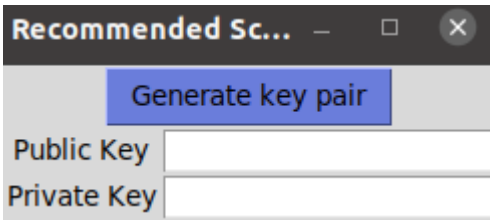
Handbook-01 signatures and setup

1.0 Key generation

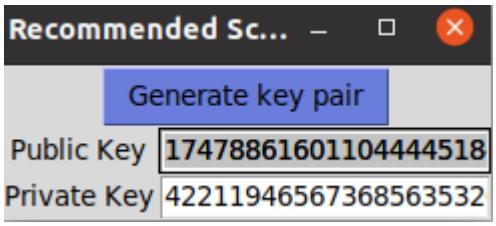
In the menu “Signature”

go to the page „Recommended Schnorr KeyPar generator with static safeprime and generator".

Press on the „Generate key pair“ button to generate your keys.



With a double left mouse click followed by the str+c press on the keyboard you can easily move your Schnorr keys.



Now both numbers must be saved on the PC. It is recommend to use the build in solution on page "Read/write text to secured file"

To keep the signatures secure you can never share your “Private Key” with anyone. If you share this key it can be used to craft messages which appear to be written by yourself.

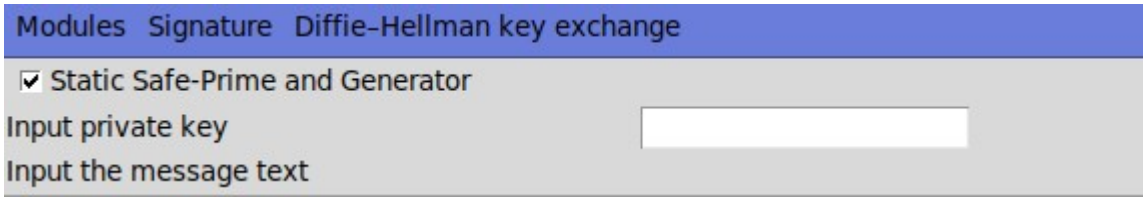
It is necessary for the receiver to have your public key to check the correctness of your generated signatures. You can post or send it as a signed massage with point 2.0.

2.0 Create a Schnorr signature

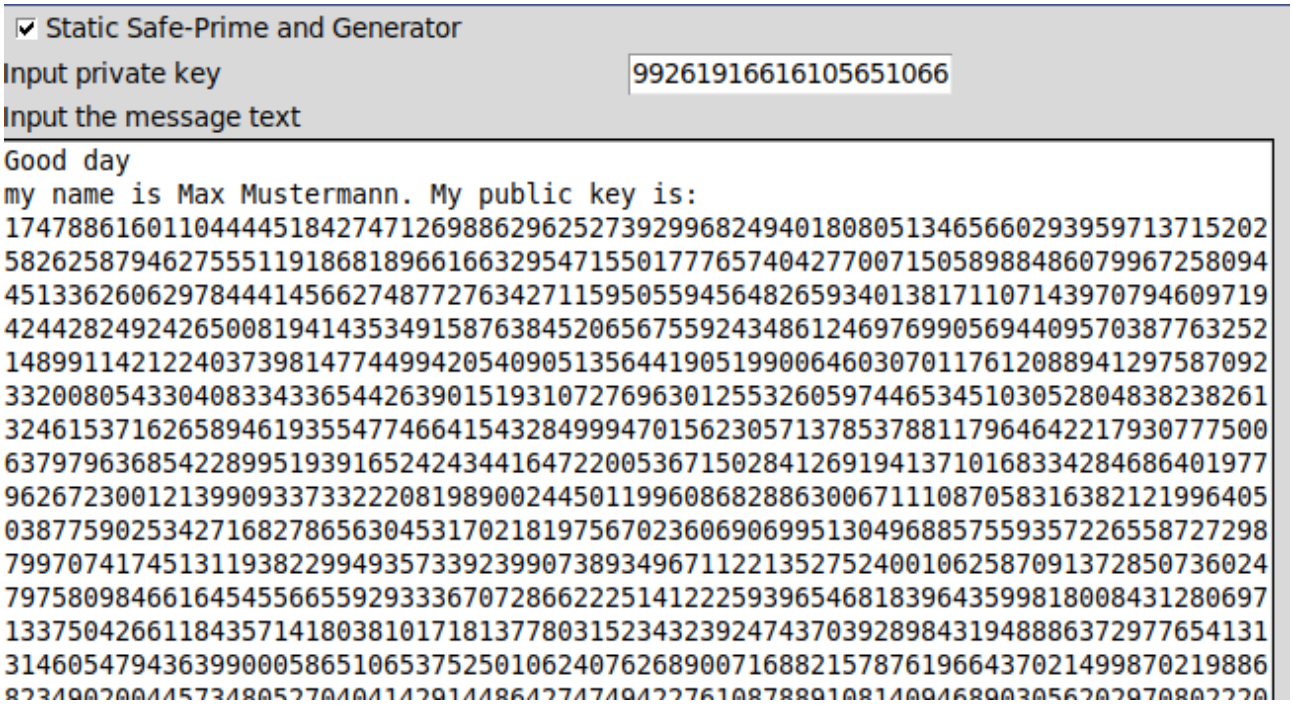
In the menu “Signature”

