



SOFTWARE

PDA

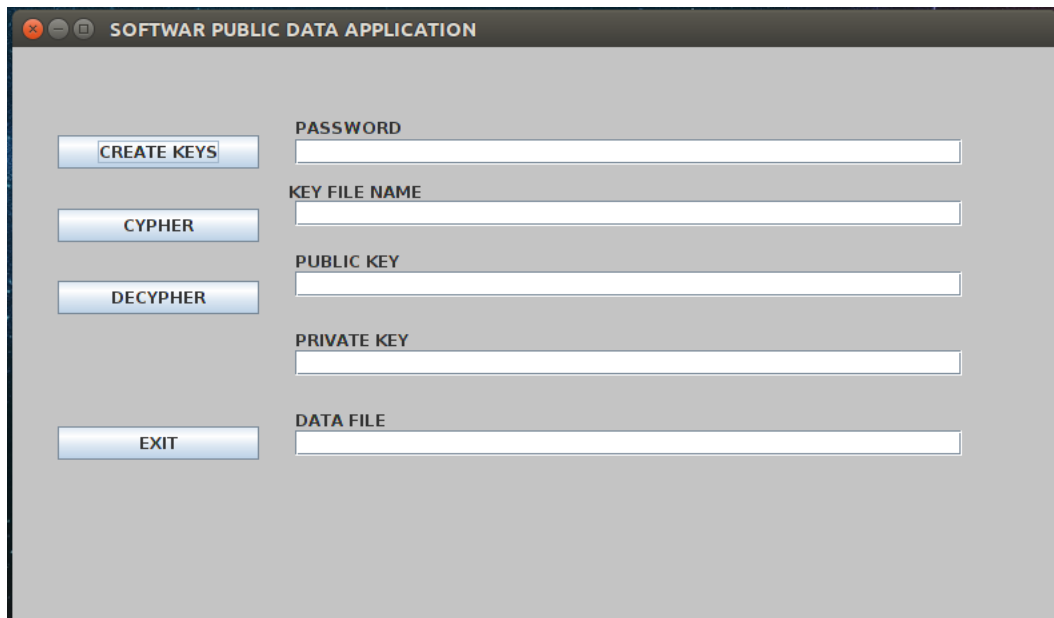
Public Data Application

SOFTWARE INC.
PO Box 325
Manquin, VA 23106

Information Security

Softwar PDA © 2016 Softwar Inc. all rights reserved.

PDA android Public Data Application software.



The PDA software application is designed to cypher and de-cypher any data file on a linux based PC using PUBLIC Key files created by the user for public distribution. PDA does not cypher files on your PC. PDA creates an output file containing the selected data file cyphered with the public -key. This allows users to exchange data in a secure manner. The PC version of PDA is fully compatible with the Android version thus files can be shared between Android devices and PCs.

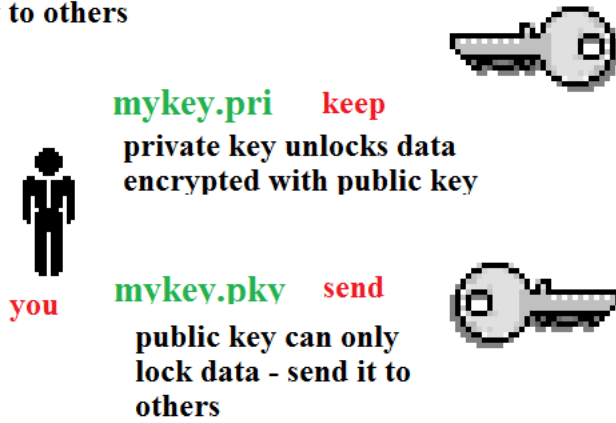
PDA for Linux Ubuntu 14.04 LTS was developed using Java 1.7. You must have Java installed on your system to run PDA. You can obtain Java from www.oracle.com or in Ubuntu select Java Open JDK Java 7 run-time.

PUBLIC KEY ENCYPTION

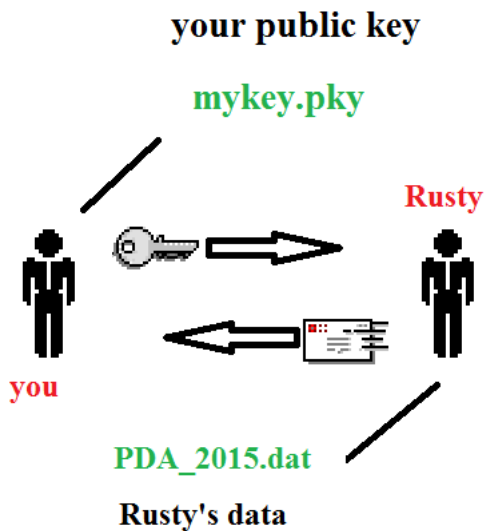
Public key encryption, also known as asymmetric cryptography, is a two key system. PDA creates a pair of two separate keys: a private key and a public key. The public key locks or cyphers data. The private key unlocks or de-cyphers data. Your PDA private key is password locked so unauthorized individuals cannot access or decode information. Data files cyphered with a public key can only be de-cyphered with the corresponding private key.

