ADL-1 OTPF Users Manual

Revision 1.4

Table of Contents

Specifications

Size (W x L x H)	8.7 x 7.5 x 3.9 inches
Weight with paper and batteries	2 lbs, 6oz
External Power	12 – 13.8 vdc. 2.1 mm center positive, 2 amps
Batteries	2 18650 2400ma or better Li-Ion batteries
Paper size (W, L)	2.25 x 1.5 inches (about 50 ft)

Introduction

The Partisan Labs One Time Pad, Field (ADL-1), is a convenient and secure way to generate and print one time pads (OTPs) . The ADL-1 is based around the Infinite Noise True Random Number Generator (https://github.com/waywardgeek/infnoise) USB key but has none of the attack surface that a PC or laptop has. It quickly prints pads of 250, 500, or 1000 digits or letters based on true random numbers. Source code and schematics are available from the Partisan Labs web page (www.partisanlabs.com).

Usage

To use the ADL-1, open the case by unlatching the two latches on the from of the case and open the unit. Power the unit on using by pushing the "1" marking on the power switch towards the back of the unit. When the unit is on the red LED on the printer will flash and the size and options LEDs will be lit.

To generate a pad:

1. Choose the number of digits or letters in the pad by pressing the Size button to cycle through the available options 250, 500, or 1000 digits or letters.

2. Press the Generate button to begin creating the pad. The Ready LED by the Printer button will begin flashing orange and the ADL-1 will begin hashing entropy to create the pad. Once the required amount of entropy has been collected and hashed, the Ready LED will turn solid green. Once the pad has been generated, a 5 minute pad timeout timer is started. If there is no print activity for 5 minutes the pad will automatically be erased from memory and cannot ever be regenerated. The "Ready" led will start blinking green 30 seconds before the timer expires and orange for the last 5 seconds. The timeout timer is reset back to 5 minutes each time the pad is printed.

3. Using the Options button, choose between "Pad" or "Pad + Codex" (conversion table). Selecting "Instructions" will only print instructions for using OTPs. It will not print a pad.

4. Press the Print button for each printed copy of the pad you want to print. You can print as many copies of the pad as you would like as long as the Size or Generate buttons are not pressed again. Pressing on of these buttons will erase the pad from memory and turn off the green "Ready" LED. The pad timeout timer is reset each time you print a pad.

To print encryption/decryption instructions

1. Using the Options button, select "Instructions". The "Ready" LED will turn green.

2. Press the Print button for each copy of the instructions you want to print. Please note it is not possible to print a pad while the Option is set to "Instructions"

Advanced Usage

Printing pads in letter mode (DIANA)

Requires firmware 2.1.2 or newer.

To print letter based pads suitable for use with the DIANA table:

1. Turn off the unit.

2. Press and hold the Size button.

3. Turn on the unit while holding the Size button.

4. Release the Size button.

The Size LEDs will blink continuously to note that you are in letter mode and the pads will print letters instead of numbers and the Codex will print a DIANA conversion table.

Using the alternative Codex

Requires firmware 2.1.2 or newer.

To enable the printing of the alternative codex (for numeric mode, DIANA trigrams for letter mode):

1. Turn off the unit.

2. Press and hold the Options button.

3. Turn on the unit while holding the Options button.

4. Release the Options button.

The Options LED will blink when it is on Pad + Codex when you are in alternate Codex mode.

Size and Options buttons can be use together to achieve the desired operating mode.

Printing firmware version

To print out the current firmware version:

1. Turn off the unit.

2. Press and hold the Generate button

3. Turn on the unit while holding the Generate button

4. Release the generate button. There is no need to hold it once the power is on.

The print will advance and print the running firmware version.

Reading entropy to a PC

To read the entropy created on the ADL-1 on a PC:

1. Power off the unit.

2. Remove the 6 1/16" hex screws holding the panel on.

3. Remove the panel, keeping the battery supported, and turn it over in the case.

4. In the bottom of the case is a piece of masking tape. Under the tape there is a jumper.

5. Remove the jumper and place it on J3, covering the middle pin and either the "W" or "R" pin. The "W" pin will capture the whitened entropy and the "R" pin will capture the raw, unwhitened entropy.

6. Place a FTDI 3.3v serial to USB cable **TTL-232R-3V3** on J4 with the black wire on the pin marked "blk".

7. Power on the ADL-1. The "Ready" LED will flash orange like it is generating a pad and the entropy will be sen out the serial port. Note that the ADL-1 will not print pads while capturing entropy as they would be compromised.

