

Pict-o-Crypt User's Guide v1.1

pict.o.crypt@gmail.com



1 Pict-o-Crypt Introduction

Pict-o-Crypt is a portable AES encryption unit that keeps your camera pictures secure with three easy steps:

1. configure the Pict-o-Crypt AES parameters (see [section 3](#))
2. use Pict-o-Crypt to encrypt camera pictures (see [section 4](#))
3. decrypt camera pictures on Windows XP (see [section 5](#))

Pict-o-Crypt is a custom adaptation of a 5-in-1 USB Charger, which adds USB device and host functionality allowing Pict-o-Crypt to be initially configured by a USB host computer and then subsequently used to directly encrypt on-camera images thru a camera's USB Mass Storage Class interface, or indirectly encrypt images on a camera's memory card thru the included USB card reader.

1.1 Auto Power-Off

The Pict-o-Crypt USB functionality will automatically power off after being idle for one minute, to save battery life.

To power the Pict-o-Crypt USB functionality back on, either disconnect and reconnect the USB host computer (when in Device Mode) or turn the Unit Switch **OFF** and then back to the **USAGE** position (when in Host Mode).

2 5-in-1 USB Charger Functionality

Please see the *Multi-Function Charger Operating Instructions* for how to:

- Charge the Pict-o-Crypt batteries from USB power, AC power, or Car power, with the Unit Switch in the **CHARGING** position,
- Use the Pict-o-Crypt batteries to charge an external USB device, with the Unit Switch in the **USAGE** position, and
- Use the Pict-o-Crypt torch (flashlight), with the Unit Switch in the **USAGE** position.

Note that the Pict-o-Crypt can be configured by a USB host computer even with the Unit Switch in the **OFF** position.

3 Configuring Pict-o-Crypt (Device Mode)

Pict-o-Crypt is configured via a USB host computer running a terminal emulator program, such as HyperTerminal on Windows XP, connected to a virtual COM port exposed by the Pict-o-Crypt USB device driver.

3.1 Connecting Pict-o-Crypt to the USB Host Computer

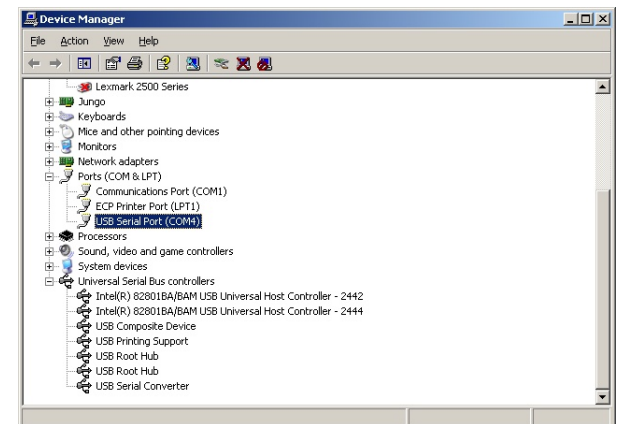
Place the Pict-o-Crypt Unit Switch in either the **OFF** or **CHARGING** position and use the USB A to A cable to connect Pict-o-Crypt to a USB host computer:



3.2 Installing the Pict-o-Crypt USB Driver

When the Pict-o-Crypt is connected to a USB host computer, it will present an Virtual COM Port function to the host computer. An appropriate driver will be loaded automatically from microsoft.com, if needed, or you can manually install the VCP driver from <http://www.ftdichip.com/FTDrivers.htm> or from the Pict-o-Crypt CD-ROM.

Once the driver is loaded, a new virtual COM port (VCP) will be present on your system. This virtual COM port will be visible in Device Manager:



3.3 LED Status Indicator (Device Mode)

When the Pict-o-Crypt is running in device mode, the LED indicator will blink *slow blue* when idle, and *fast blue* when there is USB traffic.

