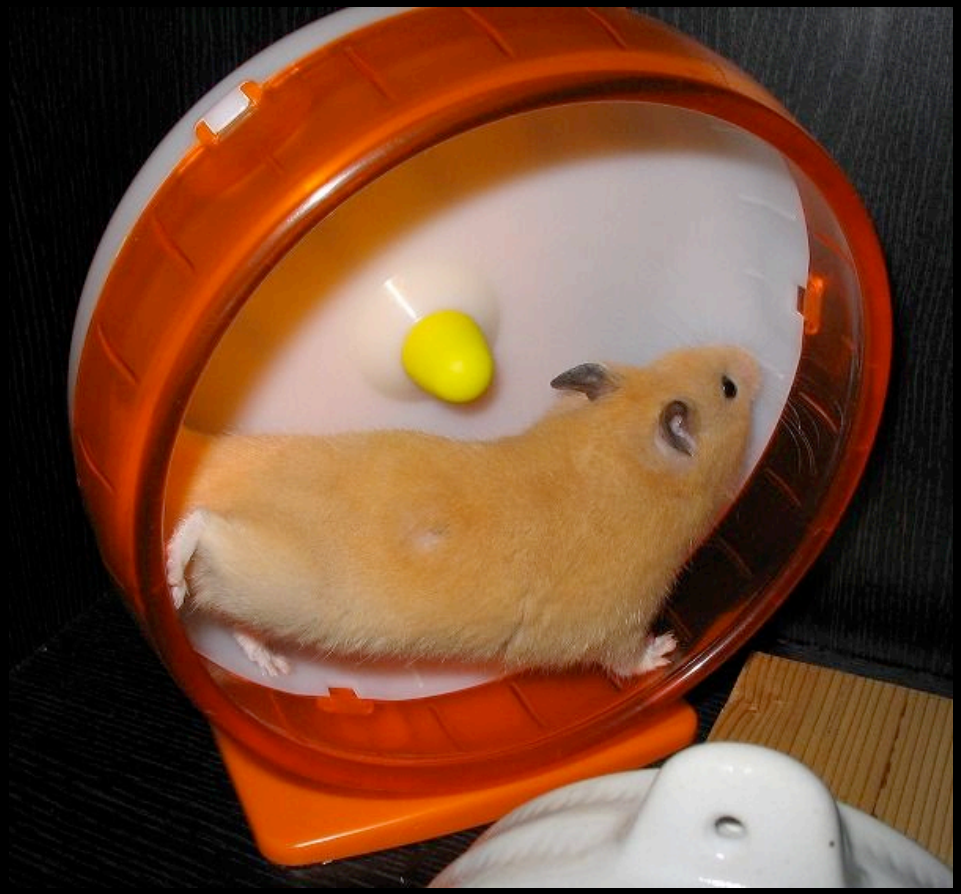
Cars, etc.

SIGMil

Things to be mentioned include..

Some mechanical topics:

.. workings of engines

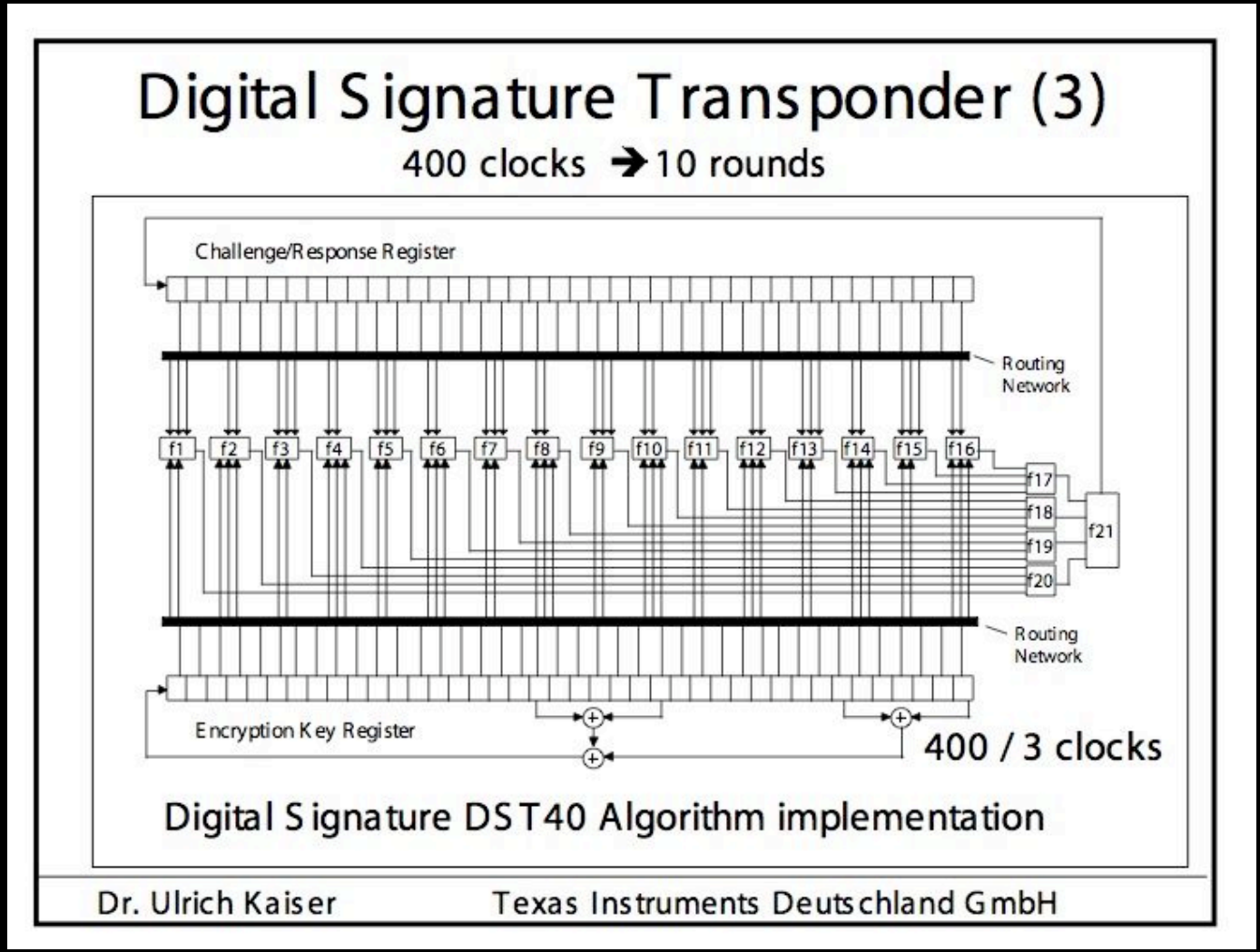


.. how ppl make cars better

.. how break-ins happen

Some electronics topics:

