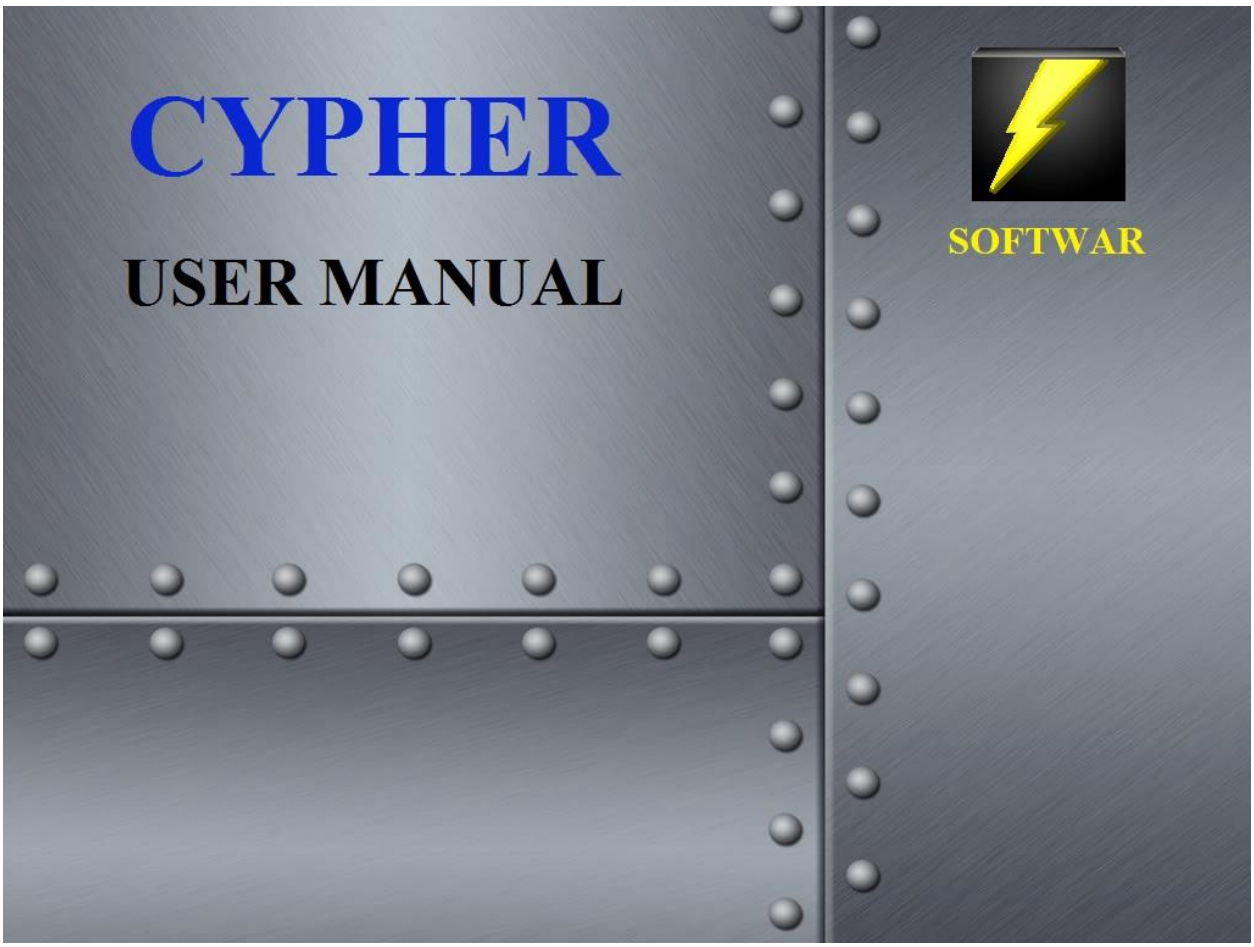


SOFTWAR INC.
PO Box 325
Manquin, VA 23106

Information Security

CYPHER personal security software.

The Cypher utility is designed to cypher and de-cypher any data file on a Linux system using key files or passwords created by the user. Key files are as their name implies keys to lock and unlock any selected data. Key files come in 3 levels of security described below.

Password – First level security:
Cypher and de-cypher using a personal password of no less than 6 characters.

User Key File – Second level security:
Any file to be used as a key to cypher and de-cypher. The user selected key file can be any document, picture, music, text or work file. It is recommended that you do not use files that contain large amounts of repeating characters such as bitmap files. However, files that are compressed such as zip, jpeg, MP3 or other media files that have been compressed are acceptable. DO NOT pick a file that will change. Just as with a physical lock on a door, a key file must be the same used to cypher (lock) a file in order to successfully de-cypher (unlock) the same data.

Crypto Key File - Third level security:
This is a key file created by the Cypher key maker that utilizes the computer Pseudo-Random Number Generator (PRNG) to create a very large set of random numbers. The Crypto Key maker utilizes several system features such as time, key strokes, position of the hard drive and

many other variables to randomly seed and create large keys using a mathematical algorithm. The crypto key file is considered to be superior to the User key in that it is much more random than regular user data files.

