Every Computer has a tell.

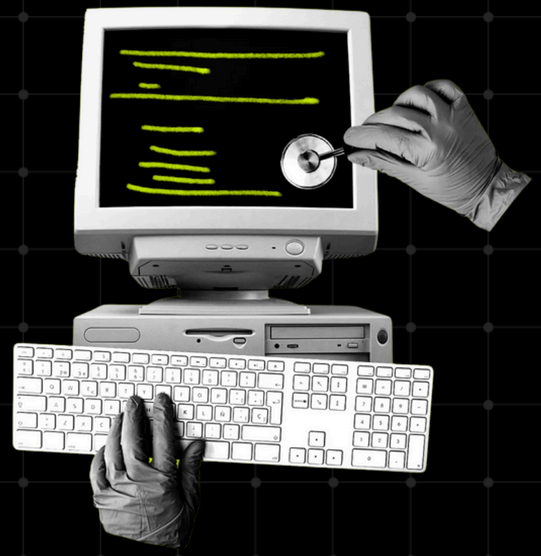
HARDHACK

ELECTRONICS & ROBOTICS CLUB | CYBERSECURITY COMMUNITY

ERC & CSeC PRESENT

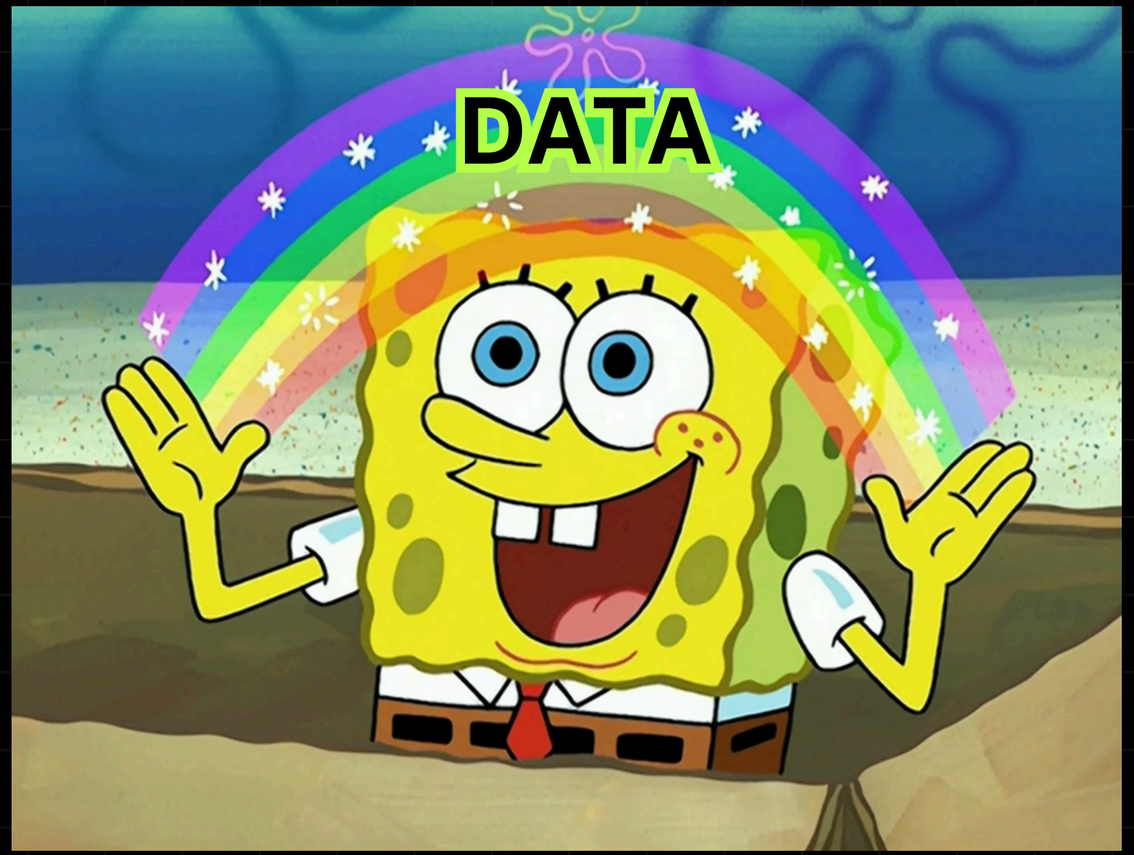
HARDHACK

Introduction to Hardware Hacking



CSEC
Gotta Hack 'em All

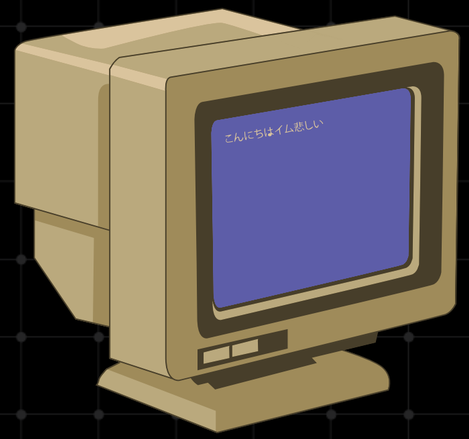
Well, Why do Hackers Hack?

