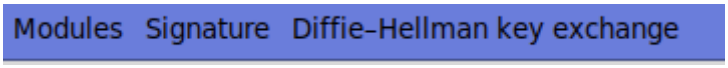
Handbook-02 encryption and decryption

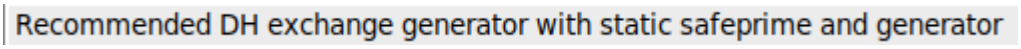
Before you start make sure you have read Handbook-01 signatures and setup .

The first step to get to an encrypted massage to your contact is to establish a shared key for your communication channel. To reach this the Diffie–Hellman key exchange is used.

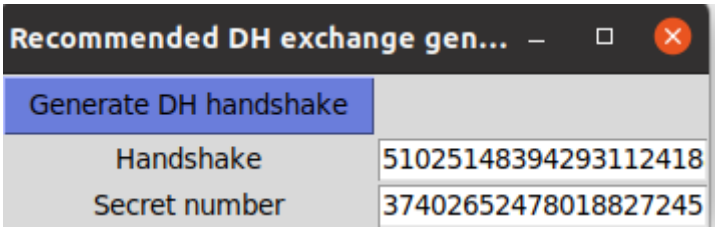
First you click on the menu “Diffie-Hellman key exchange.”



Then you go to the page

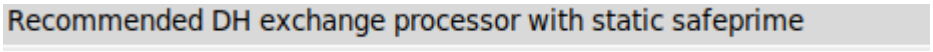


In the new window you can click the”Generate DH handshake” Button.

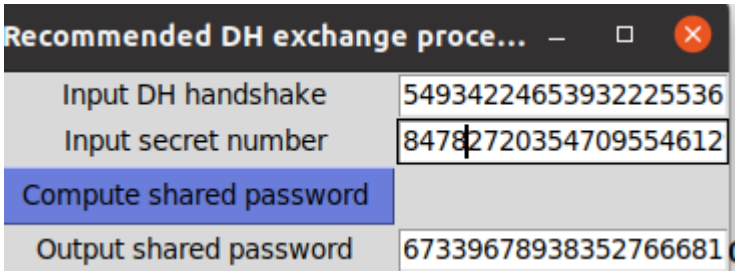


The “Handshake” output is send as a signed massage to your contact as established in Handbook-01.
Your contact does need to follow the same steps and send you his signed handshake.
!Every part of this handshake exchange must be signed and checked by both party s to guard against man in the middle attacks!
The “Secret number”output is only for use in the next step as is the checked Handshake number of your contact.

Now go to the page



Enter the handshake of your contact in the entry “ Input DH handshake”.
Enter your own private number in the entry “Input secret number”
Now press the “Compute shared password” button to generate your shared password

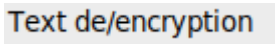


Save your password in the file menu for later use.

Text de/encryption

go to the menu “modules”

Go to the page



Input your shared password you computed with the DH module
Input your message.