
"Knock Knock Knock...
Housekeeping"
the ins and outs
of hotel locks

Hotel Rooms are a Sanctuary

At Least, They're Supposed To Be

A Place to Curl Up In Bed And Sleep

D

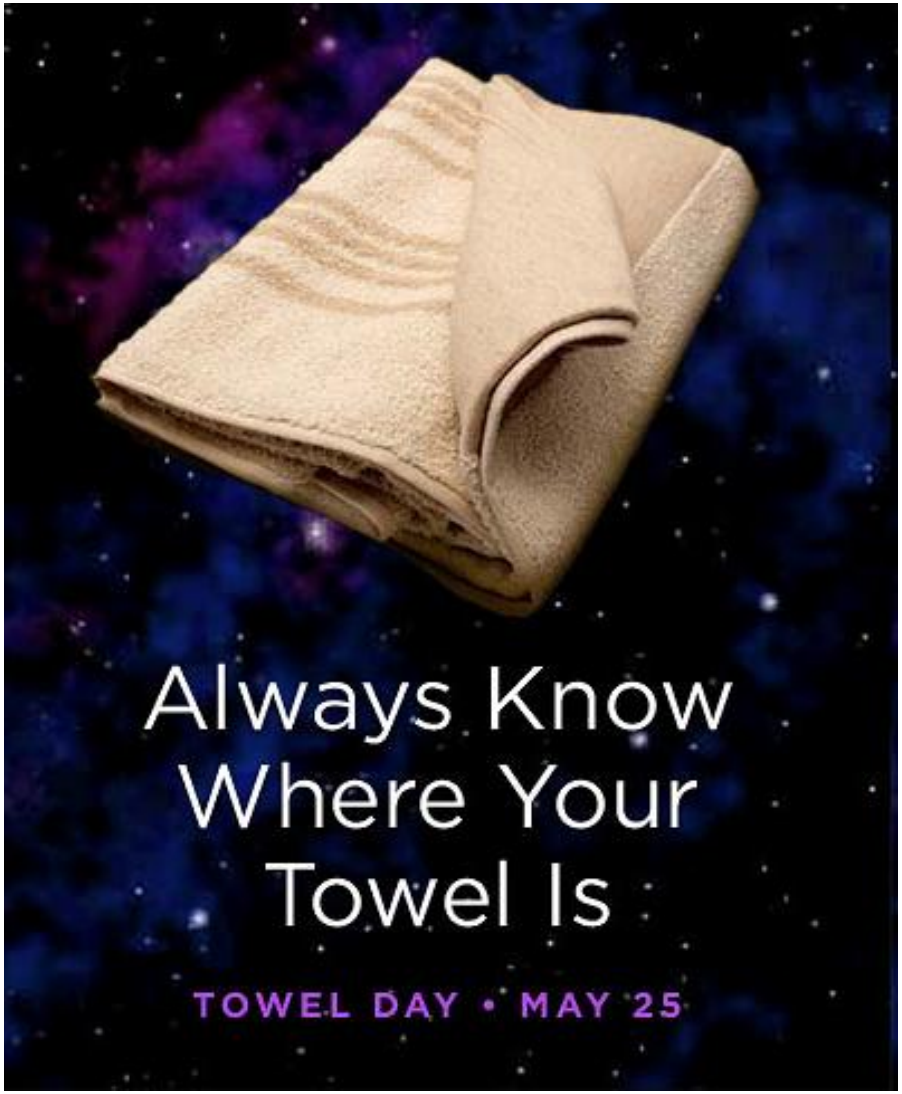
Or Do Other Things

You Don't Want This to Happen to You

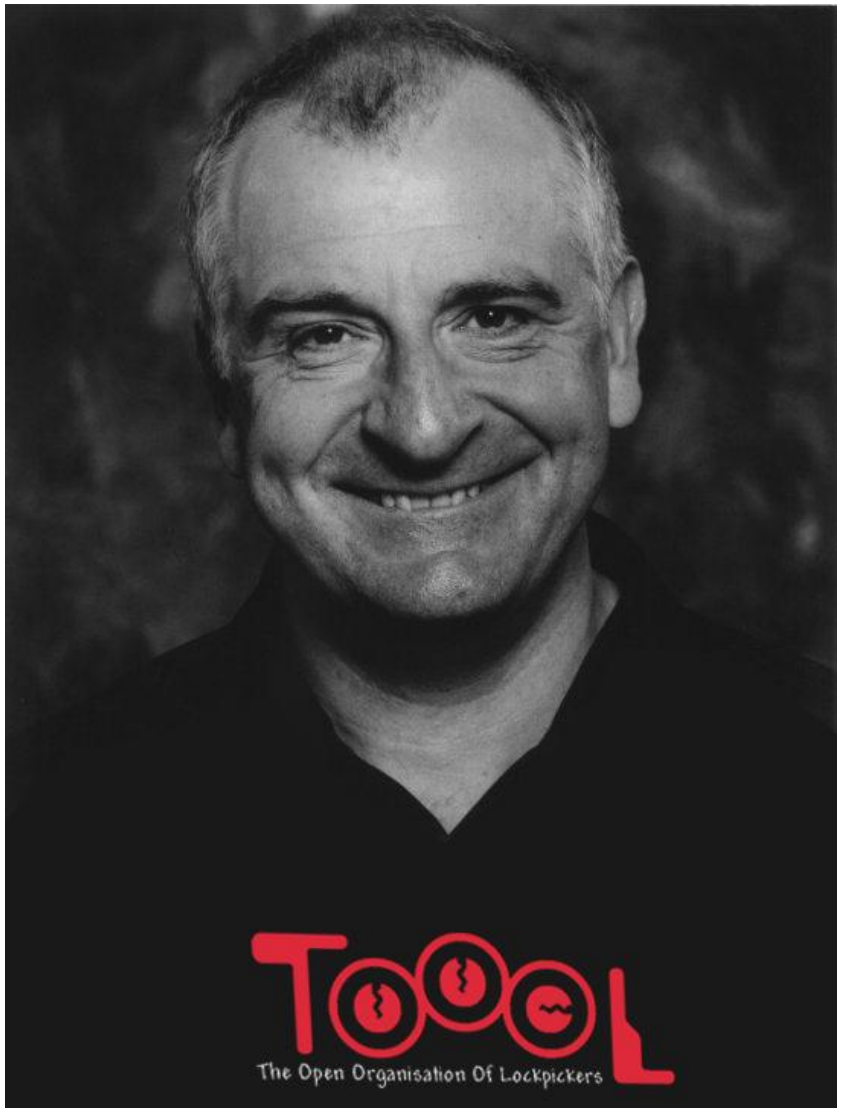
So Let's Talk About Room Doors First

Barry & Han – Under Door Reach Tool

The Solution – Always Know Where Your Towel Is



The Solution – Always Know Where Your Towel Is



Douglas Adams...

now an Honorary TOOOL Mmeber

Some People Want Extra Security

Some People Fail at Extra Security

- Attack with a Reach-Around
- Attack with a Rubber

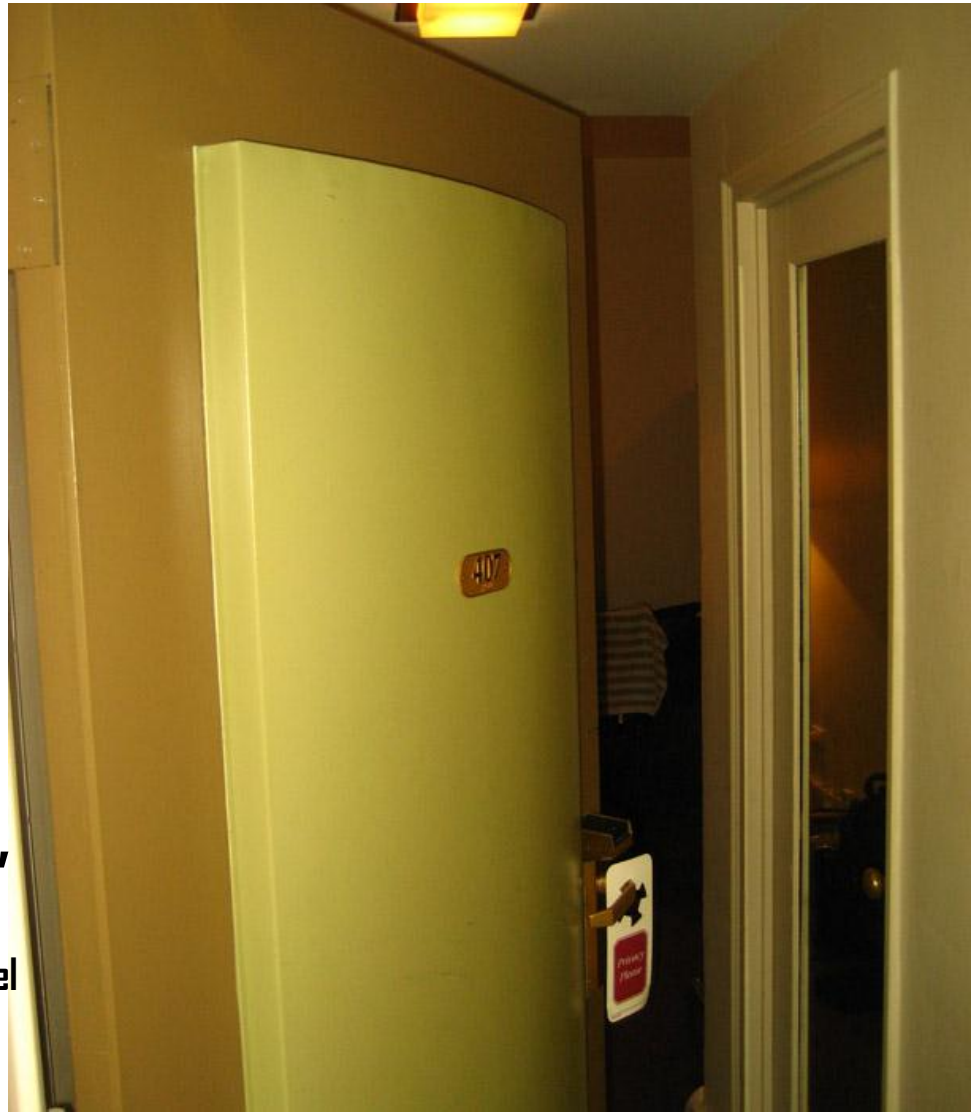
A Different Type of Door Security

D

A Different Type of Fail

- Attack with a Slap Tool
- Attack with a Maid Sign

Harder to do at Hotel Penn...



“Statler Servidoor”

first at Boston Park Plaza Hotel

not on modern hotels, alas

Modern Hotel Doors Often *Do* Have Peepholes

Peepholes are *Supposed* to be for Looking *Out*

Security Consultants Have Other Ideas

One Last Bit of Peephole Fun

One Last Bit of Peephole Fun

Let's Say You Choose to Leave Your Room

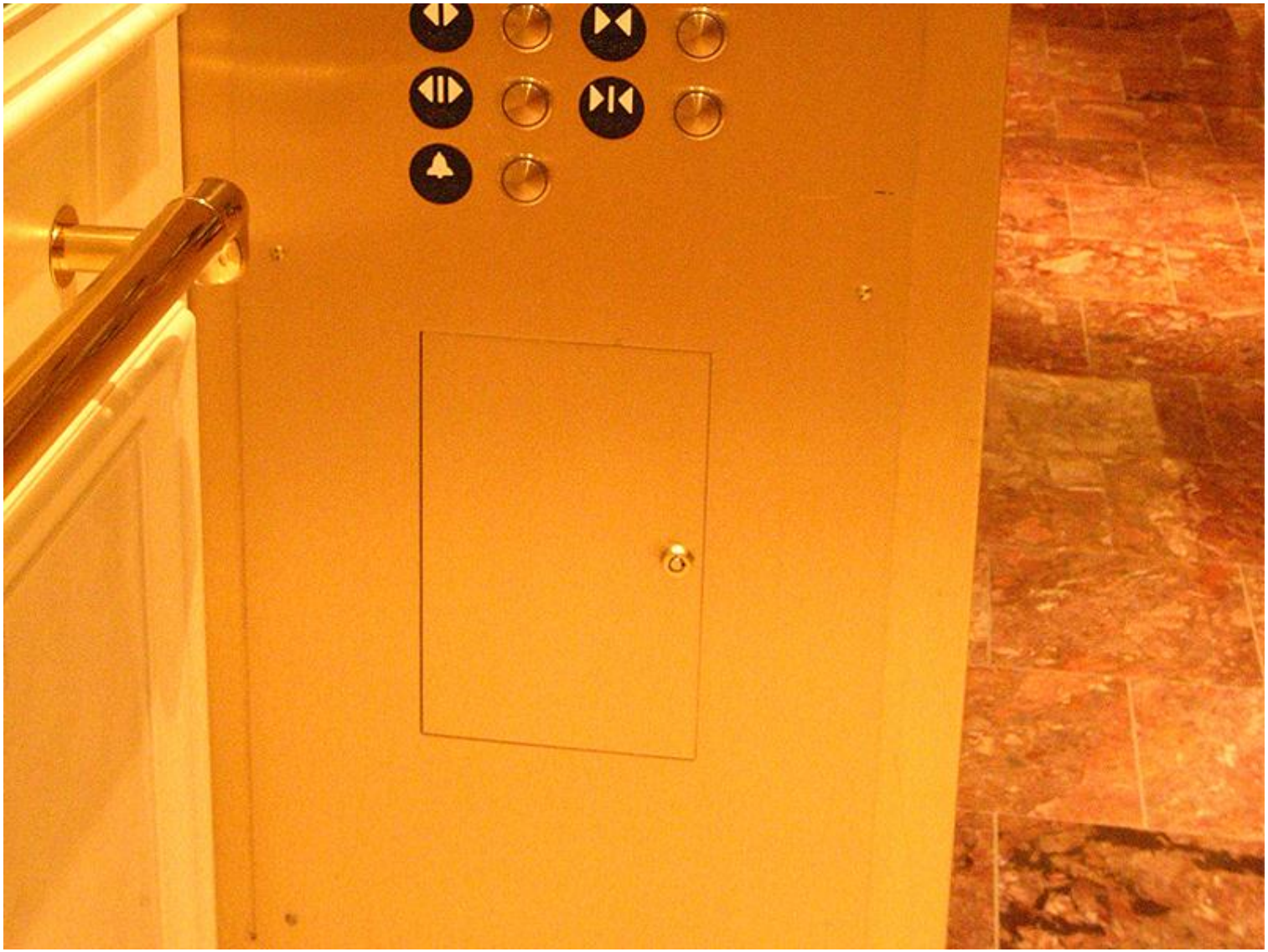
You May Take an Elevator

Time to Stop all the Lies

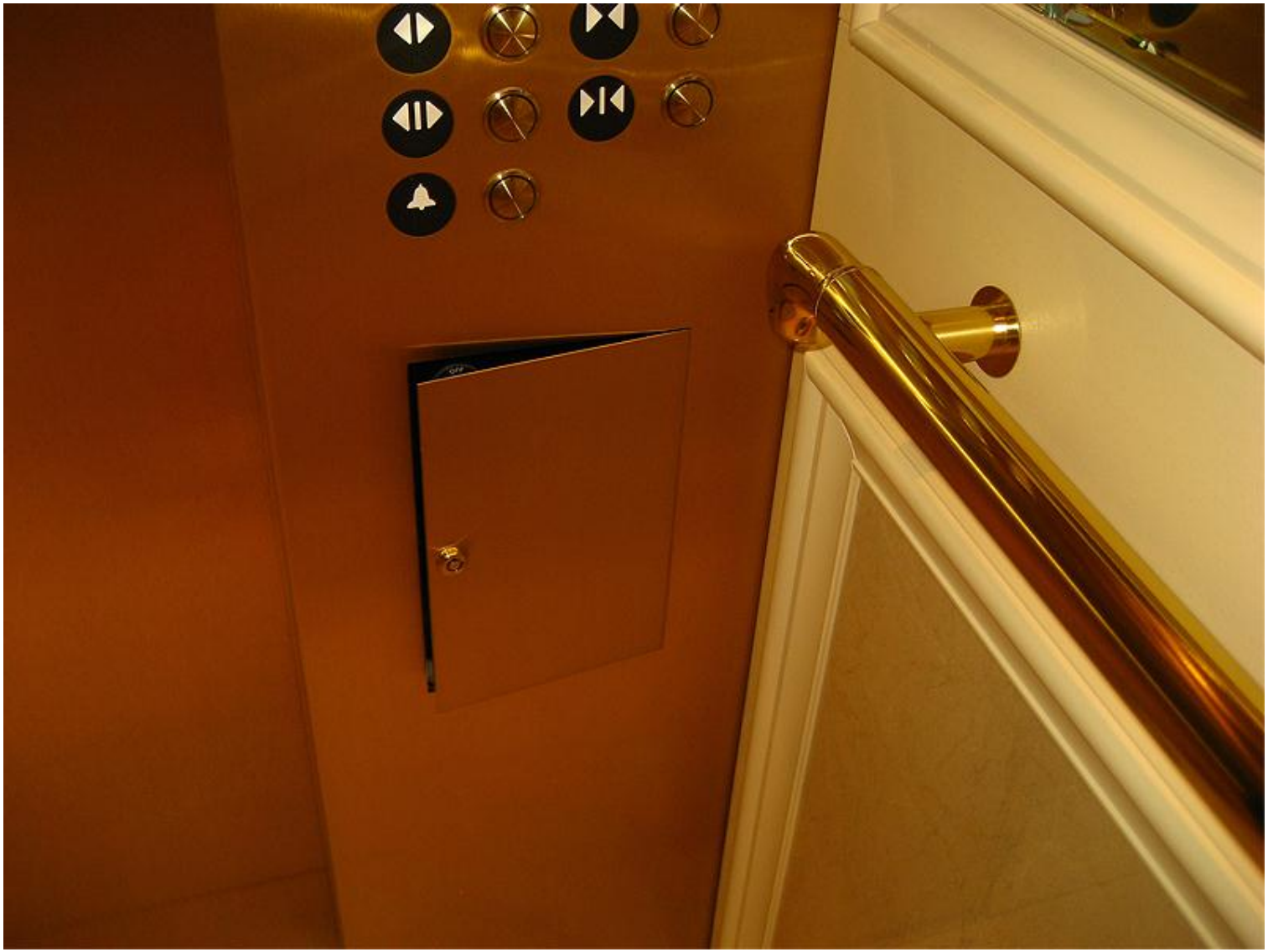
Floor Lockout

Floor Lockout

Access Panels



Who Left That Open?



What Have We Here?

Dios Mío! Es La Migra!