The public key may be published without compromising security, whereas the private key must not be revealed to any unauthorized individual. You can send your public key to other users who then can cypher any data and send it back to you. For example: PDA can be used to exchange keys created with the CYPHER utility in a secure manner.

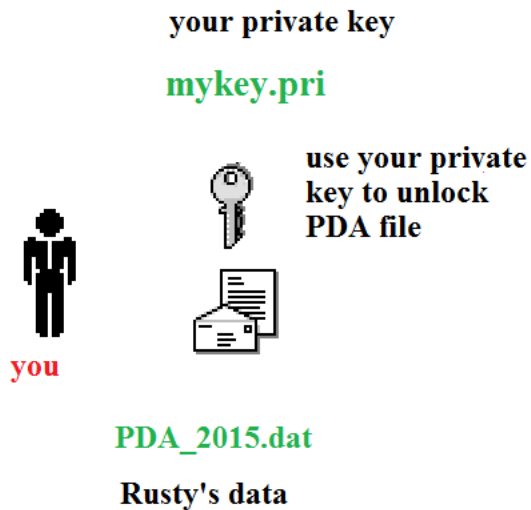
PDA makes 2 keys - you keep private key and send public key to others



In the example below – you send a public key to Rusty who then cyphers a file and sends the PDA output file back to you.



You then use your private key to unlock the PDA file and access Rusty's data.

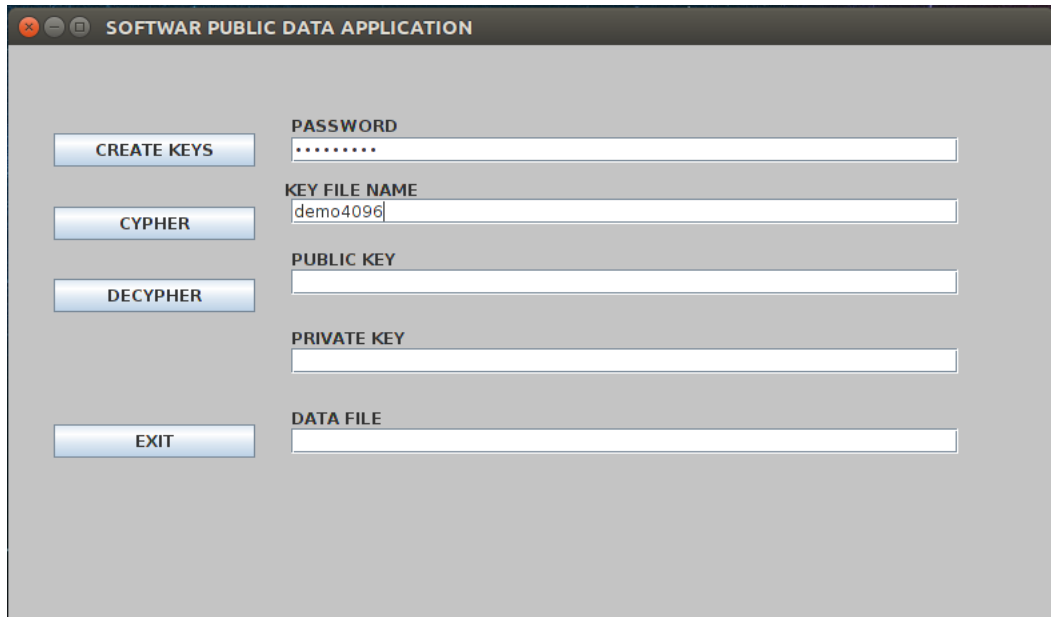


CREATE KEY

The first thing you must do to create a key is enter your password. Your password will be used to secure the PRIVATE Key that you keep on your system. The password is not stored so make sure to enter something that you will remember.

The screenshot shows a window titled "SOFTWARE PUBLIC DATA APPLICATION". On the left side, there are four buttons: "CREATE KEYS", "CYPHER", "DECYPHER", and "EXIT". On the right side, there are five input fields with labels: "PASSWORD" (with a masked password "*****"), "KEY FILE NAME", "PUBLIC KEY", "PRIVATE KEY", and "DATA FILE".

