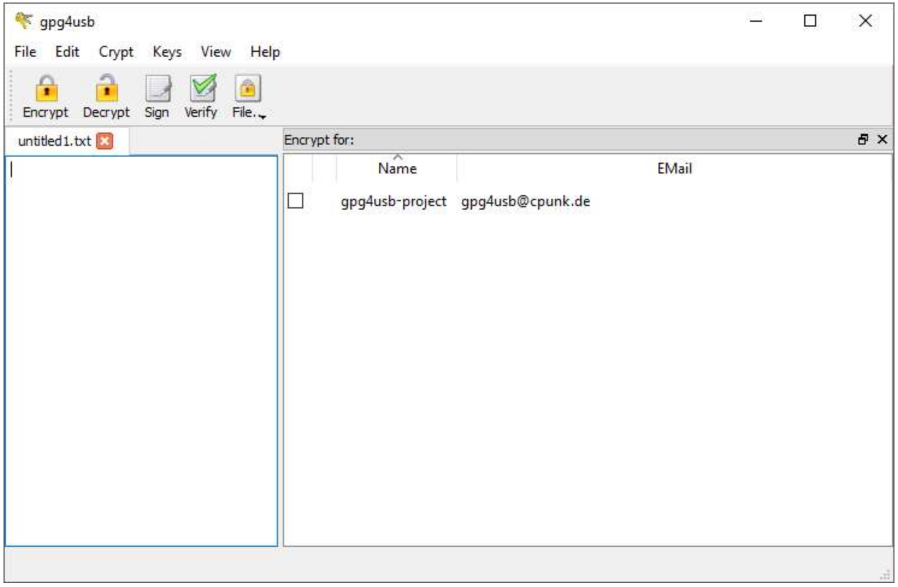
In this how-to we'll show you how to perform asymmetric encryption and decryption.

There are many free as well as proprietary (paid) tools available for implementing standard encrypting and decrypting algorithms. Here we'll use a free portable[1] piece of software called **gpg4usb**[2].

Here is what needs to done and how to proceed to use the software

1. Download and extract the software
2. Create your own pair of public-private keys
3. Export and share your public key with contacts
4. Import and have public keys from your contact
5. Encrypt a transmission to a contact
6. Decrypt a transmission from a contact

When you run the application for the first time, you are presented with the main interface window.



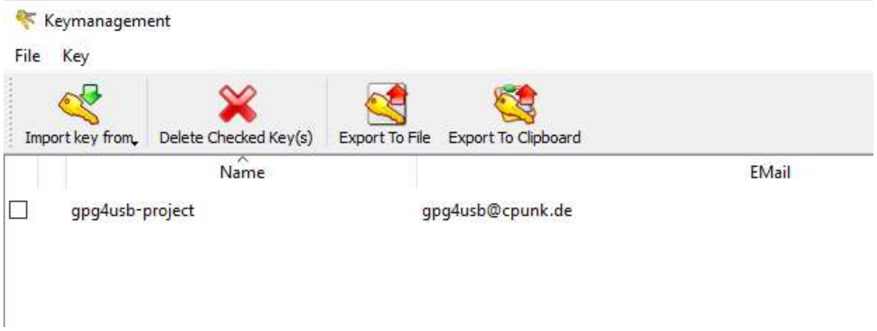
	Name	EMail
□	gpg4usb-project	gpg4usb@cpunk.de

From this starting point you can only encrypt a transmission given the public key for 'gpg4usb-project' that exists in the listing on the right. This is the area where you keep all your keys (for all your contacts). First thing to do is to create your keys

[1] A portable software does not require installation on your computer. Usually it comes in a .zip file and all you have to do is extract it at some place and run it from there. You can even run it form a USB stick.
[2] The version used for this how-to is gpg4usb 0.3.3, released on 2016. It is available for download at: https://www.gpg4usb.org/

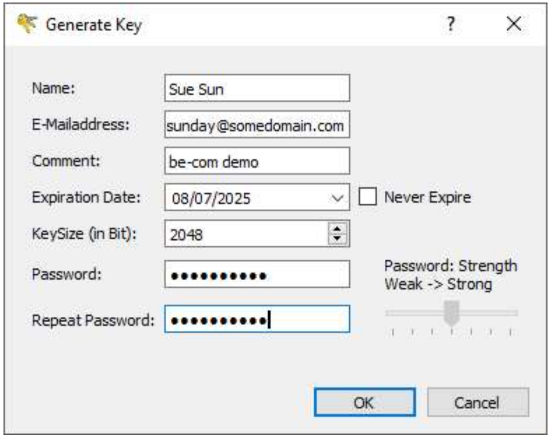
Creating your own pair of public-private keys