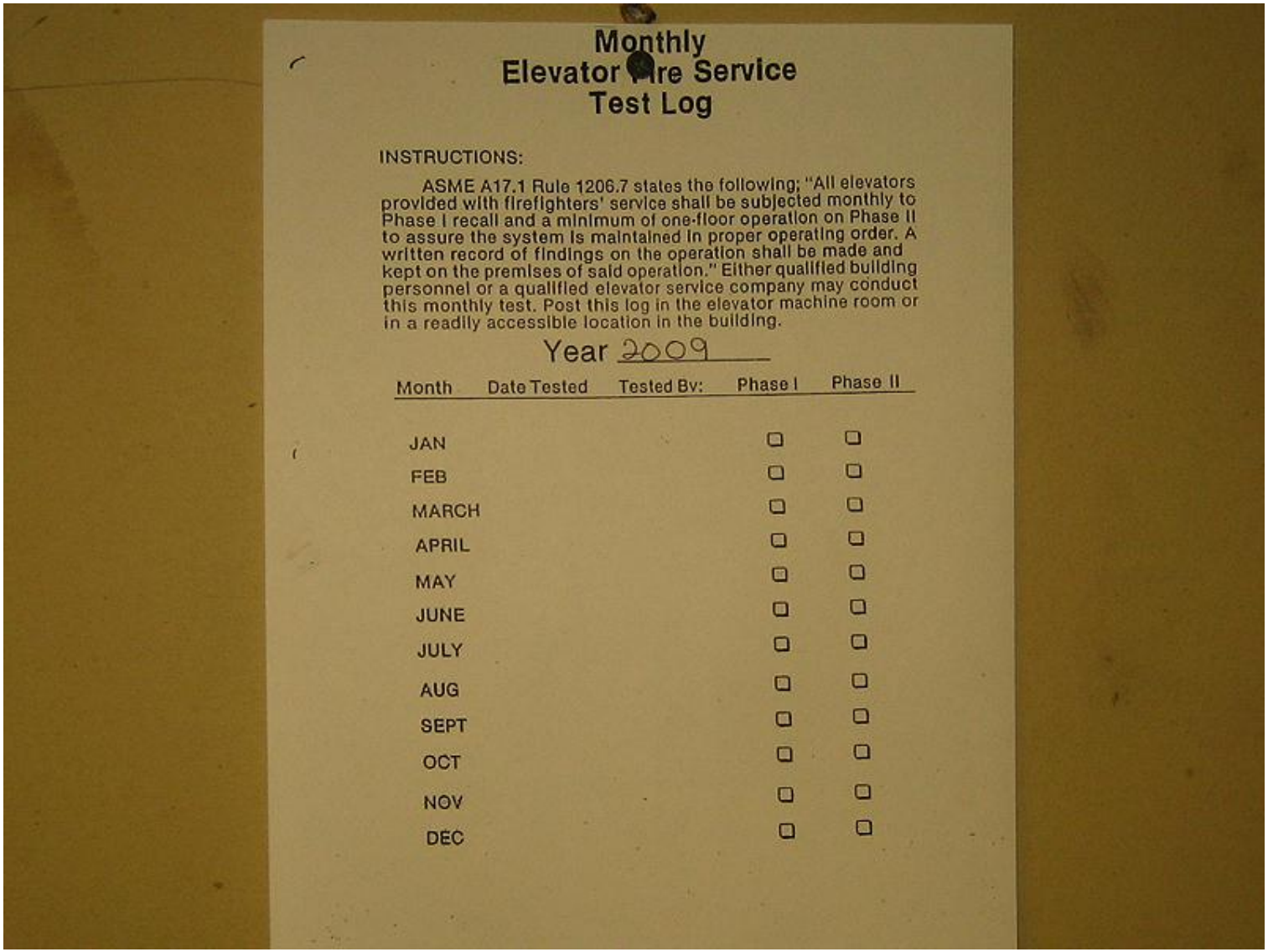
Another Panel

Yet Another Panel

Some Potential for Confusion

Fire Service Mode

Fire Service Mode



Monthly Elevator Fire Service Test Log

INSTRUCTIONS:

ASME A17.1 Rule 1206.7 states the following; "All elevators provided with firefighters' service shall be subjected monthly to Phase I recall and a minimum of one-floor operation on Phase II to assure the system is maintained in proper operating order. A written record of findings on the operation shall be made and kept on the premises of said operation." Either qualified building personnel or a qualified elevator service company may conduct this monthly test. Post this log in the elevator machine room or in a readily accessible location in the building.

Year 2009

Month	Date Tested	Tested By:	Phase I	Phase II
JAN			☐	☐
FEB			☐	☐
MARCH			☐	☐
APRIL			☐	☐
MAY			☐	☐
JUNE			☐	☐
JULY			☐	☐
AUG			☐	☐
SEPT			☐	☐
OCT			☐	☐
NOV			☐	☐
DEC			☐	☐

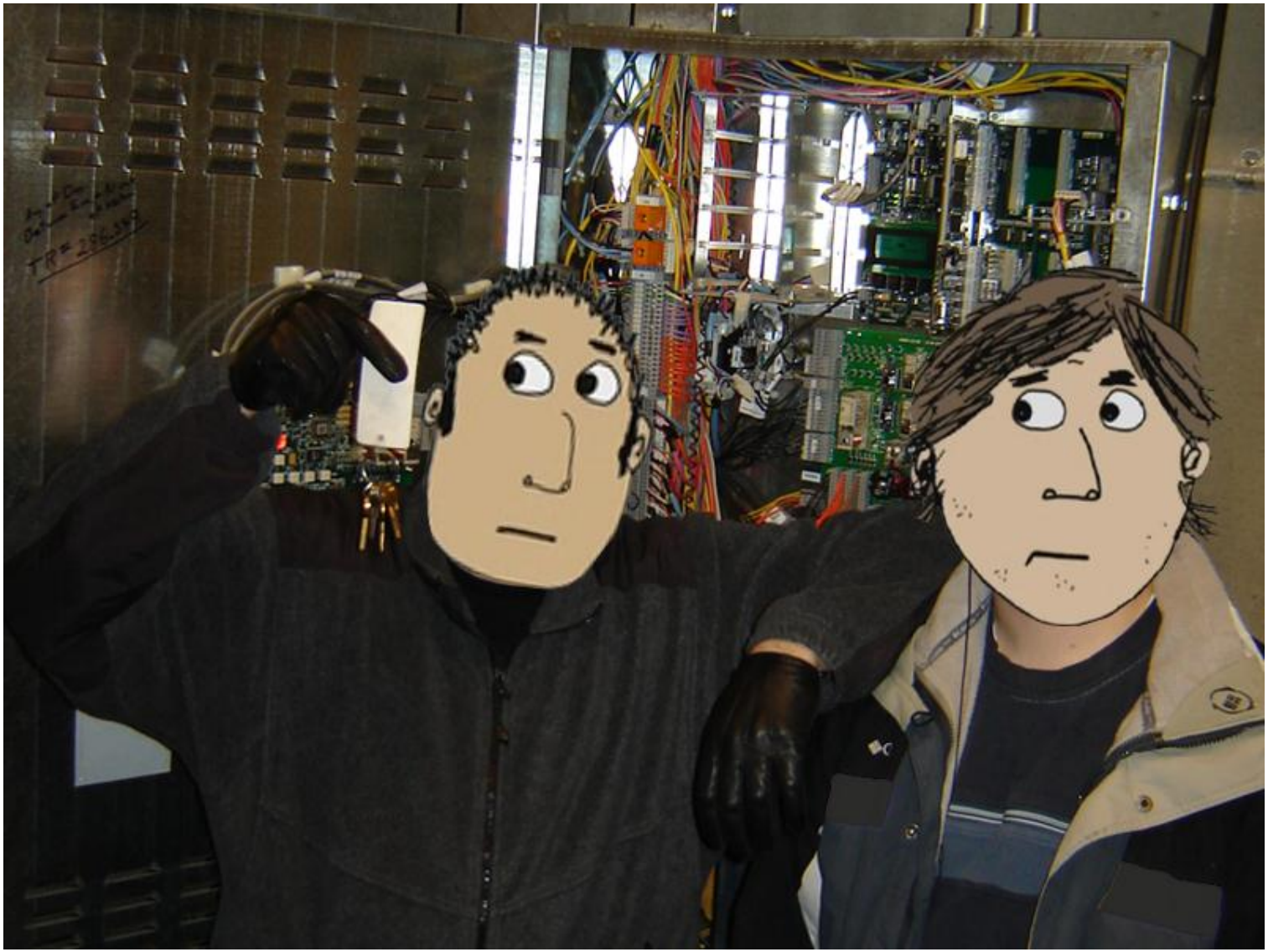
Fire Service Keys

Fire Service Keys

Sometimes Keys Do Strange Things

Hoist Equipment

Keys in a Cabinet... One Opened a Drawer



Heh, Such a Thing as Too Many Keys?

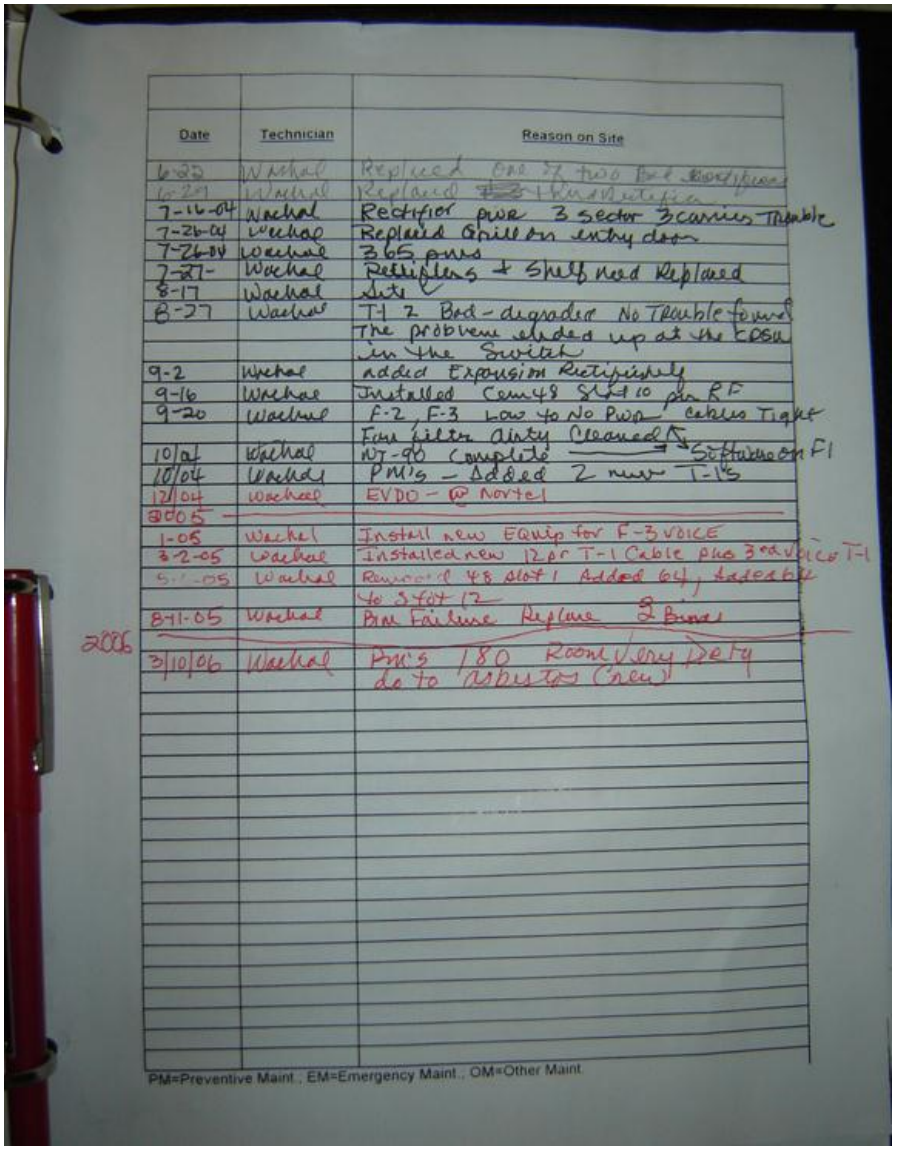
More Keys Means More Access

Lots of Noise Behind a Grill

A Closer Look

Cell Tower Equipment

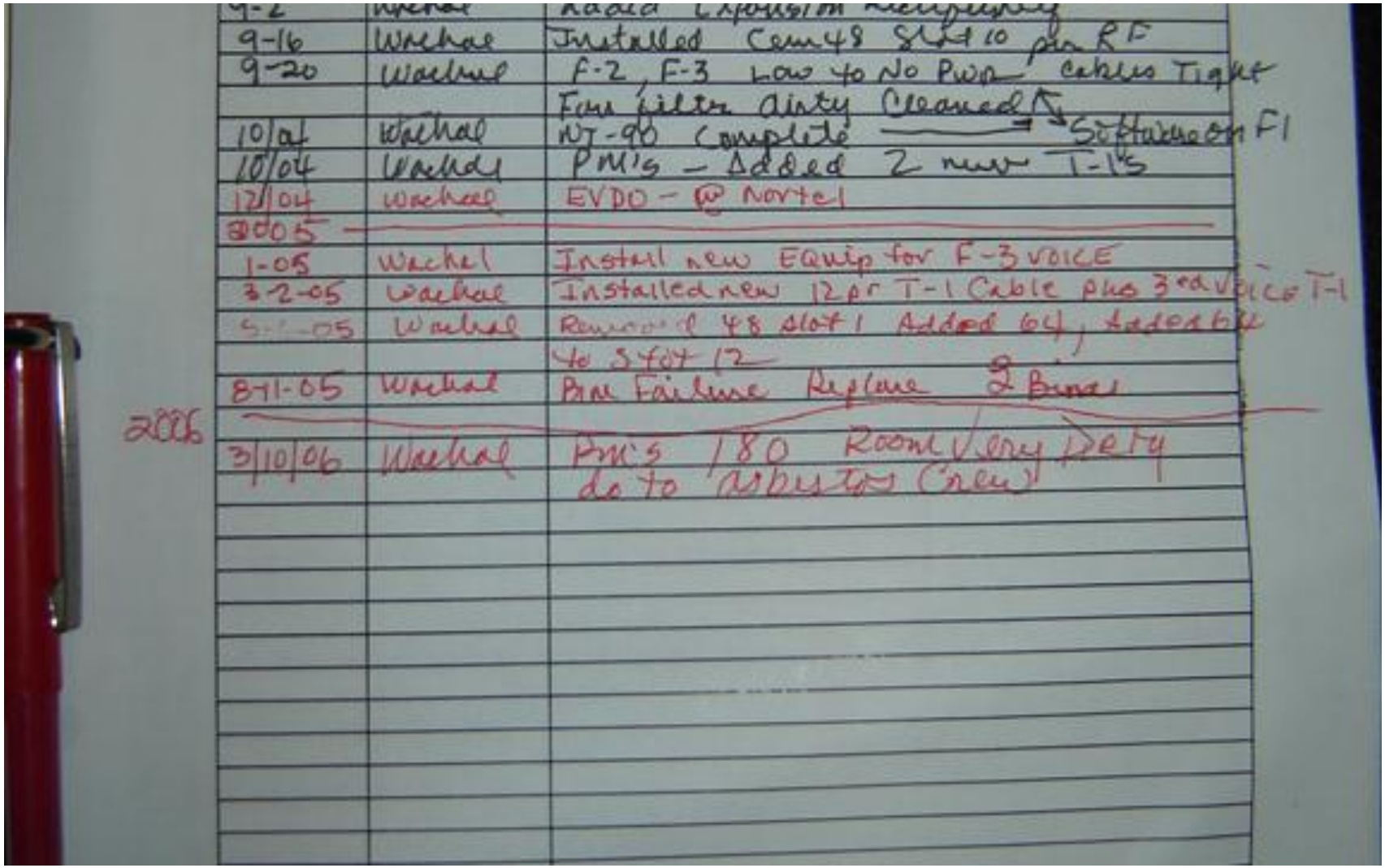
Another Service Log



Date	Technician	Reason on Site
6-22	Wachal	Replaced one 37 two Bad Rectifiers
6-29	Wachal	Replaced ~~3~~ 2 Rectifiers
7-16-04	Wachal	Rectifier pwr 3 sector 3 carrier Trouble
7-26-04	Wachal	Replaced Grill on entry door
7-26-04	Wachal	365 pwr
7-27-	Wachal	Rectifiers + Shelf need Replaced
8-17	Wachal	Site
8-27	Wachal	T-1 2 Bad - degraded No Trouble found The problem ended up at the BSC in the Switch
9-2	Wachal	added Expansion Rectifiers
9-16	Wachal	Installed Cem48 SLOT 10 plus RF
9-20	Wachal	F-2, F-3 Low to No Pwr Cables Tight Fan filter dirty Cleaned → Software on F1
10/01	Wachal	NT-90 Complete
10/04	Wachal	PM's - Added 2 new T-1's
12/04	Wachael	EVDO - @ Nortel
2005		
1-05	Wachal	Install new EQuip for F-3 VOICE
3-2-05	Wachal	Installed new 12 pr T-1 Cable plus 3rd VOICE T-1
5-?-05	Wachal	Removed 48 slot 1 Added 64, added BIC to SLOT 17
8-11-05	Wachal	BIM Failure Replace 2 Bimes
2006		
3/10/06	Wachal	PM's 180 Room Very Dirty due to Asbestos Crew

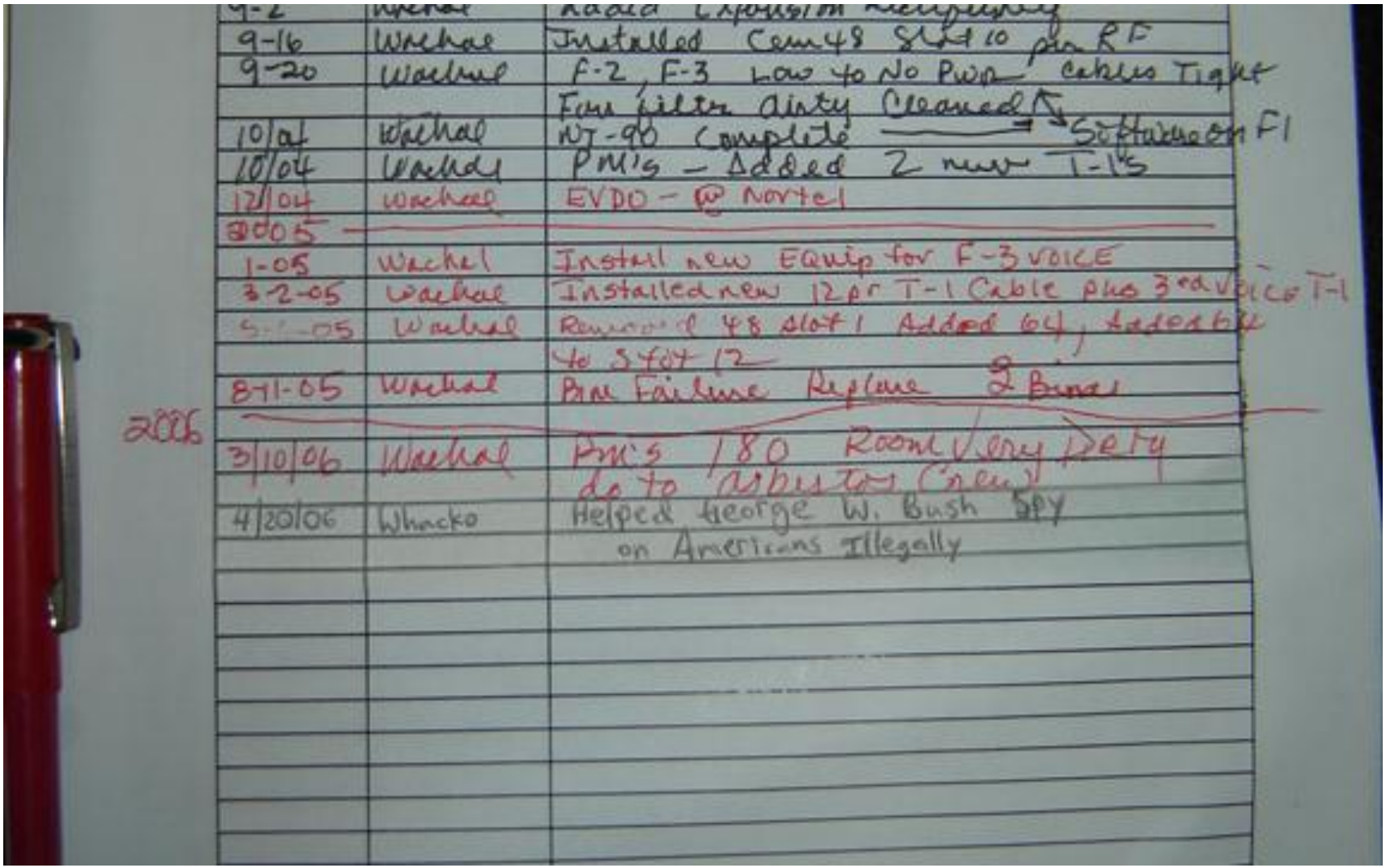
PM=Preventive Maint., EM=Emergency Maint., OM=Other Maint.