Next enter a key name. Select a key name of 1 to 30 characters. DO NOT USE slash / or period .



SOFTWARE PUBLIC DATA APPLICATION

CREATE KEYS PASSWORD
.....

CYPHER KEY FILE NAME
demo4096

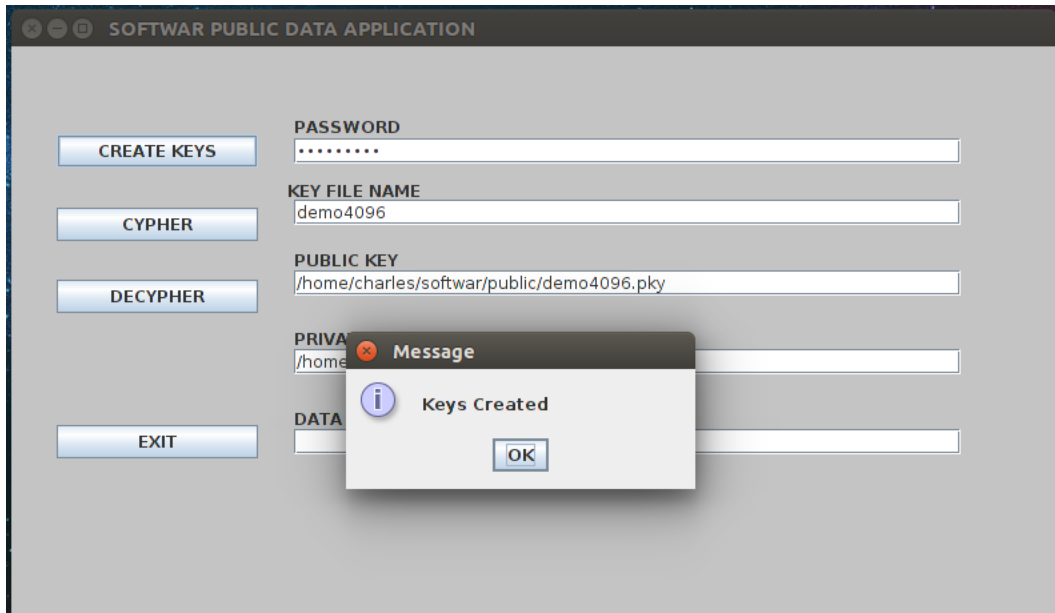
DECYPHER PUBLIC KEY

PRIVATE KEY

EXIT DATA FILE

CREATE KEYS

To create a key hit the **CREATE KEYS** button. PDA will create the key and display a **PLEASE WAIT** message until done. Once completed PDA will display a KEYS CREATED message. PDA saves public keys into the **/softwar/public directory** and saves private keys into the **/softwar/private** directory.



PUBLIC KEY


Send the public key to another user. You can send the public key to others without compromising security because the public key can only cypher data. Below is an example of what a public key looks like.