1. Select the Keys → Manage Keys commands from the main application menubar. The dialog will open and you will be presented with the current keys (you have)



	Name	EMail
□	gpg4usb-project	gpg4usb@cpunk.de

2. Now use the Key → Generate Key command to create your own pair of keys. The capture below demonstrates the completed dialog



Name: Sue Sun

E-Mailaddress: sunday@somedomain.com

Comment: be-com demo

Expiration Date: 08/07/2025 □ Never Expire

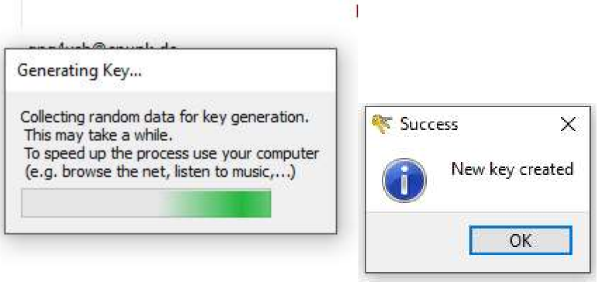
KeySize (in Bit): 2048

Password: ••••••••••

Repeat Password: ••••••••••

Password: Strength
Weak -> Strong

3. Click on OK. The software will initiate the process, and notify you when ready.

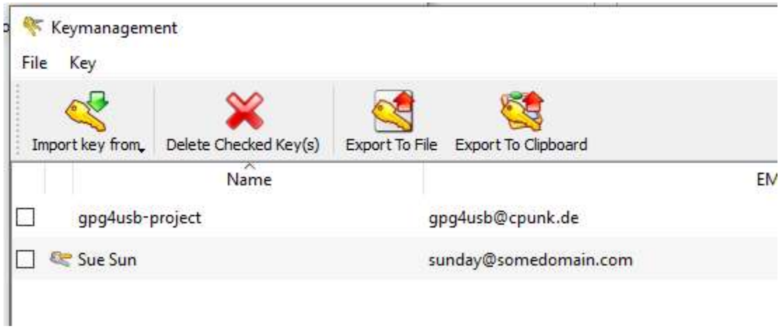


Generating Key...

Collecting random data for key generation.
This may take a while.
To speed up the process use your computer
(e.g. browse the net, listen to music,...)

New key created

4. The listing of keys now updates. Your key is indicated with the little 'key icon' on the side



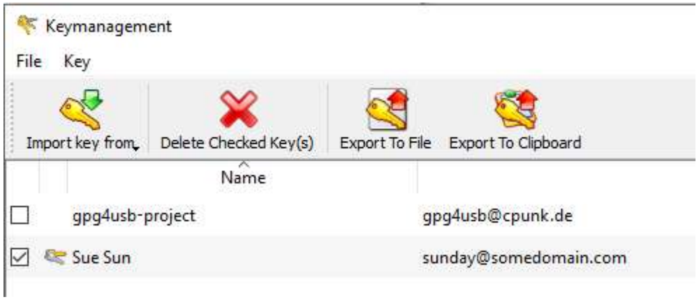
	Name	EM
□	gpg4usb-project	gpg4usb@cpunk.de
□	Sue Sun	sunday@somedomain.com