Another Service Log



9-16	Wachal	Installed Cem48 Slot 10 plus RF
9-20	Wachal	F-2, F-3 Low to No PWR Cables Tight Fans filter dirty Cleaned → Software on F1
10/04	Wachal	NT-90 Complete
10/04	Wachal	PM's - Added 2 new T-1's
12/04	Wachal	EVDO - @ Nortel
2005		
1-05	Wachal	Install new Equip for F-3 VOICE
3-2-05	Wachal	Installed new 12pr T-1 Cable plus 3rd VOICE T-1
5-[illegible]-05	Wachal	Removed 48 slot 1 Added 64, [illegible] to 3 for 12
8-1-05	Wachal	Fan Failure Replace 2 Fans
2006		
3/10/06	Wachal	PM's 180 Room Very Dirty due to Asbestos Crew

Another Service Log



9-16	Wachal	Installed Cem48 Slot 10 plus RF
9-20	Wachal	F-2, F-3 Low to No Pwr Cables Tight Fans filter dirty Cleaned → Software on F1
10/04	Wachal	NT-90 Complete
10/04	Wachal	PM's - Added 2 new T-1's
12/04	Wachal	EVDO - @ Nortel
2005		
1-05	Wachal	Install new Equip for F-3 VOICE
3-2-05	Wachal	Installed new 12pr T-1 Cable plus 3rd VOICE T-1
5-[illegible]-05	Wachal	Removed 48 slot 1 Added 64, [illegible] to Slot 12
8-1-05	Wachal	Fan Failure Replace 2 Fans
2006		
3/10/06	Wachal	PM's 180 Room Very Dirty due to Asbestos Crew
4/20/06	Whacko	Helped George W. Bush Spy on Americans Illegally

Let's Get Back To The Room

Keycard Access

Disable the Card Reader

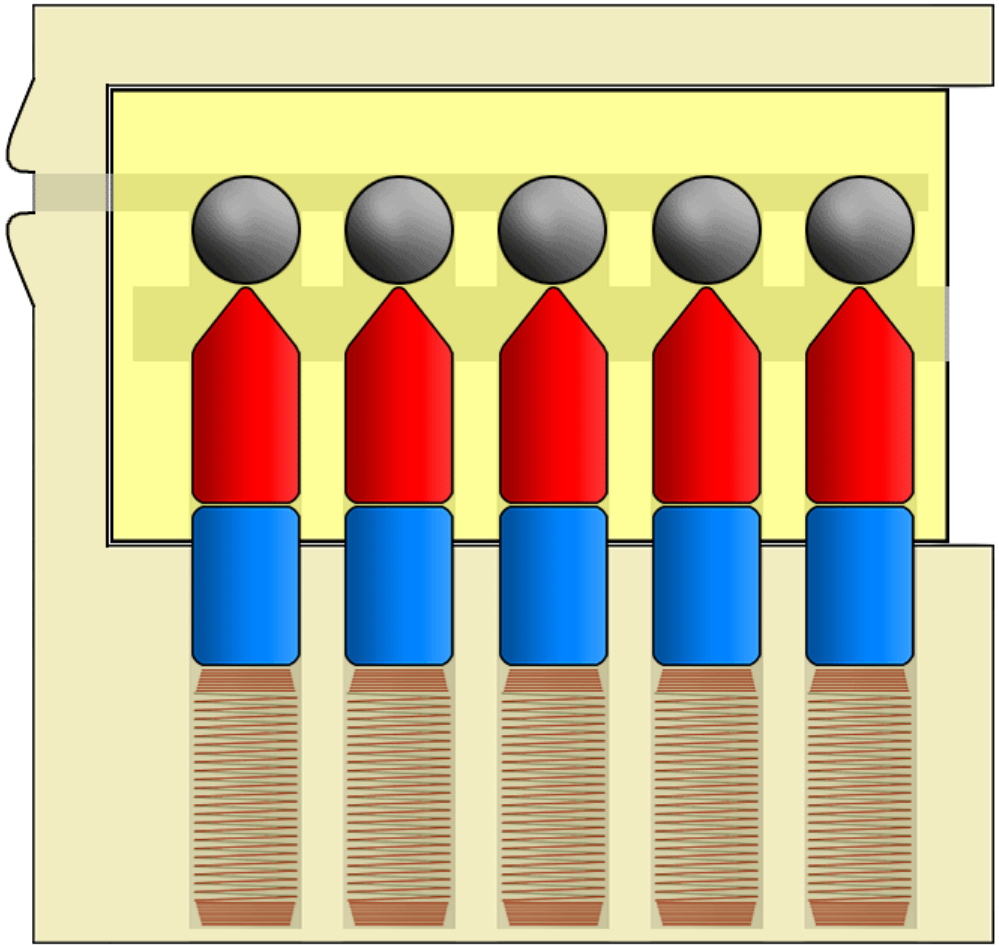
We'll Revisit This Later, Too

BTW... Does This Math Add Up?

We Don't Think So

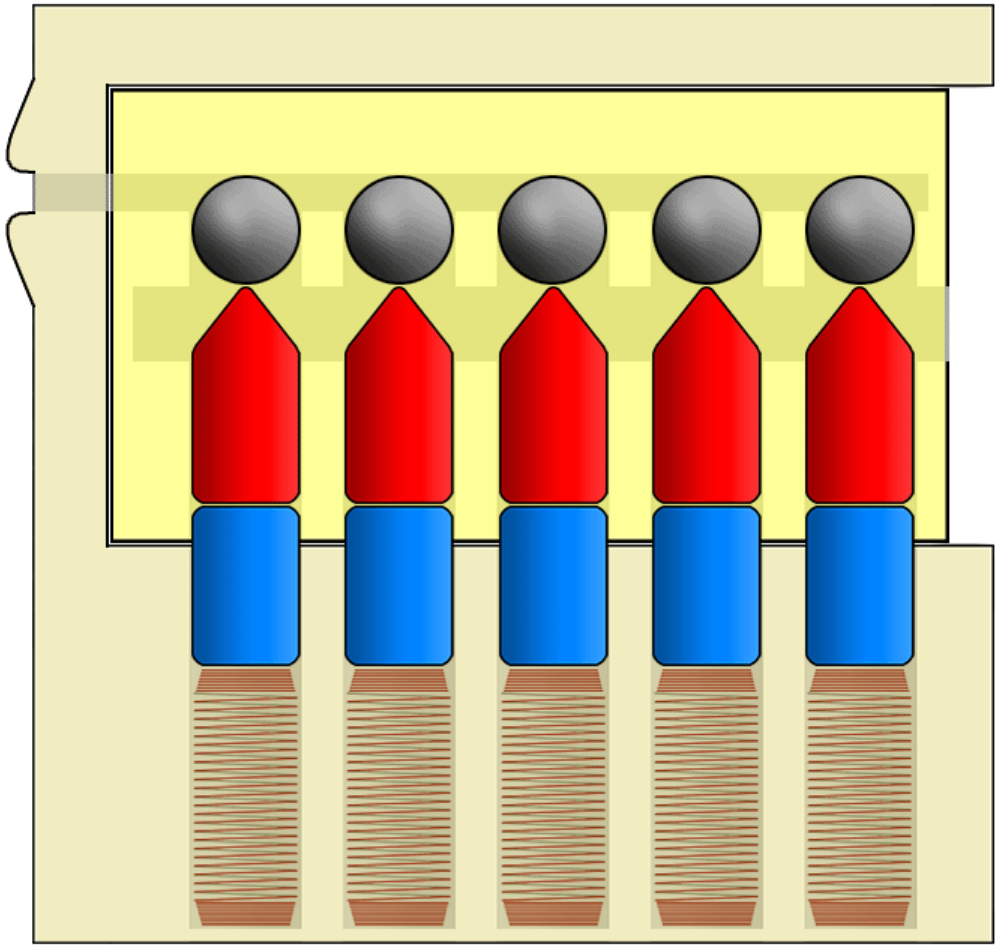
Pin Matrix Room Keys

Pin Matrix Lock

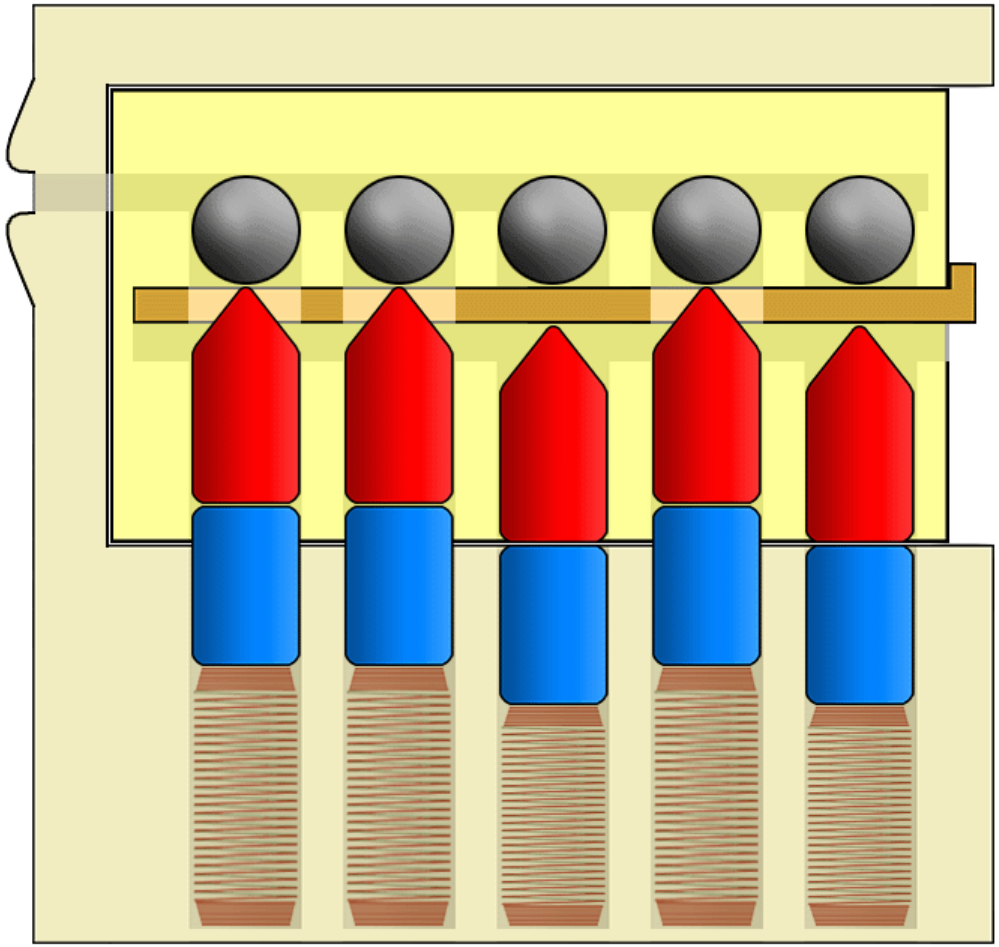


Programmed With a Control Card

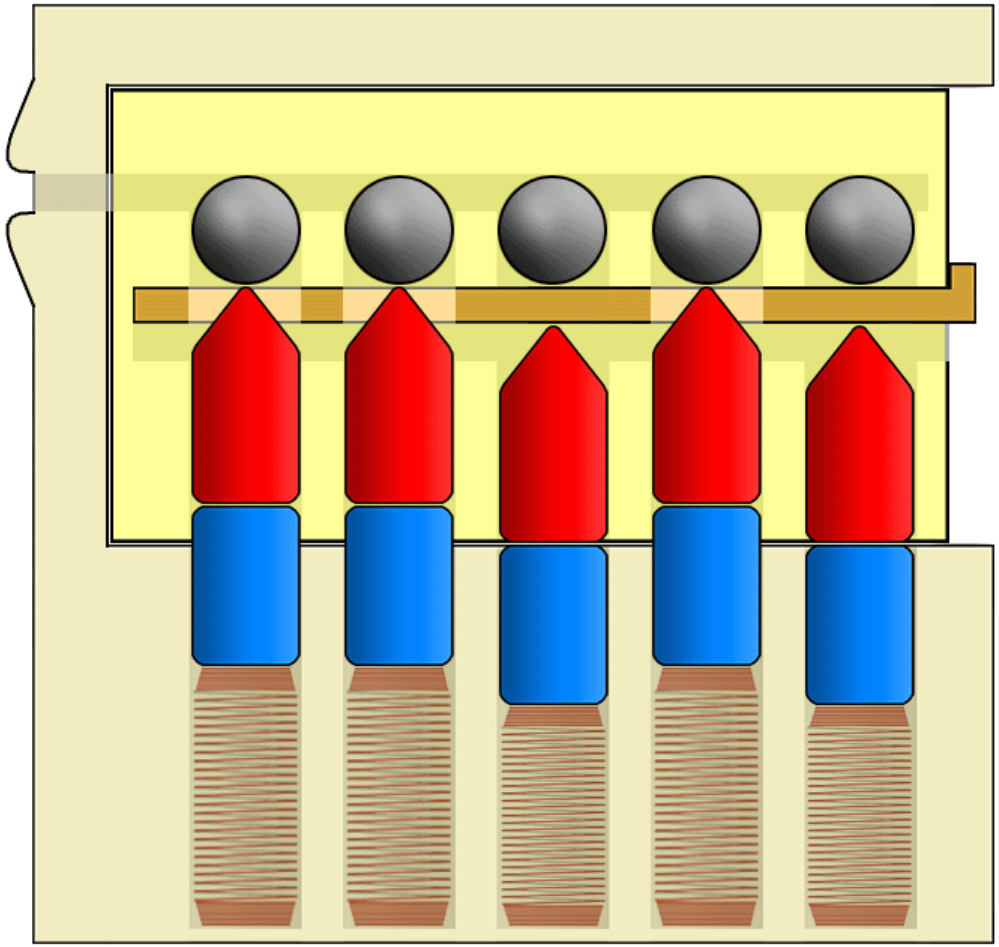
Control Card “A” Installed



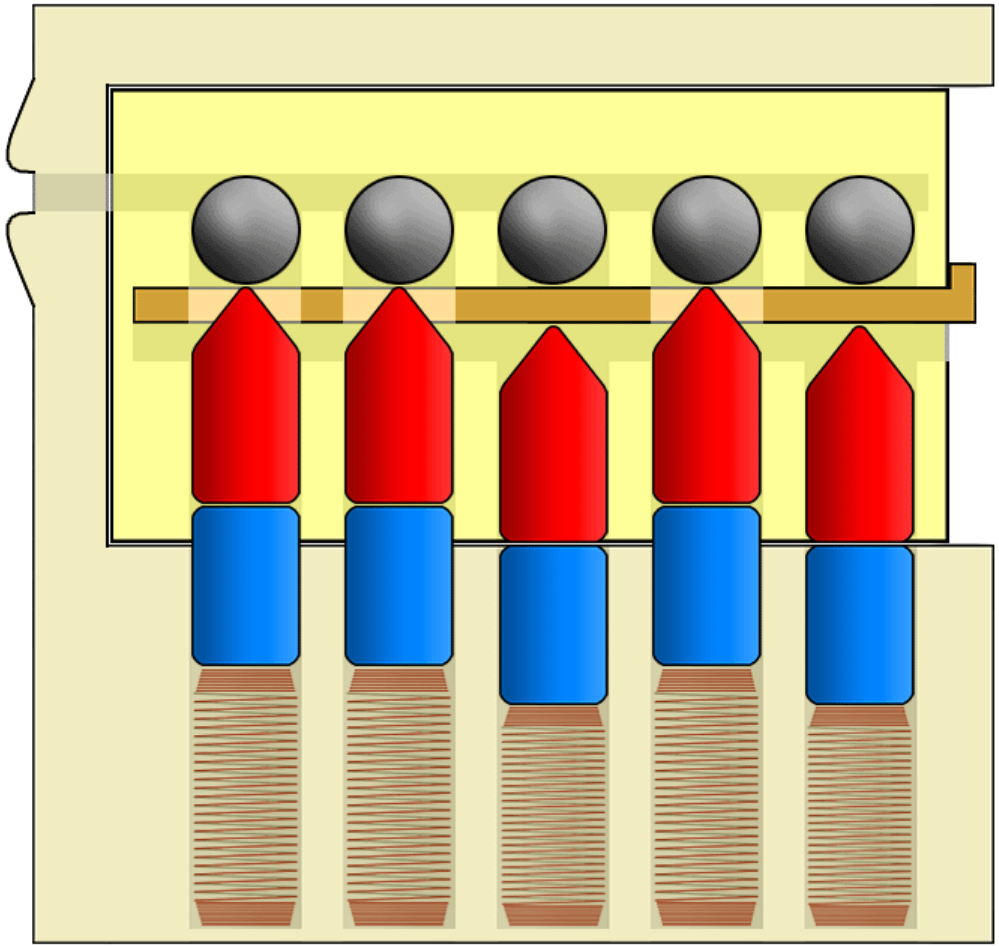
Control Card Can "Wiggle"



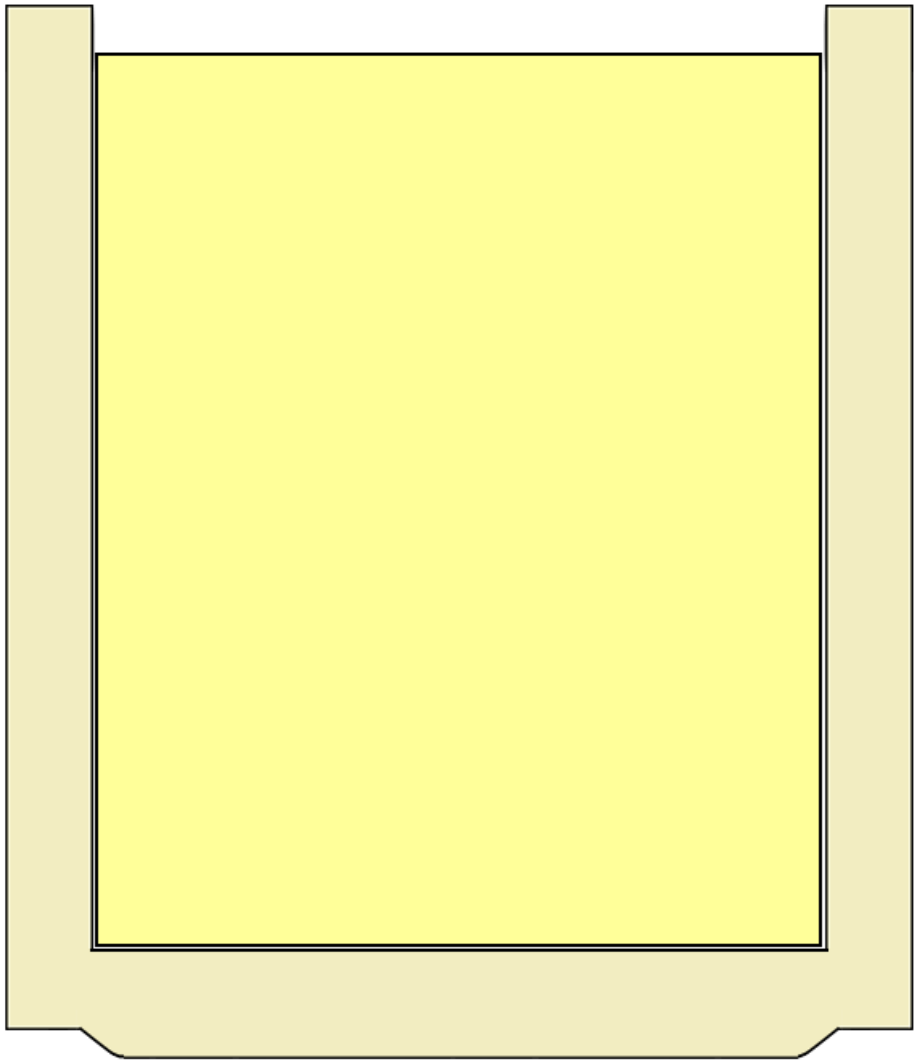
Pass Card “A” Being Used



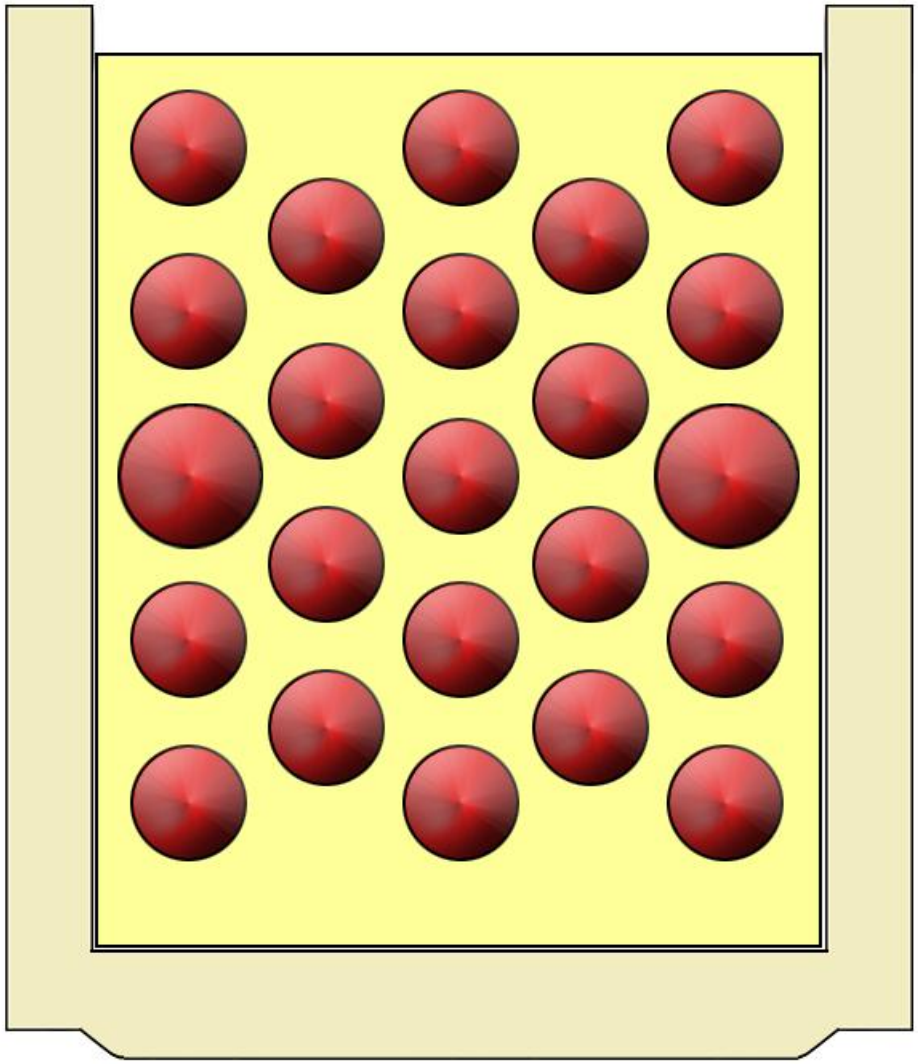
Change to Control Card "B"