.. keys and security

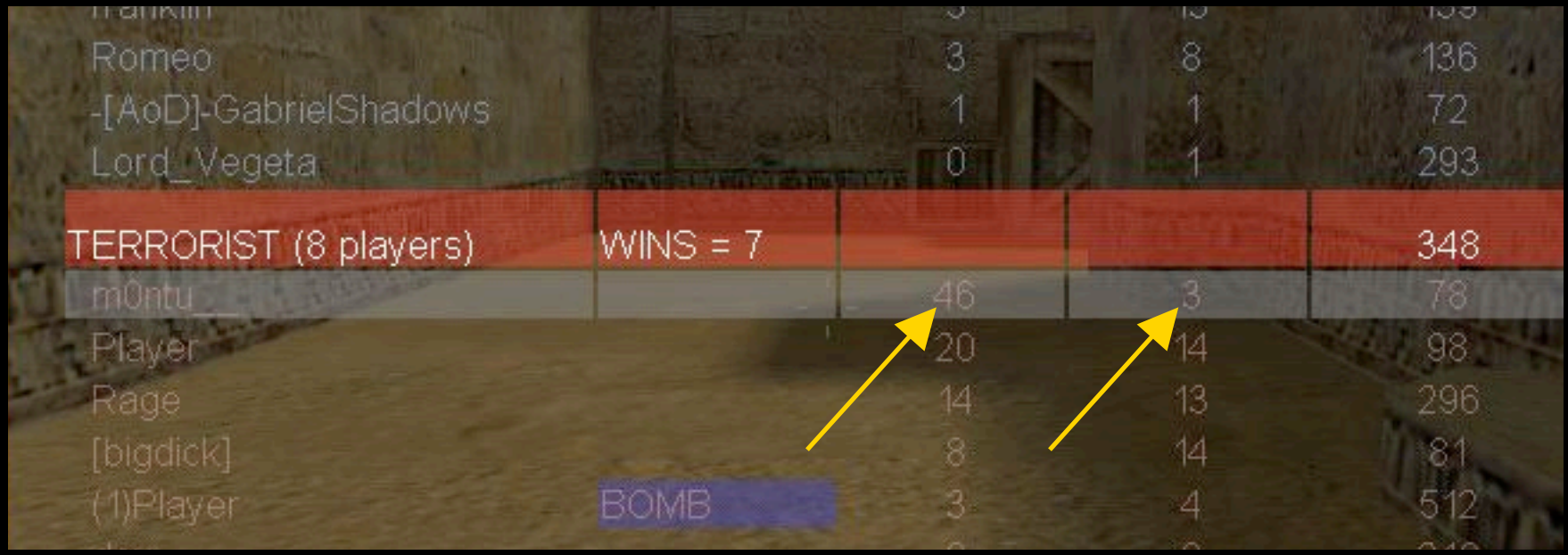


.. police

- http://tinyurl.com/2ykh2a

..computers and networks

Ok. Lets pwn some nubs



Mechanical..

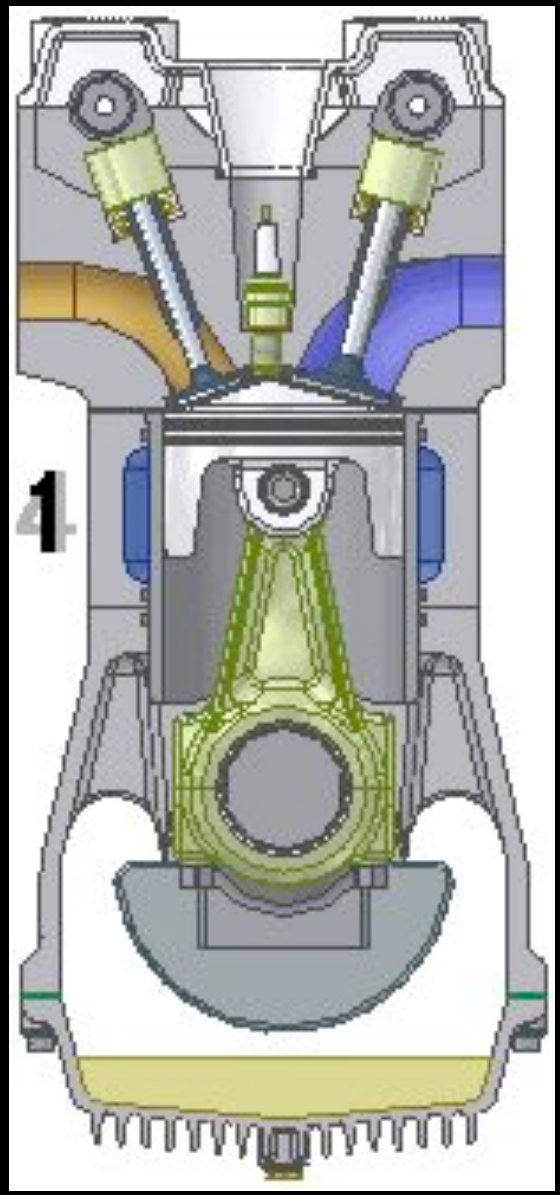
Things you should know

- Air + Gas = Acceleration
  - Spark required for gas engine combustion
  - No spark for diesel engines (self-sustaining)
- Air/gas ratio ~ 14
  - Lean means more air
  - Rich means more gas
- ‘Gas pedal’ is actually ‘air pedal’
- Efficiency around 20%
- Higher octane fuel is LESS combustive

Mechanical..