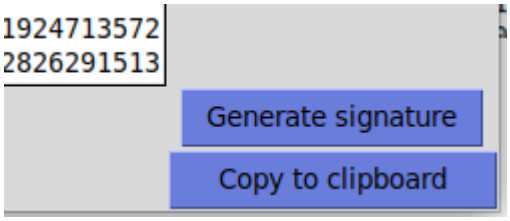
go to the page "Schnorrsig creator"

Input the private key you generated in point 1.0 in the entry with the description “Input private key”.



As an example text I use a random generated public key with a small description.


Static Safe-Prime and Generator
Input private key
9926191661610565106 6
Input the message text
Good day
my name is Max Mustermann. My public key is:
1747886160110444451842747126988629625273929968249401808051346566029395971371520 2
5826258794627555119186818966166329547155017776574042770071505898848607996725809 4
4513362606297844414566274877276342711595055945648265934013817110714397079460971 9
4244282492426500819414353491587638452065675592434861246976990569440957038776325 2
1489911421224037398147744994205409051356441905199006460307011761208894129758709 2
3320080543304083343365442639015193107276963012553260597446534510305280483823826 1
3246153716265894619355477466415432849994701562305713785378811796464221793077750 0
6379796368542289951939165242434416472200536715028412691941371016833428468640197 7
9626723001213990933733222081989002445011996086828863006711108705831638212199640 5
0387759025342716827865630453170218197567023606906995130496885755935722655872729 8
7997074174513119382299493573392399073893496711221352752400106258709137285073602 4
7975809846616454556655929333670728662225141222593965468183964359981800843128069 7
1337504266118435714180381017181377803152343239247437039289843194888637297765413 1
3146054794363990005865106537525010624076268900716882157876196643702149987021988 6
8234902004457348052704041429144864274749422761087889108140946890305620297080222 0

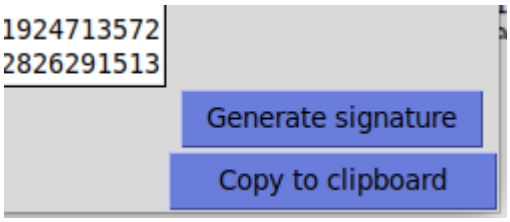


To make recognition of the exact message easier your text gets an added “start------” at the beginning and a “------end” at the end.