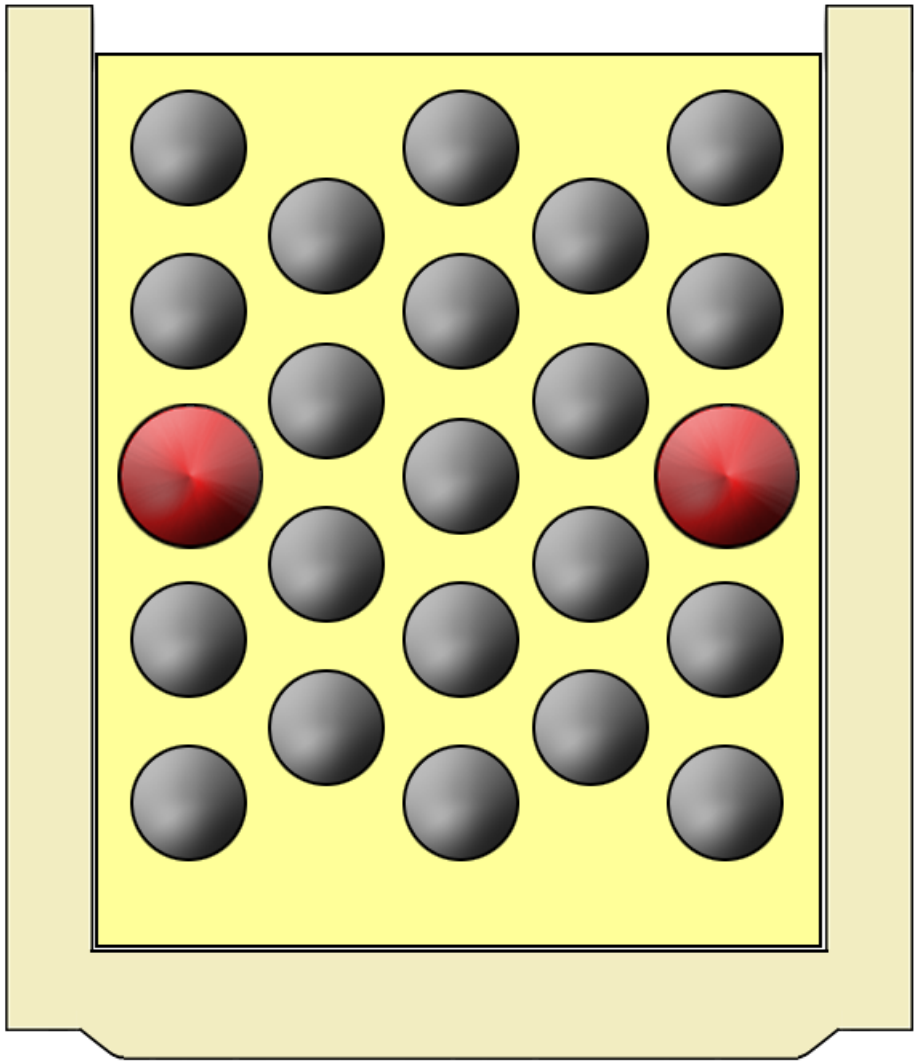
Understanding the Pin Matrix



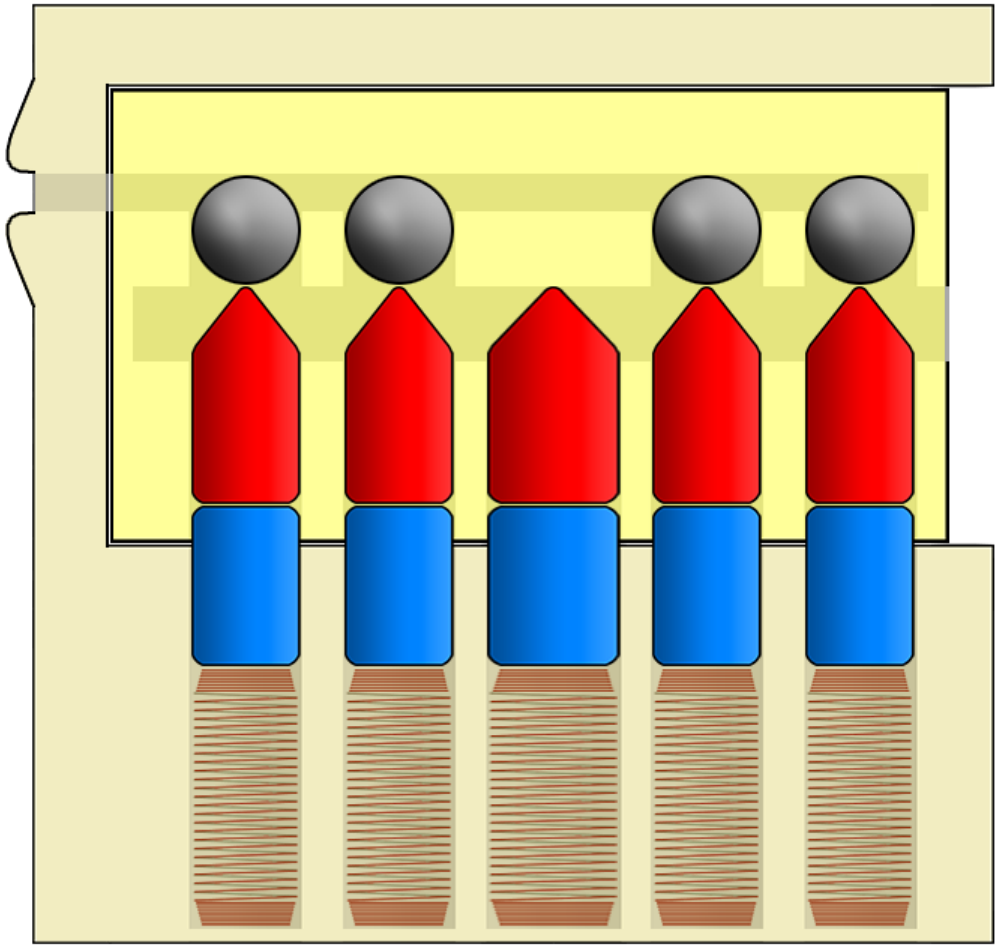
Key Pins



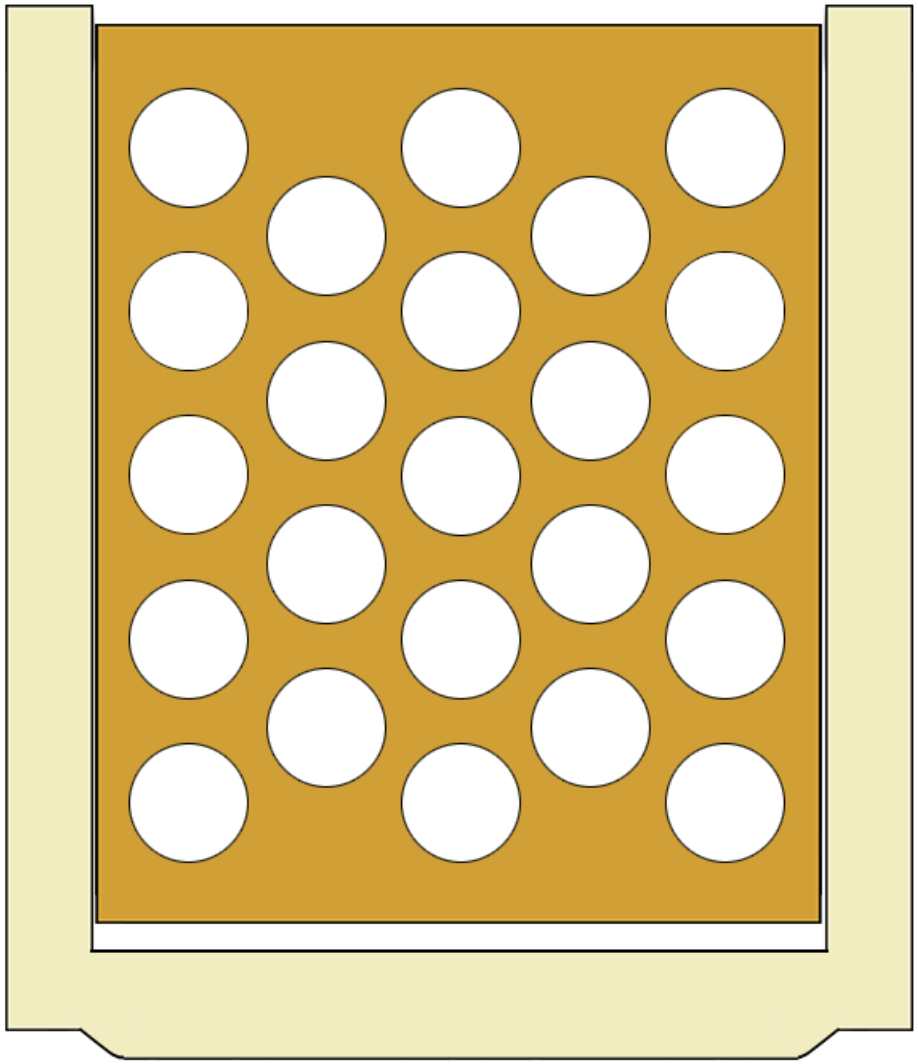
Ball Bearings On Top



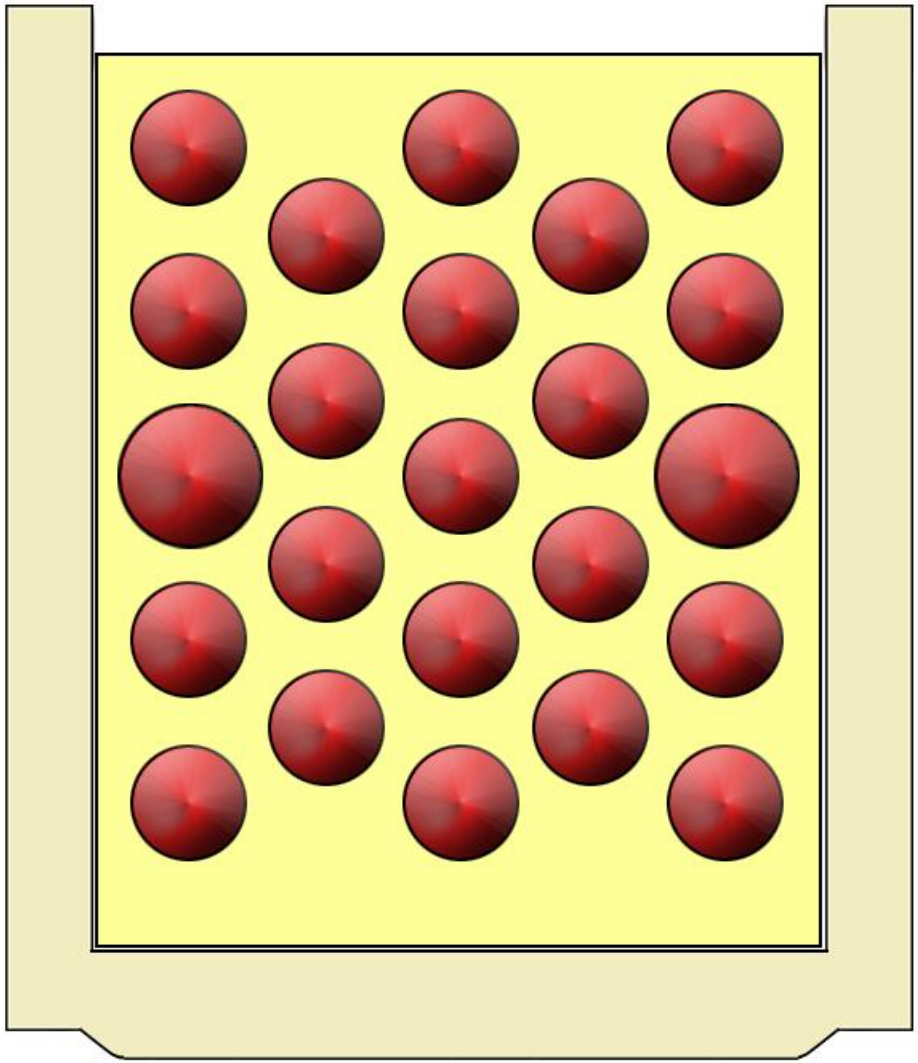
Pin Matrix Room Keys



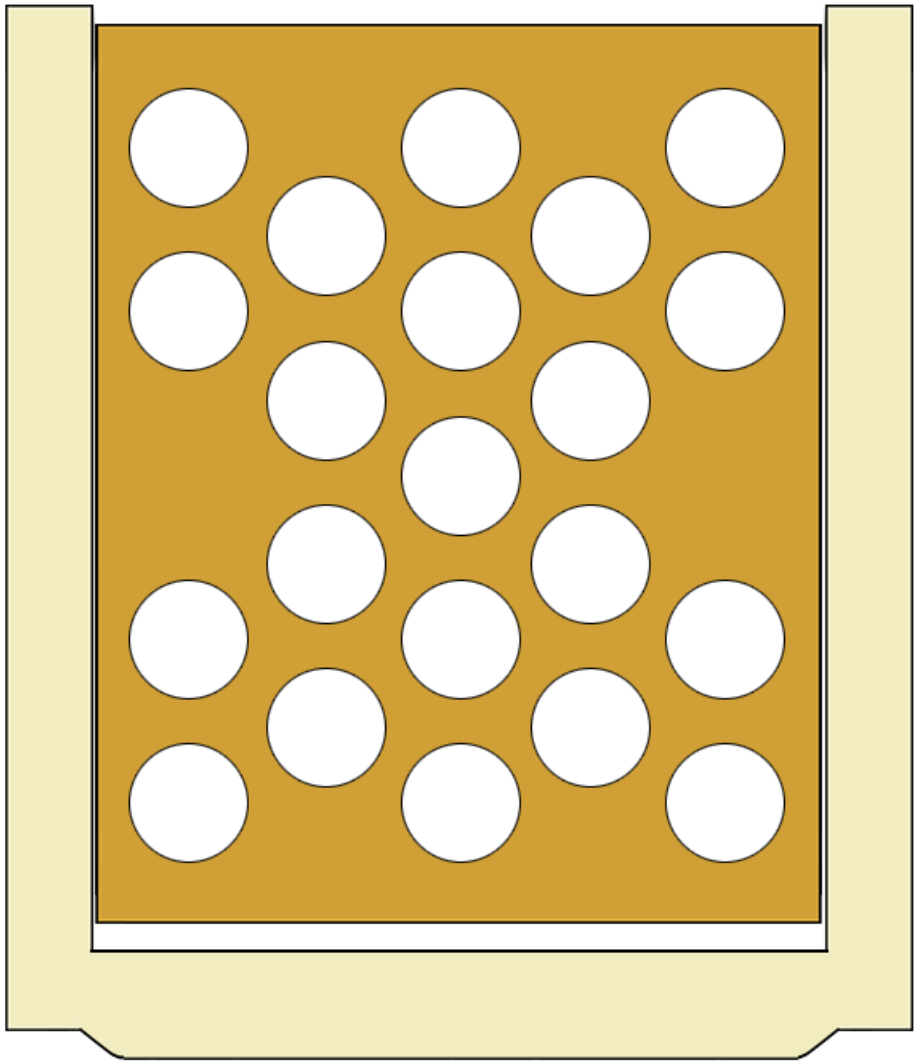
This Control Card Would Never Work



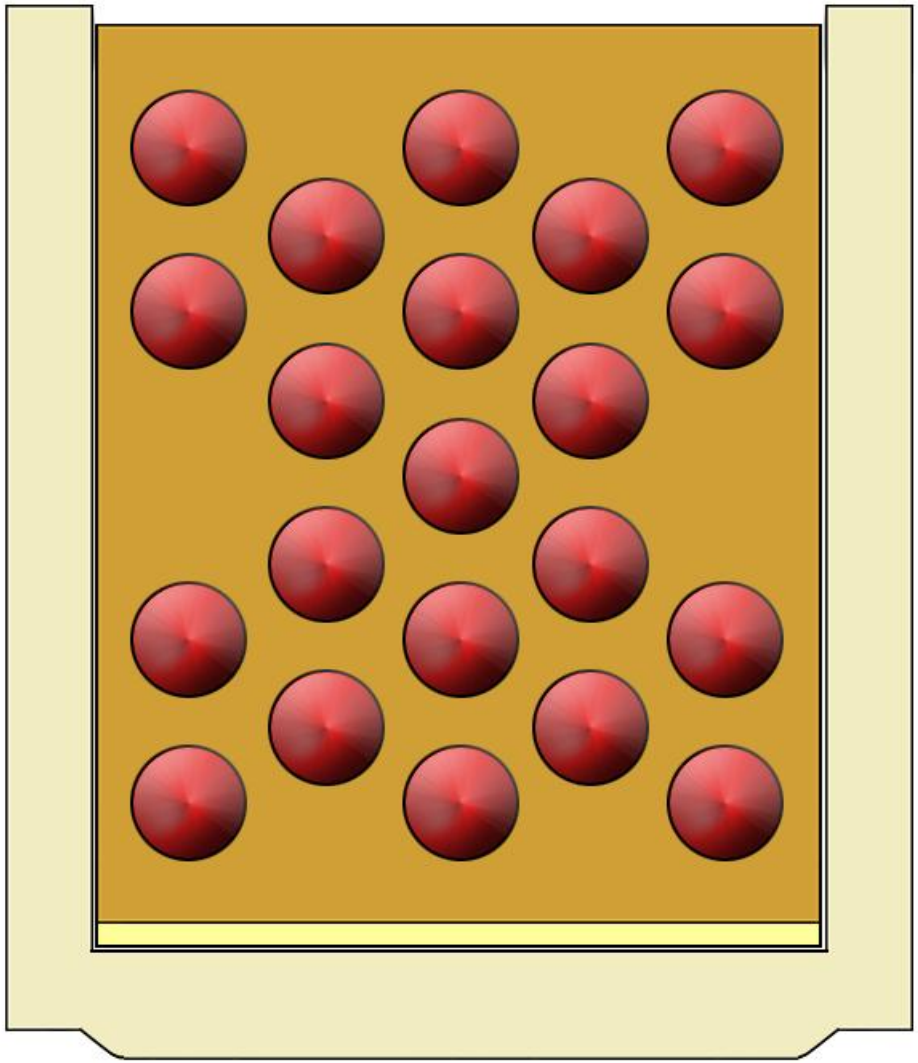
At Least Need to Depress Control Pins



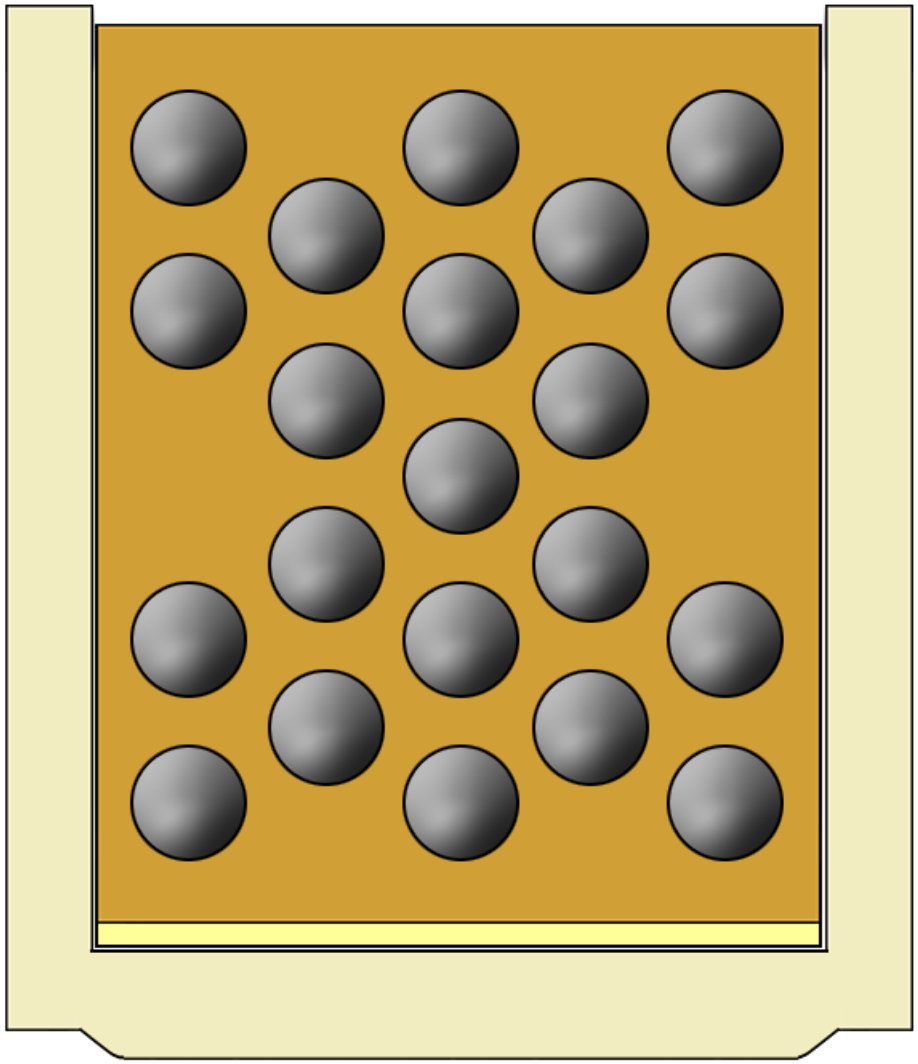
At Least Need to Depress Control Pins