Light Key File – Highest level security:
The light key is created by using your web camera equipped computer to sample light in three basic colors – red, green and blue. This system is known as a True Random Number Generator (TRNG) because the key is generated by the light recorded by your camera. The light key is the most secure because it is created using quantum physics by recording the values of photons electronically. The light key is similar in performance to keys generated by sensors inside Atomic clocks that detect radioactivity.

INSTALLATION

Cypher for Linux Ubuntu 14.04 LTS was developed using Java 1.7 and OpenCV 3.1.0 which drives the light camera systems. You must have Java installed on your system to run Cypher. You can obtain Java from www.oracle.com or in Ubuntu select Java Open JDK Java 7 run-time. The OpenCV software is included in the installation package. The installation will make several sub directories on your system to store the OpenCV software and install libraries that you may not have included in your system files.

Cypher for Linux is installed using the CYPHER_INSTALL directory on the CD. The entire directory can be copied onto other media such as a USB drive or installed using a network.

The directory contains two install SHELL (.sh) files.

normal_cypher_install.sh
This shell file contains the normal configuration for Linux installation. You should use this shell to perform a normal installation. It will unzip the required OpenCv library files and install them on your system.

full_cypher_install.sh
This shell file contains the full configuration for Linux installations including all the Linux library files required for operation. If the Cypher camera system fails use this full installation shell to copy all libraries.

Enter your terminal mode (cntrl-alt-T).
Cd to the correct drive and path of the installation disk
Enter bash ./normal_cypher_install.sh or ./full_cypher_install.sh

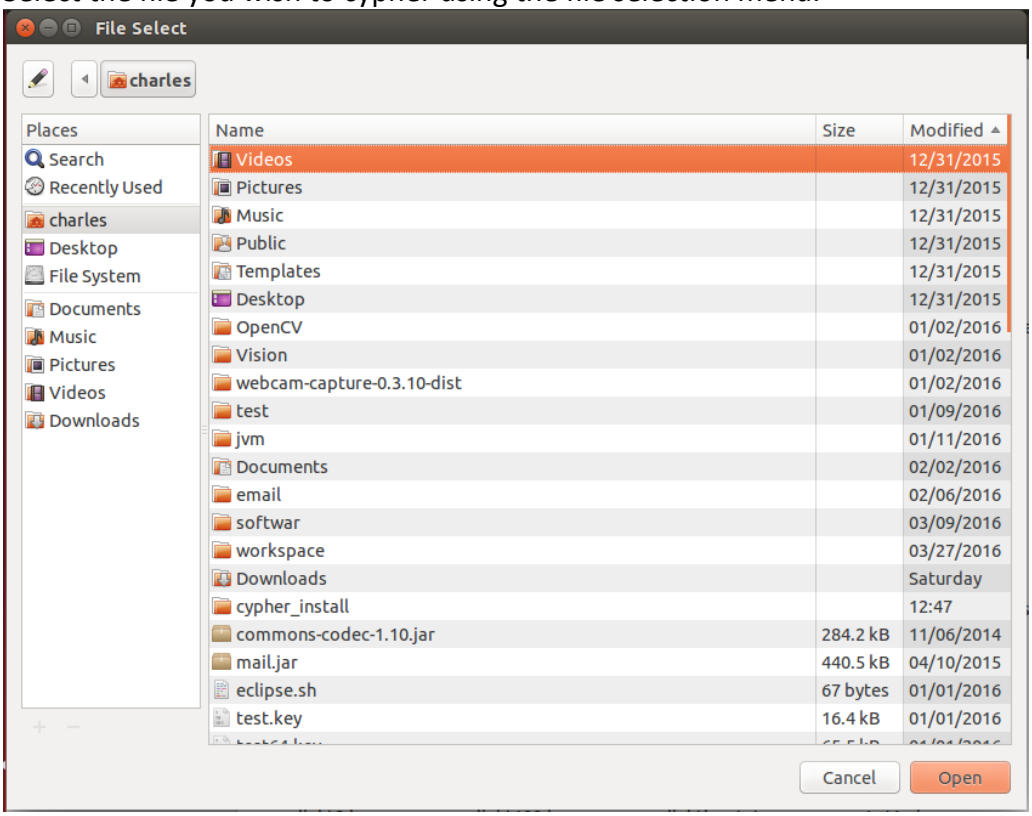
TO RUN

Copy Cypher.jar into your normal home directory
Copy the cypher.sh file into your home directory
Enter your terminal mode (cntrl-alt-T) and go to the directory where you put Cypher.jar and cypher.sh
bash ./cypher.sh