The now generated signature part 1 and 2 are used to by your message recipient check your message integrity

To copy all important parts of the signature and message,
press the button “Copy to clipboard”

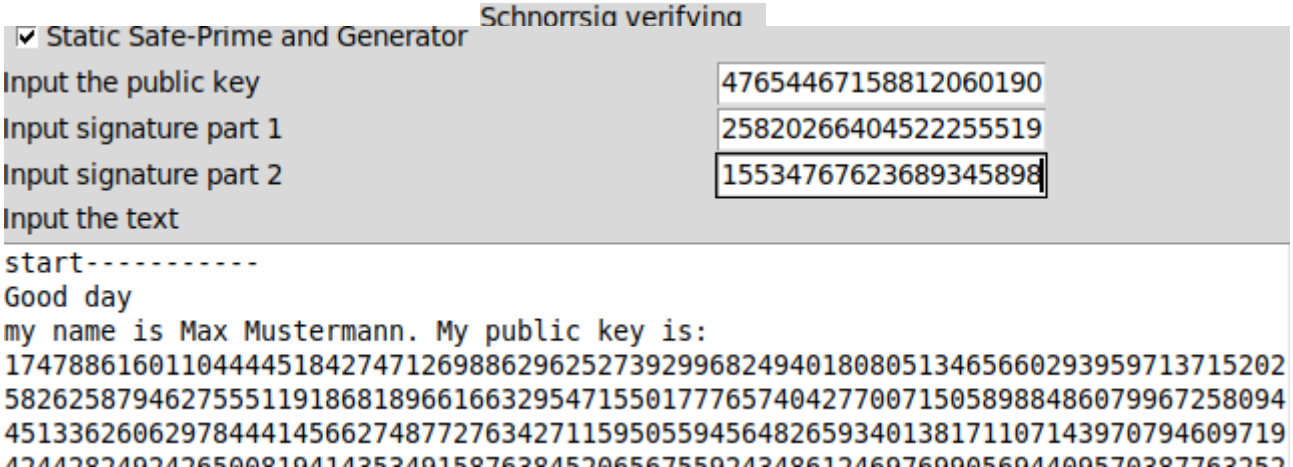
Now you can send the text to whoever you want.



3.0 Verify a Schnorr signature

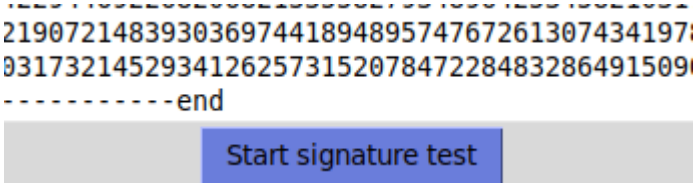
In the menu “Signature”

go to the page “Schnorrsig verifying”

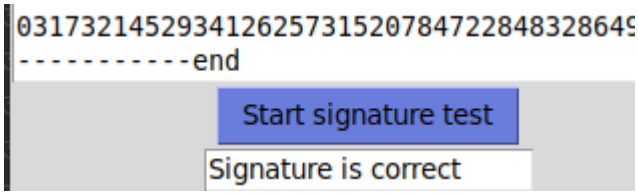


Now fill in the public key of your contact, the message from “start-------” to “----- end”. The signature part 1 and 2 are only for the entry with the description “Input signature part 1” and “Input signature part 2”

Now push the button “Start signature test”



If the message integrity is correct you revive a message about the positive test outcome.



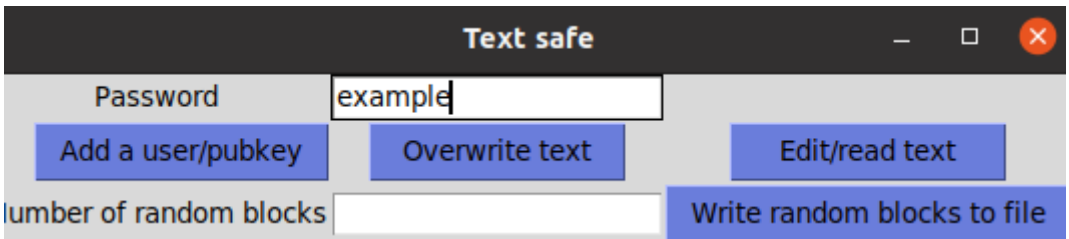
You can get a negative message if one or more of the following points is true:
-wrong public key
-wrong signature 1 or 2
-wrong message

If none of the above are true than please check in the variables have been correctly pasted in the corresponding entry points.