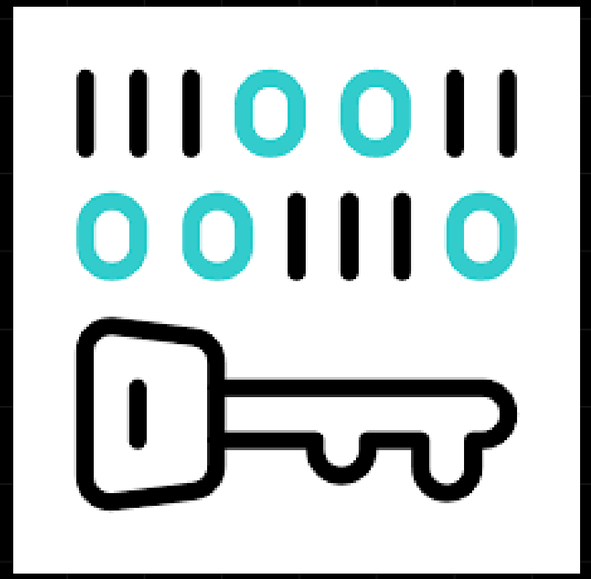


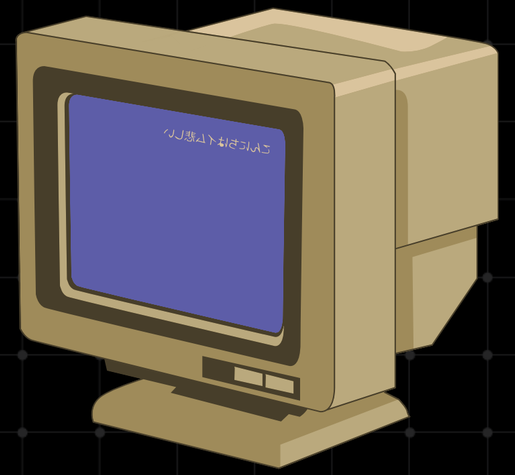
How do we send data-

SECURELY?