Engine basics

- 4-stroke engine (2 rotations):
  - Air/gas into cylinder (mixed well beforehand)
  - Compression
  - Explosion/Expansion (powers crank)
  - Exhaust



Wikipedia: four-stroke cycle

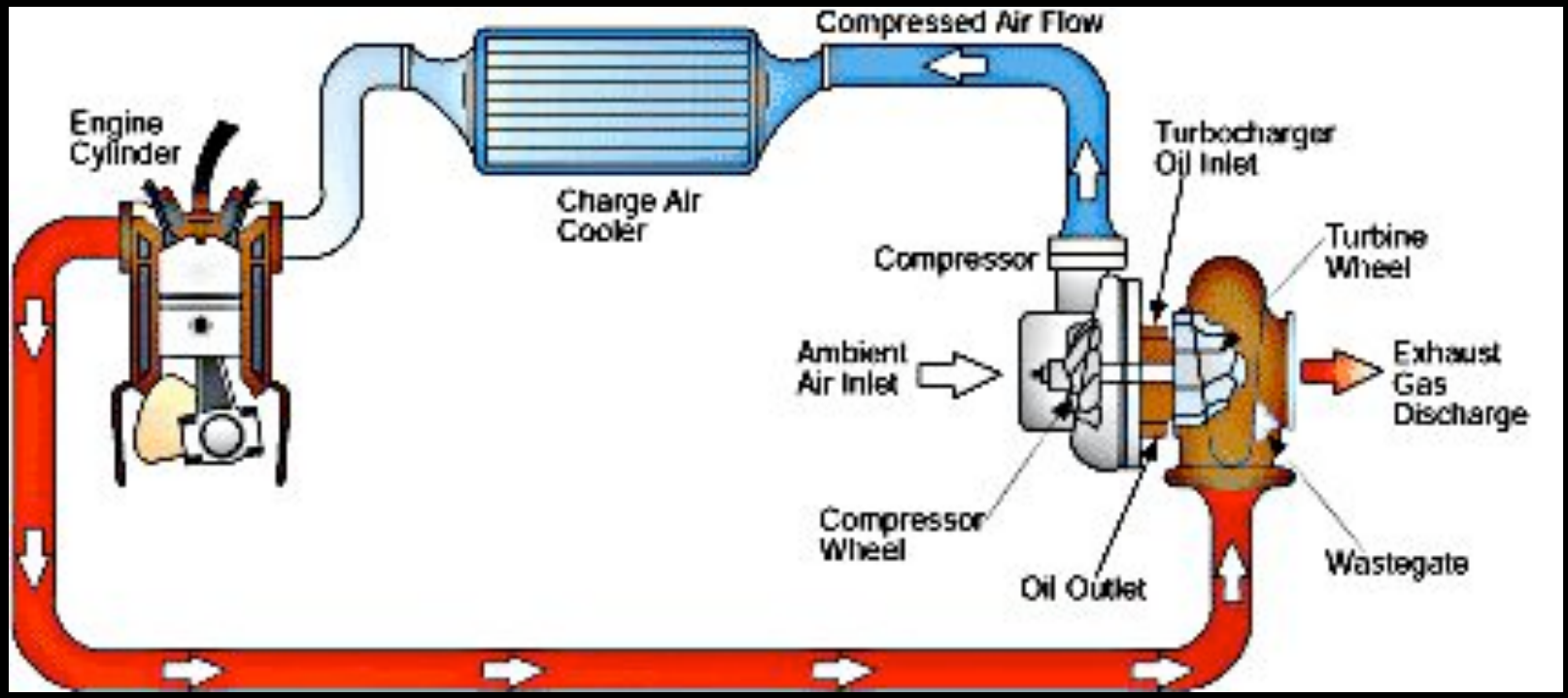
Mechanical..