8. Start your serial capture program on you PC to record the entropy. Use serial settings 57600,N,8,1

9. If you want to switch the entropy source (whitened or raw) power off the ADL-1 and move the jumper, then power it back on.

10. Power off the ADL-1 and remove the jumper to resume normal operation.

Reading the debug messages.

To read the entropy created on the ADL-1 on a PC:

1. Power off the unit.

2. Remove the 6 1/16" hex screws holding the panel on.

3. Remove the panel, keeping the battery supported, and turn it over in the case.

4. Place a FTDI 3.3v serial to USB cable **TTL-232R-3V3** on J4 with the black wire on the pin marked "blk".

5. Start your serial capture program on you PC to view the log messages. Use serial settings 57600,N,8,1

6. Power on the ADL-1.

7. As system operates debug messages are displayed. The number on the left is the number of milliseconds since the system was started.

To change the power on default mode

To change the power on default mode from numeric pads to letter based pads:

1. Power off the unit.

2. Remove the 6 1/16" hex screws holding the panel on.

3. Remove the panel, keeping the battery supported, and turn it over in the case.

4. To default to letter mode jumper J8 pin/pad 1 & 2.

5. To default to using the alt codex (numeric or letter) jumper J8 pin 2 & 3.

6. Reassemble unit.

Once this is done, the startup procedure of holding the Size and Options on power on will switch back to the other mode.

Updating the firmware

To update the firmware on the ADL-1:

1. Download the Firmware Flashing program from the AmRRON Dark Labs website and the latest firmware file. The Firmware Flashing program requires a Java 7 runtime to operate.

2. Power off the unit.

3. Remove the 6 1/16" hex screws holding the panel on.

4. Remove the panel, keeping the battery supported, and turn it over in the case.

5. Place a FTDI 3.3v serial to USB cable **TTL-232R-3V3** on J4 with the black wire on the pin marked "blk".

6. While pressing the blue button S5, power on the ADL-1. A blue LED will light up above the CPU. Release the blue button. The ADL-1 is now ready to receive new firmware.

7. Launch the Firmware Flashing program on the PC and follow the prompts.

8. Power off the ADL-1 and disconnect the serial cable. Reassemble the ADL-1.

Care and Maintenance

To clean the ADL-1

To clean you ADL-1 use a damp, not wet, towel and wipe down the face plate and case. If there is oil or grease on the unit use Isopropyl alcohol on a rag to clean it. Under no circumstances should you use Acetone, Naphtha, Mineral Spirits, or any other solvent other that Isopropyl alcohol on the ADL-1. They will damage it.

To replace the batteries

To replace the batteries:

1. Remove the battery cover by gently squeezing the long sides of the cover and lifting.

2. Gently pull the battery holder out of the case.

3. Remove the batteries. The battery holder is very tight, you may need to use something to gently lift the end of the battery out of the holder.

4. Put the new batteries in the holder. Negative side goes towards the springs.

5. Lower the holder back into the case, taking care to not damage the wires.

6. Replace the battery cover.

Troubleshooting

Problem	Solution
Printer will not print	Verify there is paper in the printer. Press the printer "Offline" button (II) and try to print again. Turn off the ADL-1, wait a few seconds then turn it back on.
Print quality is degrading	Replace batteries. Use external DC power.
"Ready" LED flashes red and system locks up.	Turn off the ADL-1, wait a few seconds then turn it back on. The run-time diagnostic in the firmware has detected abnormal operation of the random number generator. This usually only occurs if you power cycle the ADL-1 repeatedly and quickly. It is preventing you from using the ADL-1 to generate pads that may not be secure.
Size, Options, and Print Ready LEDs light up but printer light is not blinking and nothing prints.	If you are running from battery then most likely the battery does not have enough current to operate the printer. The CPU will run down to 3.3 volts but the printer requires at least 5 volts 1.5 amps to operate. Recharge the batteries. If you are seeing this using external power and are sure the external supply is 12 volts 1.5 amps or greater then contact support.

Hacking

The ADL-1 is an open system. Source code and schematics are available on the AmRRON Dark Labs web page.   You can write your own firmware and flash it in if you want to but if you do so we will no longer support it. Here are some details to get you started.

CPU	Atmel ATXMEGA256C3
Compiler	AVR GCC, easiest to use Atmel Studio. You can also use AVR Eclipse, or your favorite text editor and the command line.
Bootloader	Emulates an AVR911 boot loader, you can use AVRDude or other compatible program to flash the application section.
Programmer	AVRISP MKII or other compatible device.