ENCRYPTION

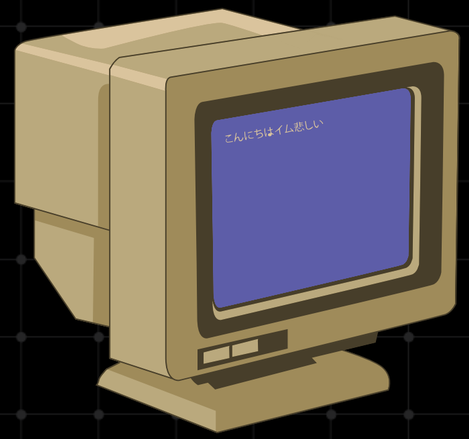


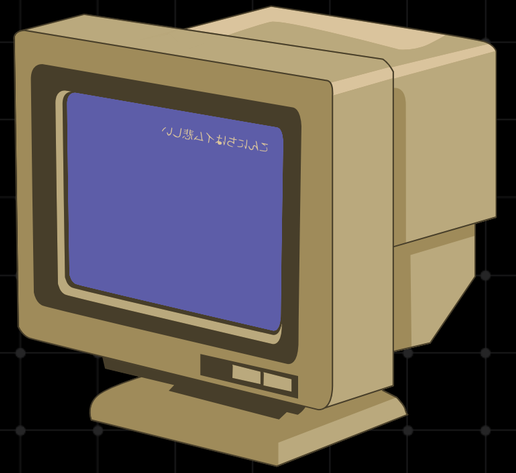




DECRYPTION

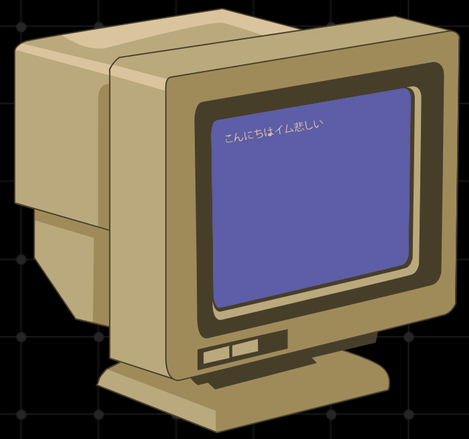
ENCRYPTION

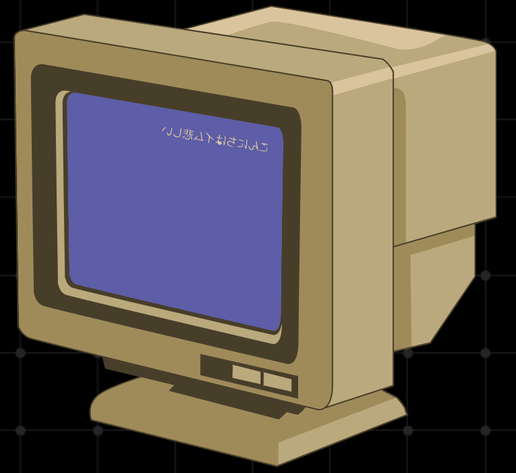




DECRYPTION

ENCRYPTION

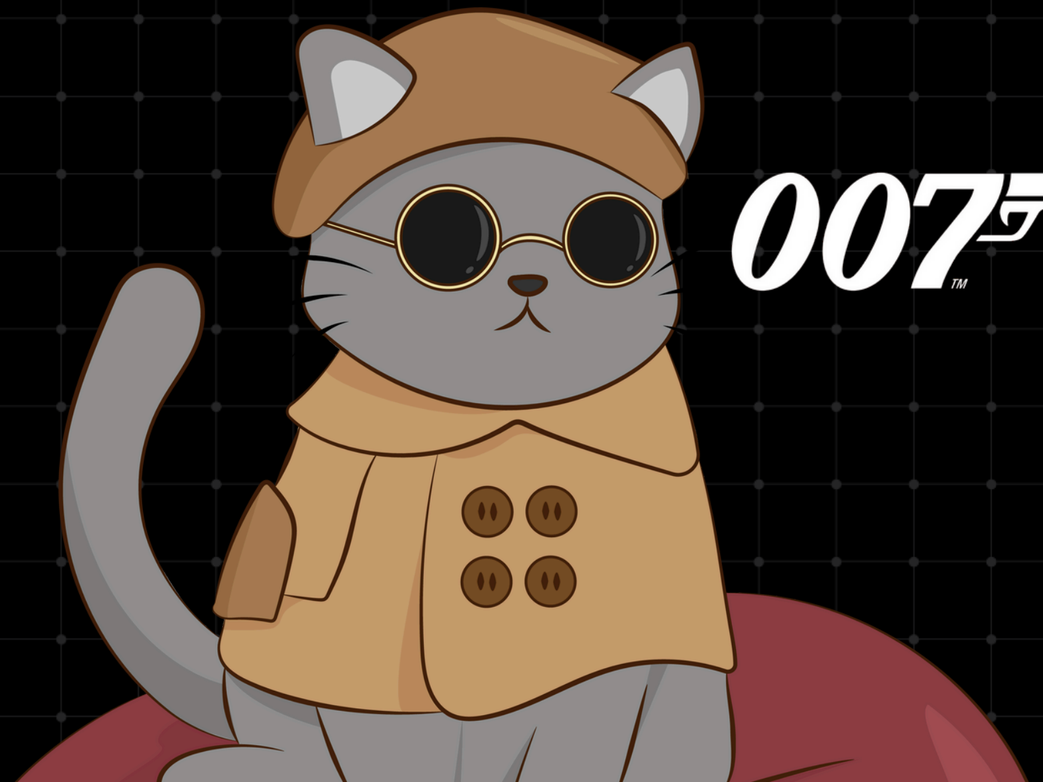




DECRYPTION

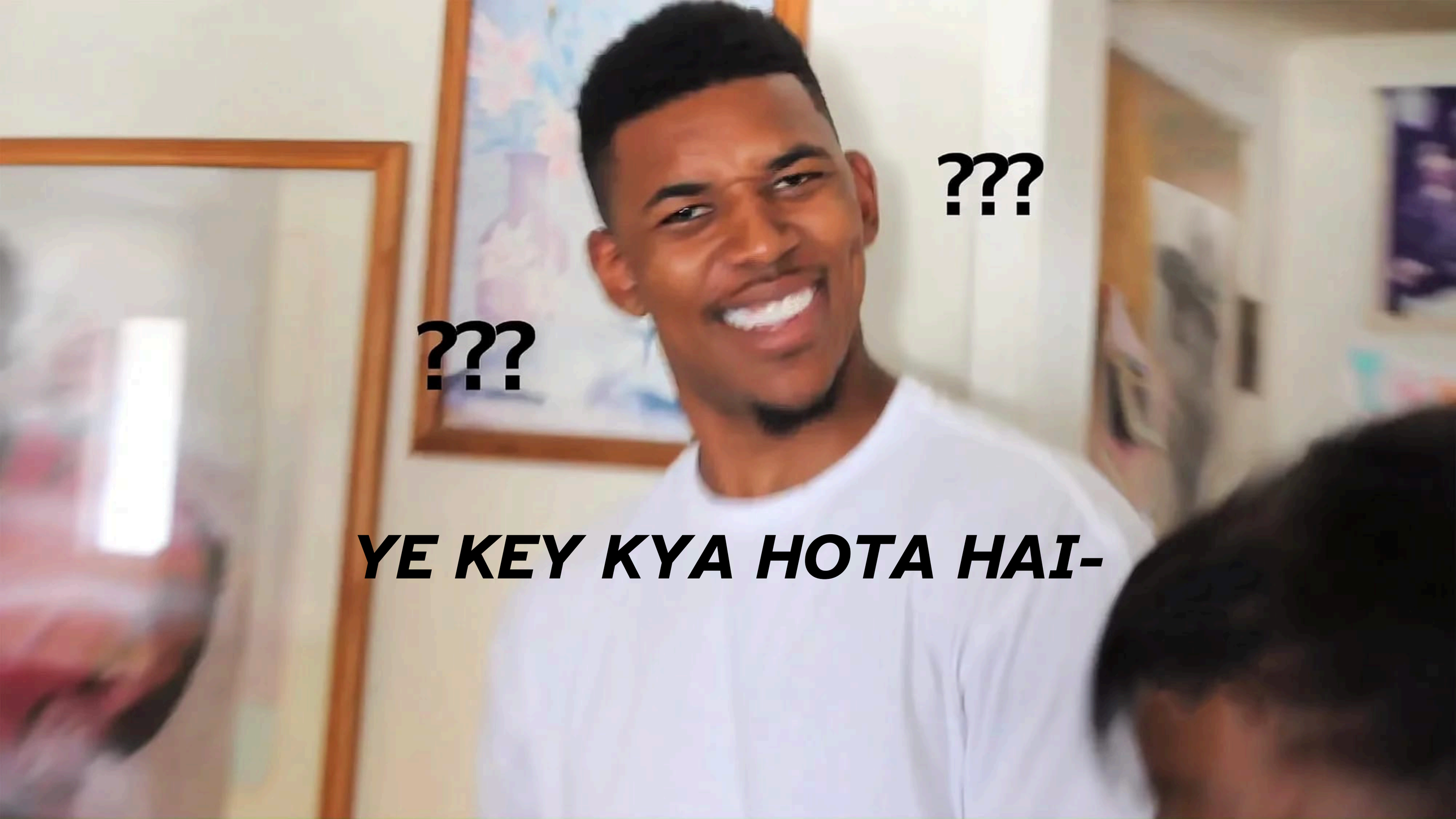
What do hackers do?