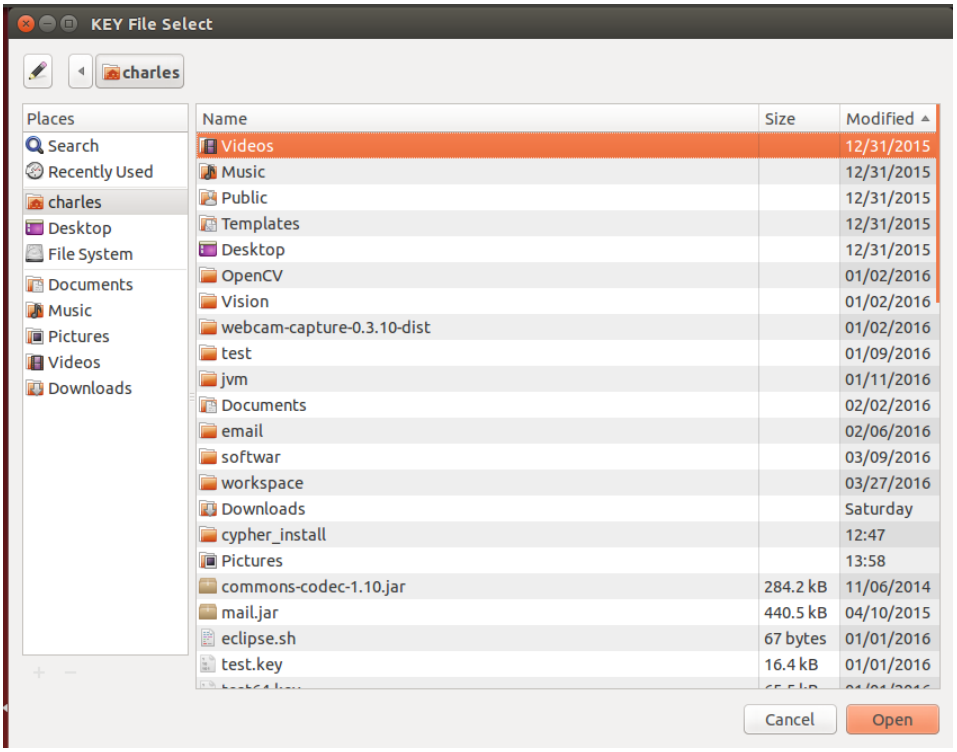
CYPHER Command:
Select the method to cypher a file using the radio buttons on the main menu:

Password – enter a password in the space provided under the PASSWORD radio button.
User Key file – any file selected on the system.
Crypto Key file – key file created with the Pseudo-Random Number Generator (PRNG).
Light Key file - key file created with the light sensor True Random Number Generator (TRNG).

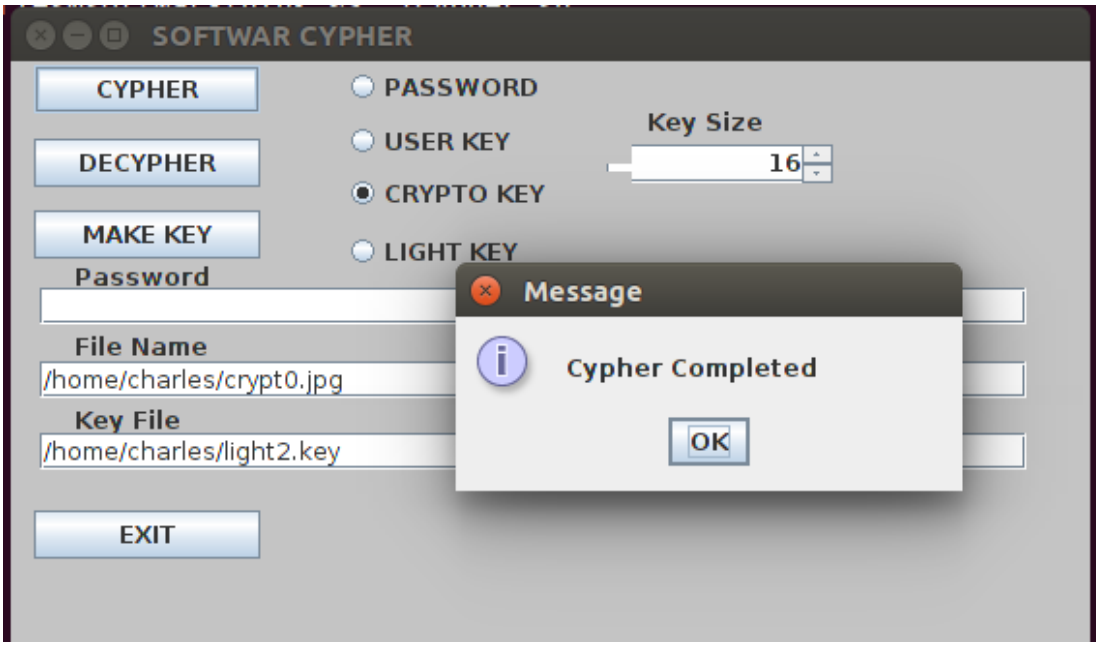
Select the file you wish to cypher using the file selection menu.



If you selected a key file method to cypher then you will need to select the key from the key file selection menu.