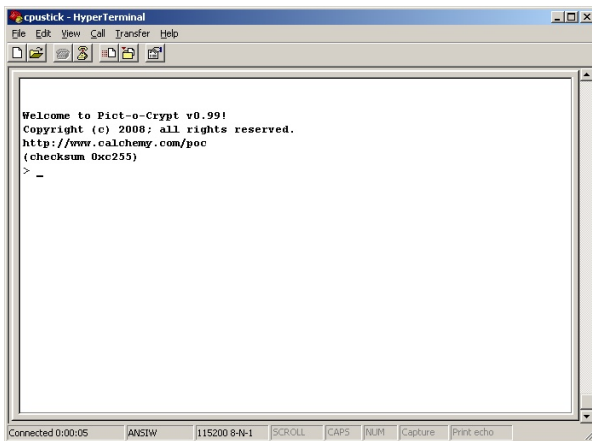
A serious software error will be indicated by a *numeric error code blinking in red*, such as eight blinks followed by five blinks, repeated until auto power-off, to indicate error code 85. Please report this error code to us. Power cycle the Pict-o-Crypt to clear the software error.

3.4 Interfacing with Pict-o-Crypt via HyperTerminal

At this point you can use HyperTerminal (typically found under Start -> All Programs -> Accessories -> Communications -> HyperTerminal) to connect to the new virtual COM port.

Specify a new connection name, such as “Pict-o-Crypt”, and then select the new virtual COM port under Connect To; the baud rate and data characteristics in Port Settings are ignored.

Press <Enter> when you are connected and you should see the command prompt:



If the USB connection is lost (such as when you unplug and re-plug in the Pict-o-Crypt), press the “Disconnect” button followed by the “Call” button, to reconnect HyperTerminal.

Note that if you do not have HyperTerminal (such as in Windows Vista or Linux), “putty” is available free from <http://www.putty.org/>; the latest version supports COM port connections.

You are now ready to enter Pict-o-Crypt administration commands.

3.4.1 The Pict-o-Crypt command line

In the command specifications that follow, the following nomenclatures are used:

bold	literal text; enter exactly as shown
<i>italics</i>	parameterized text; enter actual parameter value
(alternate1 alternate2 ...)	alternated text; enter exactly one alternate value
[optional]	optional text; enter if appropriate
regular	displayed by Pict-o-Crypt
<key>	press this key

When Pict-o-Crypt is controlled with an ansi or vt100'ish terminal emulator program, command-line editing is enabled via the terminal keys, as follows:

key	function
←	move cursor left
→	move cursor right
↑	recall previous history line
↓	recall next history line
<Home>	move cursor to start of line
<End>	move cursor to end of line
<Backspace>	delete character before cursor
<Delete>	delete character at cursor
<Ctrl-C>	clear line
<Enter>	enter line to Pict-o-Crypt

If you enter a command in error, Pict-o-Crypt will indicate the position of the error, such as:

```
> help nothing
      ^ - error
> _
```

3.4.2 Getting help

On-line help is available with the command:

```
help [about]
```

By itself, the help command displays information about available commands. With the optional **about** specifier, the help command displays information about the Pict-o-Crypt firmware version.

3.4.3 Setting the AES encryption key size

You can display or set the current AES key size, in bits, with the command:

```
aesbits [128 | 192 | 256]
```

By itself, the aesbits command displays the current AES key size; with the optional bit length specifier, it sets the current AES key size. The default AES key size is 256 bits.

3.4.4 Setting the AES encryption key

You can set the current AES encryption key, either to a hexadecimal value or to a passphrase value, with the command:

```
aeskey hexkey
aeskey passphrase
```

If *hexkey* is an even number of hexadecimal digits (0-9, a-f), then that key value, exactly will be used, up to the current AES key size. Otherwise, *passphrase* is interpreted as an easy-to-remember passphrase, from which the key value is trivially derived -- the longer the passphrase, the more secure the derived key. The *passphrase* may contain spaces, but should not contain quotes (which are difficult to enter in Windows).

You must then confirm the *hexkey* or *passphrase* before it will be updated.

To reset the AES encryption key to its default value, use the command:

```
aeskey
```

Note there is no way to display the current AES encryption key.

3.4.5 AES encryption key tips

AES key security is critical to keeping your pictures secure. You should choose an AES key that cannot be guessed by an attacker. If you are using 256 bit AES encryption, the most secure (full-length) hexkey contains exactly 64 random hexadecimal (0-9, a-f) characters.

