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!

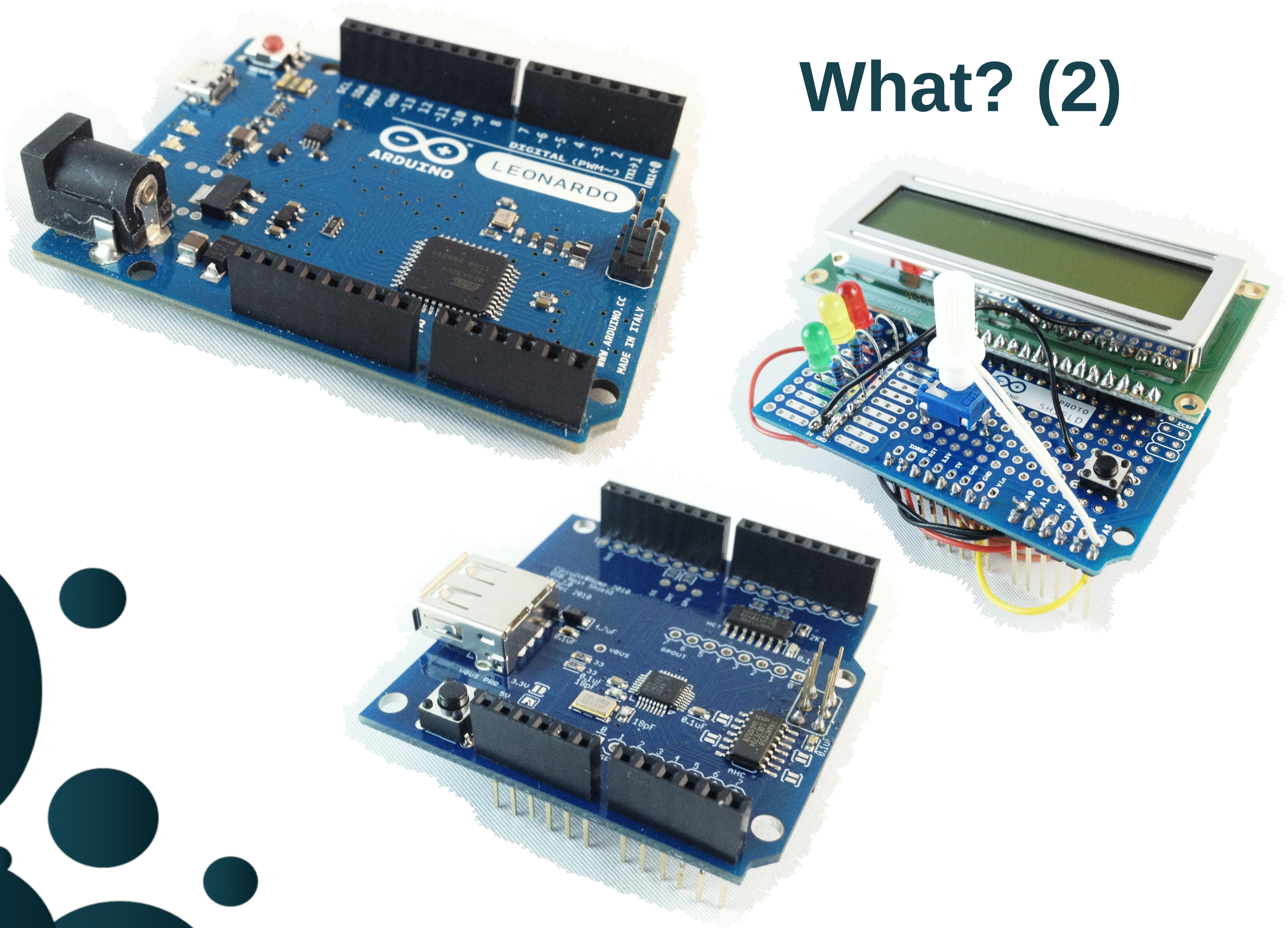
What? (1)