, we will see how you can shareyour key with your contacts

Exporting and sharing your public key with contacts

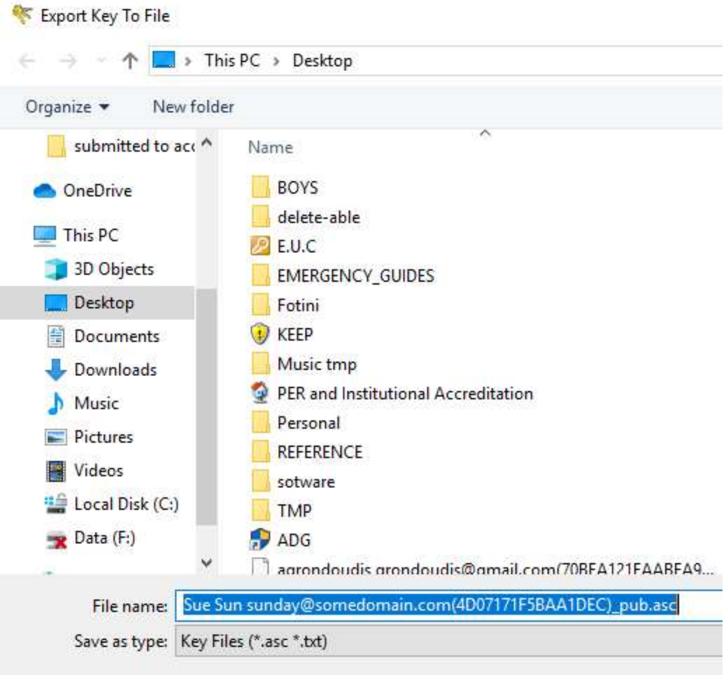
Now that you have your key, you must share it (the public key) with your contacts. Here are the steps to do that:

1. While still in the Key Management dialog, tick the box next to your key



	Name	
□	gpg4usb-project	gpg4usb@cpunk.de
☑	Sue Sun	sunday@somedomain.com

2. Now click the 'Export To File' icon. This will generate a file that will contain your public key. The application will prompt you for a location and name to save the file

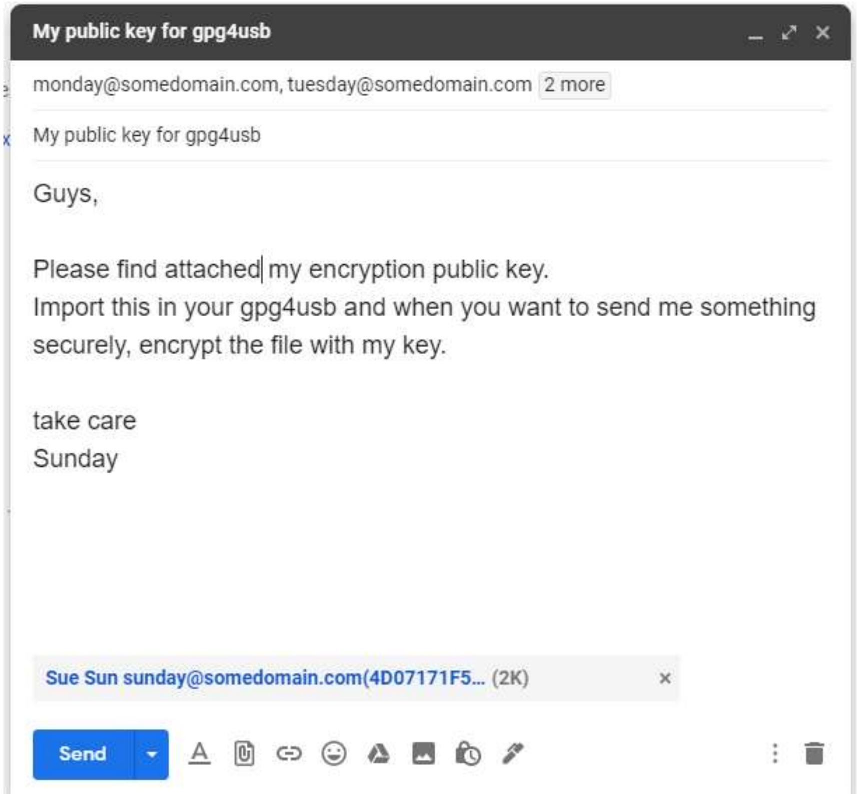


BOYS
delete-able
E.U.C
EMERGENCY_GUIDES
Fotini
KEEP
Music tmp
PER and Institutional Accreditation
Personal
REFERENCE
sotware
TMP
ADG
agrondoudis grondoudis@gmail.com(70BFA121FAABFA9...

File name: Sue Sun sunday@somedomain.com(4D07171F5BAA1DEC)_pub.asc

Save as type: Key Files (*.asc *.txt)

3. Save the file and then send this file as an attachment to your contacts



My public key for gpg4usb

monday@somedomain.com, tuesday@somedomain.com 2 more

My public key for gpg4usb

Guys,

Please find attached my encryption public key.
Import this in your gpg4usb and when you want to send me something securely, encrypt the file with my key.

take care
Sunday

Sue Sun sunday@somedomain.com(4D07171F5... (2K)