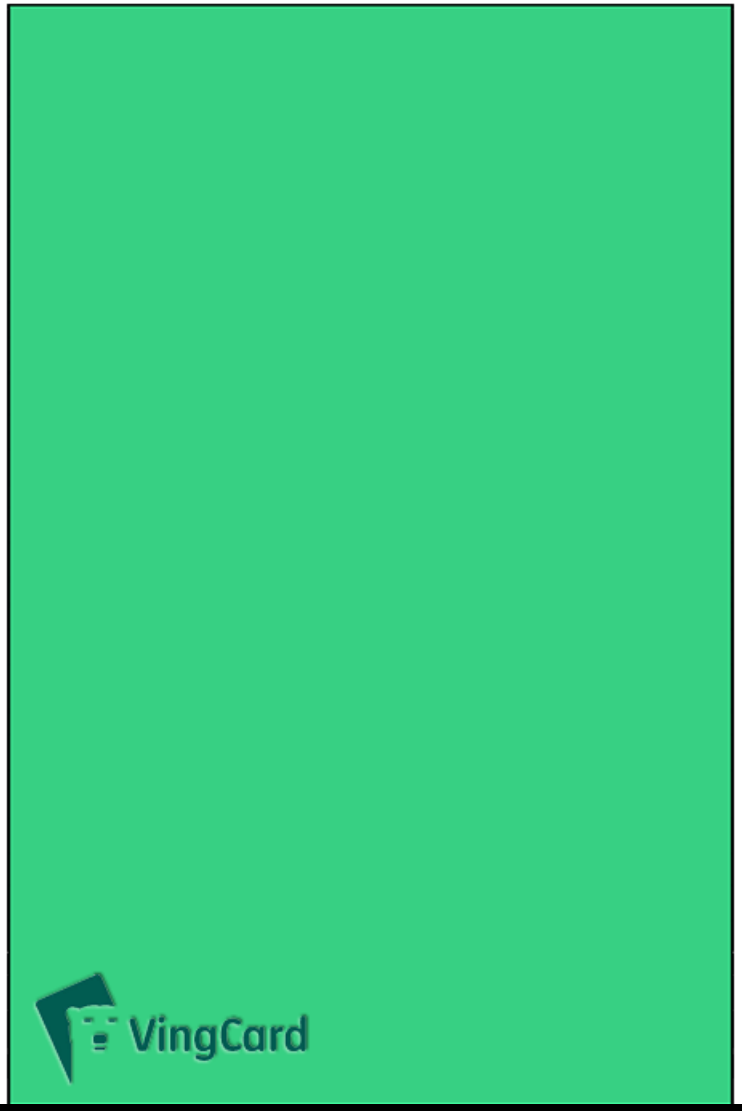
Very Punched Control Card



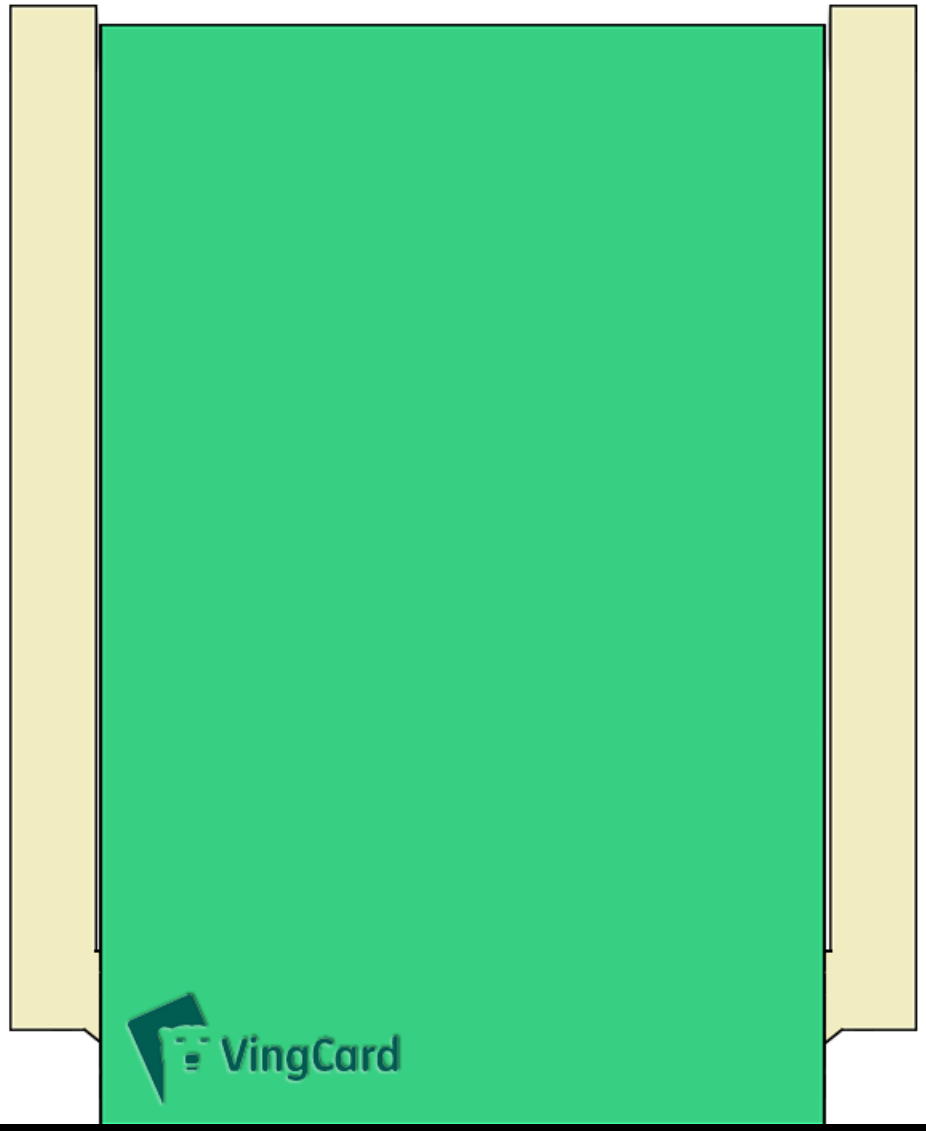
All Ball Bearings Free To Move



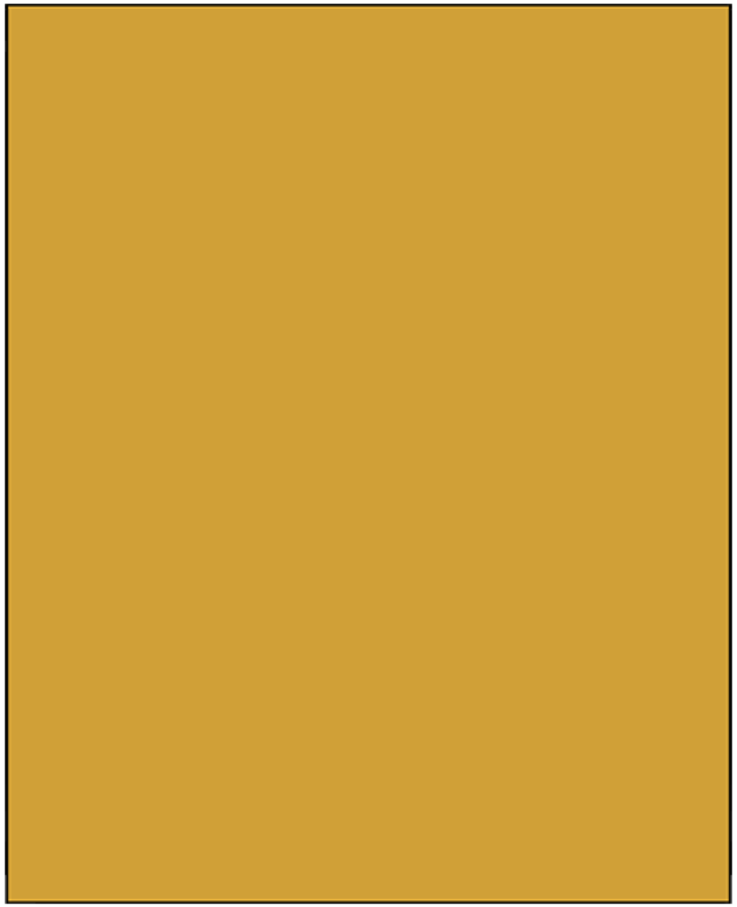
A Solid Pass Key Would be Needed



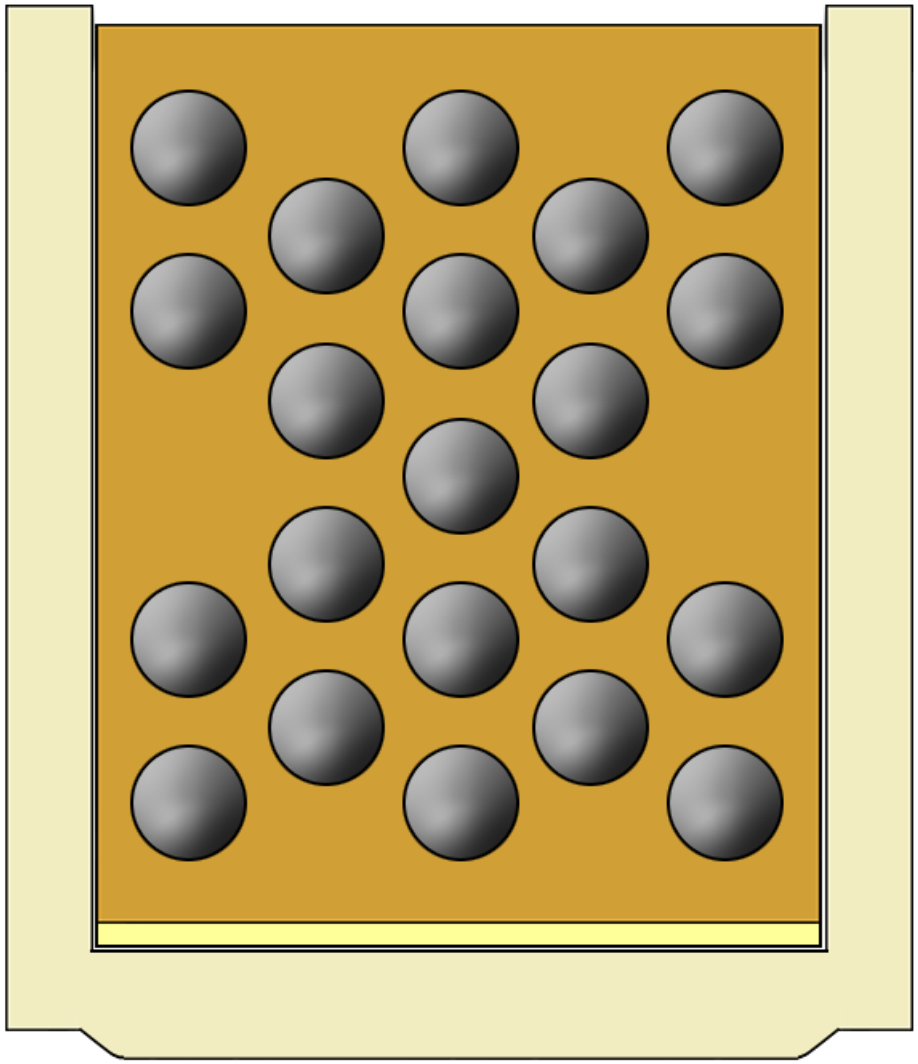
The Solid Pass Key Pushes All The Stacks



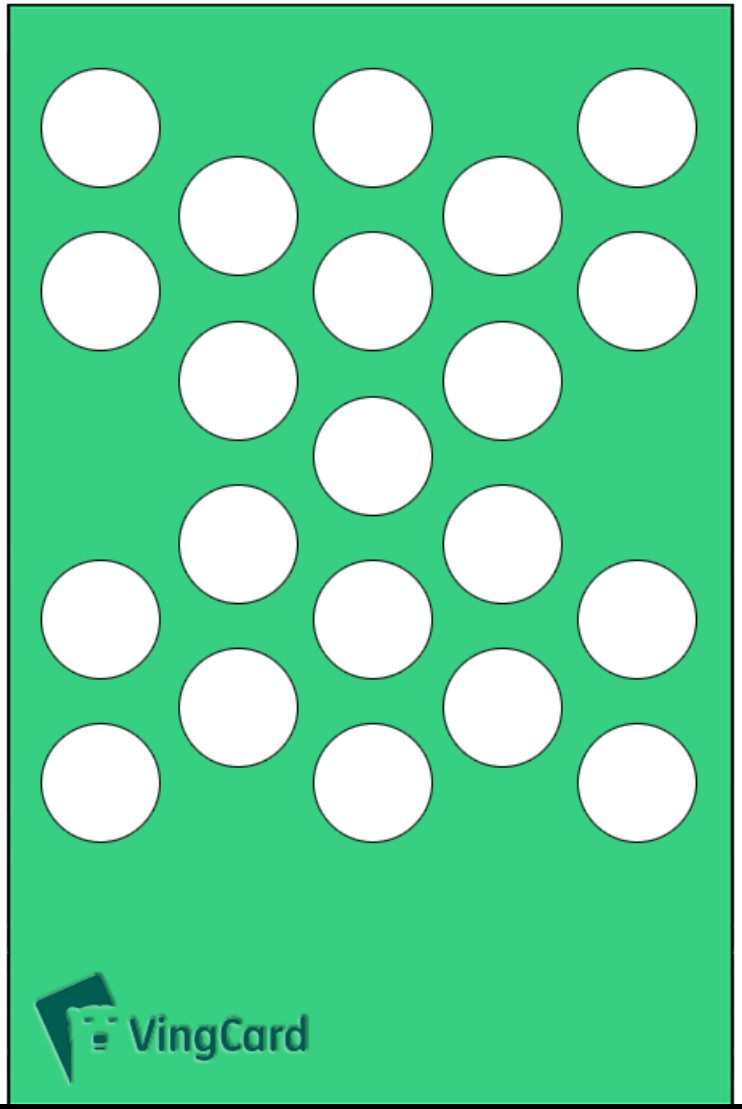
Imagine The Reverse... A Solid Control Card



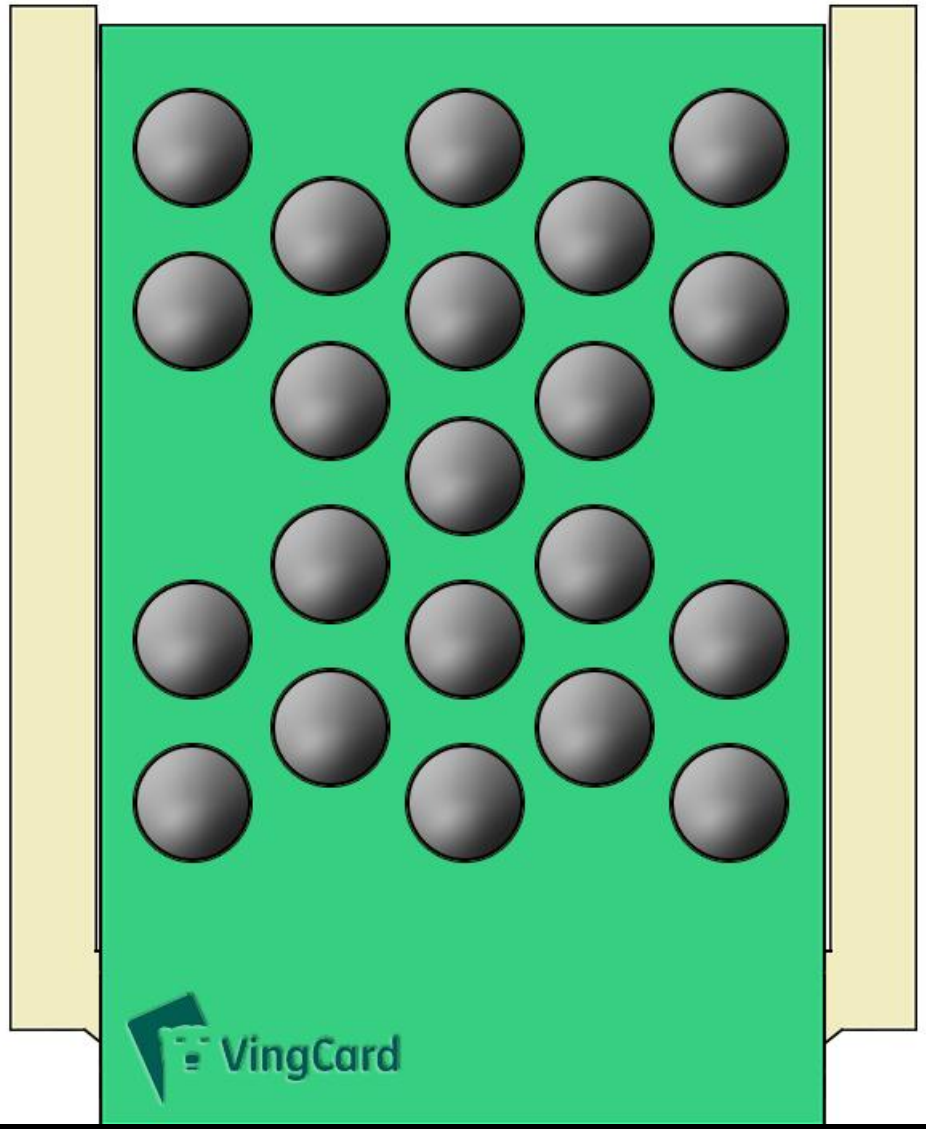
All Pin Stacks are now Correctly Aligned