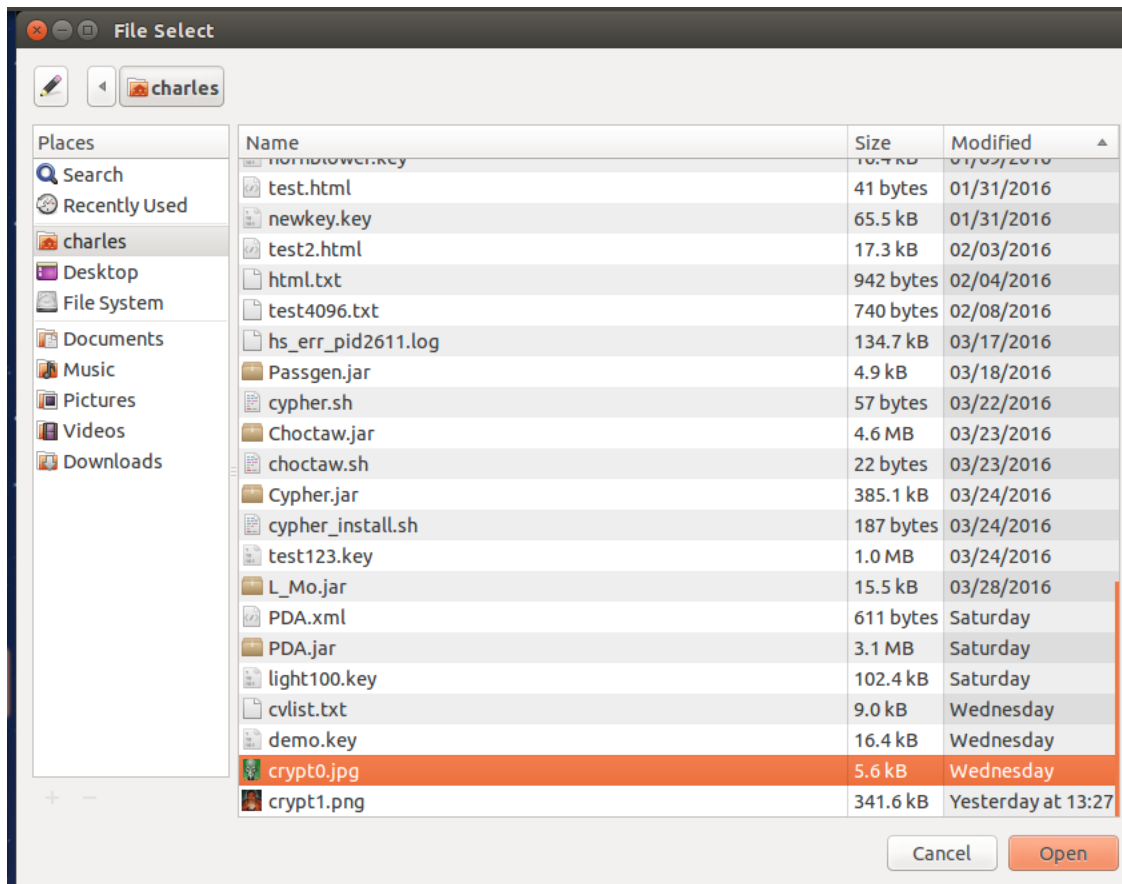
```
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAz9wProzZE6bc90CyIf4qehZsAaO9
rLFPL21NpbyqR/Ma12jReVcETipVV8R17x7rqTXOXOzdM49YVvvmJTrZMempkceH7Ni3ZzrU
ZCYW5XC/UQRdehc3F3bndULtYvbk0ZXzeeHdzrXpr2vxg34+U+1EzB8fe1/vFSH5DmFByXgF
o0WSPiB2WESfc6uhitk0MbKJuQxvsdruVIzzOBHBnnurhv1tuKPI3mY41tyjBnbRrXtSw4+p
YEAJtTcqL4f0i1toLgwEXtN97Zbwa9NUxKame9F1iCGDZgT1+39mysk7bcvtetow0CHU9GwN
32bY6qw+dhGQI9USohJt6KCOFwIDAQAB
-----END PUBLIC KEY-----
```

You can send the key as a file or insert it as text into a message such as email. If inserted into a message the key must be copied in its entirety and pasted into a standard text file beginning with "-----BEGIN PUBLIC KEY-----" and ending with "-----END PUBLIC KEY-----".

