

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 message 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.”

Modules Signature Diffie–Hellman key exchange

Then you go to the page

Recommended DH exchange generator with static safeprime and generator

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

Recommended DH exchange gen... — □ ×	
Generate DH handshake	
Handshake	51025148394293112418
Secret number	37402652478018827245

The “Handshake” output is send as a signed message 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 Recommended DH exchange processor with static safeprime

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

Recommended DH exchange proce... — □ ×	
Input DH handshake	54934224653932225536
Input secret number	84782720354709554612
Compute shared password	
Output shared password	67339678938352766681

Save your password in the file menu for later use.

Text de/encryption

go to the menu “modules”

Modules Signature Diffie-Hellman key exchange

Go to the page

Text de/encryption

Input your shared password you computed with the DH module

Input your message.

Modules Signature Diffie-Hellman key exchange	
Password zum Ver/Entschlüsseln	<input type="text" value="examplepassword"/>
<input type="button" value="Verschlüsseln"/>	<input type="button" value="Entschlüsseln"/>
<div>Here is you signed or not signed massage</div>	