



calc.pw

Password Calculation with Arduino

Kenneth “Kenny” Newwood

E-Mail: kenneth@newwood.de

Jabber: cware@cwar.es

Twitter: @weizenspreu

Website: <http://weizenspr.eu>



Who?



Agenda

Why?

What?

How?

Sources!

Why?

Password memorization? (e.g. [1], [2] or [3])

Password databases? (e.g. [4])

Password calculation!

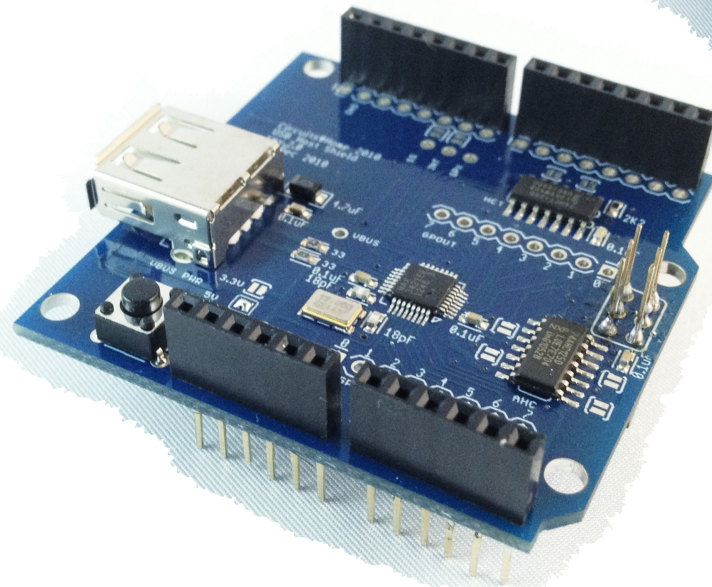
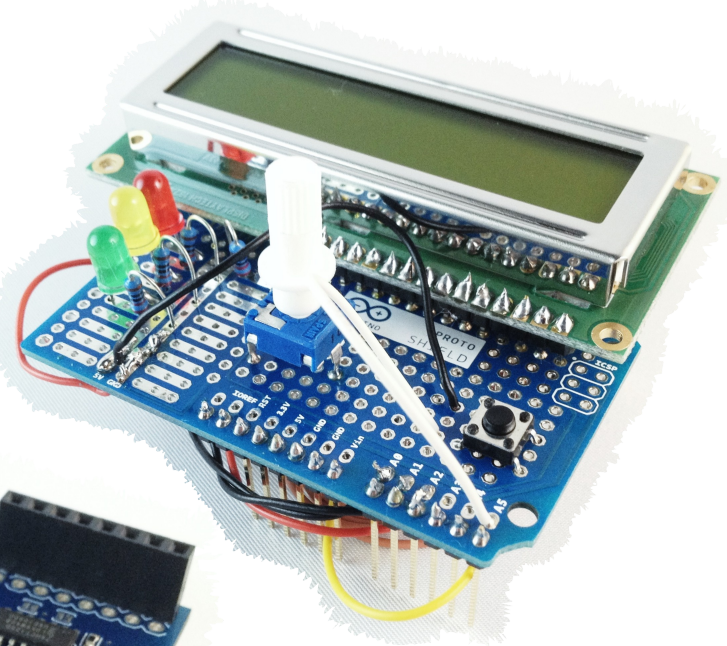
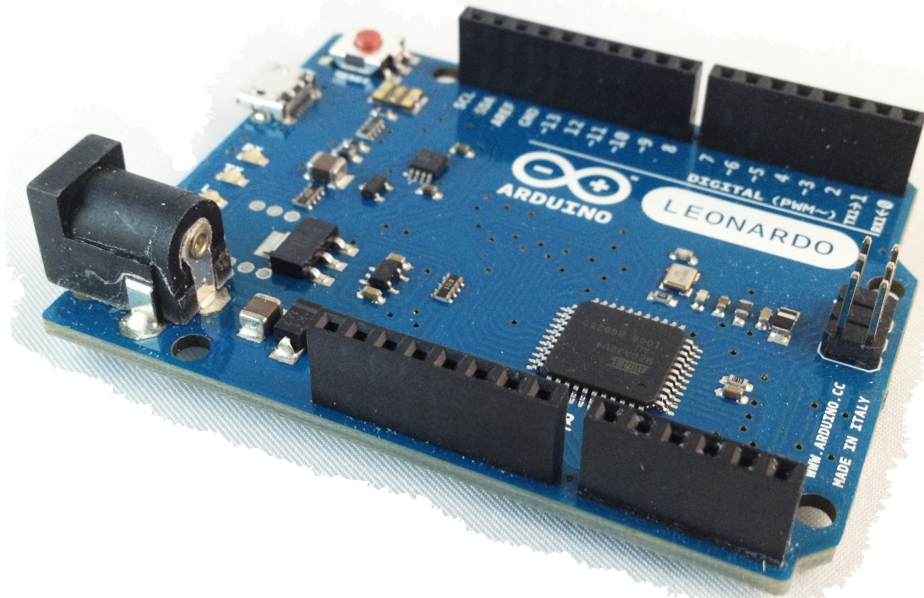
What? (1)