Try *whatever* they can to get the key.



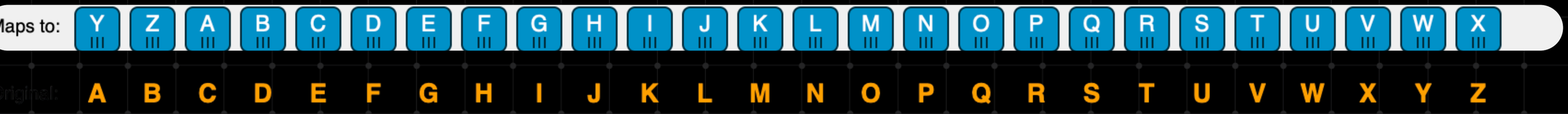
007™

Par Didi...


???
???
YE KEY KYA HOTA HAI-

DECRYPTION KEY

UCJAMKC RM FYPBUYPC FYAIGLE



“SHIFTING 2 LETTERS”

WELCOME TO HARDWARE HACKING

DECRYPTION KEY

```
&>ydd>yR &>nCEdQ Ex
Gvxw HBCRy dEwF >
nBcHvwRy- Ew wRBBxg
LBv n>wnFi
```

But, How exactly?

SIDE CHANNELS

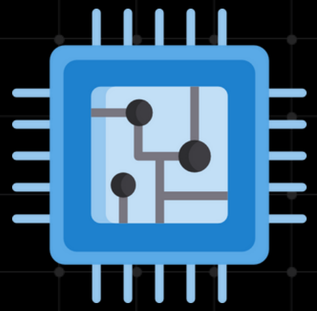
GERMAN **TANK PROBLEM**

But, How exactly?

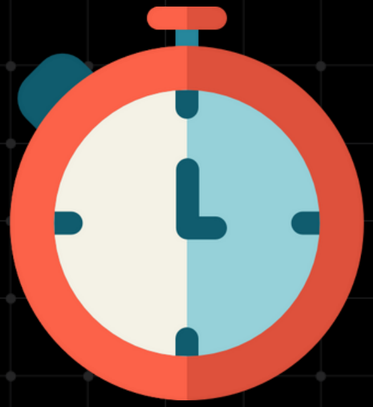
SIDE CHANNELS

TANK PROBLEM

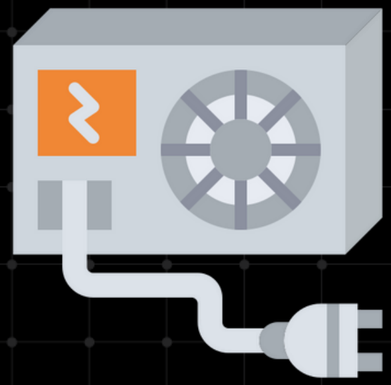
SIDE-CHANNEL ANALYSIS



TIMING ATTACKS



POWER ANALYSIS



TIMING ATTACKS

Let’s say,
Hypothetically,
You were to hack your TA’s phone.

This is completely hypothetical ~~for legal reasons~~

TIMING ATTACKS

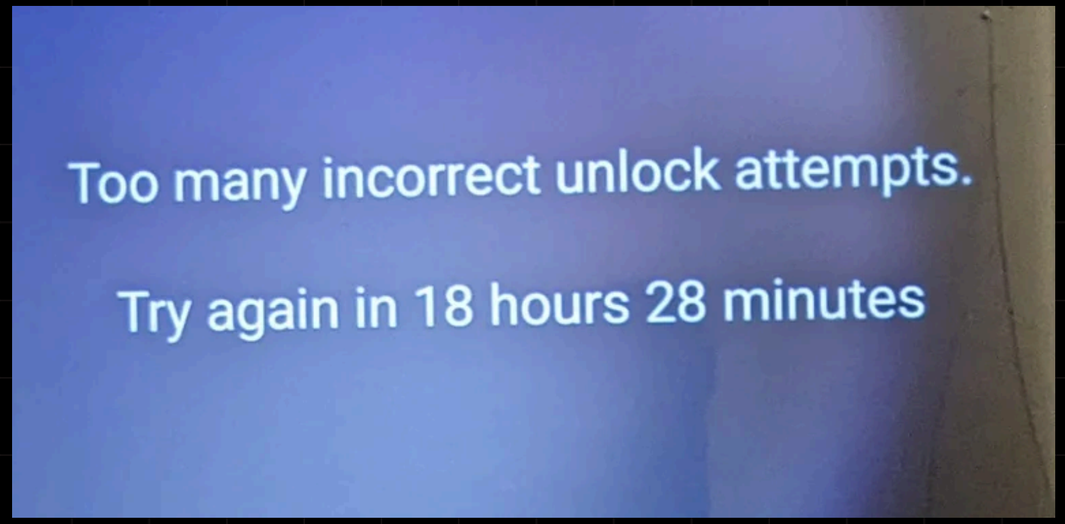
Now, how to crack this?