Fast cars

- More air + More gas = More acceleration
- Ways of achieving this:
  - Different fuels
  - Bigger engine
  - **Air compression**
  - **More ‘revs’**
  - Tuning

Mechanical..

Air compression



- Ambient air pressure around 14.7 PSI
- Crazy turbo can increase pressure by 30+ PSI
  - Means you have 3x air, 3x gas and almost 3x power

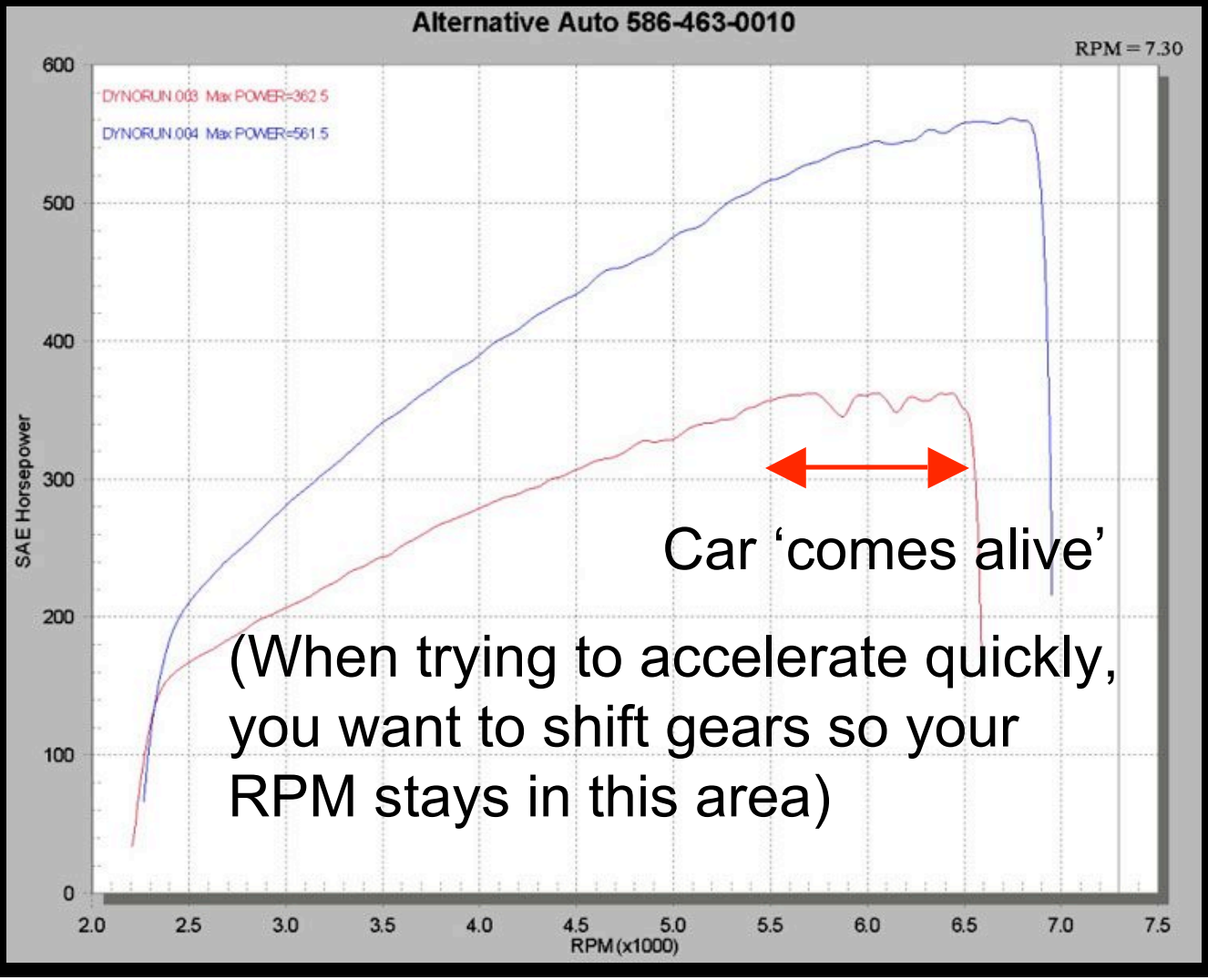
Mechanical..