Hardware plugged between keyboard and PC

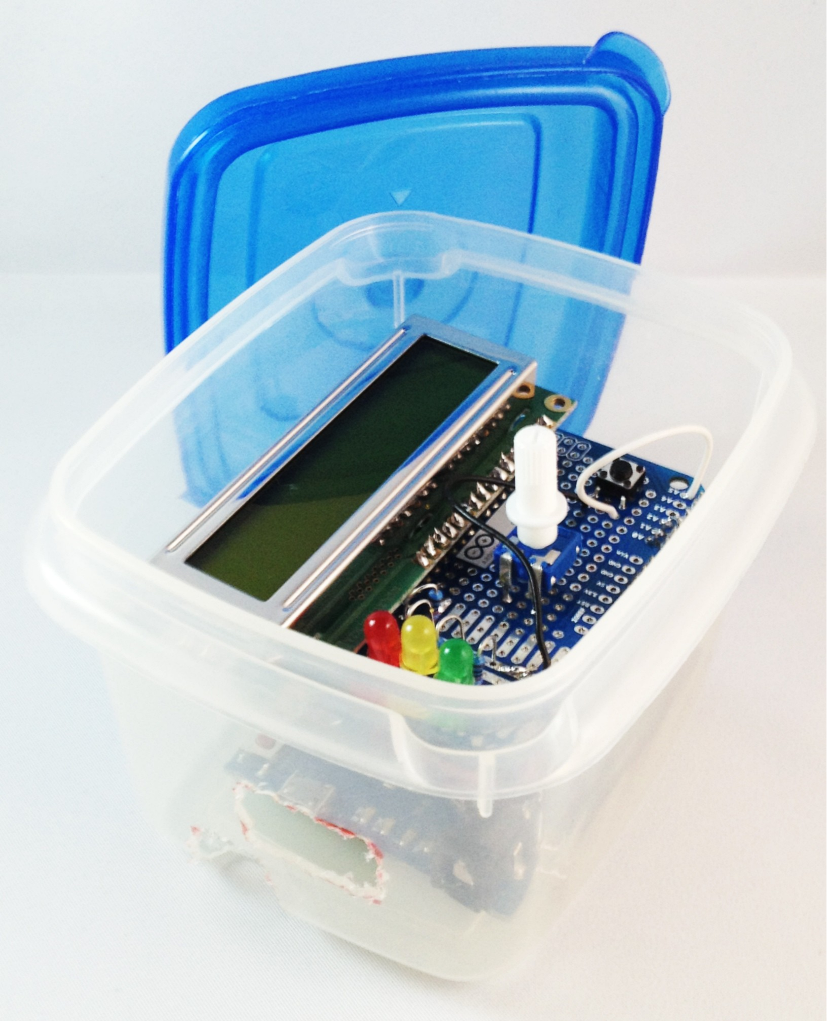
- Intercept keyboard
- Act as keyboard

Password = Magic(Information, Masterpassword)