PDA CYPHER DATA

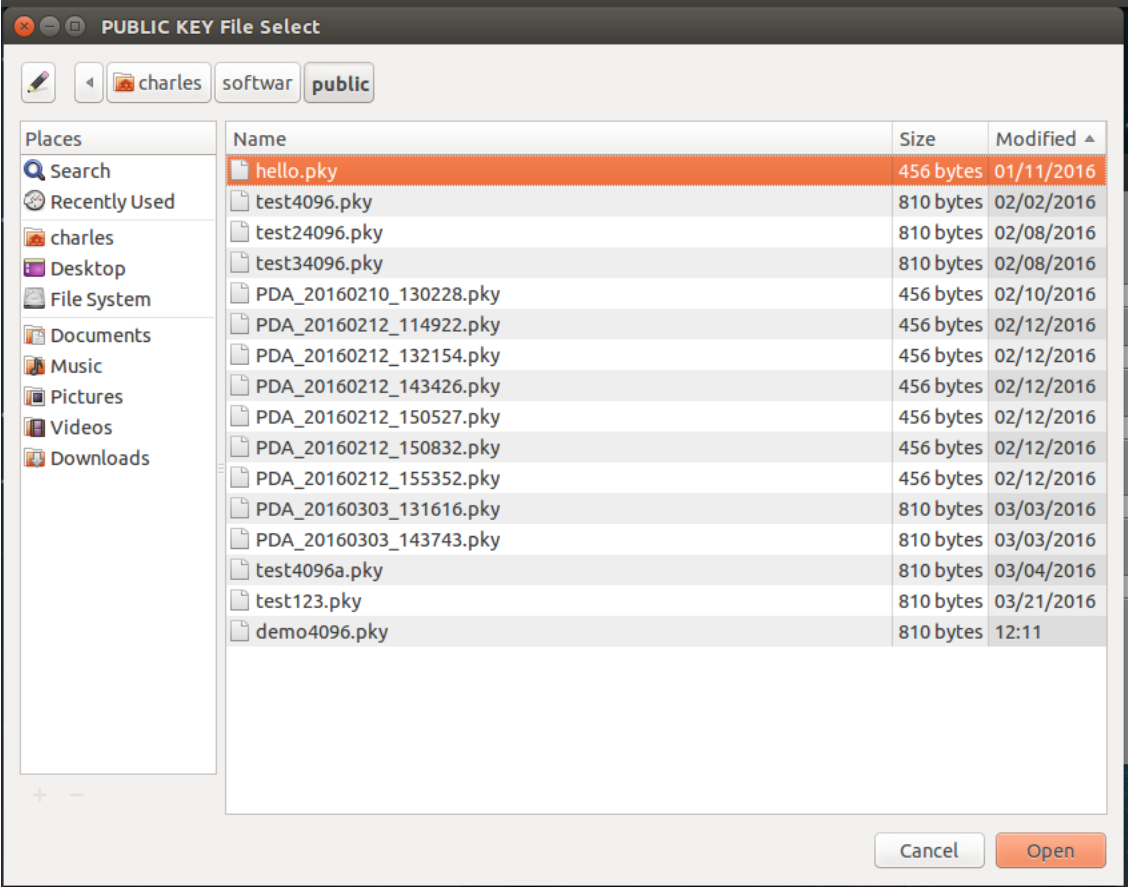


Hit the  button. Select the file you wish to cypher by first using the directory selection menu.

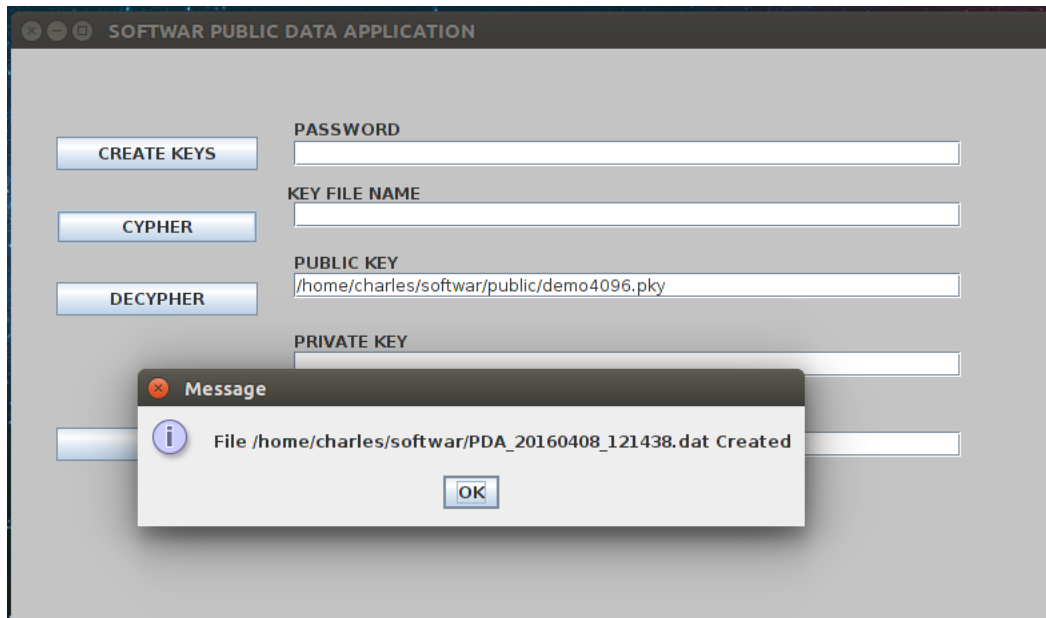


SELECT PUBLIC KEY

Select the location where the PDA PUBLIC key is located. The public key was sent to you by another PDA user – so you can store it in any location on your PC. PDA public key files usually are named with a .PKY extension. For example: myfilename.pky.




When the cyphering process is completed PDA will display the output file name and note that it has been CREATED.