Next, we will see how you can import your contacts' public keys

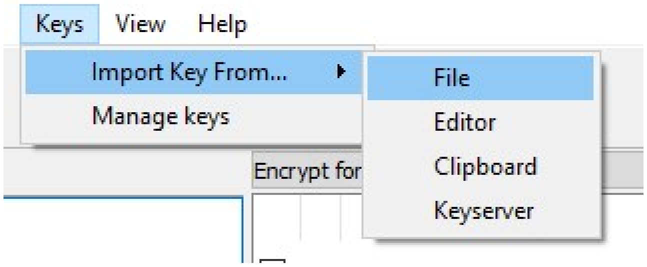
Importing and having public keys from your contact

In order for you to encrypt information and send it to your contacts you need their public key. Just like you emailed your public key, all contacts can email you their public keys and you can import them in gpg4usb. Here are the steps to do that.

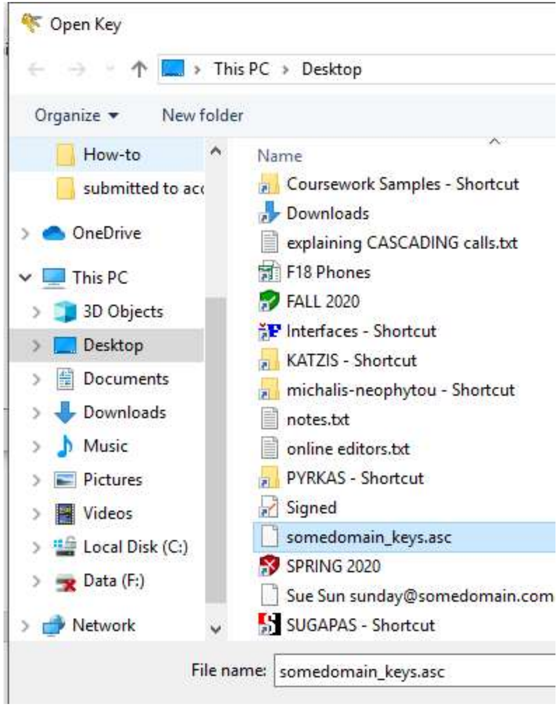
1. Assume that you have received a file that you need to import

somedomain_keys.asc
ASC File
7.00 KB

2. In this main window for gpg4usb select the Keys→Import Key From→File command

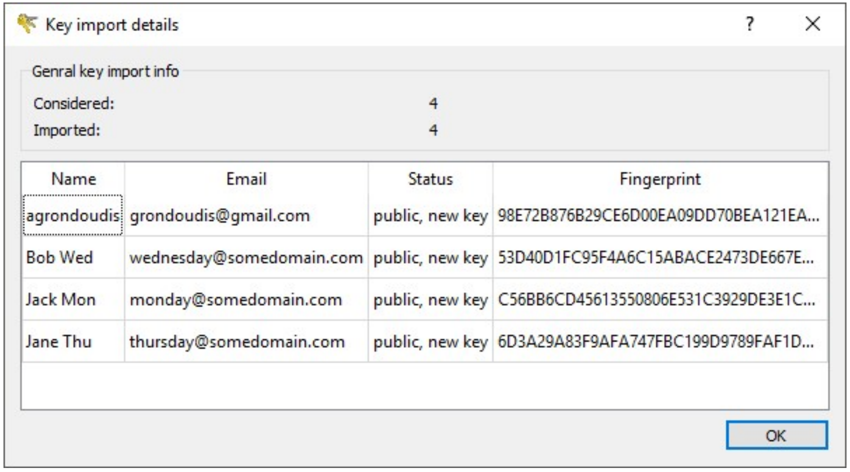


3. The open file dialog appears, find and select the somedomain_keys.asc file



File name: somedomain_keys.asc

4. When you click “open the application”, it shows you what is to be imported. As you can see in the capture below the file included 4 keys. Click OK to proceed