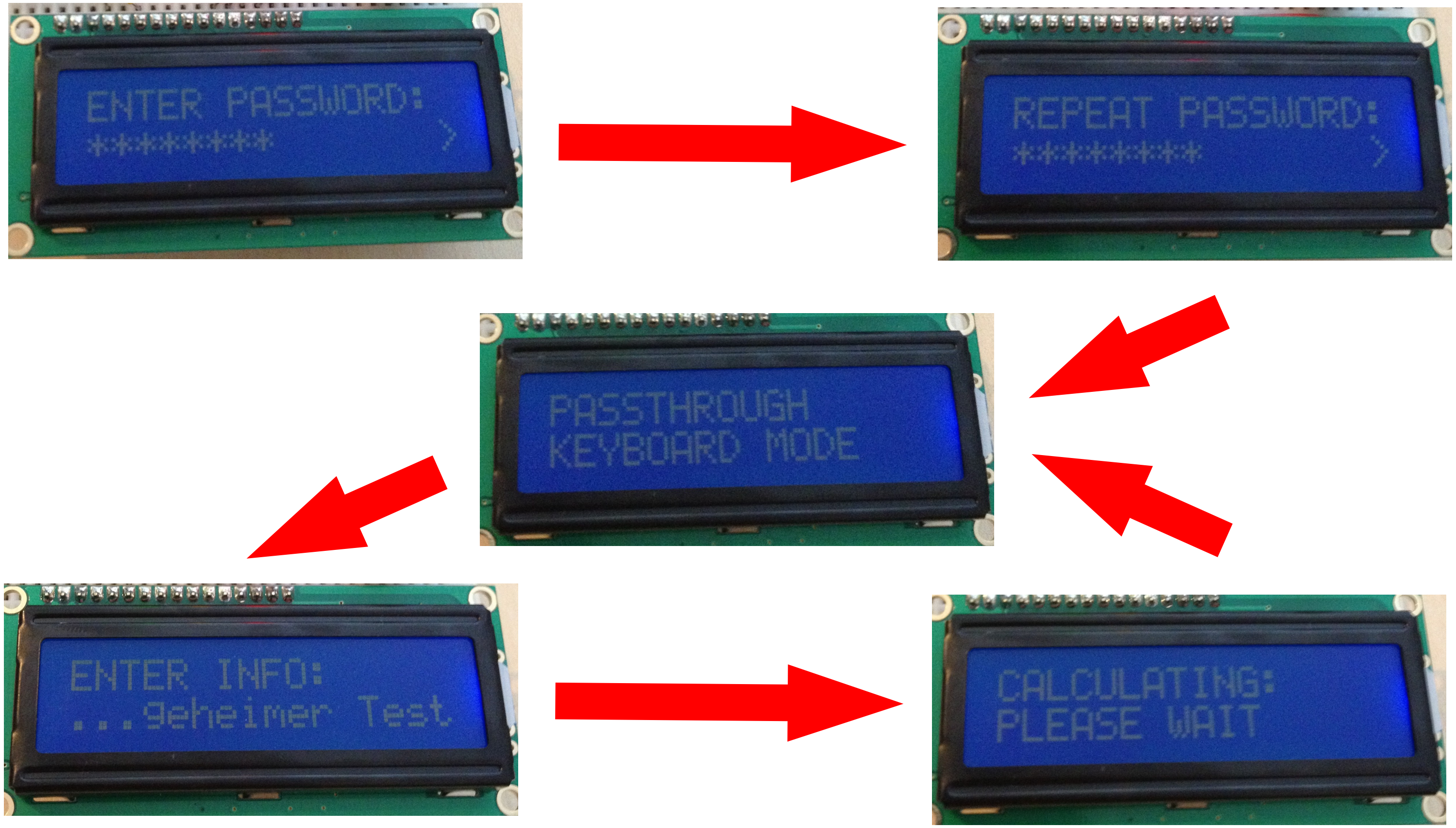
What? (2)



What? (3)



How? (1)


ENTER PASSWORD:
****
>
REPEAT PASSWORD:
****
>
PASSTHROUGH
KEYBOARD MODE
ENTER INFO:
...geheimer Test
CALCULATING:
PLEASE WAIT

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

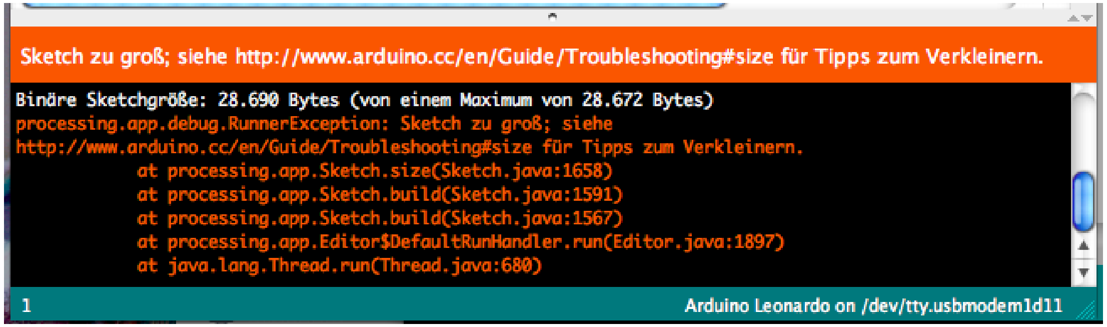
[3] http://xkcd.com/936/

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

Problems? (1)