Well... You try all the combinations.

10000

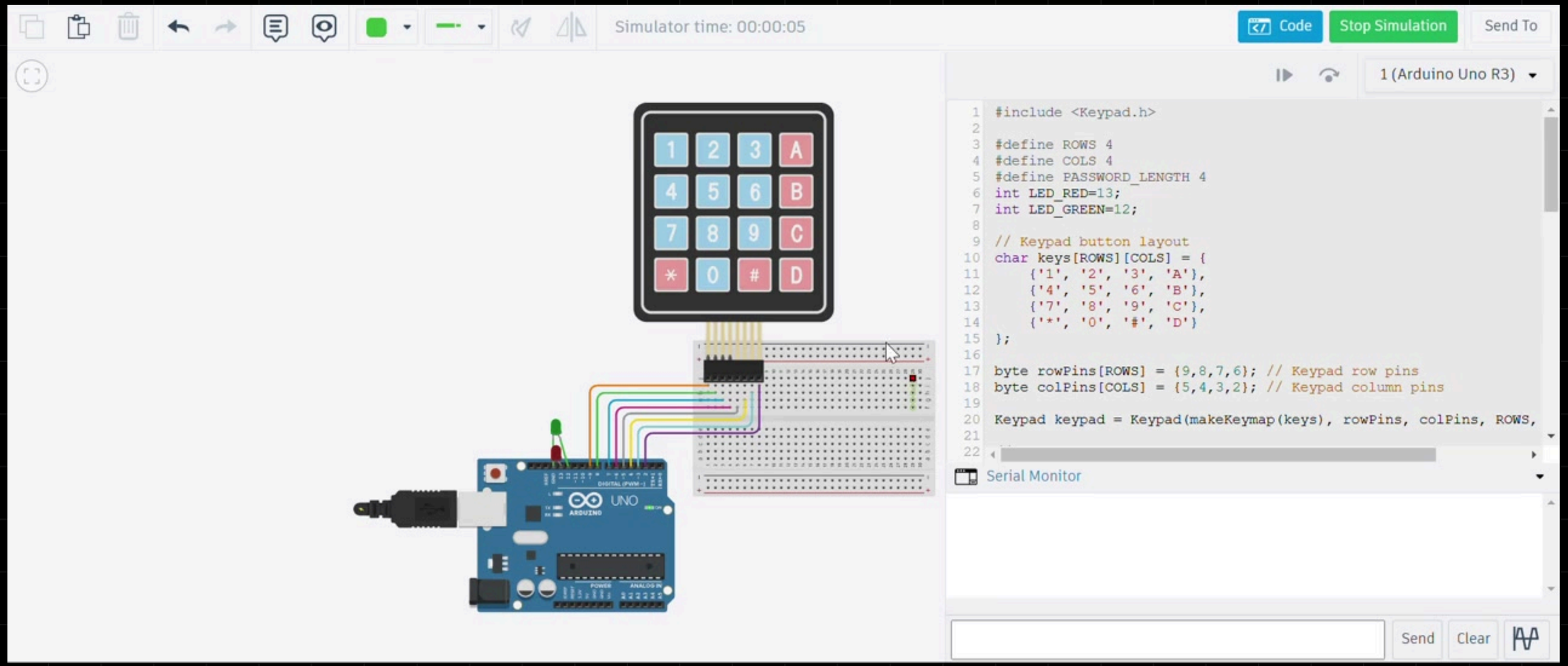
DIFFERENT COMBINATIONS

But this guy pops up



Hypothetically, for legal reasons

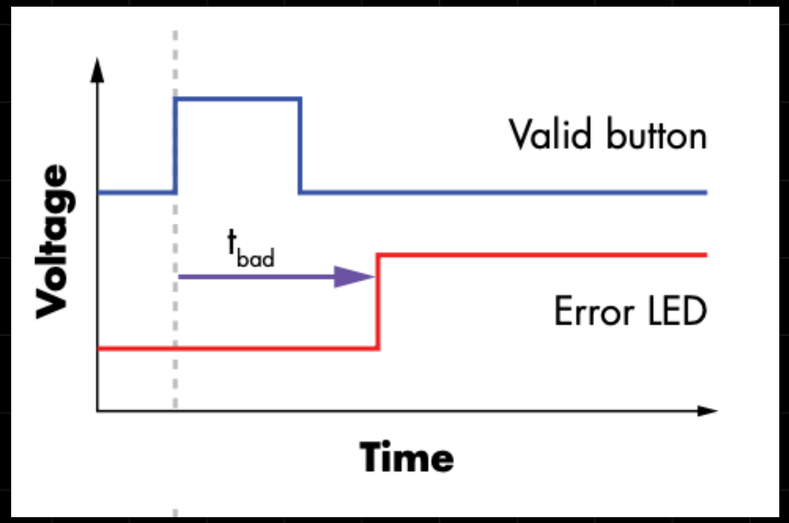
A SIMPLER EXAMPLE!