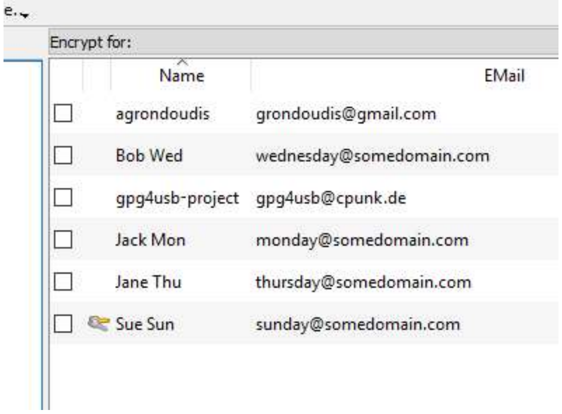
Genral key import info

Considered: 4

Imported: 4

Name	Email	Status	Fingerprint
agrondoudis	grondoudis@gmail.com	public, new key	98E72B876B29CE6D00EA09DD70BEA121EA...
Bob Wed	wednesday@somedomain.com	public, new key	53D40D1FC95F4A6C15ABACE2473DE667E...
Jack Mon	monday@somedomain.com	public, new key	C56BB6CD45613550806E531C3929DE3E1C...
Jane Thu	thursday@somedomain.com	public, new key	6D3A29A83F9AFA747FBC199D9789FAF1D...

5. Importing will complete and your list of keys will update



	Name	EMail
□	agrondoudis	grondoudis@gmail.com
□	Bob Wed	wednesday@somedomain.com
□	gpg4usb-project	gpg4usb@cpunk.de
□	Jack Mon	monday@somedomain.com
□	Jane Thu	thursday@somedomain.com
□	Sue Sun	sunday@somedomain.com

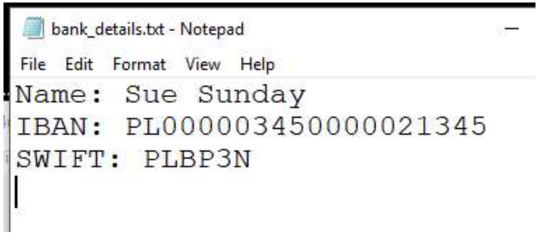
Now you can send encrypted files to Bob, Jack and Jane from somedomain.com.

Next, let’s see how to encrypt a file for a contact.

Encrypting a transmission to a contact

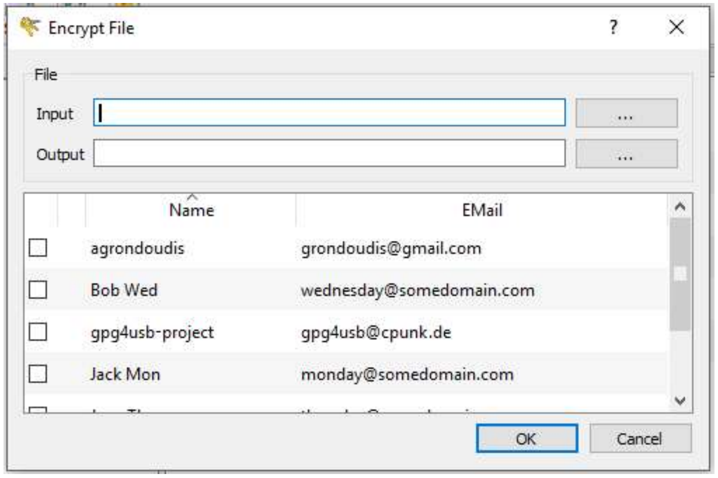
So now you want to encrypt a file and send it to Bob. Here are the steps

1. Assume you want to encrypt a file called 'bank_details.txt' (content shown below)



```
Name: Sue Sunday
IBAN: PL00003450000021345
SWIFT: PLBP3N
```

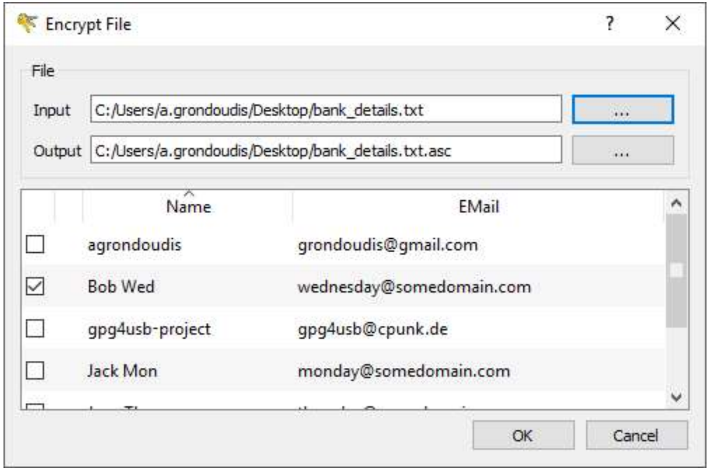
2. In gpg4usb select the Crypt→Encrypt File command. The dialog shown below appears.