Hardware plugged between keyboard and PC

- Intercept keyboard
- Act as keyboard

Password = Magic(Information, Masterpassword)

What? (2)

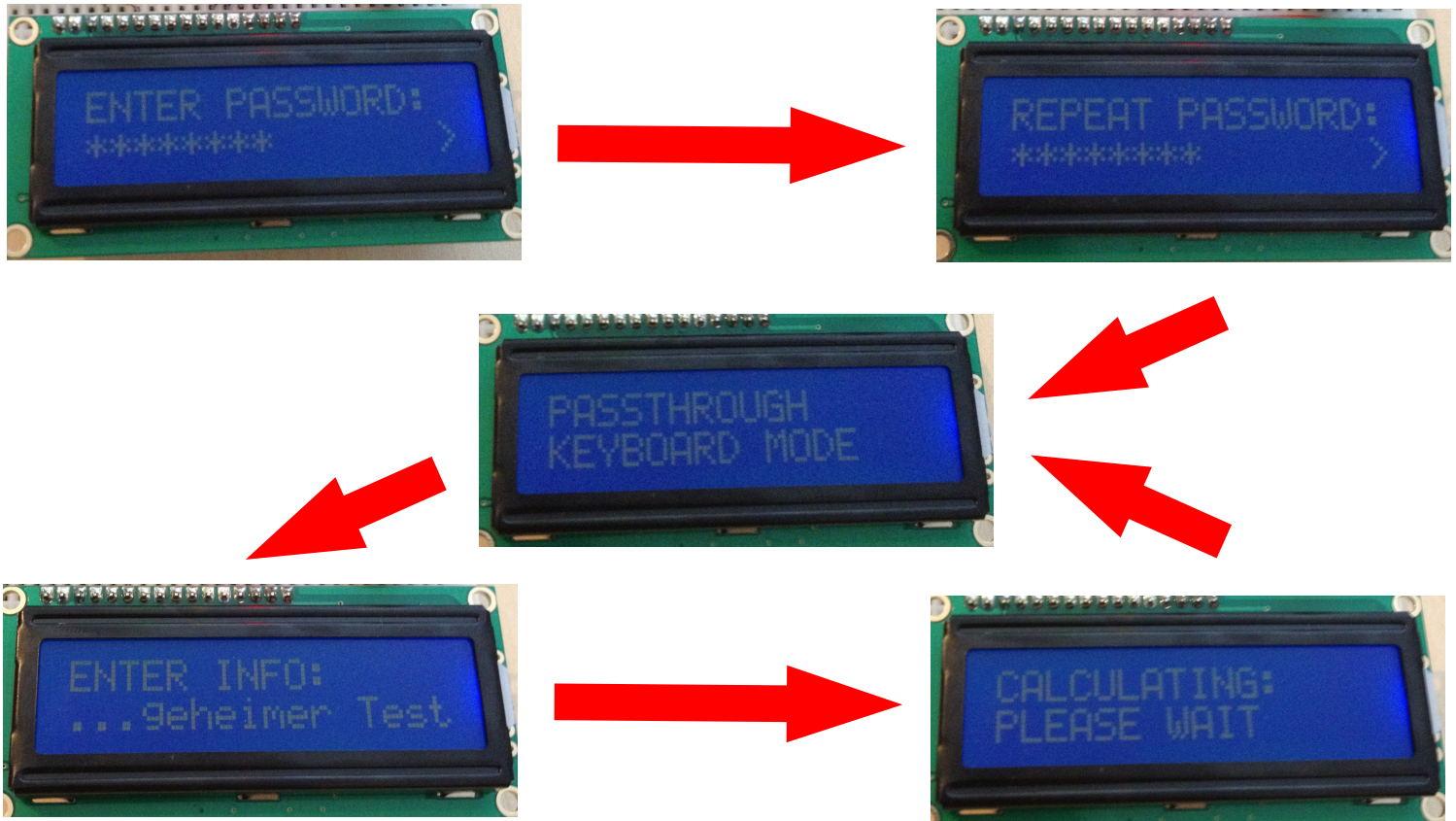


What? (3)



calc.pw – Password Calculation with Arduino

How? (1)



How? (2)

hash() = **SHA-1**

hmac() = HMAC-**SHA-1**

crypt() = **RC4-drop1024**

Magic(Information, Masterpassword)* =

hmacPassword = hmac(Information, Masterpassword)

hmacInfo[i=0] = hmac(hash(Information), Information)

hmacInfo[i=1..2] = hmac(hmacInfo[i-1], Information)

Password = base64(crypt(hmacInfo, hmacPassword))

(* simplified)

Sources!