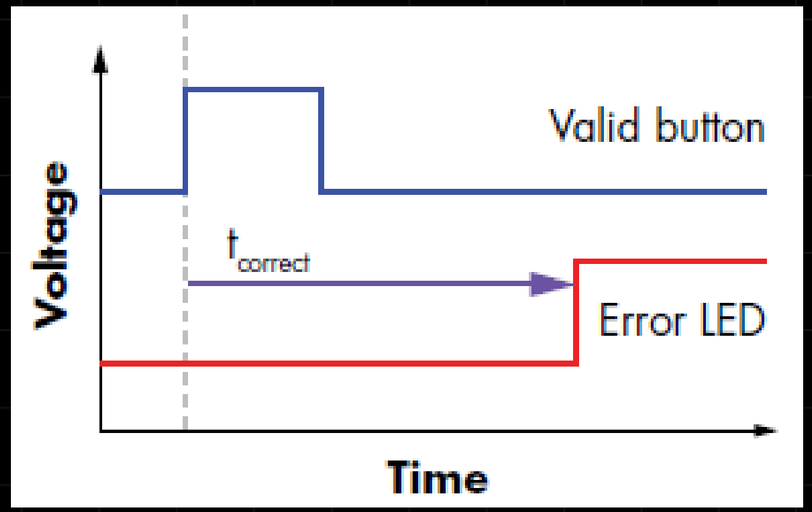


What does this code do?

```
int checkPassword() {
    int user_pin[] = {1, 1, 1, 1};
    int correct_pin[] = {5, 9, 8, 2};

    error_led_off();

    for(int i = 0; i < 4; i++) {
        user_pin[i] = read_button();
    }

    while(done_pressed() == 0);

    for(int i = 0; i < 4; i++) {
        if(user_pin[i] != correct_pin[i]) {
            error_led_on();
            return 0;
        }
    }

    return 1;
}
```

TIMING GRAPHS





GUESS: **0000**

first digit itself is wrong

5000

your luck was restricted to 1st digit :)

“Timing is Everything.”

3691

```c
#include <stdlib.h>

int checkPassword() {
    int user_pin[] = {1, 1, 1, 1};
    int correct_pin[] = {5, 9, 8, 2};

    error_led_off();

    int delay_index =  rand() % 4; // Returns a random integer from {0, 1, 2, 3}

    for(int i = 0; i < 4; i++) {
        user_pin[i] = read_button();
    }

    while(done_pressed() == 0);

    for(int i = 0; i < 4; i++) {

        if (i == delay_index) {  // Adding delay at the chosen index
            delay_ms(100); // Delay of 100 ms
        }

        if(user_pin[i] != correct_pin[i]) {
            error_led_on();
            return 0;
        }
    }
    return 1;
}
```

Random Delay

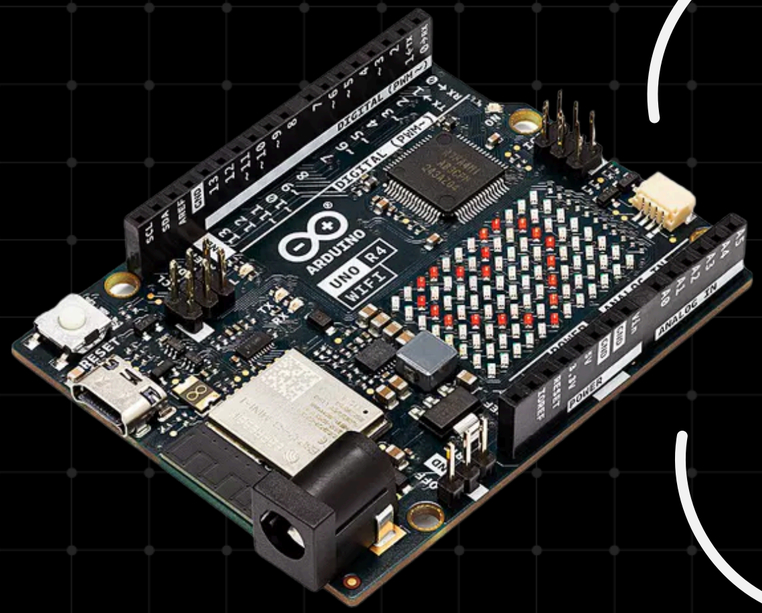
Oh, Crap.

Well, it appears timing isn’t good enough.

~~WOMP WOMP~~

That brings us to...