	Name	EMail
□	agrondoudis	grondoudis@gmail.com
□	Bob Wed	wednesday@somedomain.com
□	gpg4usb-project	gpg4usb@cpunk.de
□	Jack Mon	monday@somedomain.com

3. Use the button on the top right to find the source file (bank_details.txt). The application will automatically fill the output using the same name with the extension .asc added.

Click the 'Bob Wed' key to use for the encryption. The capture below demonstrates.

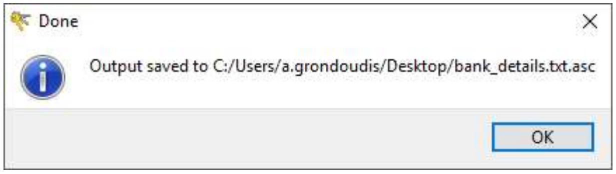


Input C:/Users/a.grondoudis/Desktop/bank_details.txt

Output C:/Users/a.grondoudis/Desktop/bank_details.txt.asc

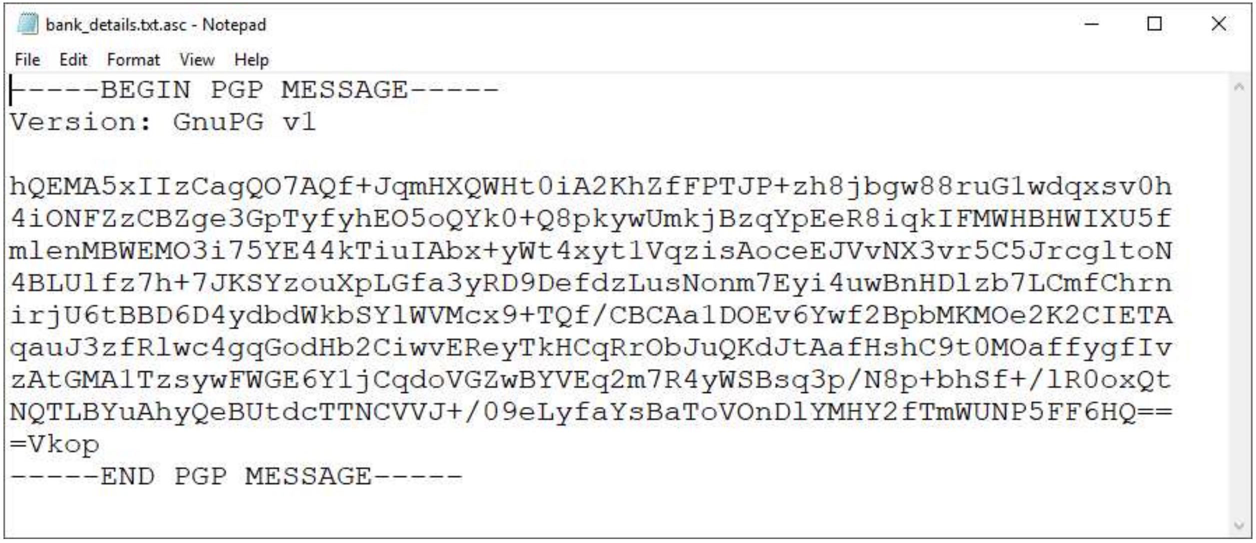
	Name	EMail
☐	agrondoudis	grondoudis@gmail.com
☑	Bob Wed	wednesday@somedomain.com
☐	gpg4usb-project	gpg4usb@cpunk.de
☐	Jack Mon	monday@somedomain.com

4. Click OK to complete the operation. The application confirms this.



Output saved to C:/Users/a.grondoudis/Desktop/bank_details.txt.asc

5. If you open the newly created file you can see that it is encrypted



```
-----BEGIN PGP MESSAGE-----
Version: GnuPG v1

hQEMA5xIIzCagQO7AQf+JqmHXQWHt0iA2KhZfFPTJP+zh8jbgw88ruG1wdqxsv0h
4iONFZzCBZge3GpTyfyhEO5oQYk0+Q8pkywUmkjBzqYpEeR8iqkIFMWHBHWIXU5f
mlenMBWEMO3i75YE44kTiuIAbx+yWt4xytlVqzisAoceEJVvNX3vr5C5JrcgltoN
4BLUlfz7h+7JKSYzouXpLGfa3yRD9DefdzLusNonm7Eyi4uwBnHDlzb7LCmfChrn
irjU6tBBD6D4ydbdWkbSYlWVMcx9+TQf/CBCAa1DOEv6Ywf2BpbMKMOe2K2CIETA
qauJ3zfRlwc4gqGodHb2CiwvEReyTkHCqRrObJuQKdJtAafHshC9t0MOaffygfIv
zAtGMA1TzsywFWGE6Y1jCqdoVGZwBYVEq2m7R4yWSBsq3p/N8p+bhSf+/lR0oxQt
NQTLBYuAhyQeBUtdcTTNCVVJ+/09eLyfaYsBaToVOnDlYMHY2fTmWUNP5FF6HQ==
=Vkop
-----END PGP MESSAGE-----
```

