UNIVERSITY OF Southampton
School of Electronics and Computer Science

Design Exercise D1

An encrypting PC keyboard

January 2013

The task

Your boss has found a big pile of NOS (new old stock) PS/2 keyboards and has had an *idea*.

He wants to sell them as secure encrypting keyboards for modern tablets.

Your task, in groups of four, is to realize his dream.

So far, along with the keyboards in the stock-room, you have found a pile of educational boards from a now-closed University—it failed its *Institutional Audit* and was closed by David Willetts. There are complete *Il Mateo AVR* boards and kits of parts for *Il Bagatto* CPLD boards.

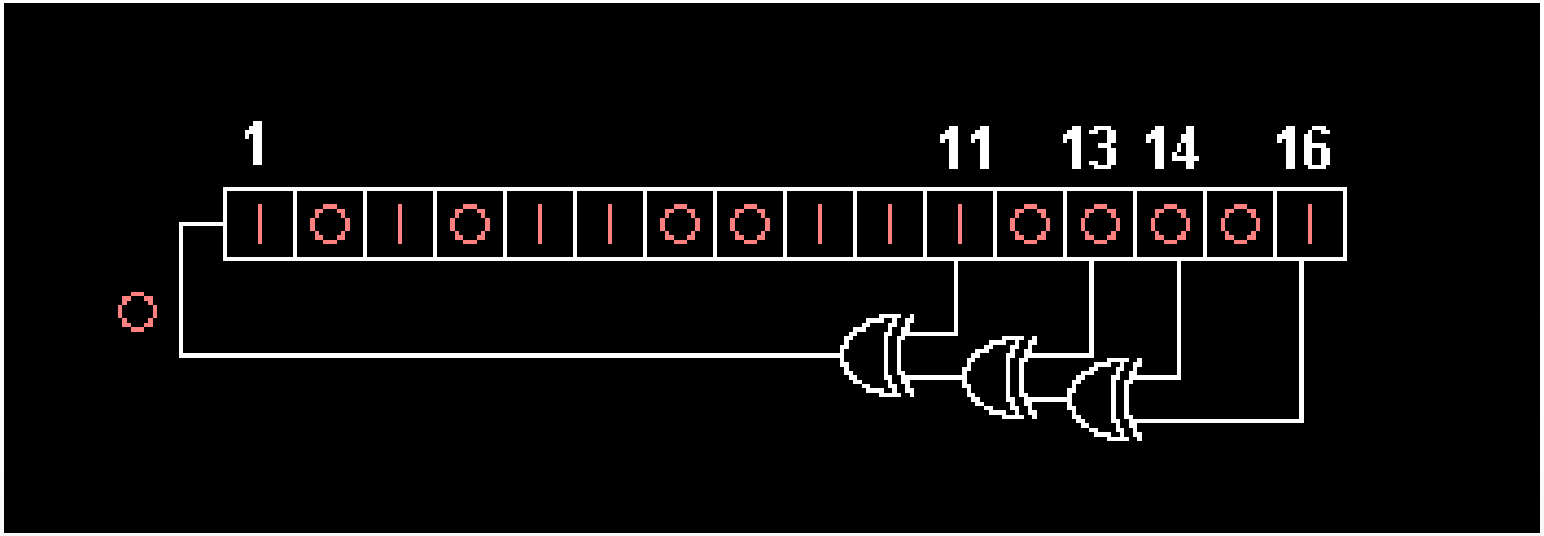
This is what you have to work with, and you have two weeks to prototype the product before the VCs (venture capitalists) from 3i turn up to see if you are viable.

UNIVERSITY OF Southampton
School of Electronics and Computer Science

A concept

- Level-shift the keyboard to 3V3 logic. Power it from USB.
- Stream-encipher the serial stream from the keyboard with a 16-bit LFSR using the CPLD.
- << LONG INSECURE CABLE>>
- Decrypt in the AVR which also acts as a USB HID device.

LFSR



Generates a pseudo-random bit stream.

And running:
http://upload.wikimedia.org/wikipedia/commons/7/7f/LFSR-F4.GIF

Team working

- The main learning outcome is effective group working. Technical skills are secondary

- *Division of labour has caused a greater increase in production than any other factor. This diversification is greatest for nations with more industry and improvement, and is responsible for "universal opulence" in those countries.*

  Adam Smith, *An Inquiry into the Nature and Causes of the Wealth of Nations*

- There is plenty to do; this is a very difficult task. Don't sit and watch each other! You don't all need to understand everything, but it's best if at least two of you cover each technical issue.

Initial setup

UNIVERSITY OF Southampton
School of Electronics and Computer Science

- Decide who is doing what. Leadership? Management style? PERT and Gantt? Play to individual strengths.
- Communication?
- Decide where you are going to work; where you'll keep the kit.
- Decide how to record work and progress. Logbooks? Wiki? CMS?
- How will you retain code and test cases? SVN? GIT?
- How will you write the report?

Key initial tasks

- Production line:
  - Build all four Il Bagattos.
  - Test the Il Bagattos *carefully*, as you did the Il Mateo.
  - Learn to program the Il Bagatto.
- Build the PS/2 cable
  - Analyse the keyboard on the web, and with oscilloscopes etc. Understand exactly what it does. Will it work reliably at 3V3?

More tasks

- Get a USB HID working on the AVR
- Think *hard* about the wire protocol between the CPLD and AVR. Can the CPLD generate it? Can the AVR read it and also run USB?
- How will you build an engineered prototype?
- Get the Il Bagatto to listen to the keyboard. Have the light come on when you press <enter> and go out when you release the key.

Support

- There are some further details at https://secure.ecs.soton.ac.uk/notes/ellabs/1/d1/notes.html
- We're in the lab. Think *first*, look on the web, ask each other, but use us too.
- The web notes will improve as the fortnight progresses.
- There will be some additional seminars on interesting topics.

Engineering

- Getting things to work is *hard*.
- Don’t take big steps.
- Understand and test each subsystem before you compose them.
- Horrid things can happen along buses.

Assessment

- A lab check-sheet will record progress, including a basic USB HID implementation and the Il Bagatto to keyboard interface: *Get the Il Bagatto to listen to the keyboard. Have the light come on when you press <enter> and go out when you release the key*.
- A single 2000 word report sufficient to reimplement your prototype is due in at 17:00 on the last Friday.
- A show-and tell will take place on the last Friday afternoon.

The Motto
Strenuis Ardua Cedunt
may be translated:
The Heights yield to Endeavour.