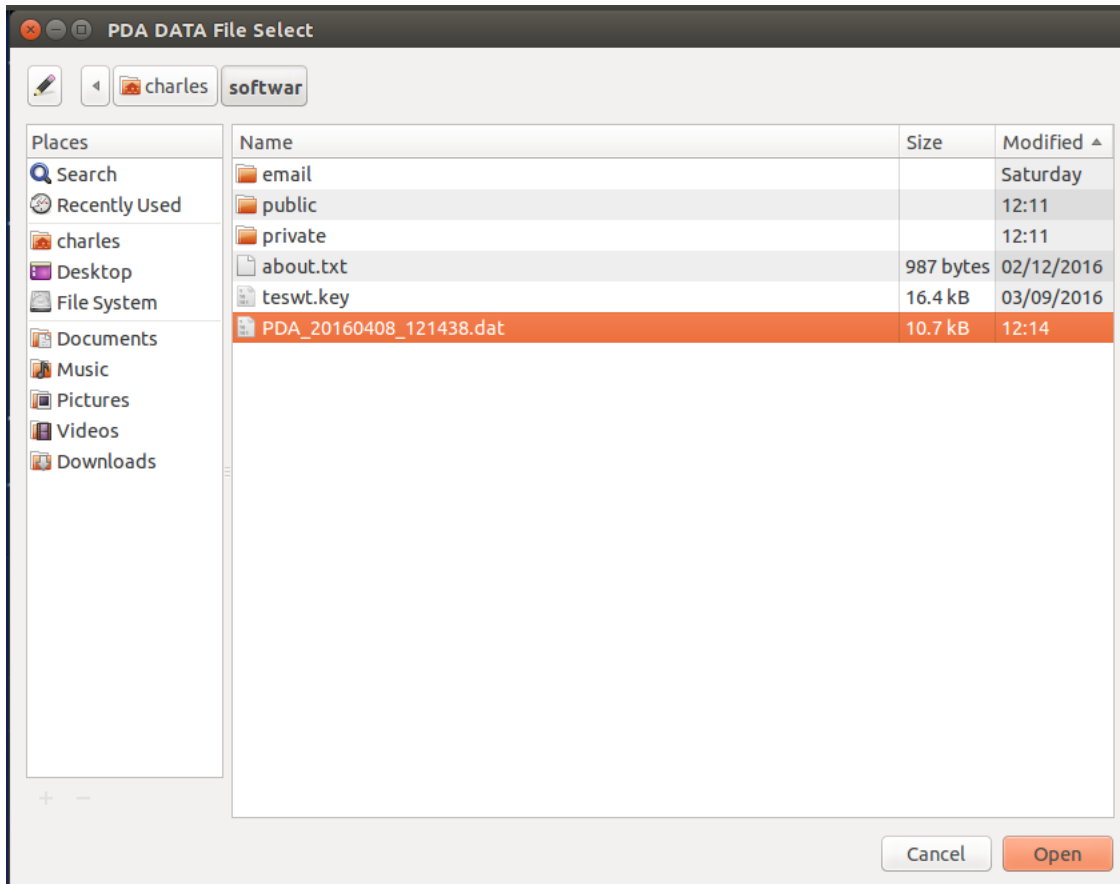


PDA output files are named in the following format: PDA_yyyymmdd_hhmmss.dat. For example: **PDA_20150211_130159.dat**