An AES passphrase is designed to be easy to remember, but is not as secure as an AES hexkey. To make your AES passphrase as secure as possible, be sure to use a mix of as many printable (upper case, lower case, numeric, symbolic) characters as possible. If you are using 256 bit AES encryption, the most secure (full-length) passphrase contains at least 32 characters; this passphrase is approximately 35% as secure in key length against a brute force attack as a (full-length) random hexkey.

3.4.6 Selecting which files to encrypt

By default, Pict-o-Crypt encrypts all read/write (i.e., unprotected) files in the filesystem with the following file extensions: *.JPG, *.MOV, *.MPG, *.MP4, *.NEF.

The user can change whether read/write (i.e., unprotected) or read-only (i.e., protected) files are encrypted with the command:

```
select [ro|rw]
```

By itself, the select command displays the current protection setting; with the optional read/write or read-only specifier, it sets the protection setting.

Additionally, the user can change the default file extension list with the command:

```
files [clear|default|  
+extension|-extension]
```

By itself, the files command displays the current file extension list; with the **clear** specifier, the list is cleared (no files will be encrypted); with the **default** specifier, the list is reset as indicated above; with the **+** or **-** specifier, the specified *extension* is added to or removed from the list of files to be encrypted.

3.4.7 Examples

```
Welcome to Pict-o-Crypt v1.1!  
Copyright (c) 2008; all rights reserved.  
pict.o.crypt@gmail.com  
(checksum 0x14a6)  
> help  
commands:  
  aesbits [(128|192|256)]  
  aeskey (<hexkey>|<passphrase>)  
  files [clear|default|+<extension>|-<extension>]  
  help  
  reset  
  select [ro|rw]  
  upgrade  
  uptime  
  
for more information:  
  help about  
  
see also:  
  pict.o.crypt@gmail.com  
> aesbits 256  
> aesbits  
files will be encrypted with:  
  256 bits  
> aeskey 112233445566778899aabbccddeeff00  
confirm hexkey:  
? 112233445566778899aabbccddeeff00  
hexkey updated  
> aeskey this is my private key nobody can guess  
confirm passphrase:  
? this is my private key nobody can guess  
passphrase updated  
> select  
files will be encrypted if:  
  rw (read/write)  
> select ro  
> select  
files will be encrypted if:  
  ro (read-only)  
> files  
the following files will be encrypted:  
  *.JPG  
  *.MOV  
  *.MPG  
  *.MP4  
  *.NEF
```

```
> files -*.NEF  
> files +*.RAW  
> files  
the following files will be encrypted:  
  *.JPG  
  *.MOV  
  *.MPG  
  *.MP4  
  *.RAW  
> files default  
> -
```

3.4.8 Upgrading the Pict-o-Crypt firmware

To upgrade the Pict-o-Crypt firmware, use the following command:

```
upgrade
```

Pict-o-Crypt will indicate when it is ready for the new firmware with the message:

```
paste S19 upgrade file now...
```

At that point you should open the S19 file in a text editor, such as Notepad, select all of the text, copy it to the clipboard, and then paste the entire contents into your terminal emulator window.

When upgrade is nearly complete (about two minutes), you will see:

```
paste done!  
programming flash...  
wait for LED to blink!
```

Then wait for the Pict-o-Crypt indicator LED to blink, indicating flash programming is complete. Then reconnect your HyperTerminal. Note that once flash programming begins, a failed (or interrupted) upgrade procedure can only be recovered by us.

Note that the upgrade procedure wipes out all encryption parameters from flash memory.

4 Using Pict-o-Crypt to Encrypt Pictures (Host Mode)

Use the USB A to mini-B cable to connect Pict-o-Crypt to either the camera or the included USB card reader:



Alternately, use the USB A adapter cable that came with your USB Mass Storage Class interface capable camera.

Place the Pict-o-Crypt Unit Switch in the *USAGE* position; encryption will begin and end automatically, as indicated on the LED status indicator, below.