To delete the input of an entry double click with your left mouse button to choose the input and then press delete. You can not overwrite input with double click select and strg+v with the new input. It has to be deleted first

4.0 Save a username and the corresponding public key

Input your chosen password in the password entry.
Then press the “Add a user/pubkey” button.



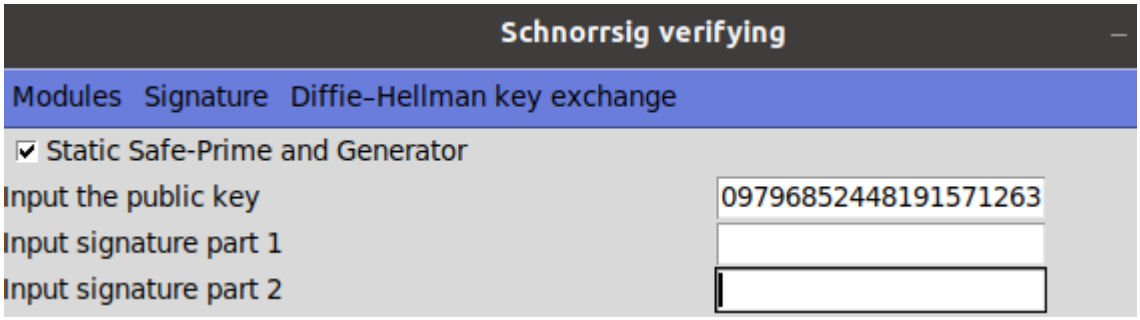
Input in the the “user name” you want to pair to the public key.
Now press the “add user/pubkey pair” button

This adds the pair to your text file. It is important to not change the formating. |user:key since other functions depend on it.

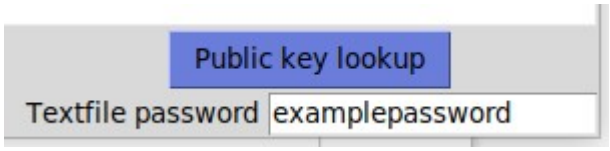
5.0 Check if an public key from a signature is from a known user

Go to the menu “Signatures” and click on “Schnorrsig verifying”

Input the public key of your contact.

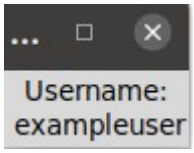


Now input your text file password in the botton right corner of the window.



Now click the button “Public key lookup”

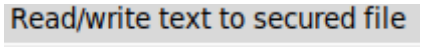
Now a small window will pop up and tell you if you have saved this pubkey to a username and saved it under the given text file password.



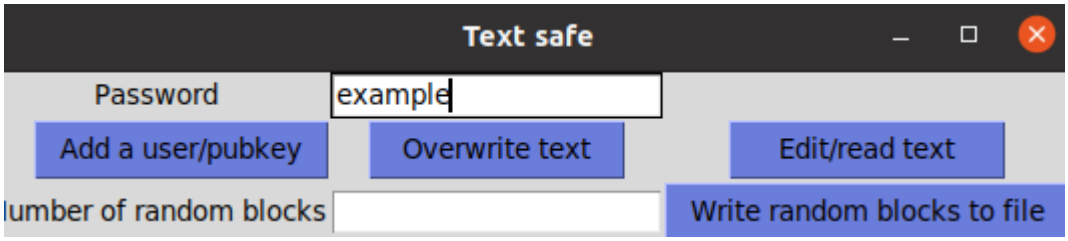
6.0 Write and read from the secured text file

In the menu “Modules”

