administrator sees such, it may open the door for more difficulties.

IV. DECRYPTING THE MESSAGE

So now let's pretend that you are the associate and you just received a new message in your Inbox that has all this code. How do you decrypt this code?

First copy the code and open Asrar.[1] Click on your private key and choose the red arrow. Then click on your associate's

[1] Keep in mind, you can only do this part if you have your associate's private key and password since you cannot decrypt your own message unless if you sent it to yourself originallay in the Asrar program; you can always create a set of test keys to try this out.


Secure Messaging
Message to Send
Message to Send Encrypted
Received Encrypted Message
Received Message Decrypted
Clear
Paste
Decrypt

Remote User (Public Key): alkawthar Key ID: 3A15C27B
Local User (Private Key): test1 Key ID: FC8CFCBC
Passphrase: 12345678 □ Mask

[illegible]

public key (that has sent the message) and choose the blue arrow. Click 'Messaging' and then click 'Received Encrypted Message'. In the Passphrase, enter your password. If your password is in English, make sure to click on the button that is left to the top right button. You can uncheck 'Mask' to see if you are entering in your password correctly. Once you enter your password, paste the code into the empty box below and click 'Decrypt'. It will then take a moment to decrypt. If the code decrypted successfully, you will see the secret message from your associate. If you get an error, then it could be because of any of the following reasons:

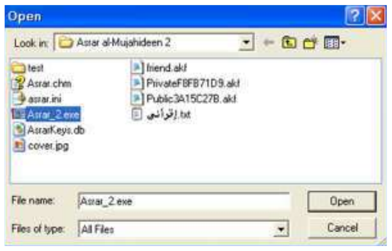
a) You have more than one 'Pub/Priv' key and you chose the wrong one or did not put it in the correct place (i.e., local user).
b) The message is intended for someone else.
c) You copied the code incorrectly; make sure that the code is left aligned. You can do this by pasting it into Microsoft Word or a Rich Text Editor.
d) Your associate did not copy the code correctly.
e) Your associate changed his public key and used a new one to send you the message.
f) You imported the wrong public key.

If you get an error, try to troubleshoot with these reasons in mind. The program is very easy to use, so it's easy to find where the error lies.

Lastly, you can click on 'Save' on the top right to save the message as a text file to your computer.

V. CHECKING THE AUTHENTICITY

Now before you start using Asrar to send and receive encrypted messages, you need to first check if your copy of the Asrar program is legit or not. This is because the enemy has created an Asrar program identical to what the brothers created; the only difference is that the enemy had built in a mechanism that would allow them to spy on your program if they were to just have access to your public key.



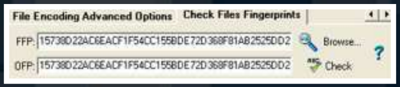
Look in: Asrar al-Mujahideen 2

test
Asrar.chm
asrar.ini
Asrar_2.exe
AsrarKeys.db
cover.jpg
friend.akf
PrivateF8FB71D9.akf
Public3A15C27B.akf
إقرأني.txt

File name: Asrar_2.exe
Files of type: All Files

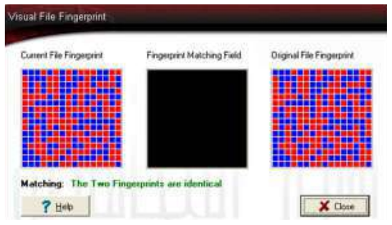
So how do you check the authenticity? First open Asrar. Towards the bottom, you will see a few tabs starting with 'Select File to Encrypt'. Click on the arrow pointing right to go to the last tab entitled, 'Check Files Fingerprints'. Click on 'Browse' and select your Asrar program.

Click 'Open'. You will then see in the FFP field a bunch of characters. Copy and Paste these characters onto the OFP field below.

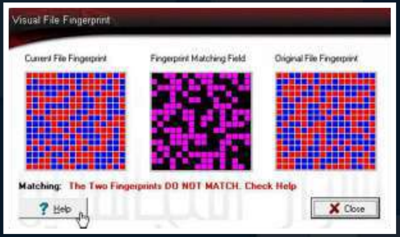


FFP: 15738D22AC6EACF1F54CC155BDE72D368F81AB2525DD2
OFP: 15738D22AC6EACF1F54CC155BDE72D368F81AB2525DD2

Then click on 'Check'. A pop-up box will appear to immediately tell you if your copy of the program is legit or not. If it is legit, it will look like the image to the left. If it is not legit, it will look like the image to the right:



Matching: The Two Fingerprints are identical



Matching: The Two Fingerprints DO NOT MATCH. Check Help

If your program is fraudulent, you would have to find the authentic copy over the Internet and download it and re-run the fingerprint check to make sure it's safe to use. If you have the authentic copy, it's good to story a few extra copies on various formats such as CD, DVD, External Storage Devices and whatnot.

VI. ADVICE

Finally, I would like to give some practical advice to the ones using this program. Firstly, don't trust the program 100% even though it's been proven to be effective and safe. Strive to use other means such as writing letters or leaving messages using special symbols in uninhabited areas. If you need to use the program to contact someone that you have no other way of contacting except through the Internet, then follow these procedures:

a) Never keep the Asrar program on your computer's hard drive. Always have it ready on a USB flash drive that you don't use for anything else. This is because if the Asrar program is available on the hard drive and you access the Internet with that computer, it's possible that the enemy will use spy programs to infiltrate your computer and figure out your password for your private key by recording your key strokes.

b) Don't use this USB flash drive whilst connected to the Internet. Keep your computer offline while writing, encrypting and decrypting messages.

c) Get in the habit of changing your private key password as much as possible. The ideal way would be to change it every time before compiling a new message. To change the password, click on, 'Keys Manager' and 'Change Passphrase'.

d) Use any program that provides USB flash drive protection just in case. Some flash drives now come with security protection; invest in security.

e) When you send your message to your associate over the Internet, use a proxy and an Internet connection that you don't regularly use (such as coffee shops).

f) If you and your associate will use Email as the primary means of communication, then obviously, don't use your regular public Email to send encrypted messages; create a new Email using a proxy and an Internet connection you don't regularly use.

g) Do careful research (using a proxy) and exploration to figure out other alternatives besides Email; if you are confident about its security, use it.