Air compression

2 liters, 500+ horsepower with 15 PSI boost

Mechanical..

Higher revs



Mechanical..

Security

- Many ways people get into a locked car
  - Jimmy
  - Jiggle key
  - Wedge
  - Tennis ball ?
  - Honda override
  - More later..
- Starting without keys

Mechanical..

Jimmy/Slim Jim

- Make one with a coat hanger or buy at store/online
  - Slide down door next to window and lift up locking mechanism
  - Takes 5 seconds with practice
    - Watch a tow truck driver if you get the chance..

Mechanical..

Others

- Jiggle key will work on older vehicles that the Jimmy can’t get
- Make a wedge out of wood
  - Jam into door until it is bent open a little, stick wire down and pull top of lock up
  - Very Hi-tech

Mechanical..

Tennis Ball

- ‘Famous’ video..
  - http://tinyurl.com/ytol27
  - Maybe fake, but..
- This works on older cars when using high air pressure (compressor)
  - Lifts locking mechanism up if there’s enough force

Mechanical..

Honda Override

- Hondas have a ‘secret sequence’ linked to the car’s VIN number
- Allows a combination of presses and pulls of the hand break to start the car

- Anyone have a Honda? More info about this? Hard to find..

Mechanical..

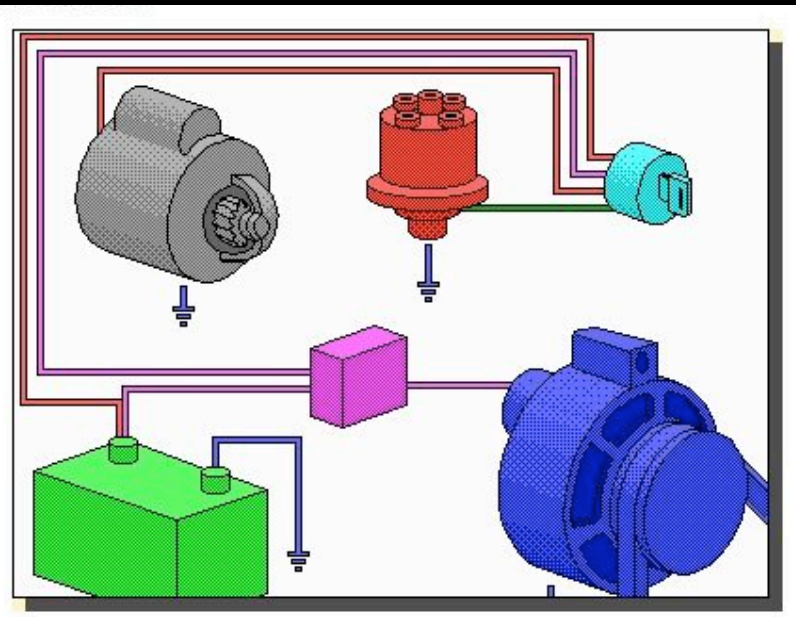
Starting Without Keys..

- For the newest cars, this isn't always so straight forward..
  - Except that many dealers leave a 2nd key in the glove compartment inside the car owner's manual

Mechanical..

Starting Without Keys..