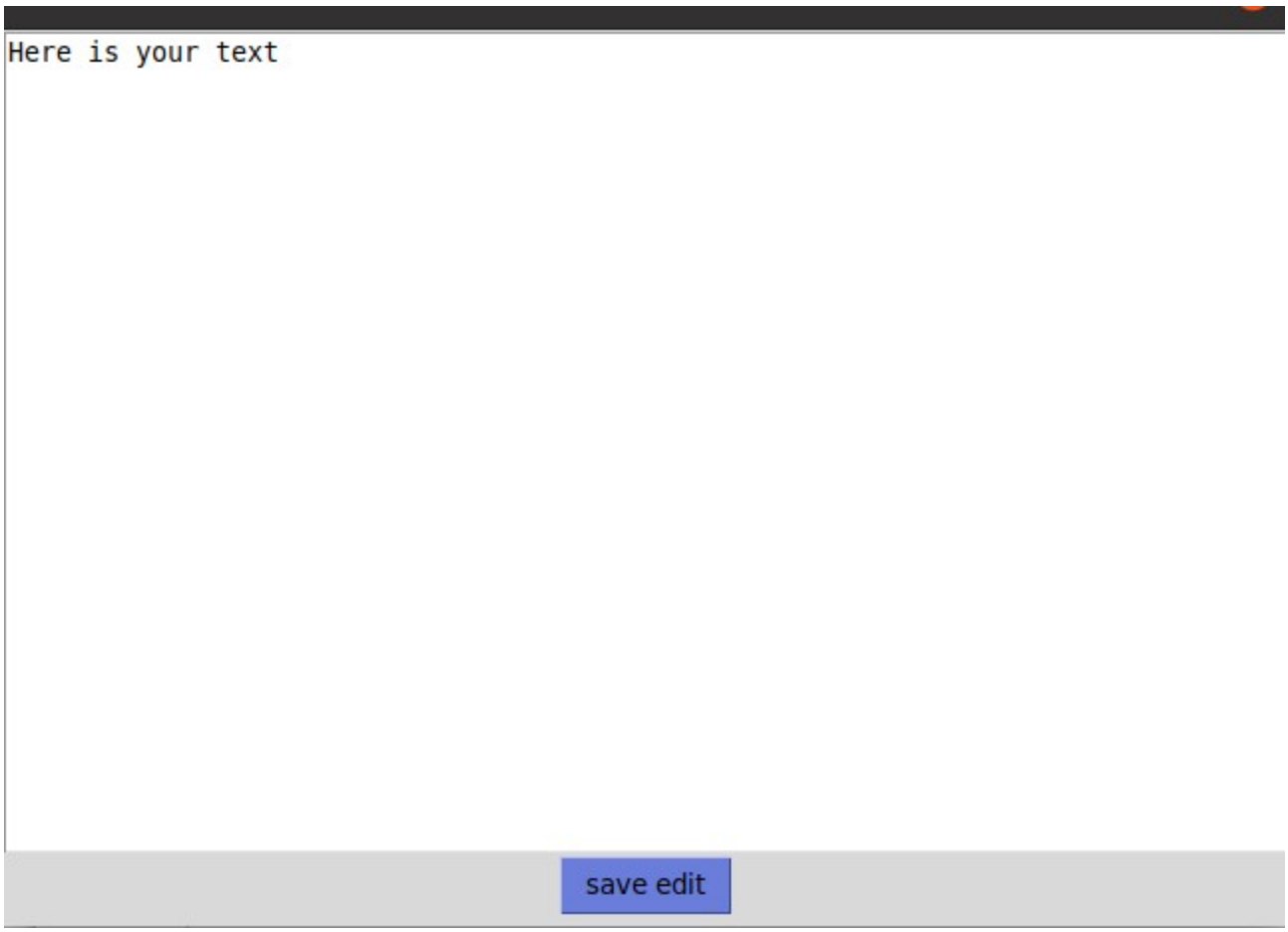
go to the page “Read/write text to secure file”



First input your chosen password for your secure text file.



If you want to read or edit your saved text press the “Edit/read text” button. If there is text saved for this password it will be displayed in the text field.



To save the changed text click in “save change”.

7.0 overwriting text file information

To delete the text saved under a password enter the password and press the button “overwrite text”

8.0 random blocks in the file

This option is important for **deniable encryption.** Only if this option is important to you should the fuction be used. Be carful what your input is. Each block cost an 129byte of disk space!