ROM SIZE (Harvard Architecture!)

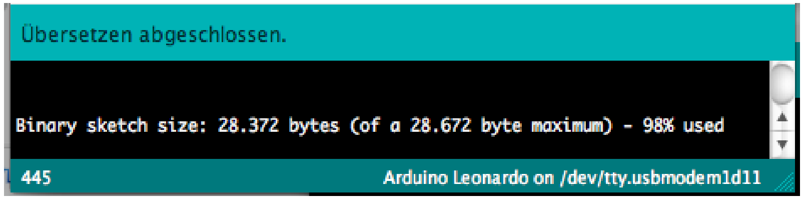
Arduino 1.0.5



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)
```

Arduino 1.5.2

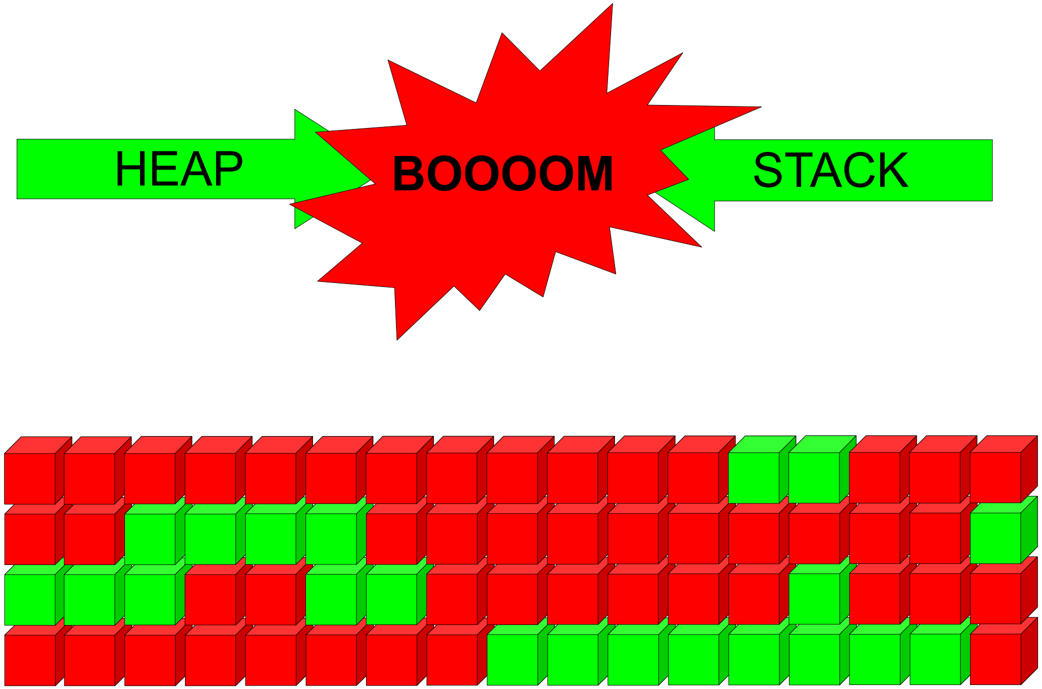


Übersetzen abgeschlossen.

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

Problems? (2)

RAM SIZE (Stack-Heap Collision, Fragmentation)



HEAP

BOOOOM

STACK

Conditions of use

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

http://www.showeet.com

http://creativecommons.org/licenses/by-nd/3.0/