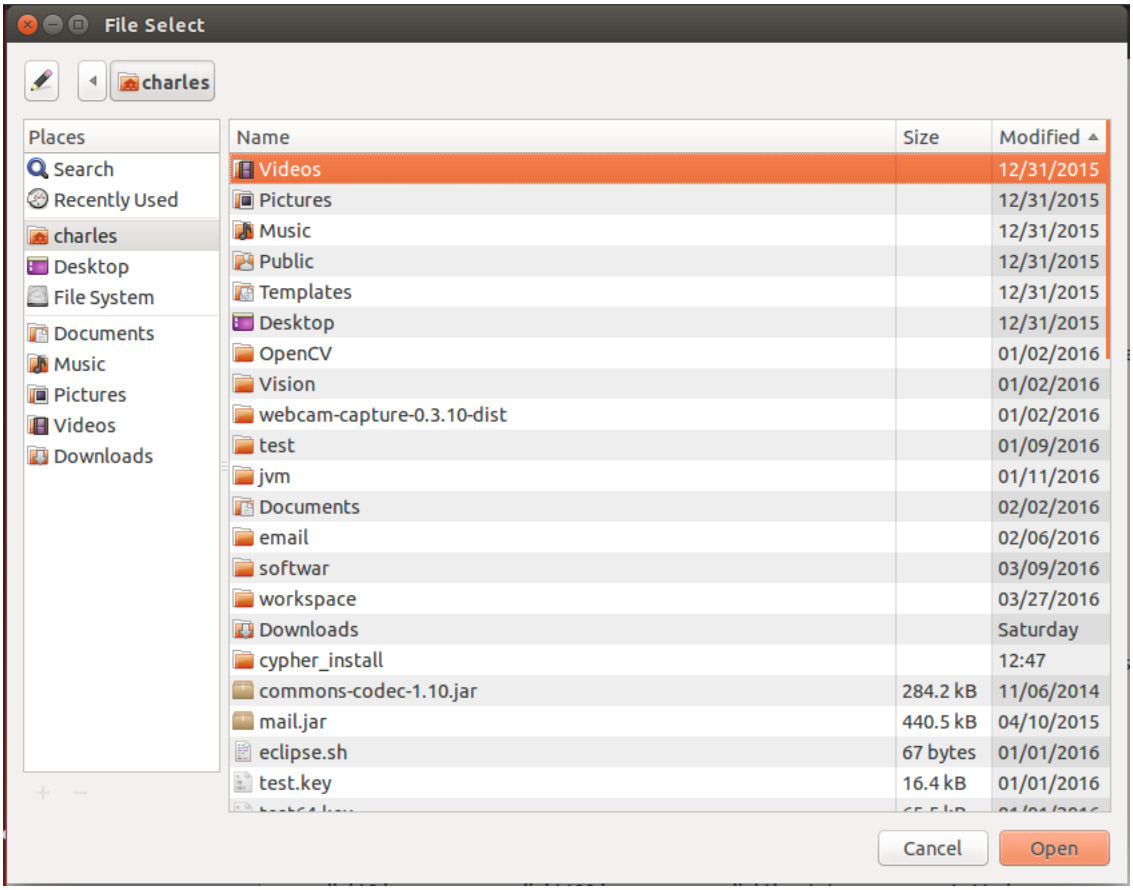
The cyphering process will display with a CYPHER COMPLETE message on the main menu once the process is completed.



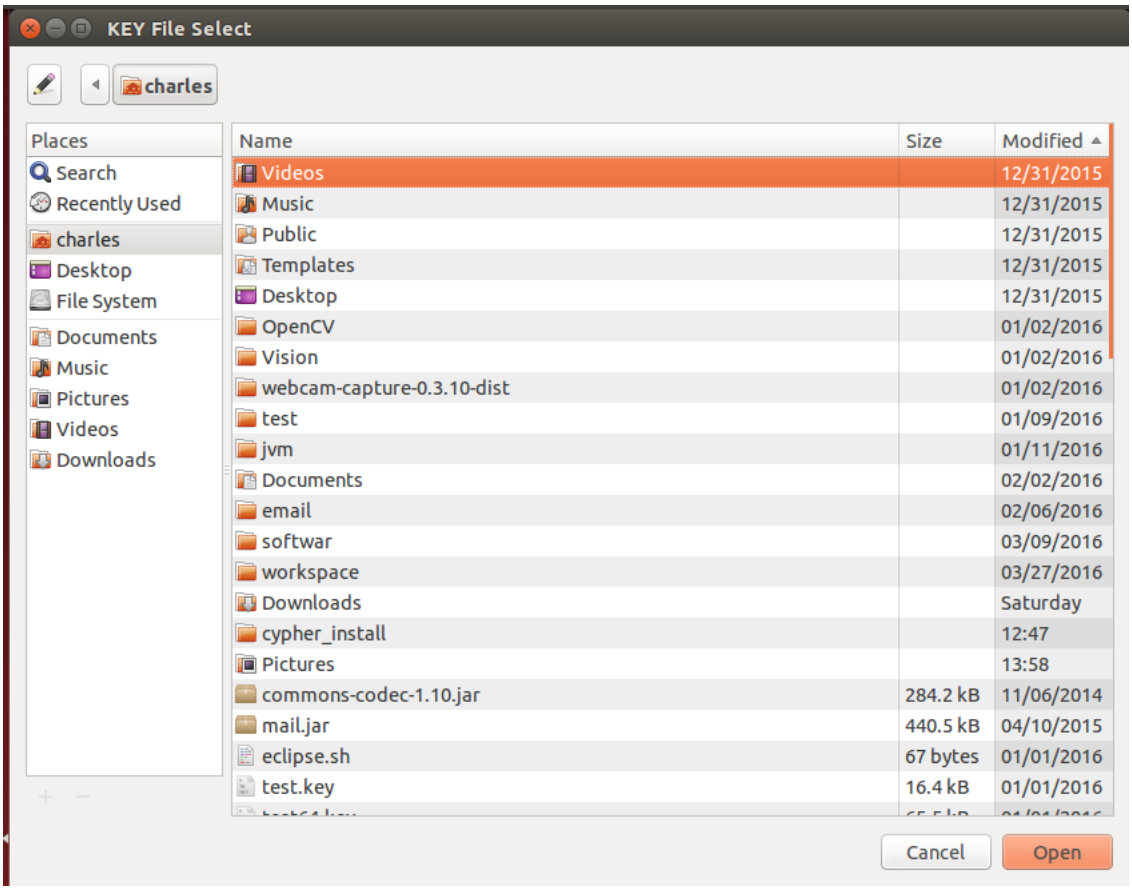
DE-CYPHER Command:
Select the method to de-cypher a file using the radio buttons on the main menu:

Password – enter a password in the space provided under the PASSWORD radio button.
User Key file – any file selected on the system.
Crypto Key file – key file created with the Pseudo-Random Number Generator (PRNG).
Light Key file - key file created with the light sensor True Random Number Generator (TRNG).

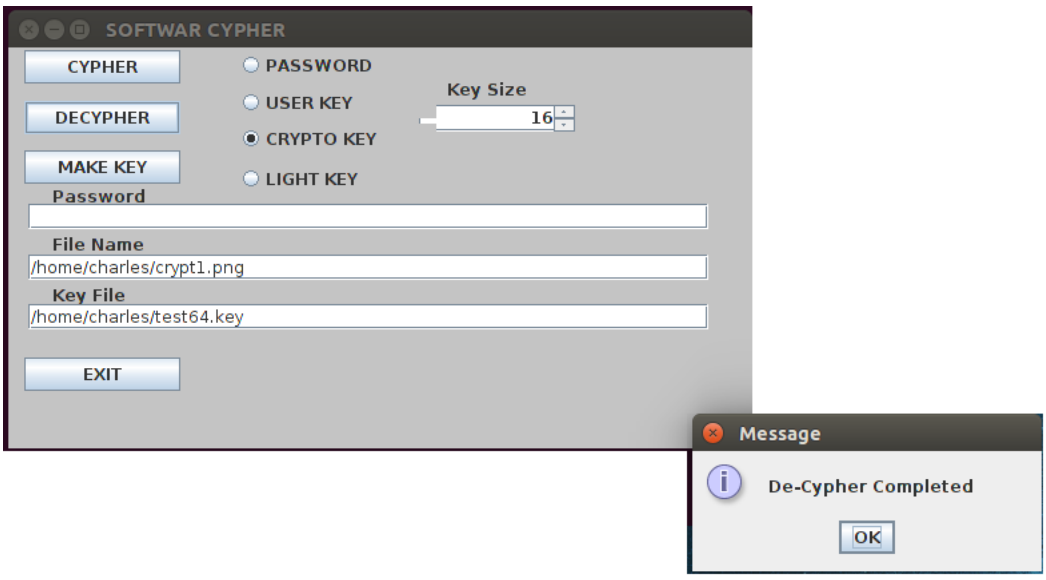
Select the file you wish to de-cypher using the file selection menu.



If you selected a key file method to de-cypher then you will need to select the key from the key file selection menu.



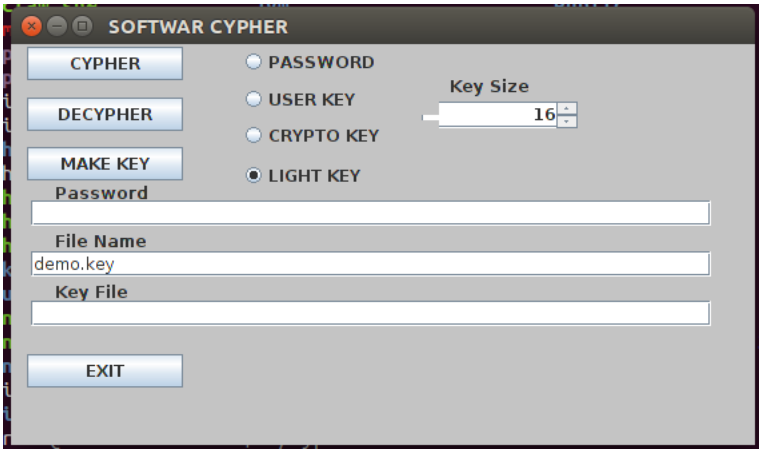
The de-cyphering process will display a status box DE-CYPHER COMPLETE.