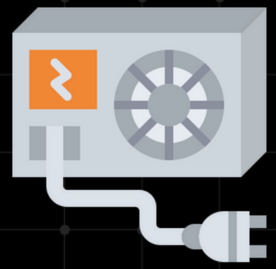
POWER ANALYSIS



ARITHMETIC OPERATIONS

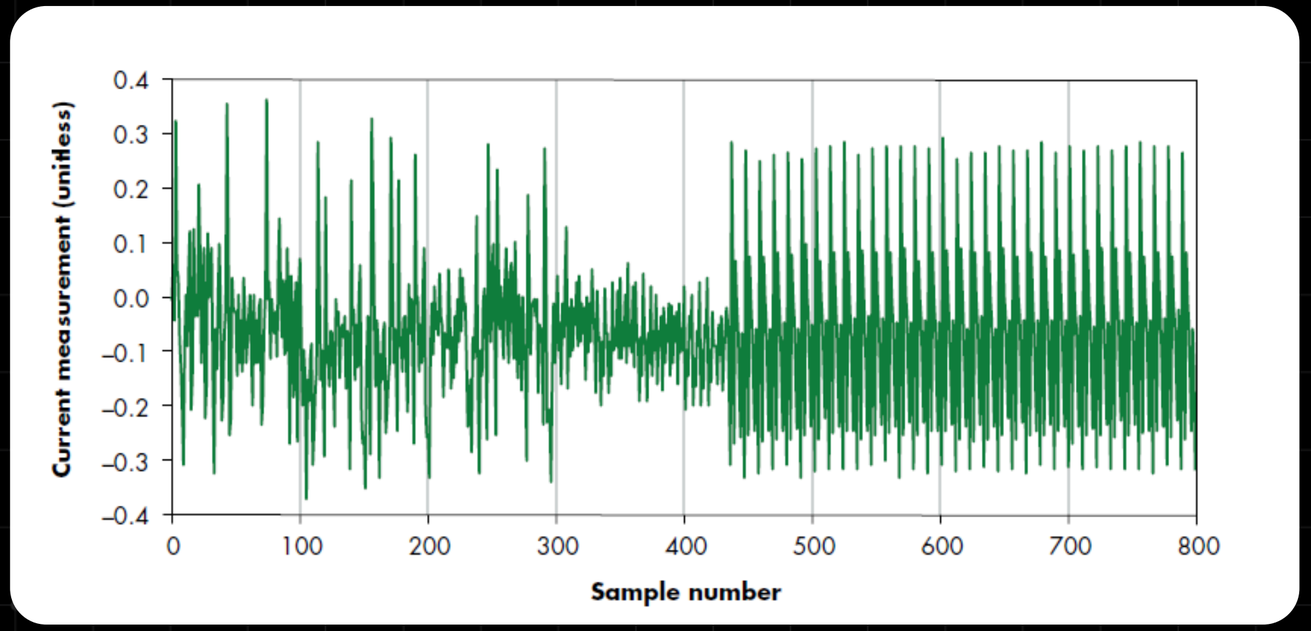
MEMORY OPERATIONS

DIFFERENT **POWER CONSUMPTION**



POWER ANALYSIS

Capturing power traces