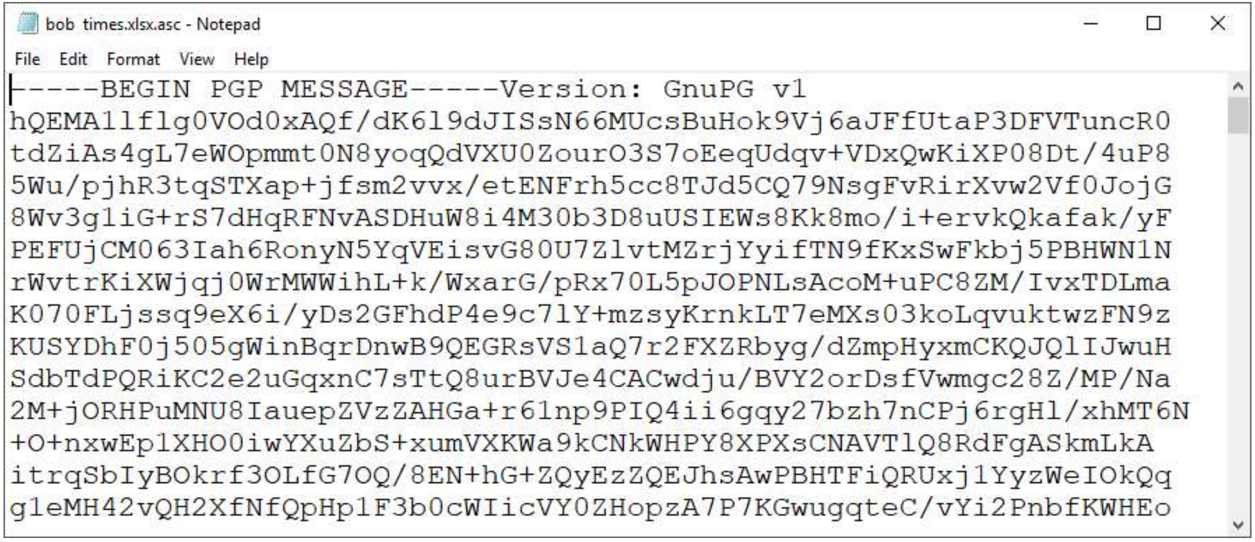
You can now email this file to Bob and he will be able to decrypt gpg4usb using his private key.

Finally, we will see how to decrypt a file.

Decrypting a transmission from a contact

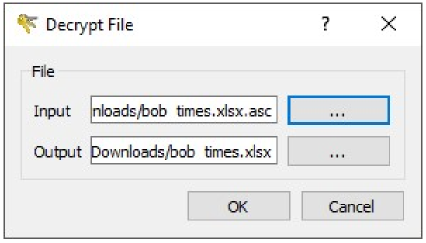
Bob has just sent you a file with some work time details. The file was encrypted with your public key and you can now decrypt using your private key. Here are the steps to follow.