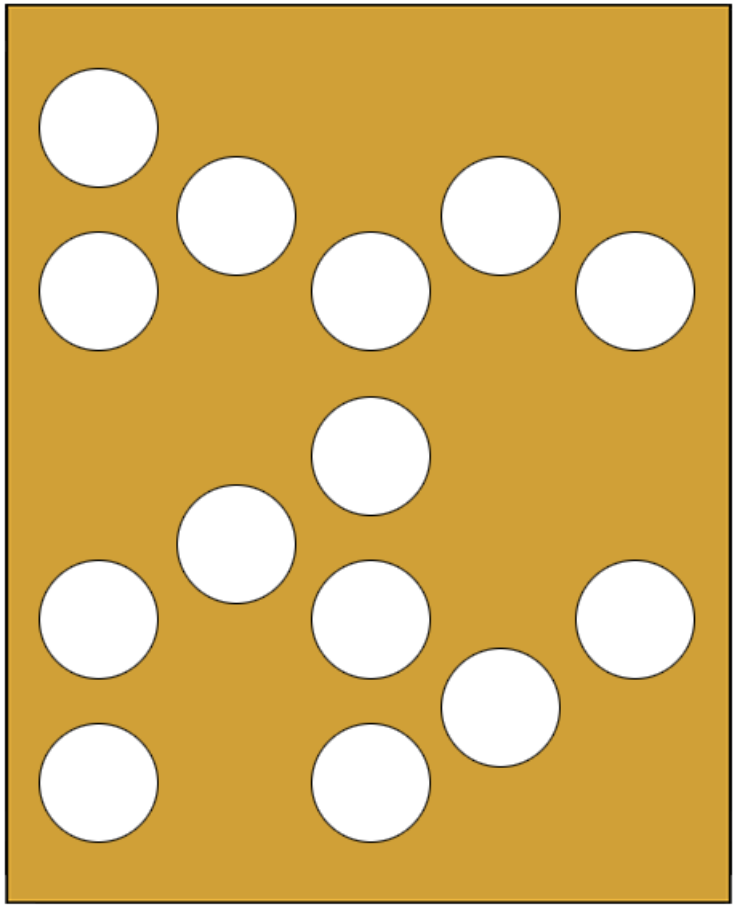
This Pass Card Would be Needed



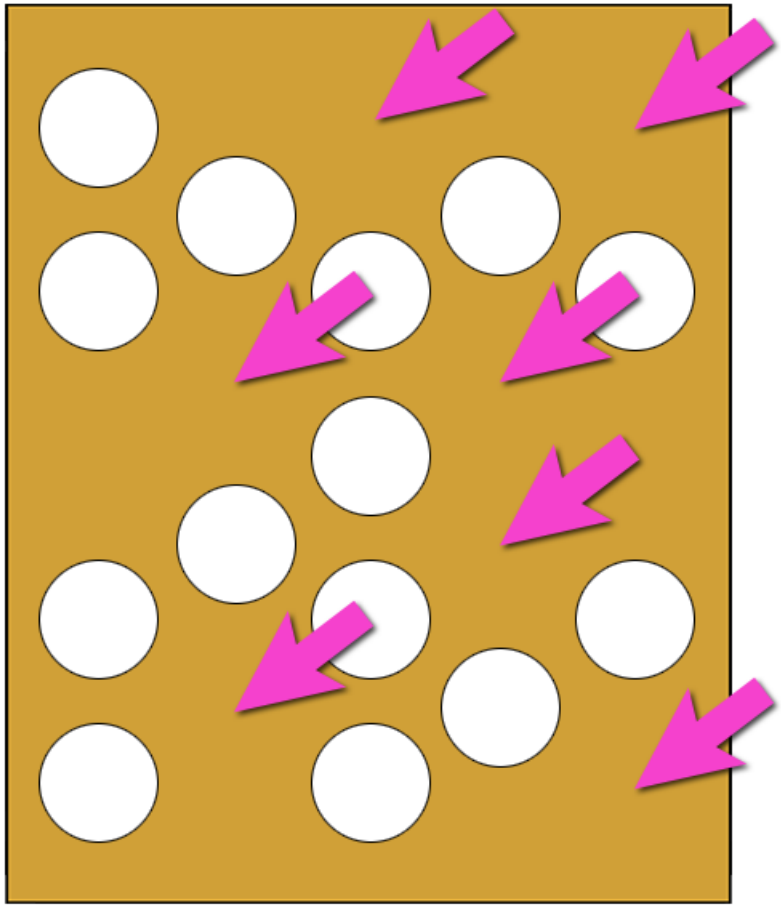
Ventilated Pass Card Works



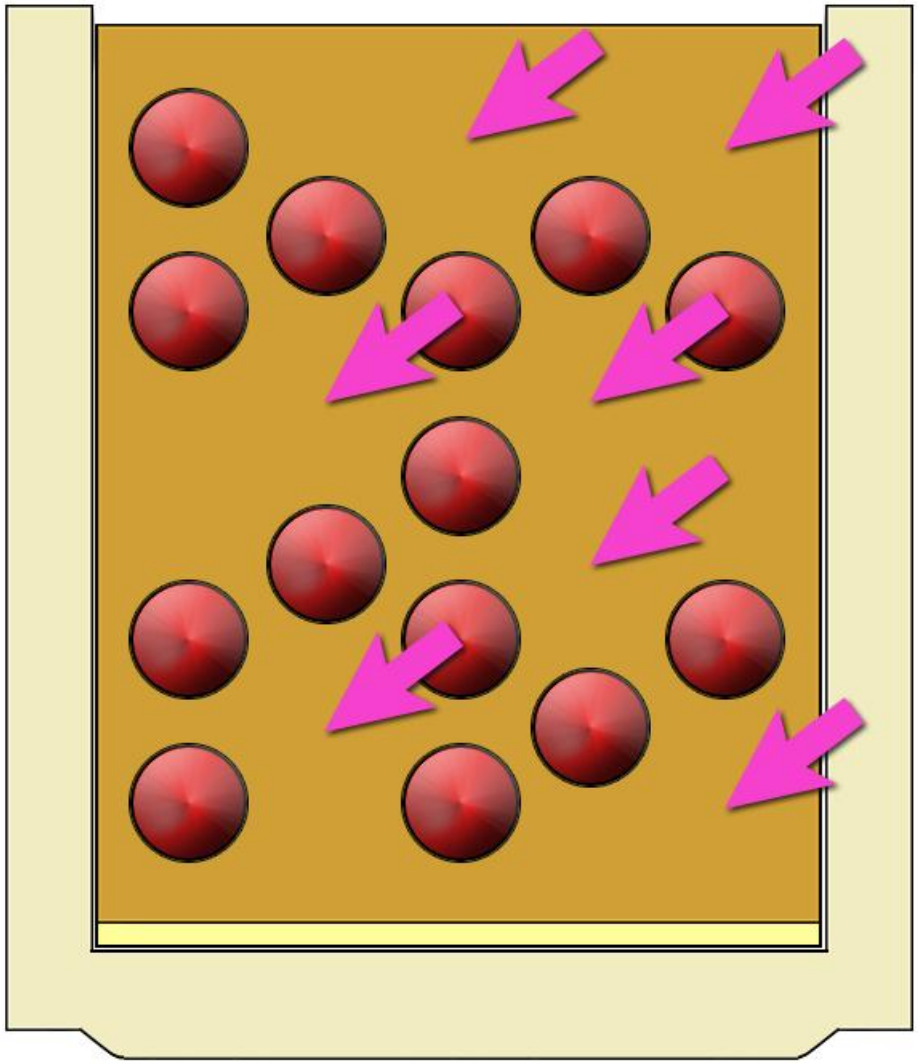
A More Typical Control Card



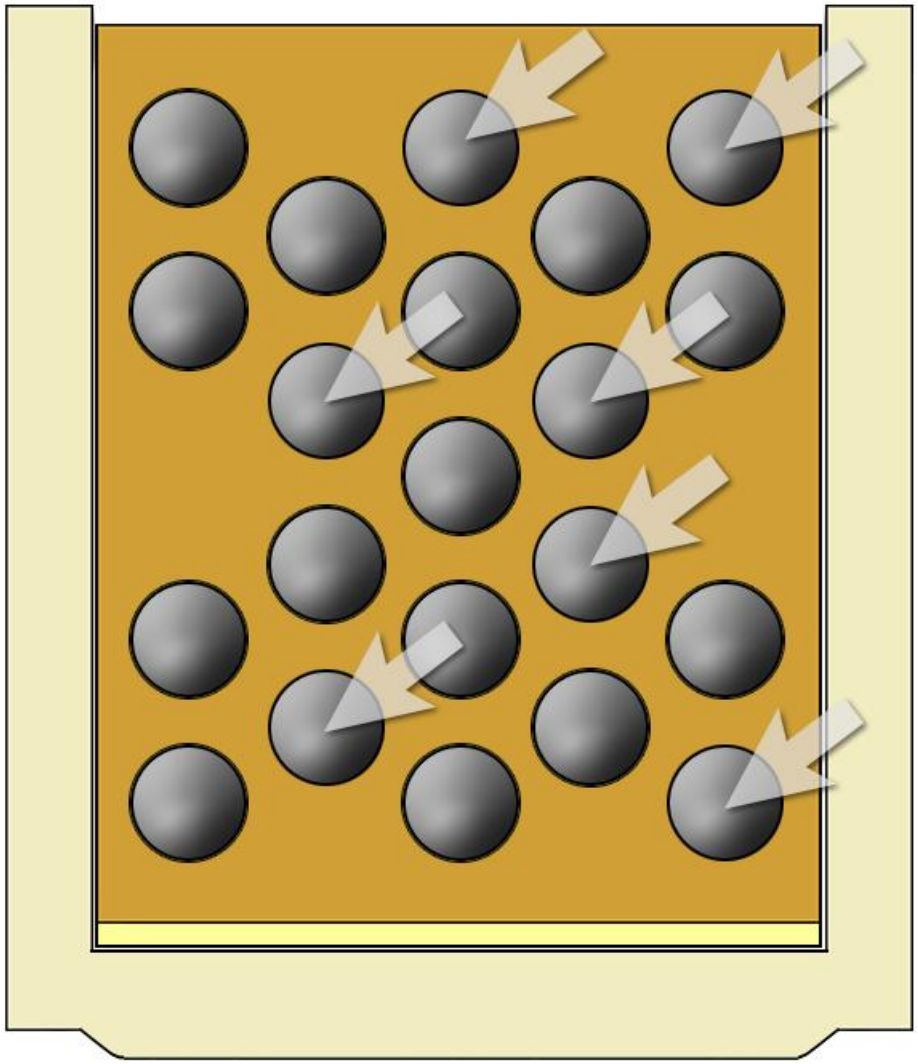
These Stacks are In Position



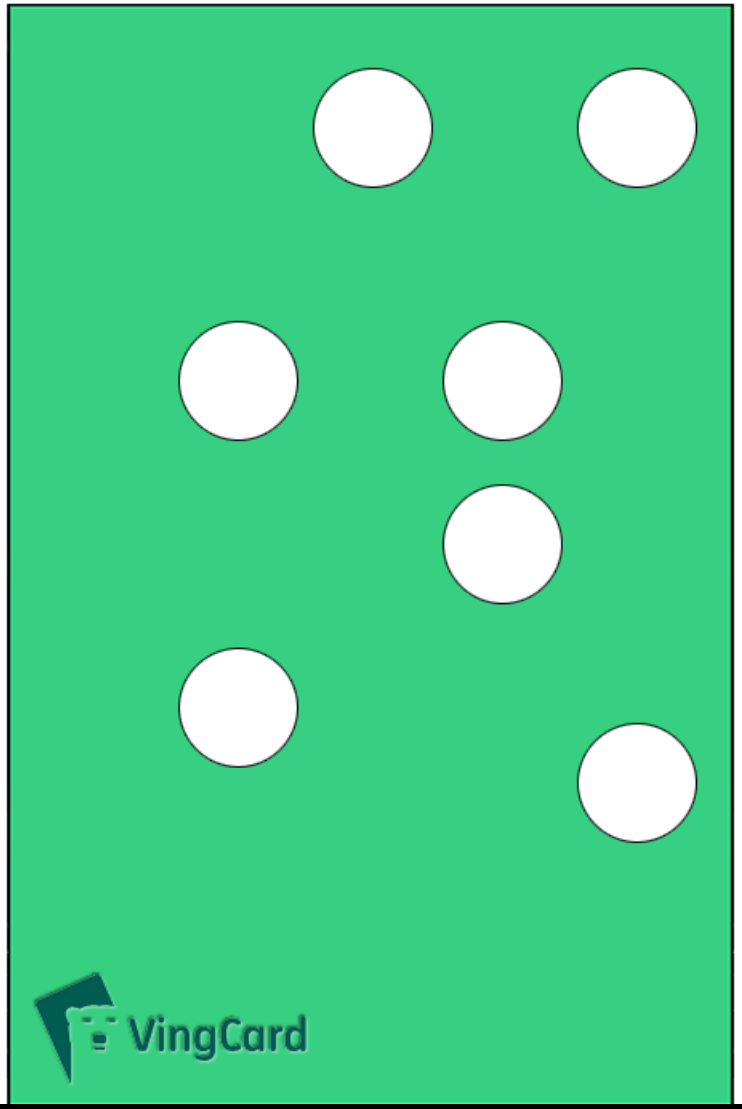
These Stacks are In Position



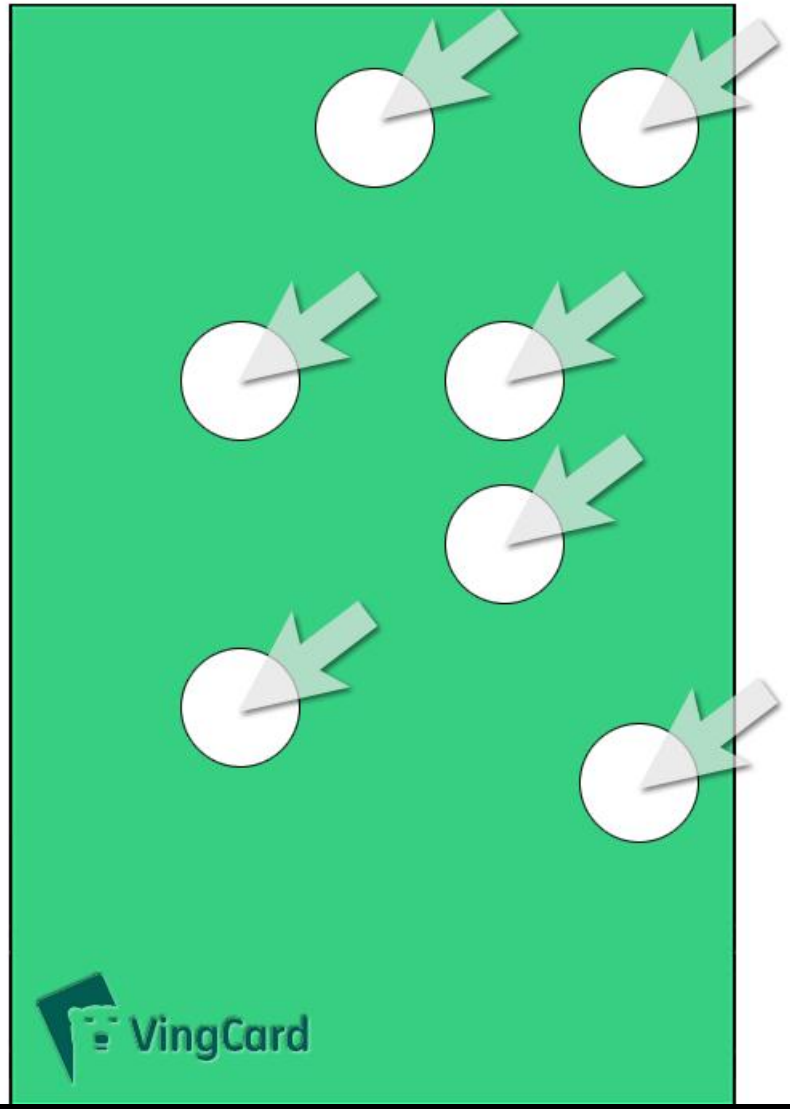
These Balls Shouldn't Move Further



So... This Would be the Corresponding Pass Key

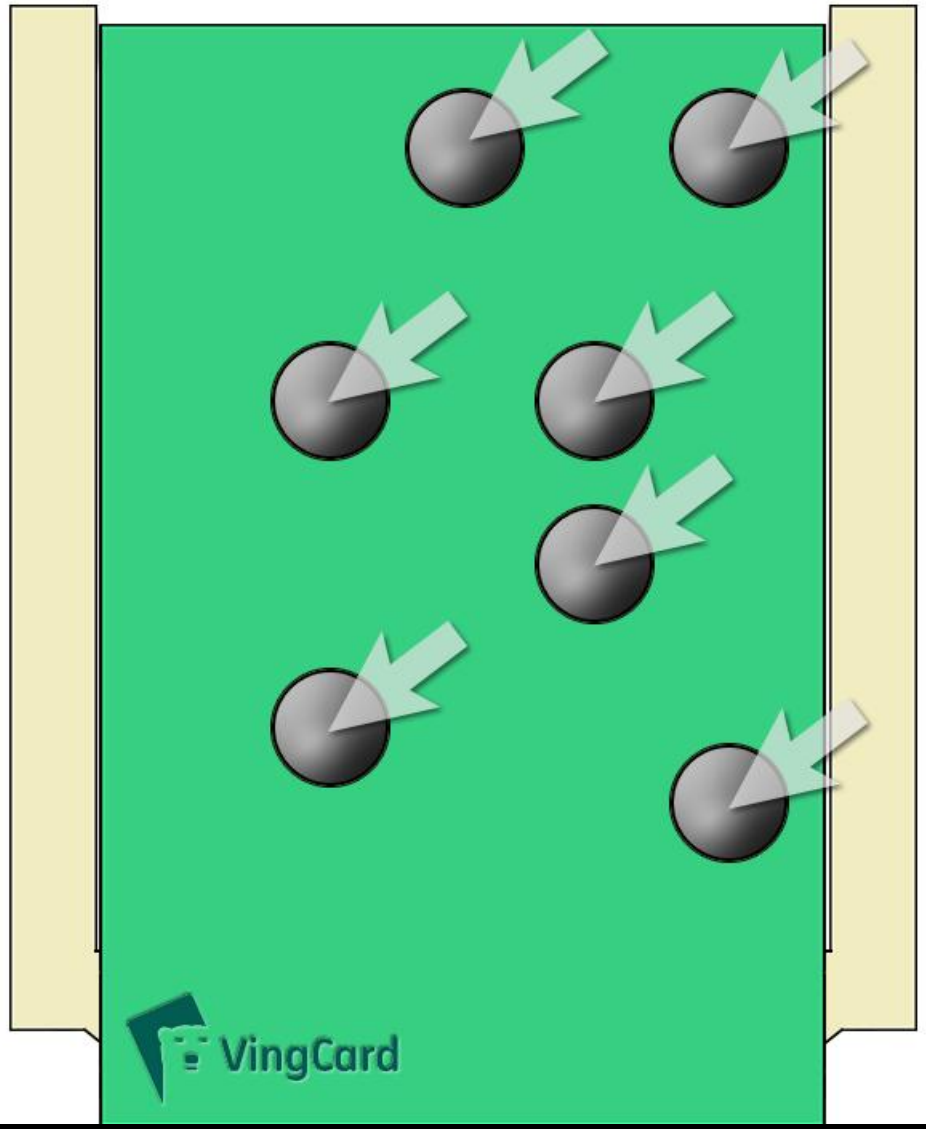


These Stacks Were Already In Position

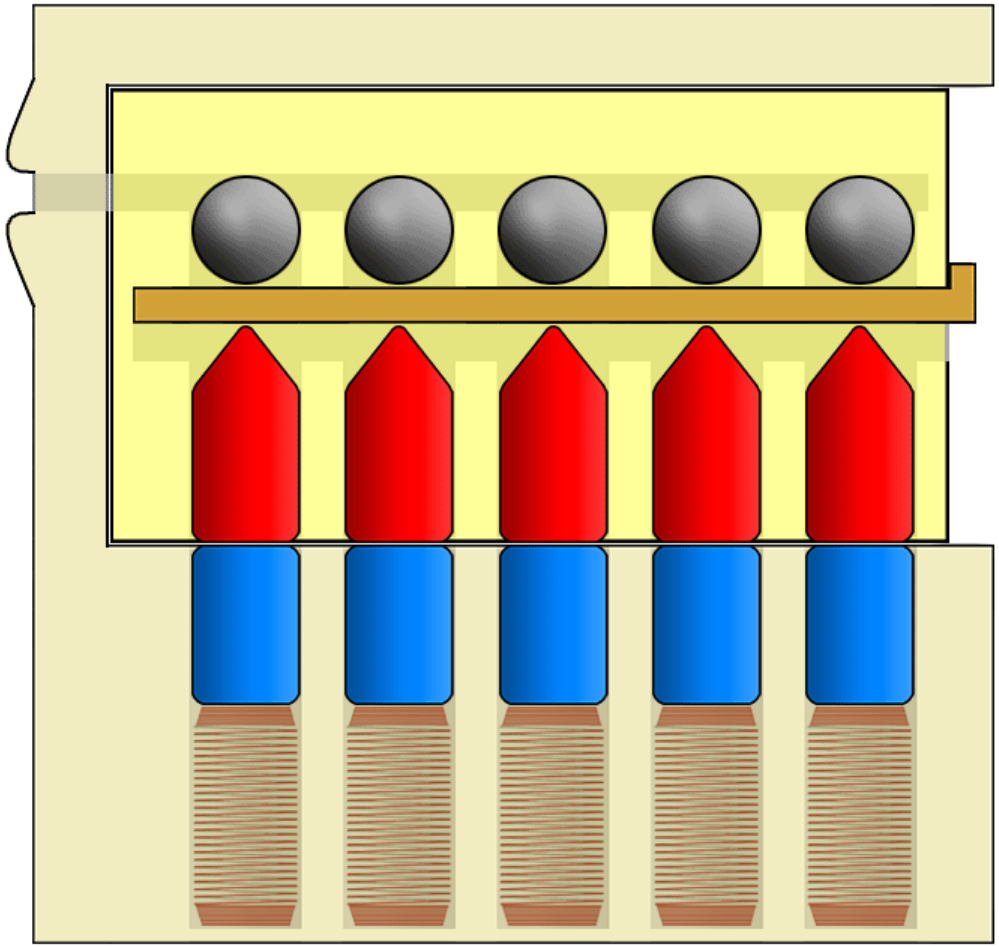


Only These Ball Bearings Should Stick Through

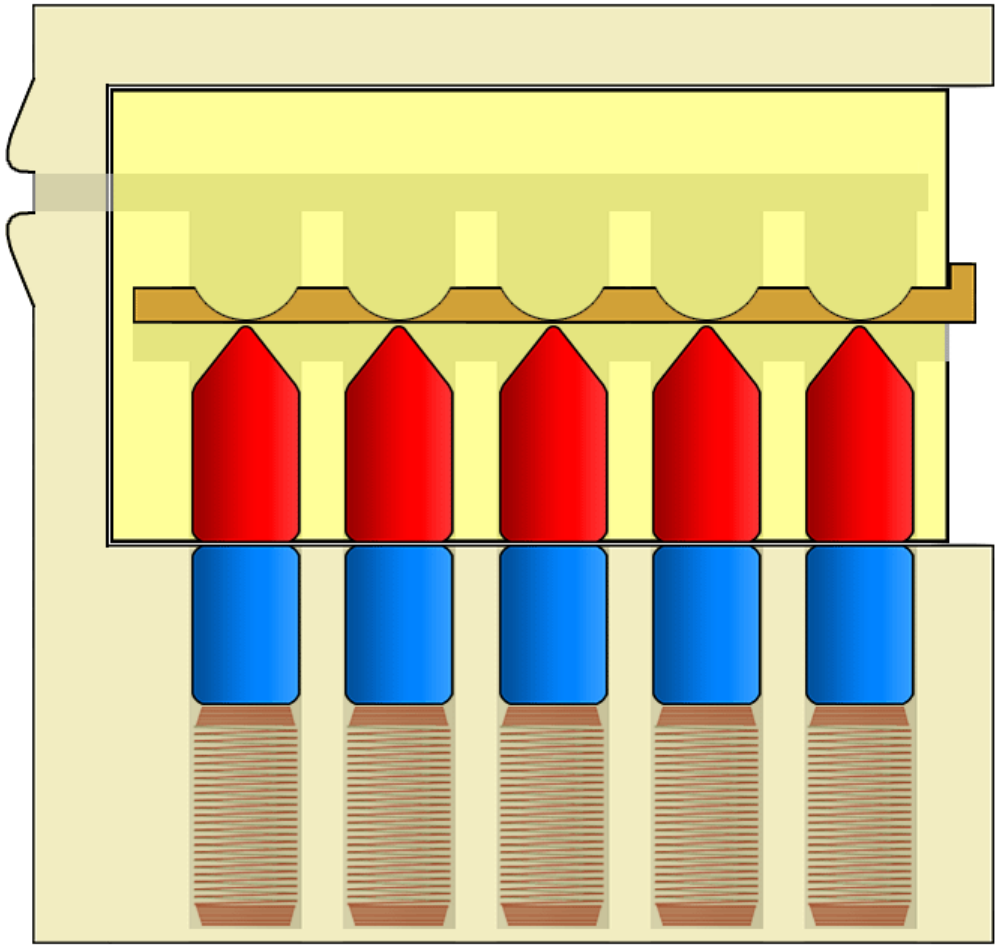
D



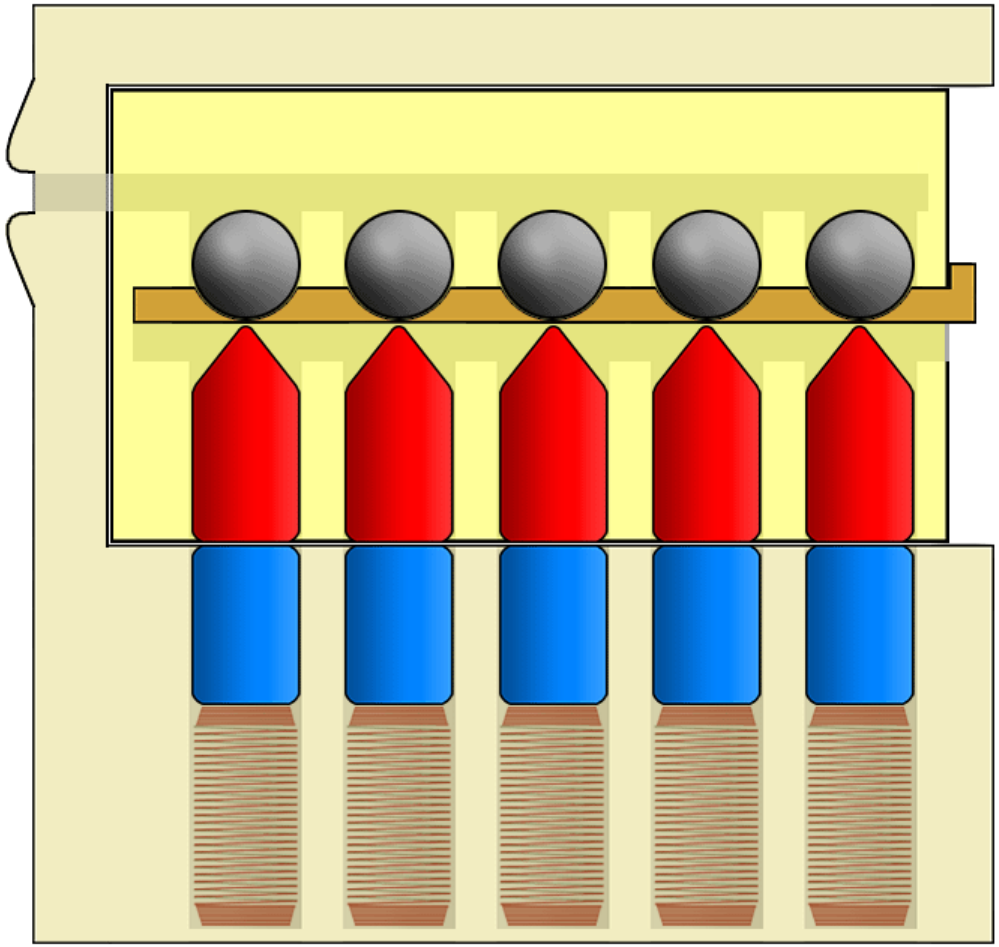
Control-Card Based Attacks



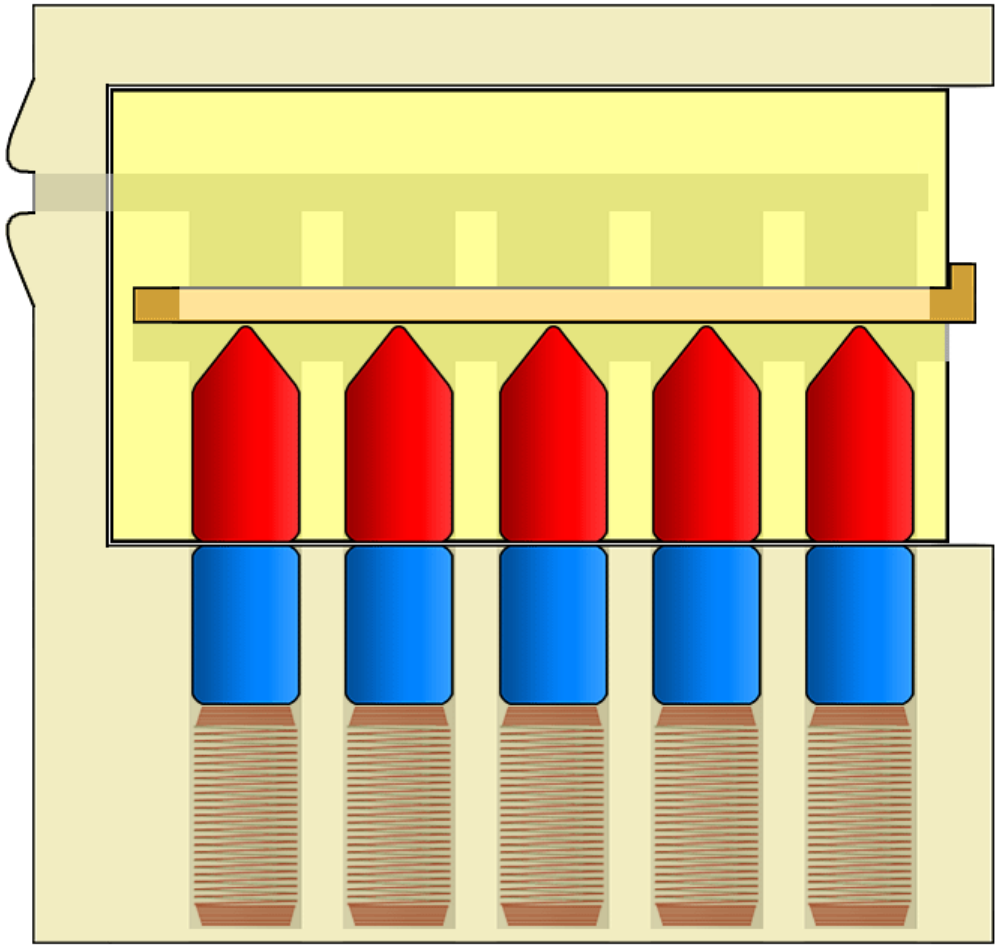
Dimpled Control-Card



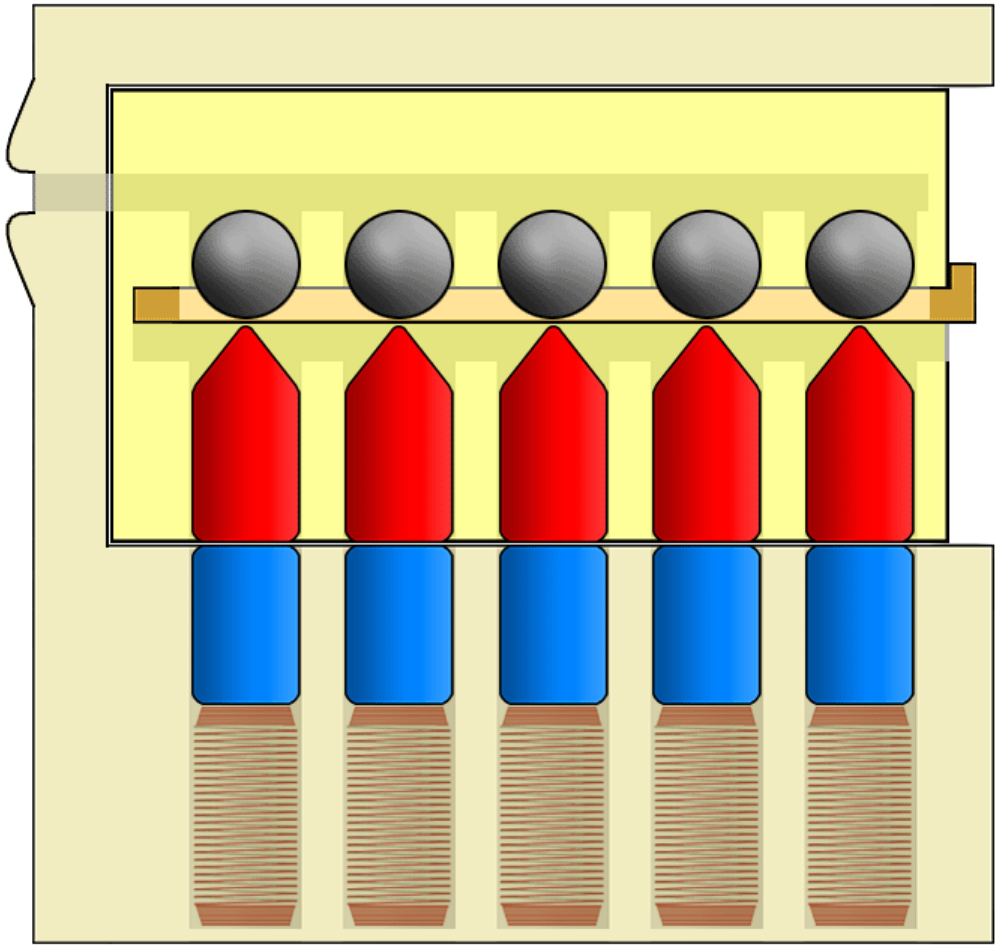
Ball Bearings Can Sit Lower



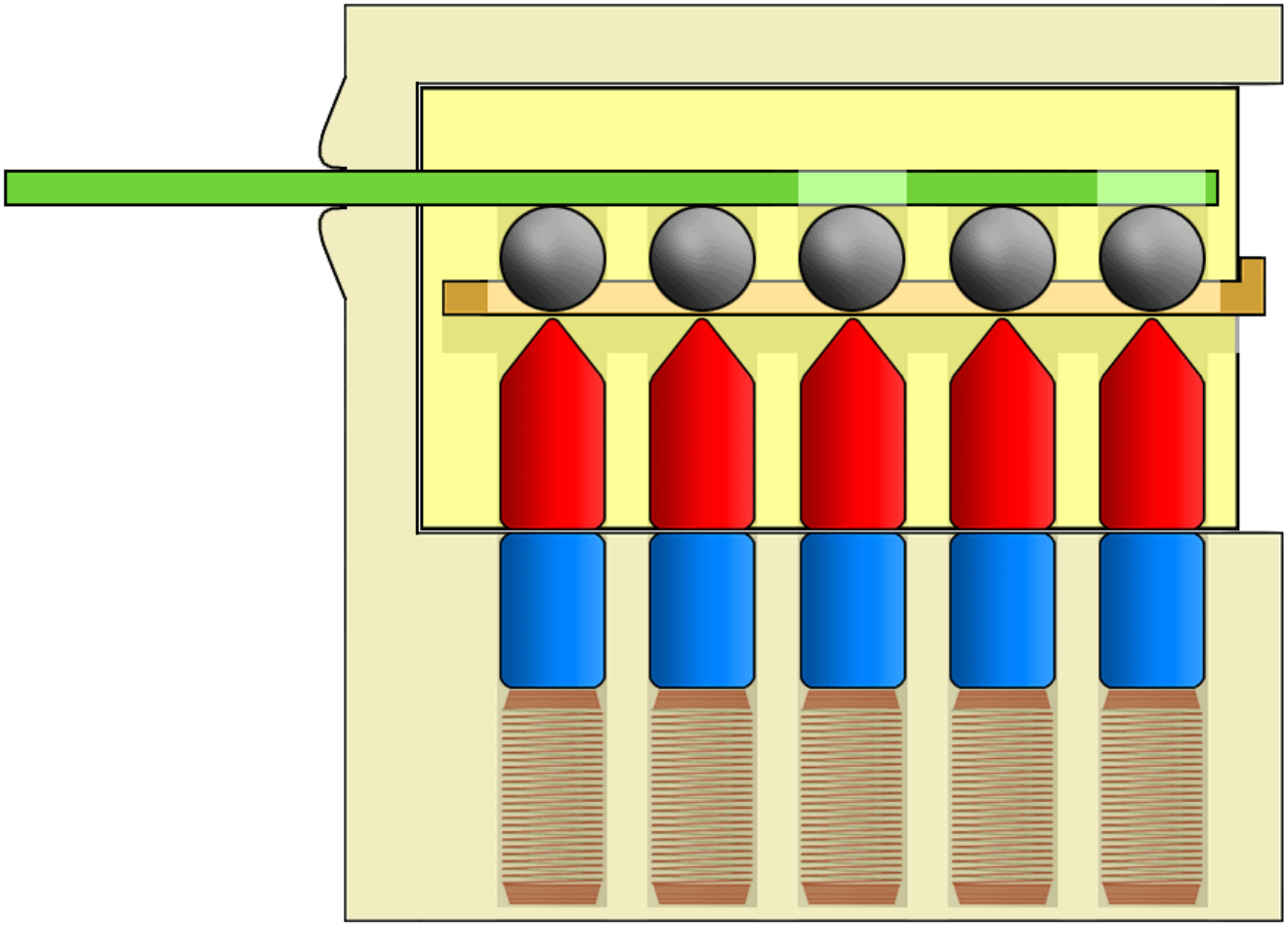
“Cookie Tray” Control Card



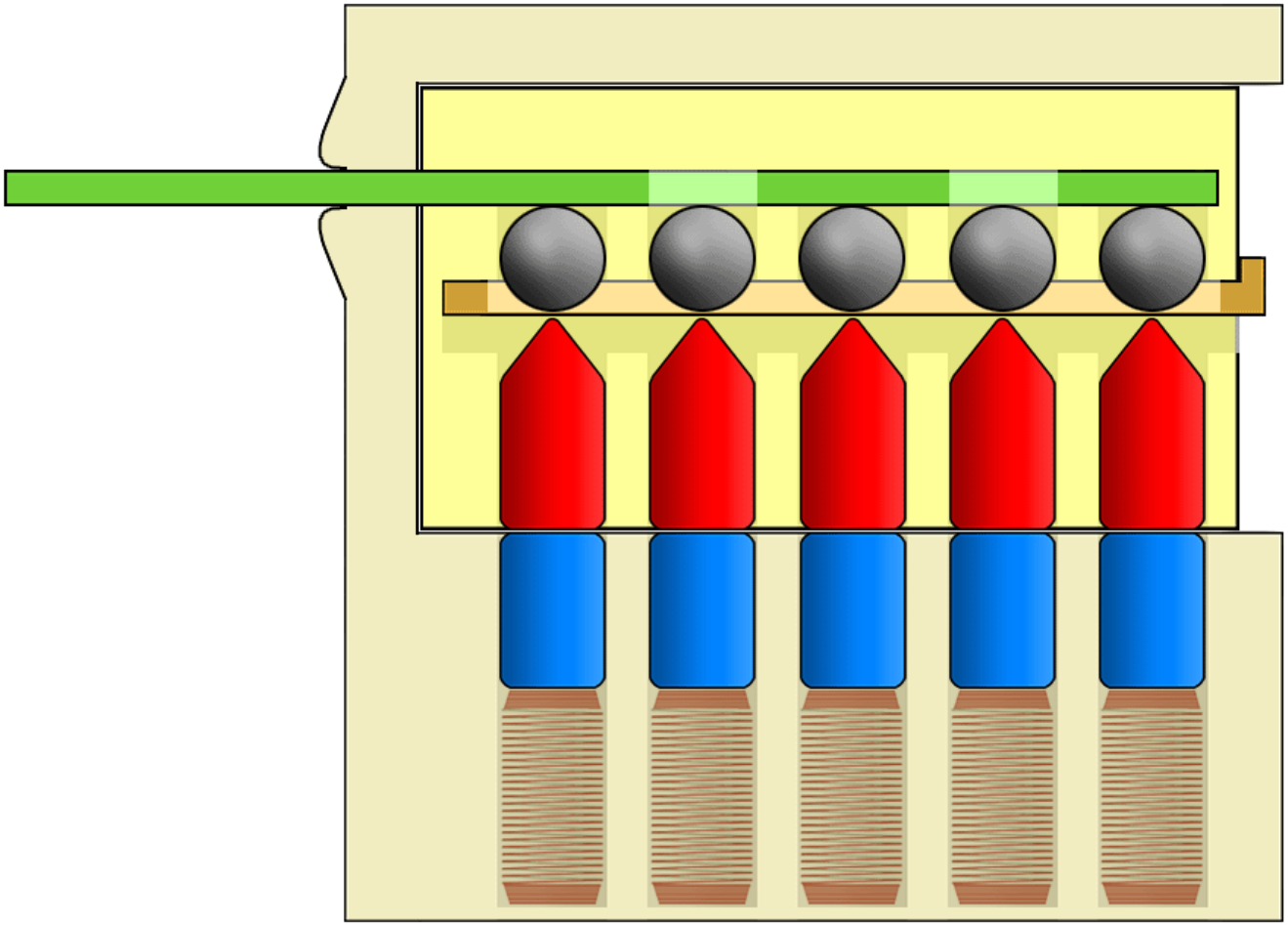
Ball Bearings Can Sit Lower



Pass Key “A” Can Work

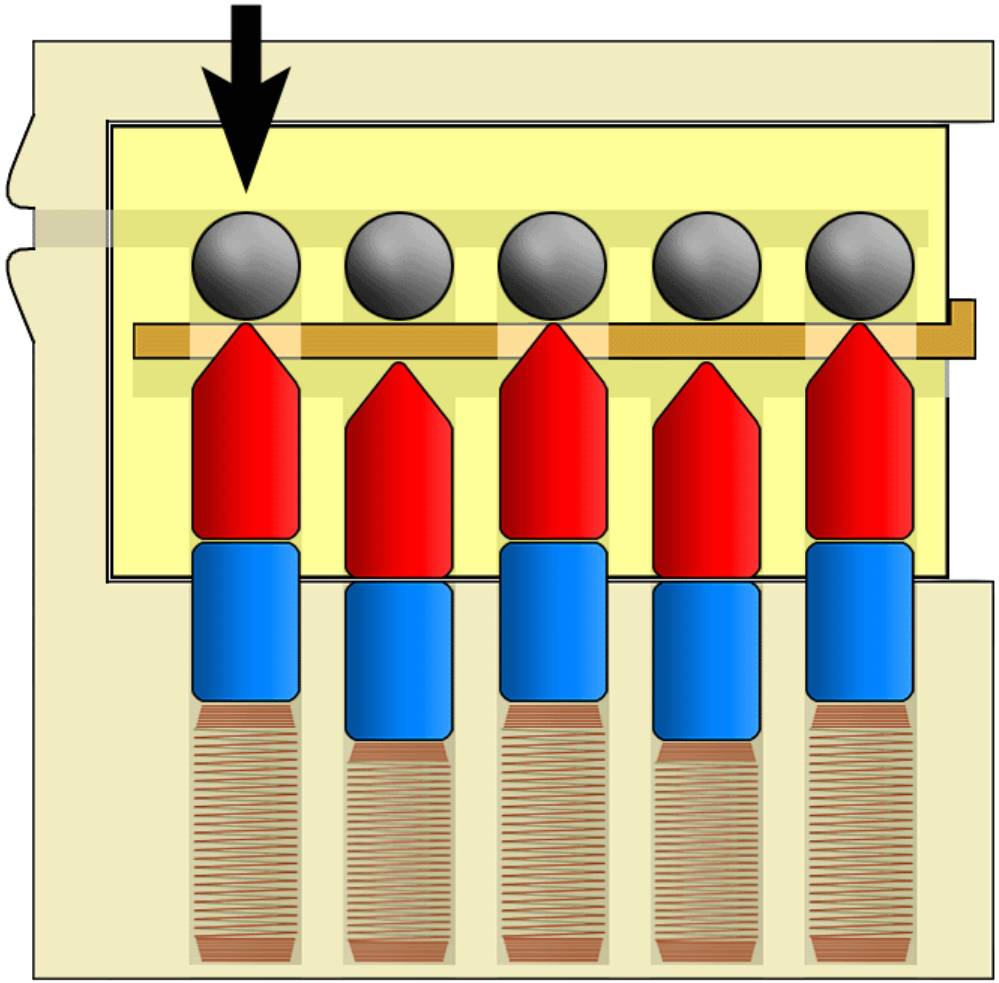


Pass Key “B” Can Work

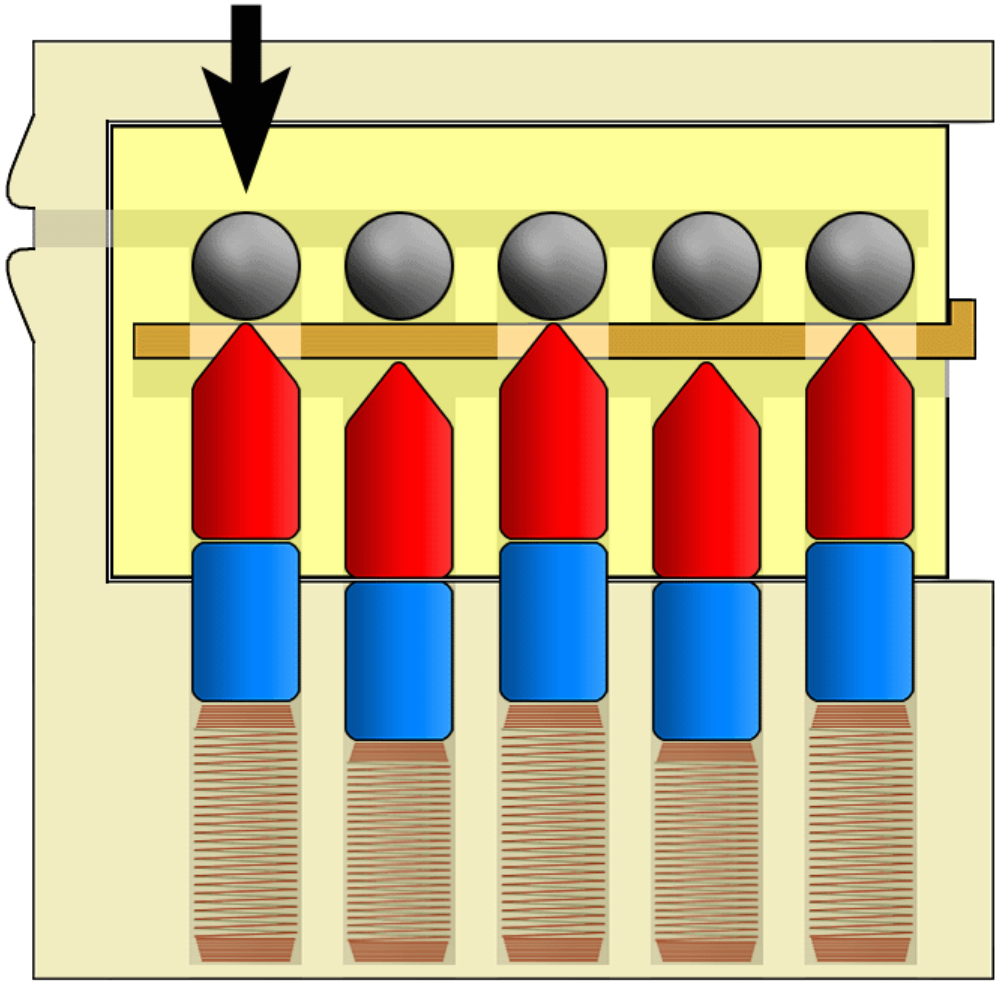


Decoding and Picking Attacks?