<http://calc.pw/sigint13>

[1] <http://www.google.de/goodtoknow/online-safety/passwords/>

[2] <http://passwordadvisor.com/TipsUsers.aspx>

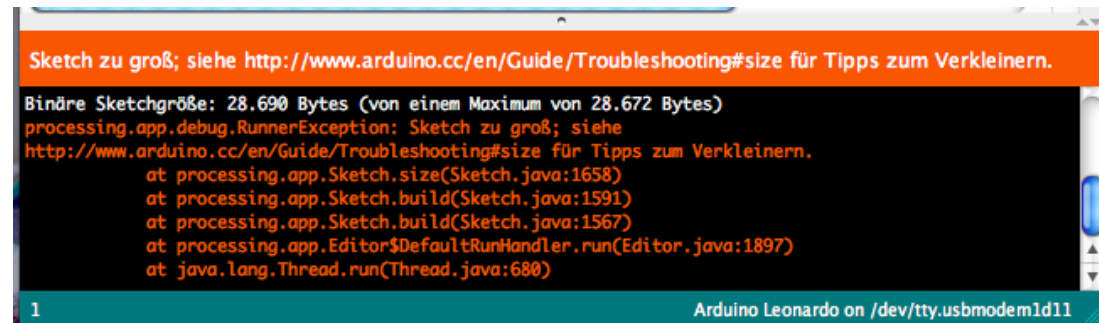
[3] <http://xkcd.com/936/>

[4] <https://bitbucket.org/HexRx/kpdatasave/wiki/Home>

Problems? (1)

ROM SIZE (Harvard Architecture!)

Arduino 1.0.5



```
Sketch zu groß; siehe http://www.arduino.cc/en/Guide/Troubleshooting#size für Tipps zum Verkleinern.  
Binäre Sketchgröße: 28.690 Bytes (von einem Maximum von 28.672 Bytes)  
processing.app.debug.RunnerException: Sketch zu groß; siehe  
http://www.arduino.cc/en/Guide/Troubleshooting#size für Tipps zum Verkleinern.  
    at processing.app.Sketch.size(Sketch.java:1658)  
    at processing.app.Sketch.build(Sketch.java:1591)  
    at processing.app.Sketch.build(Sketch.java:1567)  
    at processing.app.Editor$DefaultRunHandler.run(Editor.java:1897)  
    at java.lang.Thread.run(Thread.java:680)
```

1 Arduino Leonardo on /dev/tty.usbmodem1d11

Arduino 1.5.2

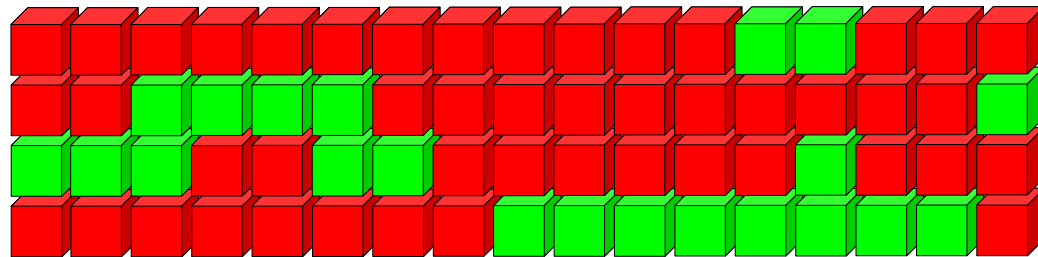


```
Übersetzen abgeschlossen.  
  
Binary sketch size: 28.372 bytes (of a 28.672 byte maximum) - 98% used
```

445 Arduino Leonardo on /dev/tty.usbmodem1d11

Problems? (2)

RAM SIZE (Stack-Heap Collision, Fragmentation)



Conditions of use

You can use this **OpenOffice** template for your personal, educational and business presentations.



With the use of this free template you accept the following use and license conditions.

You are free:

To Share — to copy, distribute and transmit the work

Under the following conditions:



Attribution — You must attribute the work in the manner specified by the author or licensor (but not in any way that suggests that they endorse you or your use of the work).



No Derivative Works — You may not alter, transform, or build upon this work.

In no event shall [Showeet.com](http://www.showeet.com) be liable for any indirect, special or consequential damages arising out of or in connection with the use of the template, diagram or map.