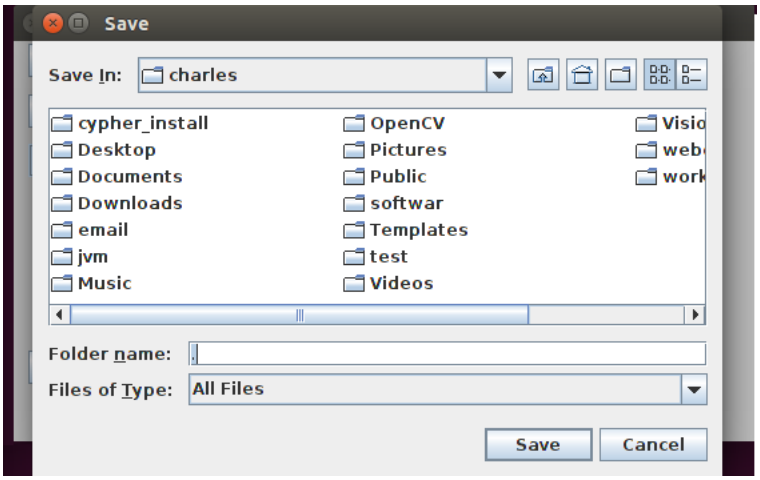
CREATE KEY:
There are two types of keys that you can make with cypher; Crypto-key files and Light Key files. Select the type of key you wish to create using the Crypto-Key File or Light Key File radio buttons on the main menu.

Enter a KEY FILE name in the main menu then select CREATE KEY. The name can be any name plus extension, for example: test.key, myface.jpg, data.txt, Jeffery.doc.

The key maker has a KEY SIZE selector to allow you to dial up the size of the key file you wish to create. You may enter any value that is allowed. The key size is limited to 16 Kbytes minimum to 640,000 Kbytes maximum (16,384 bytes to 655,360,000 bytes). Make sure you have enough space on the designated drive to store the key.



The key maker will then request what drive and directory you will to save the key in. Select the drive and the directory using the box and click the save button.



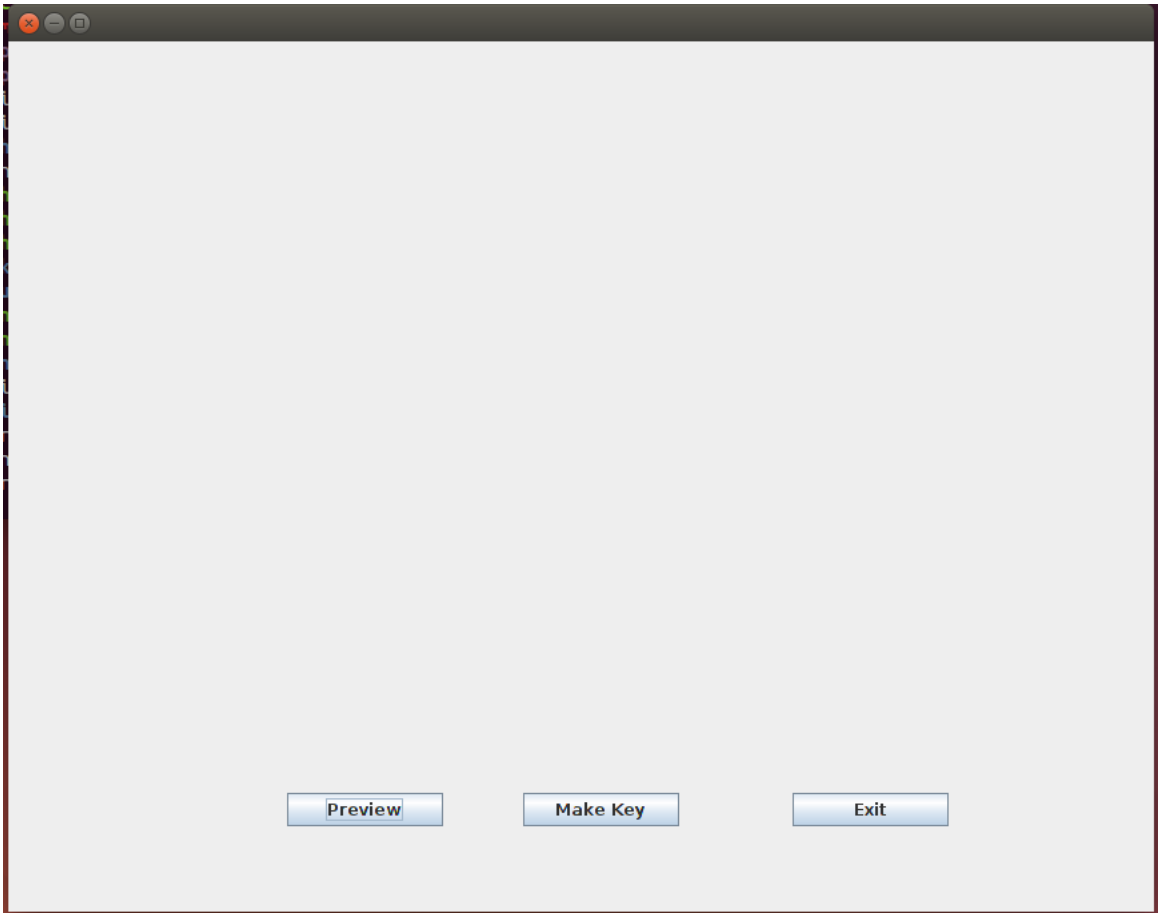
LIGHT KEY instructions:

If your computer is equipped with a web camera you can skip the installation and proceed to the key creation.

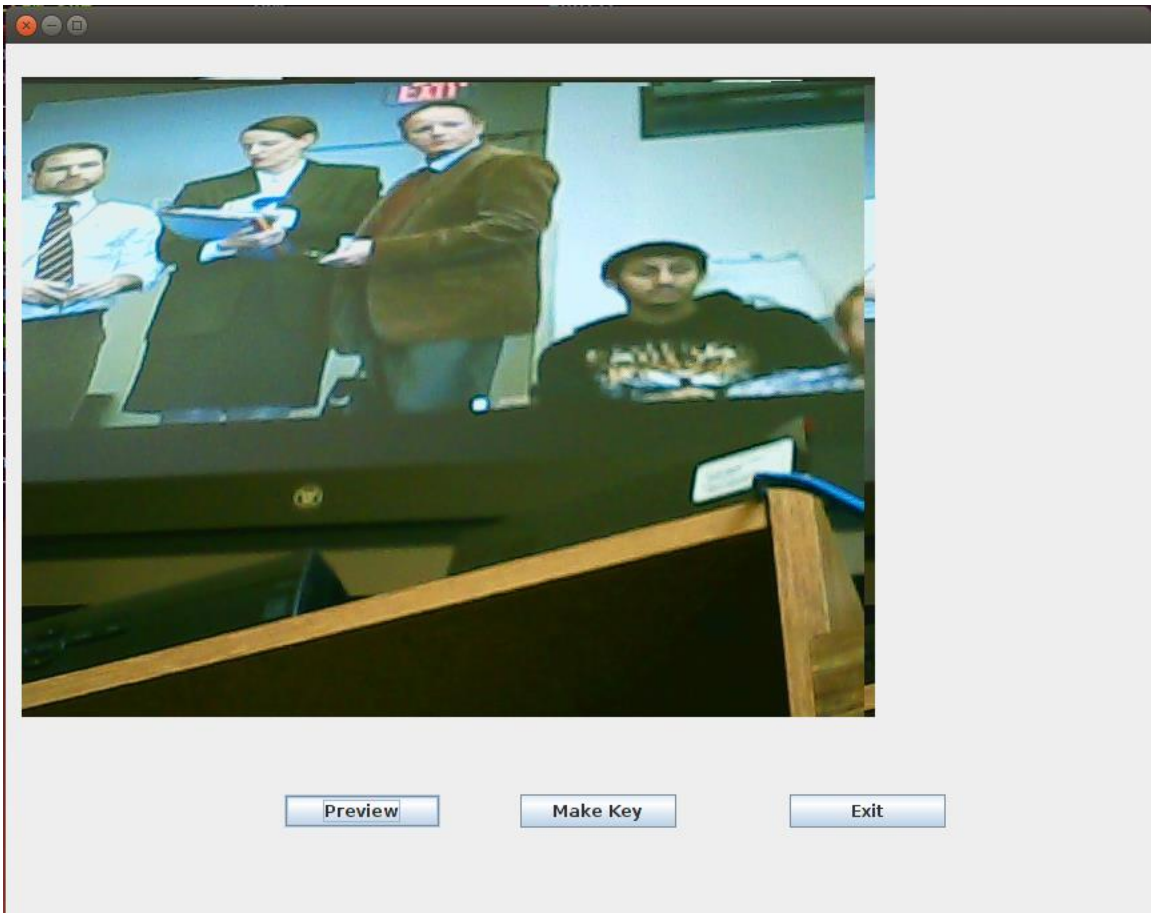
INSTALL THE SUPPLIED USB CAM
The camera supplied with Cypher is very simple to install into a USB port. It is designed to be a plug and play device that is automatically installed on Linux systems. Make sure you have the OpenCV libraries created using the installation shell programs.