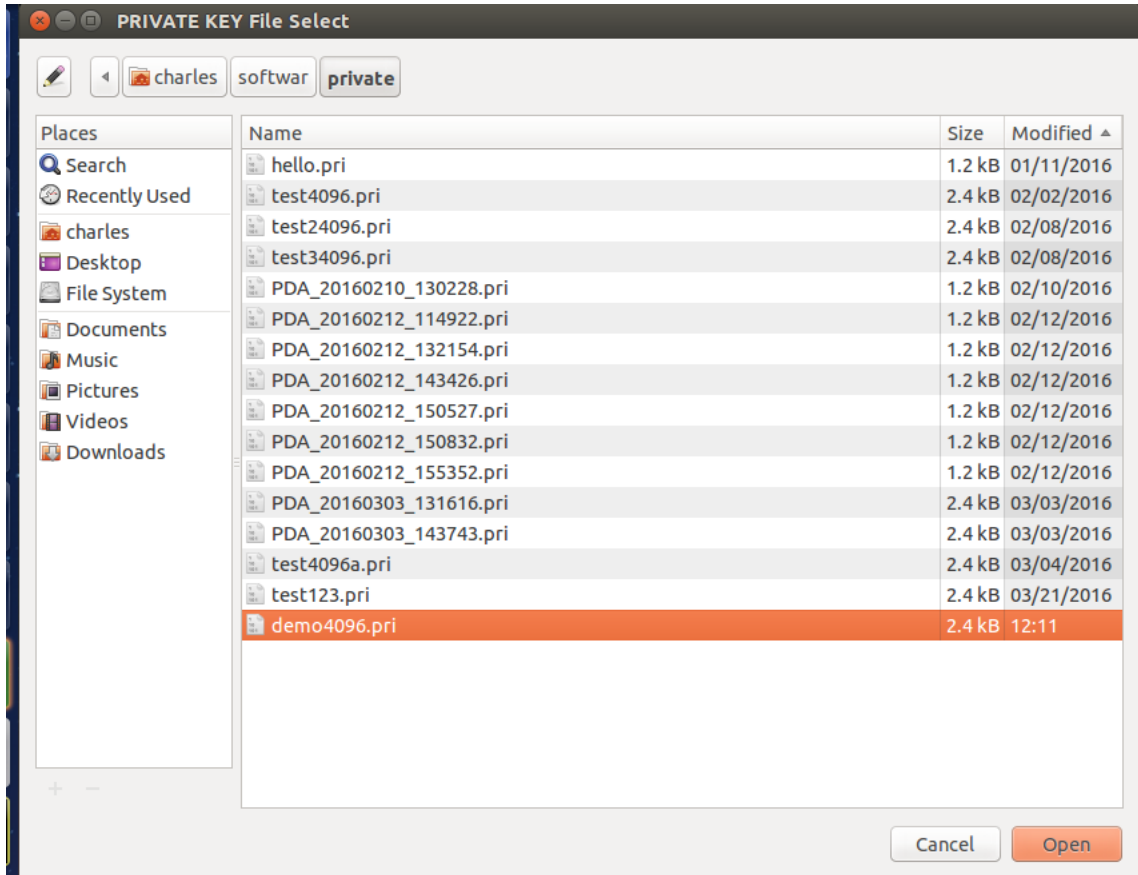
DE-CYPHER Command

When you receive a PDA file you will need to de-cypher it to access the data. The first thing you must do to de-cypher a PDA file is enter your password to access your private key.

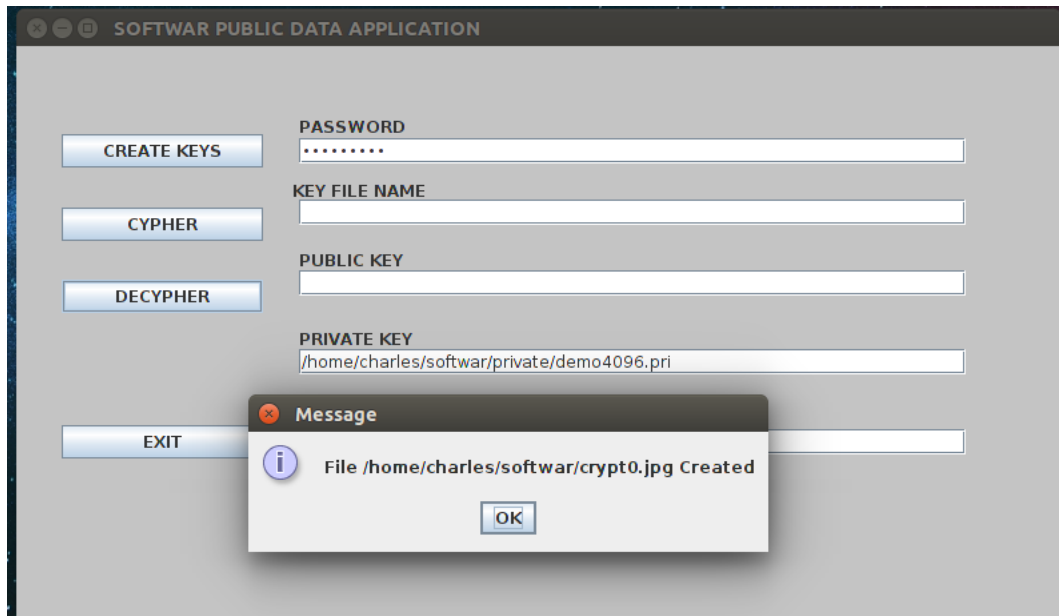
Hit the  button. Select the file you wish to de- cypher by first using the directory selection menu.



To de-cypher then you will need to select the PRIVATE Key from the Key Directory and Key selection menus. Private keys are normally stored in the /softwar/private directory.



Once the de-cyphering process is completed the status will note the output file has been CREATED. PDA will output the new data file into the /softwar directory.



TECHNICAL SPECIFICATIONS

PDA is an asymmetrical public key system using an internal 4096 bit key and a built in unique session key for each PDA file.

SYSTEM REQUIREMENTS:

Ubuntu 14.04 LTS or higher

CONTACT INFORMATION:

<http://www.softwar.net>

Email : softwar@softwar.net

Copyright notice:

Softwar PDA © 2015 Softwar Inc. all rights reserved.