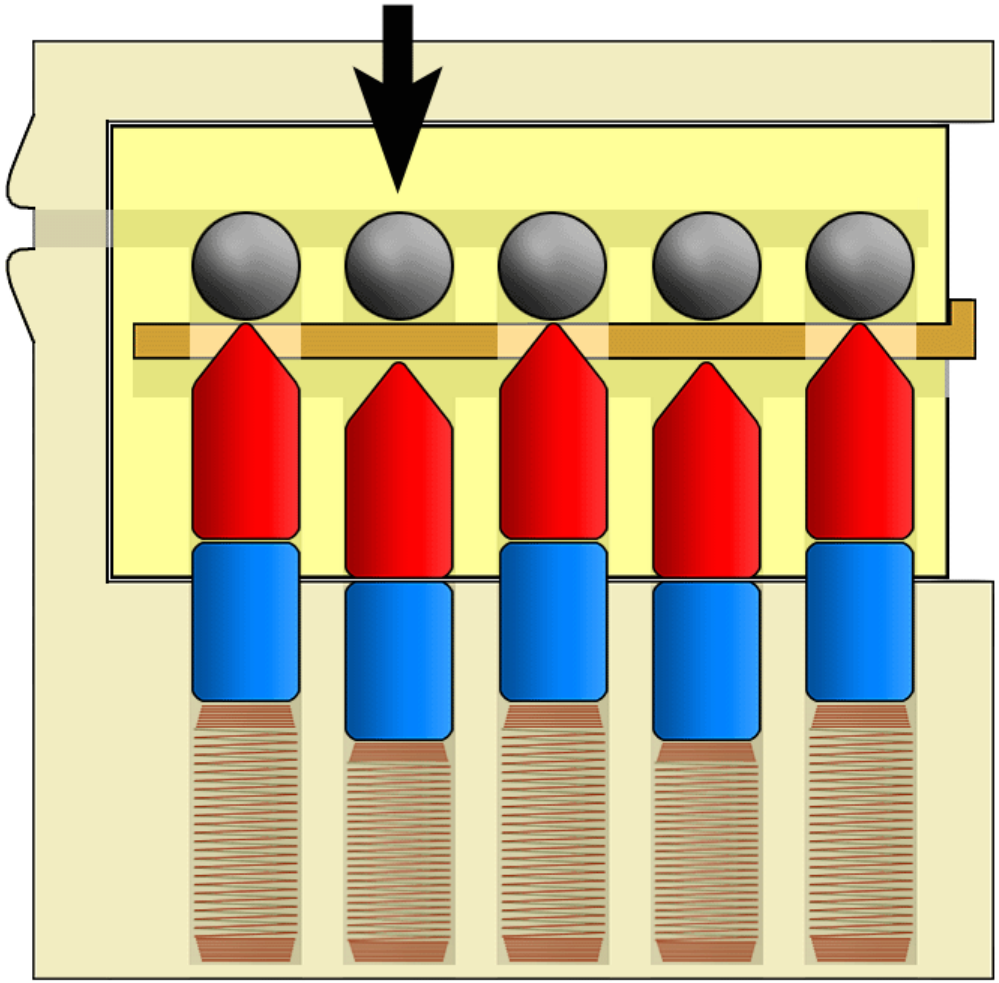
Consider This Ball Bearing



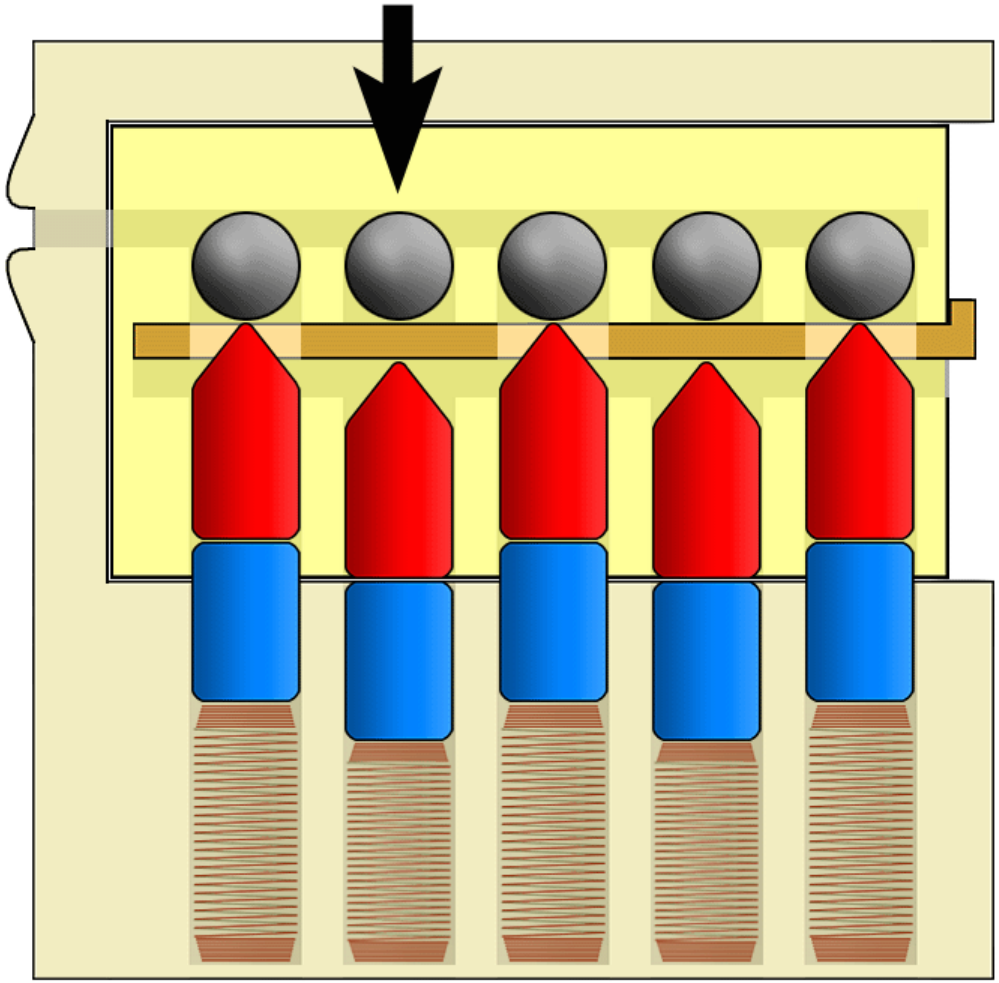
Very Springy



Consider This Ball Bearing

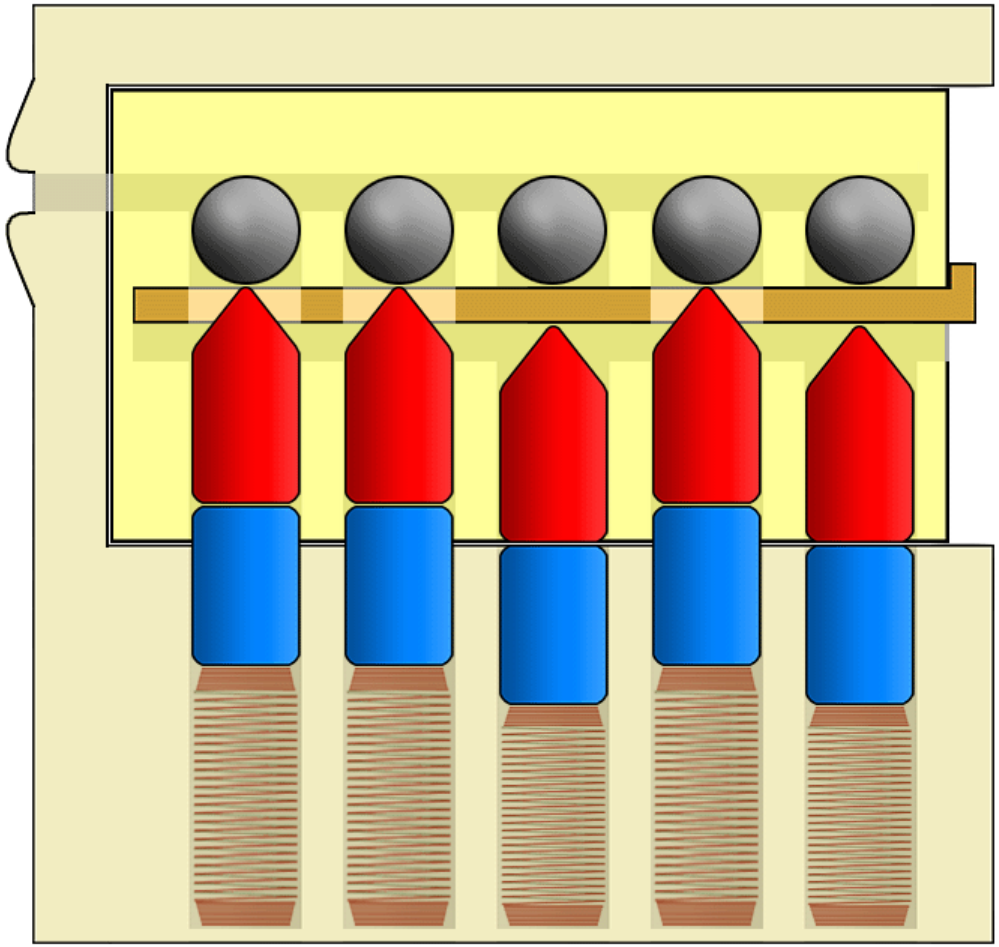


Not Nearly as Springy



You May Have Guessed... No Easy Master Keying

D



No Master Keying Means Override Keys

Override Lock... Sometimes Hidden

Override Lock... Sometimes Installed Badly

Override Lock... Sometimes Installed Badly

Override Lock... Sometimes Installed Badly

Magnetic Locks Also Feature Keyways

Magnetic Hotel Keys

Magnetic Hotel Keys

Magnetic Hotel Keys

start bit	site code	room number	key number	"magic" number	expire date	expire time	end bit	checksum
;000000	0420	0069	01	0016	20100720	1200	999	CRC

Magnetic Hotel Keys

start bit	site code	room number	key number	"magic" number	expire date	expire time	end bit	checksum
;000000	0420	0069	01	0016	20100720	1200	999	CRC
;000000	0420	0069	02	0016	20100720	1200	999	CRC

Magnetic Hotel Keys

start bit	site code	room number	key number	"magic" number	expire date	expire time	end bit	checksum
;000000	0420	0069	01	0016	20100720	1200	999	CRC
;000000	0420	0069	02	0016	20100720	1200	999	CRC
;000000	0420	0069	01	0032	20100720	1200	999	CRC