KEY CREATION

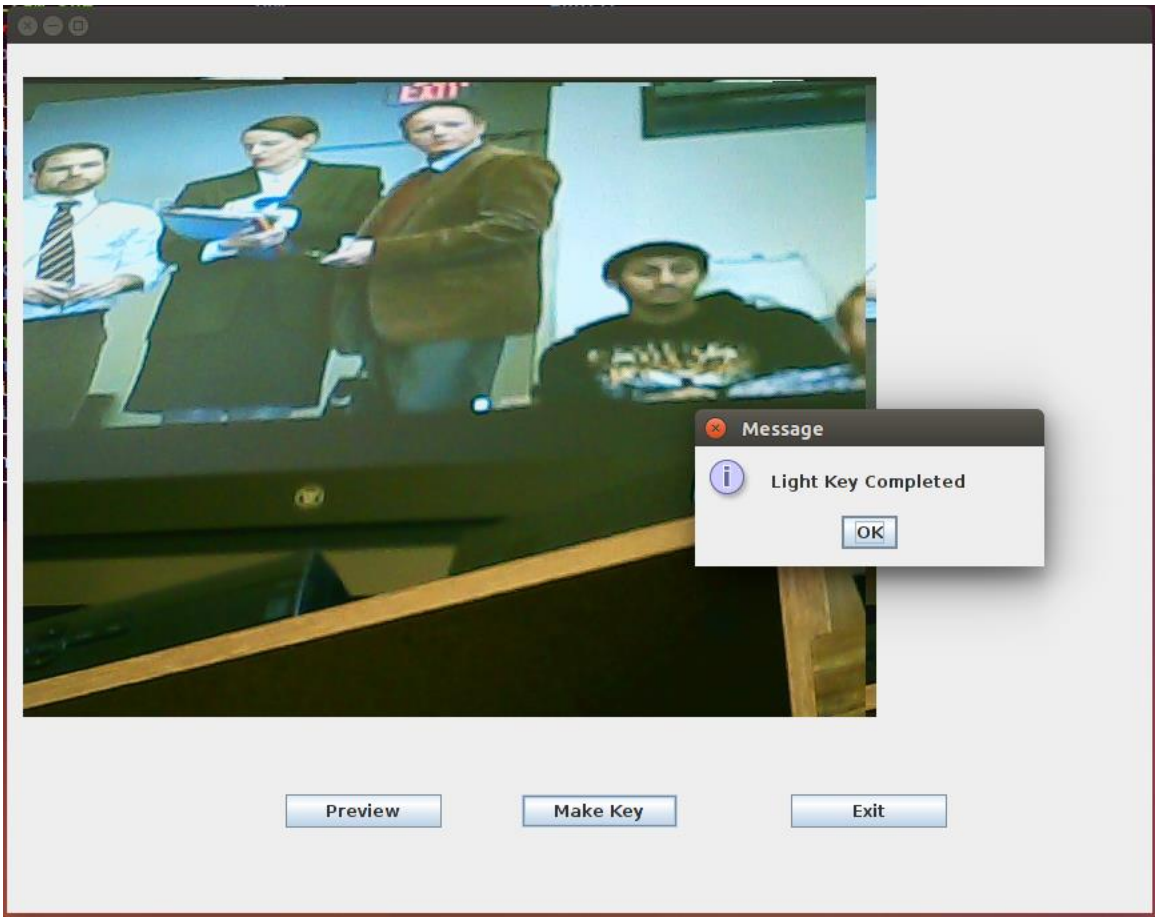
The light key preview menu



Select the desired camera in the camera selection box at the top of the menu and click the START PREVIEW button. The menu will display the image from the selected camera.



The Light key creator will display a preview image of the image you wish to convert into a key file. When you are satisfied with the preview image hit the MAKE KEY button.



The light key creator will create a key to the size specified unless there is not enough data inside the image. If the image does not contain enough random data the creator will continue to take images until the key is completed. You may change the camera position to alter the image at any time

Once completed click the OK button on the pop up LIGHT KEY COMPLETED message and hit the EXIT button.

IMAGE KEY TIPS:
It is desirable to use images that have a large variety of objects and colors. Images of a single color such as sky or walls will yield a low amount of random values while complex images of many objects and moving objects will yield larger volumes of usable data.

GOOD IMAGE  **NOT GOOD** 

SYSTEM REQUIREMENTS:
Linux Ubuntu 14.04 LTS or equivalent
USB port for USB camera (supplied)
or pre-installed web camera

TECHNICAL SPECIFICATIONS
CYPHER is a symmetrical block cipher private key system that can be used in a ONE TIME PAD mode. This means that you must exchange keys with the individuals you wish to communicate to and use the entire key only ONE TIME. Private key systems are far more secure than any PUBLIC key encryption and the ONE TIME system has been used by US presidents to communicate with Moscow and by the US military to lock down nuclear weapons.

CONTACT INFORMATION:
http://www.softwar.net
Email : softwar@softwar.net

Trademarks:
Ubuntu and Canonical are registered trademarks of Canonical Ltd
Java is a registered trademarks of Oracle Corporation
OpenCV information http://opencv.org/

SOFTWAR End-User License Agreement

BY INSTALLING OR USING THE LICENSED SOFTWARE AND HARDWARE FROM SOFTWAR 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 SOFTWAR INC.

IN NO EVENT SHALL SOFTWAR 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 SOFTWAR 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 SOFTWAR 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. SOFTWAR 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.