Trademarks:

Ubuntu and Canonical are registered trademarks of Canonical Ltd

Java is a registered trademarks of Oracle Corporation

SOFTWARE End-User

License Agreement

BY INSTALLING OR USING THE LICENSED SOFTWARE AND HARDWARE FROM SOFTWARE INC. THE INDIVIDUAL IF ACTING ON BEHALF OF HIMSELF OR HERSELF ("INDIVIDUAL CUSTOMER") OR THE INDIVIDUAL WHO IS ACTING ON BEHALF OF AN EDUCATIONAL OR NONPROFIT INSTITUTION, GOVERNMENTAL AGENCY, OR OTHER ("ENTITY CUSTOMER", THE INDIVIDUAL CUSTOMER AND ENTITIY CUSTOMER TOGETHER ARE "CUSTOMER") IS AGREEING TO BE BOUND BY THIS SOFTWARE LICENSE AGREEMENT ("AGREEMENT").

IF CUSTOMER DOES NOT AGREE TO THIS AGREEMENT, CUSTOMER MAY NOT INSTALL, COPY, OR USE THE LICENSED SOFTWARE.

THE "EFFECTIVE DATE" FOR THIS AGREEMENT IS THE DAY CUSTOMER INSTALLS THE SOFTWARE.

The export and re-export of Softwar Inc. products are controlled by the United States Export Administration Regulations and such software may not be exported or re-exported. This product is classified as information security encryption technology under Category 5, Part 2 in the U.S. Commerce Control List and IS NOT eligible for export outside the United States.

In addition, Softwar Inc. software may not be distributed to persons on the Table of Denial Orders, the Entity List, or the List of Specially Designated Nationals. By using an Softwar Inc. software product you are certifying that you are not a national of Cuba, Iran, Iraq, Libya, North Korea, Sudan, Syria, or any country to which the United States embargoes goods and that you

are not a person on the Table of Denial Orders, the Entity List, or the List of Specially Designated Nationals.

Customer shall not, nor permit any person (including any Authorized User) to: (i) reverse engineer, reverse compile, decrypt, disassemble, or otherwise attempt to derive the source code of the Licensed Software (except to the extent that this restriction is expressly prohibited by law); (ii) modify, translate, or create derivative works of the Licensed Software; (iii) sublicense, resell, rent, lease, distribute, market, commercialize, or otherwise transfer rights or usage to the Licensed Software (except as expressly permitted under this Agreement); (iv) remove, modify, or obscure any copyright notices or other proprietary notices or legends appearing on or in the Licensed Software, or any portion thereof; (v) transfer, use, or export the Licensed Software in violation of any applicable laws, rules, or regulations of any government or governmental agency; (vi) use the Licensed Software or any system services accessed through the Licensed Software to disrupt, disable, or otherwise harm the operations, software, hardware, equipment, and/or systems of a business, institution, or other entity, including, without limitation, exposing the business, institution, or other entity to any computer virus, trojan horse, or other harmful, disruptive, or unauthorized component; or (vii) embed the Licensed Software in any third-party applications, unless otherwise authorized in writing in advance by an officer of SOFTWARE INC.

IN NO EVENT SHALL SOFTWARE INC. HAVE ANY LIABILITY FOR ANY LOST REVENUE, LOST PROFIT, OR LOST OR DAMAGED DATA, BUSINESS INTERRUPTION, LOSS OF CAPITAL, ANY INCIDENTAL, CONSEQUENTIAL, INDIRECT, SPECIAL, OR PUNITIVE DAMAGES ARISING OUT OF OR IN CONNECTION WITH THIS AGREEMENT, REGARDLESS OF THE FORM OF THE ACTION, WHETHER IN CONTRACT, TORT (INCLUDING NEGLIGENCE), STRICT PRODUCT LIABILITY, OR OTHERWISE, EVEN IF ANY REPRESENTATIVE OF SOFTWARE INC. HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES AND NOTWITHSTANDING THE FAILURE OF THE ESSENTIAL PURPOSE OF THIS AGREEMENT OR ANY LIMITED REMEDY HEREUNDER.

DISCLAIMER OF WARRANTIES: YOU AGREE THAT SOFTWARE INC. HAS MADE NO EXPRESS WARRANTIES TO YOU REGARDING THE SOFTWARE AND THAT THE SOFTWARE IS BEING PROVIDED TO YOU "AS IS" WITHOUT WARRANTY OF ANY KIND. SOFTWARE INC. DISCLAIMS ALL WARRANTIES WITH REGARD TO THE SOFTWARE, EXPRESS OR IMPLIED, INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, MERCHANTABLE QUALITY, OR NONINFRINGEMENT OF THIRD-PARTY RIGHTS.