- However.. for many cars:
  - Enter via slimjim/etc
  - Pop hood
  - Put car in neutral/park (manual/auto)
  - Find ignition coil (follow spark plug wires down) and connect positive side to battery
  - Find starter solenoid and touch positive side of battery to its positive (you're looking for the thing pictured at the top-right)



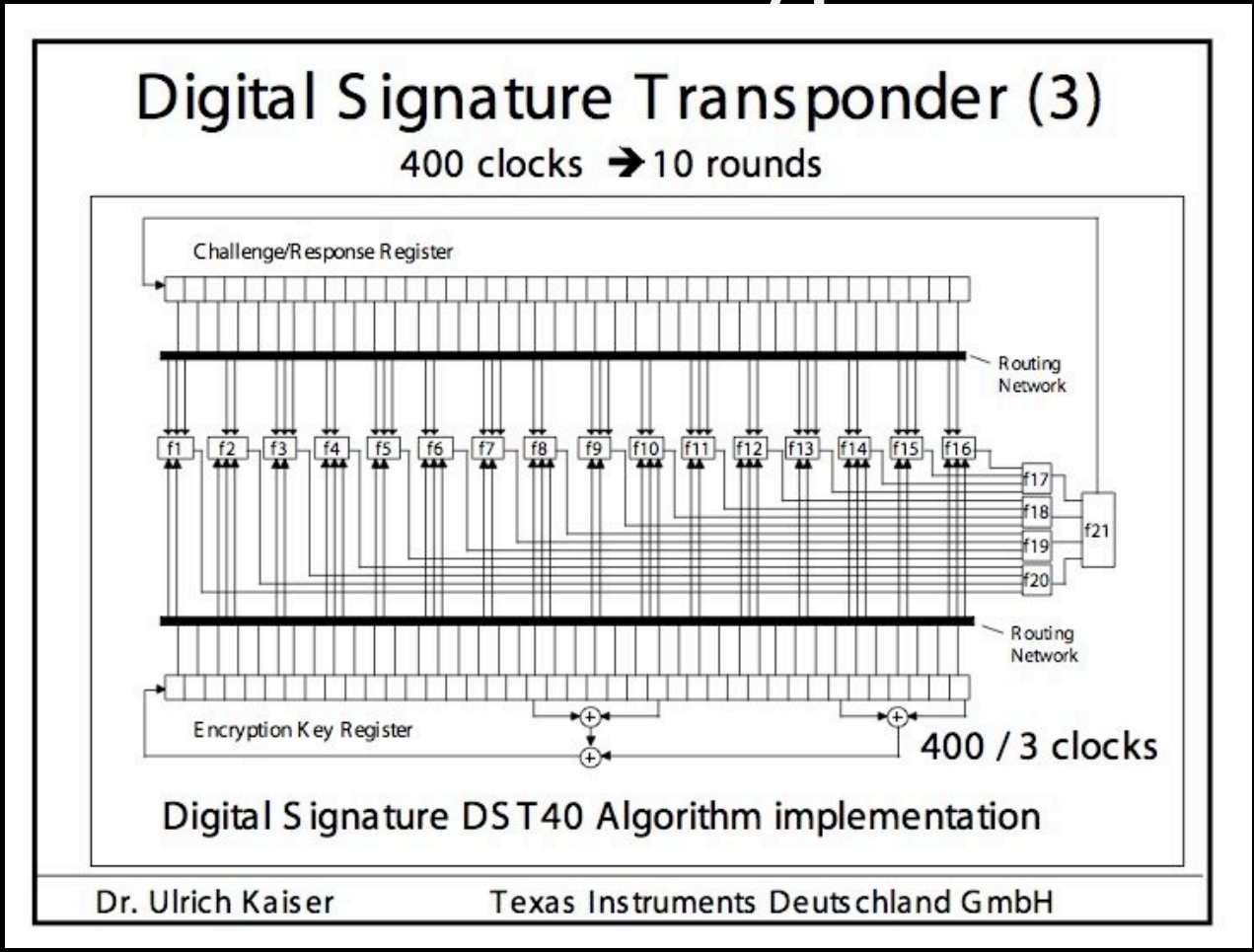
Electronics..

Keys

- All new cars have ‘transponders’ (Digital Signal Transponder system by TI)
- Basically 134 KHz RFID in key that does challenge response when trying to start the car
  - Once an example challenge-response is recorded cracking is possible in 15 min
    - Or a 10 GB database will have 99% chance of successful lookup
    - http://www.renderlab.net/temp/DSTbreak.pdf details

Electronics..