1. Assume the following file has been received from Bob



```
-----BEGIN PGP MESSAGE-----Version: GnuPG v1
hQEMA1lflg0VOd0xAQf/dK6l9dJISsN66MUcsBuHok9Vj6aJFfUtaP3DFVTuncR0
tdZiAs4gL7eWOpmmt0N8yoqQdVXU0ZourO3S7oEeqUdqv+VDxQwKiXP08Dt/4uP8
5Wu/pjhR3tqSTXap+jfsm2vvx/etENFrh5cc8TJd5CQ79NsgFvRirXvw2Vf0JojG
8Wv3gliG+rS7dHqRFNvASDHuW8i4M30b3D8uUSIEWs8Kk8mo/i+ervkQkafak/yF
PEFUjCM063Iah6RonyN5YqVEisvG80U7ZlvtMZrjYyifTN9fKxSwFkbj5PBHWN1N
rWvtrKiXWjqj0WrMWWihL+k/WxarG/pRx70L5pJOPNLsAcoM+uPC8ZM/IvxTDLma
K070FLjssq9eX6i/yDs2GFhdP4e9c7lY+mzsyKrnkLT7eMXs03koLqvuktwzFN9z
KUSYDhF0j505gWinBqrDnwB9QEGRsVS1aQ7r2FXZRbyg/dZmpHyxmCKQJQlIJwuH
SdbTdPQRiKC2e2uGqxnC7sTtQ8urBVJe4CACwdju/BVY2orDsfVwmgc28Z/MP/Na
2M+jORHPuMNU8IauepZVzZAHGa+r6lnp9PIQ4ii6gqy27bzh7nCPj6rgHl/xhMT6N
+O+nxwEp1XHO0iwYXuZbS+xumVXKWa9kCNkWHPY8XPXsCNAVTlQ8RdFgASkmLkA
itrqSbIyBOkrf3OLfG7OQ/8EN+hG+ZQyEzZQEJhsAwPBHTFiQRUxj1YyzWeIOkQq
g1eMH42vQH2XfNfQpHp1F3b0cWIicVY0ZHopzA7P7KGwugqteC/vYi2PnbfKWHEo
```

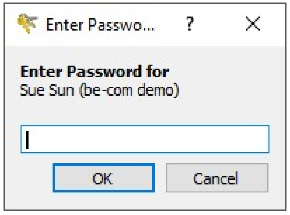
2. In gpg4usb select the Crypt→Decrypt File command. The decrypt file dialog appears. Use the button on the top right and locate the source file (bob times.xlsx.asc). gpg4usb automatically fills the 'output' field and removes the asc extension form the file.



Input nloads/bob times.xlsx.asc

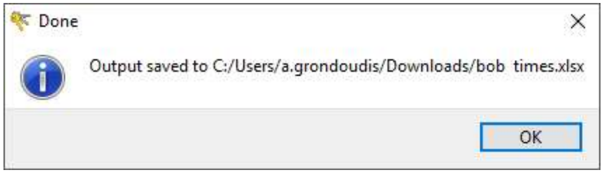
Output Downloads/bob times.xlsx

3. Click OK, the application will prompt you for the password associated with your private key. Enter the password and press enter or click OK to complete the operation.



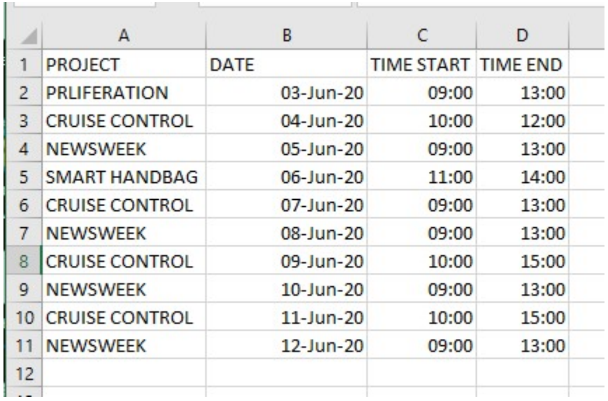
Enter Password for
Sue Sun (be-com demo)

4. The application confirms the completion and shows you where the file is



Output saved to C:/Users/a.grondoudis/Downloads/bob times.xlsx

5. If you navigate to that location and open the file you will see its contents



	A	B	C	D
1	PROJECT	DATE	TIME START	TIME END
2	PRLIFERATION	03-Jun-20	09:00	13:00
3	CRUISE CONTROL	04-Jun-20	10:00	12:00
4	NEWSWEEK	05-Jun-20	09:00	13:00
5	SMART HANDBAG	06-Jun-20	11:00	14:00
6	CRUISE CONTROL	07-Jun-20	09:00	13:00
7	NEWSWEEK	08-Jun-20	09:00	13:00
8	CRUISE CONTROL	09-Jun-20	10:00	15:00
9	NEWSWEEK	10-Jun-20	09:00	13:00
10	CRUISE CONTROL	11-Jun-20	10:00	15:00
11	NEWSWEEK	12-Jun-20	09:00	13:00
12				

With asymmetric encryption you have to remember that: 1) you encrypt using the recipient's public key (form your key listing) and 2) you decrypt by entering your password.