Magnetic Hotel Keys

start bit	site code	room number	key number	"magic" number	expire date	expire time	end bit	checksum
;000000	0420	0069	01	0016	20100720	1200	999	CRC
;000000	0420	0069	02	0016	20100720	1200	999	CRC
;000000	0420	0069	01	0032	20100720	1200	999	CRC

(last 100 "magic" numbers stored)

Special Hotel Keys

start bit	site code	room number	key number	"magic" number	expire date	expire time	end bit	checksum
;000000	0420	0000	01	0000	20100820	1200	999	CRC

Special Hotel Keys

start bit	site code	room number	key number	"magic" number	expire date	expire time	end bit	checksum
;000000	0420	0000	01	0000	20100820	1200	999	CRC

Special Hotel Keys

Special Hotel Keys

Special Thanks...

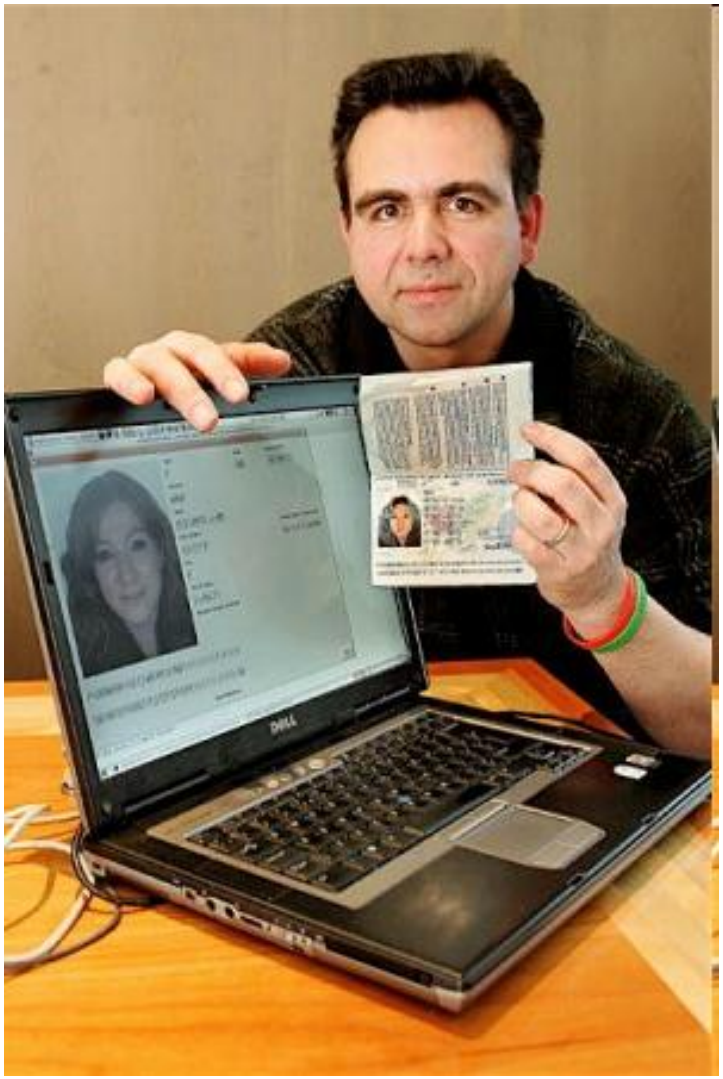
Major Malfunction

Über Hacker Extraordinaire

From The U.K.

- Yet Loves Firearms
- Not a Nanny-State-Loving Nancy
- All Around Awesome Fellow

Check Out *"Magstripe Madness"*
and *"Old Skewl Hacking"*



Come Visit the Lockpick Village !

Thank You Very Much!

Questions?

http://toool.us http://toool.nl

Thank you to Barry, Han, Major Malfunction, The 2600 Staff, The Hotel Pennsylvania,

and all of our friends and associates in the locksport community.