DST Encryption



- 40 bits, Feistel network with some lookup tables

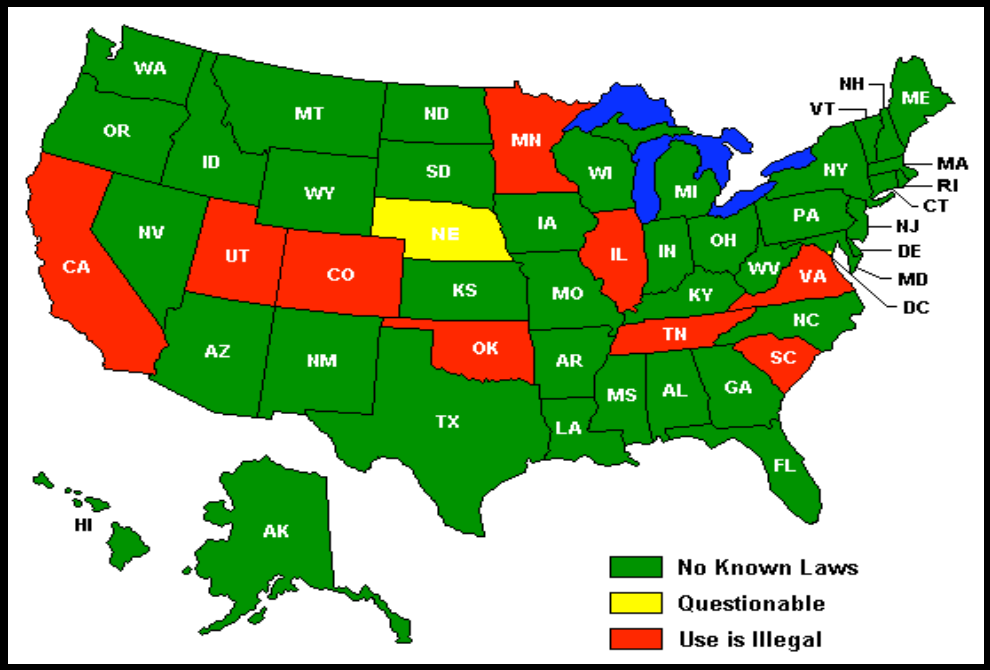
Electronics..

Changing the Traffic Lights

- Ever notice how an emergency vehicle always gets green lights?
- ‘Optical Traffic Signal Pre-emption’
- Basically, a large array of IR emitting-diodes pulsing at a frequency (14.035 or 9.639 Hz)
  - Some require encoded IR strobes
  - Others require RF stuff also
- This is a felony to use unless you’re an on-duty officer

Electronics..

Laser Jammers



- There are very good ones out there for about $350, see sites for good forums and reviews:
  - http://www.radardetector.net
  - http://www.guysoflidar.com

Electronics..

IWIN

- What is this?
  - A subscription-based CDMA network for law enforcement
- So?
  - It has lots and lots of interesting features..

Electronics..

IWIN - Features

“The Premier MDC™ IWIN Client provides IWIN users with the following Windows-based functionality.

* LEADS, SOS and NCIC access
* Car-to-car and workstation-to-car messaging
* In-vehicle printer support
* In-vehicle paging
* In-vehicle mapping/GPS support
* Text-to-voice module
* Barcode/image capture device interface
* Day/night vision
* Terminal Emulation software
* SCA's TalkThru RF
* Future access to SOS driver's photos
* Future integration with accident and citation software
* Future chat capability”

And more, actually..

Electronics..

IWIN - o rly?

- Interesting:
  - All their request forms freely available online
  - Give many technical details
  - Phone/email contacts, etc also online
  - Check it: http://www.state.il.us/iwin/
- Sadly:
  - System being depreciated soon
  - Replacement details not as easy to find

Things to do

- For those with free time:
  - Find Honda Override Info
  - Emergency Vehicle IR Transmitter Research
  - DST Reading/Emulation
    - We can buy RFID stuff if someone has serious interest
  - Slimjim/etc practice on your own car
  - Talking to some IWIN people for research