4.1 LED Status Indicator (Host Mode)

When the Pict-o-Crypt is running in host mode, the LED indicator will blink *slow blue* when idle, and *fast blue* when there is USB traffic to the USB Mass Storage Class device and encryption is in progress.

Additionally, as each file is encrypted, there will be *two fast green blinks interleaved with the fast blue blinks*.

When all selected files have been encrypted, the LED indicator will blink *slow green*, indicating it is safe to turn the unit off or remove the USB Mass Storage Class device.

If the battery voltage drops below acceptable levels during encryption, the LED indicator will blink *one red blink*, repeatedly. If a USB error occurs talking to the USB Mass Storage Class device (such as filesystem full), the LED indicator will blink *two red blinks*, repeatedly.

A serious software error will be indicated by a *numeric error code blinking in red*, such as eight blinks

followed by five blinks, repeated until auto power-off, to indicate error code 85. Please report this error code to us. Power cycle the Pict-o-Crypt to clear the software error.

4.2 Pause Button

While the Unit Switch is in the *USAGE* position, the torch (flashlight) switch can be used to pause file encryption, by turning the torch on. Encryption will pause after the completion of the current file, and the LED indicator will return to the idle (*slow blue*) status. If necessary, it is permissible to turn the unit off or remove the USB Mass Storage Class device when paused and idle.

4.3 Panic Button

While the Unit Switch is in the *USAGE* position, the flashlight (torch) switch can be used to panic and erase the contents of the USB Mass Storage Class device (unrecoverably), by turning the torch on and off rapidly between 6-10 times. Erasure will commence immediately and the LED indicator will blink *fast green blinks interleaved with the fast blue blinks*. When erasure is complete, the LED indicator will blink *slow green*.

4.4 Performance

Encryption:	approx. 4-7 seconds/MB, depending mostly on filesystem cluster size
Panic/Erase:	approx. 1-2 seconds/MB, depending mostly on memory card
Battery Life:	
encrypting:	4 hours (approx. 2-3.6 GB)
erasing:	4 hours (approx. 7-14 GB)
auto power-off:	80 hours

5 Decrypting Pictures

The decryption software consists of a single Windows XP executable on the CD-ROM: **pdcc.exe**, which is run from the Windows command prompt (Start -> Run... -> cmd -> OK).

To decrypt files, use the following command:

```
pdcc [-b (128|192|256)]  
      [-k aeskey]  
      sourcedir destdir
```

The **-b** option sets the AES encryption key size, in bits, to match the value of Pict-o-Crypt; the **-k** option sets the AES encryption key (hexkey or passphrase) to match the value of Pict-o-Crypt. The default values for the options match the default values of Pict-o-Crypt, though please note that it is patently unsafe to use the default aeskey for encryption!!!

Note that if the Pict-o-Crypt passphrase includes spaces, it must be enclosed in double quotes at the Windows command line, such as:

```
-k "this is my private key nobody can guess"
```

The command will then read all files below *sourcedir* looking for encrypted files. It will unencrypt them to their corresponding location under *destdir*, and then remove the encrypted file. Typically *sourcedir* will be the drive letter where your USB Mass Storage Class device is mounted. If *sourcedir* and *destdir* are the same, then decryption occurs "in place"; if either directory specifier is omitted, it defaults to the current directory. If decryption fails, an error is printed.

5.1.1 Examples

```
c:\temp>pdcc -?  
pdcc [-b <aesbits>] [-k <aeskey>] <sourcedir>  
<destdir>  
  
c:\temp>pdcc f: f:  
Decryption failed (zero check)  
  
c:\temp>pdcc -k "this is my private key nobody can  
guess" f: f:  
passphrase updated  
decrypting DCIM\101MSDCF\DSC00010.JPG (2364124 bytes)  
decrypting DCIM\101MSDCF\DSC00011.JPG (2085177 bytes)  
decrypting DCIM\101MSDCF\DSC00012.JPG (2172091 bytes)  
decrypting DCIM\101MSDCF\DSC00009.JPG (2332215 bytes)  
  
c:\temp> _
```

6 Support

We are available by e-mail at pict.o.crypt@gmail.com