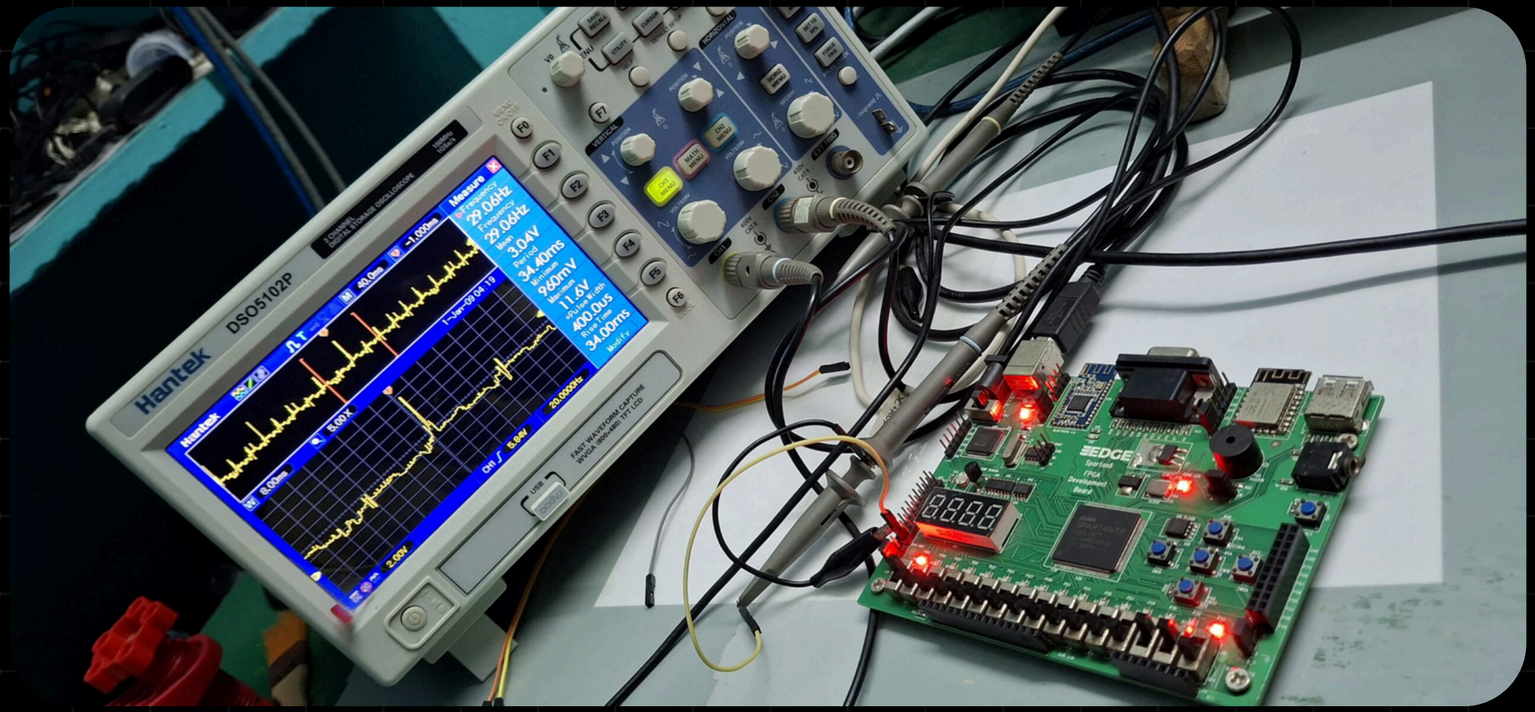


POWER CONSUMED BY THE MICROCONTROLLER OVER TIME

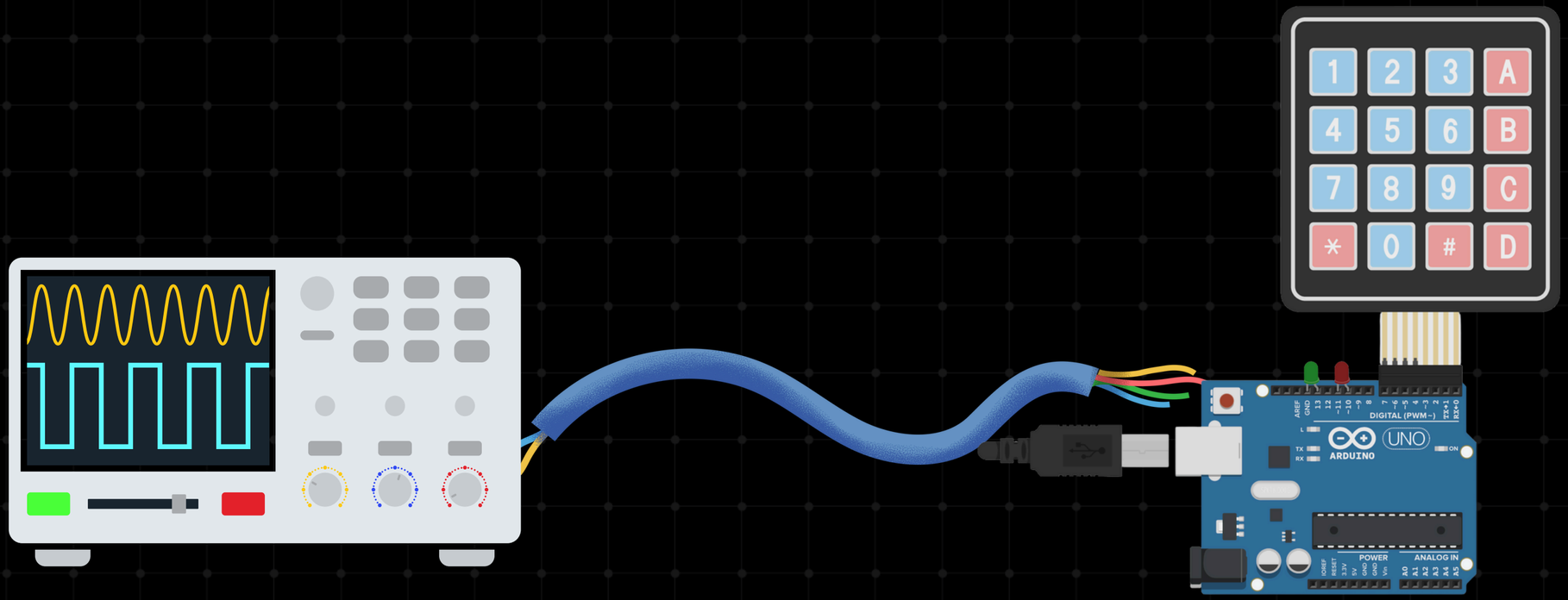
But How do we capture the power traces?


FLASHBACK
nick

OSCILLOSCOPE

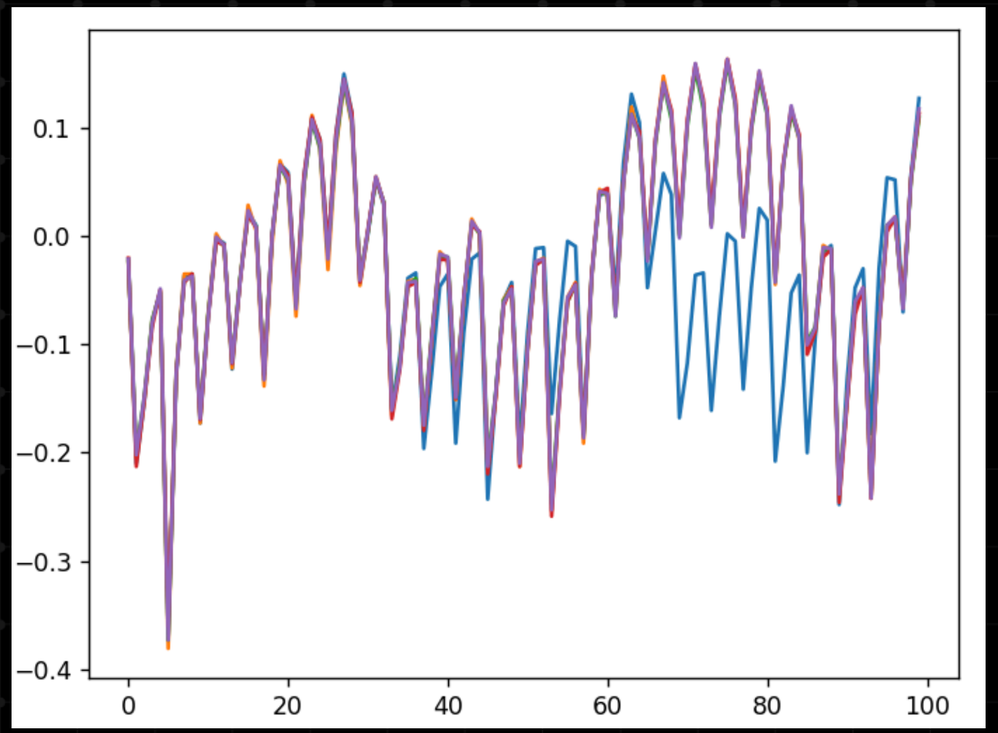


FULL SETUP

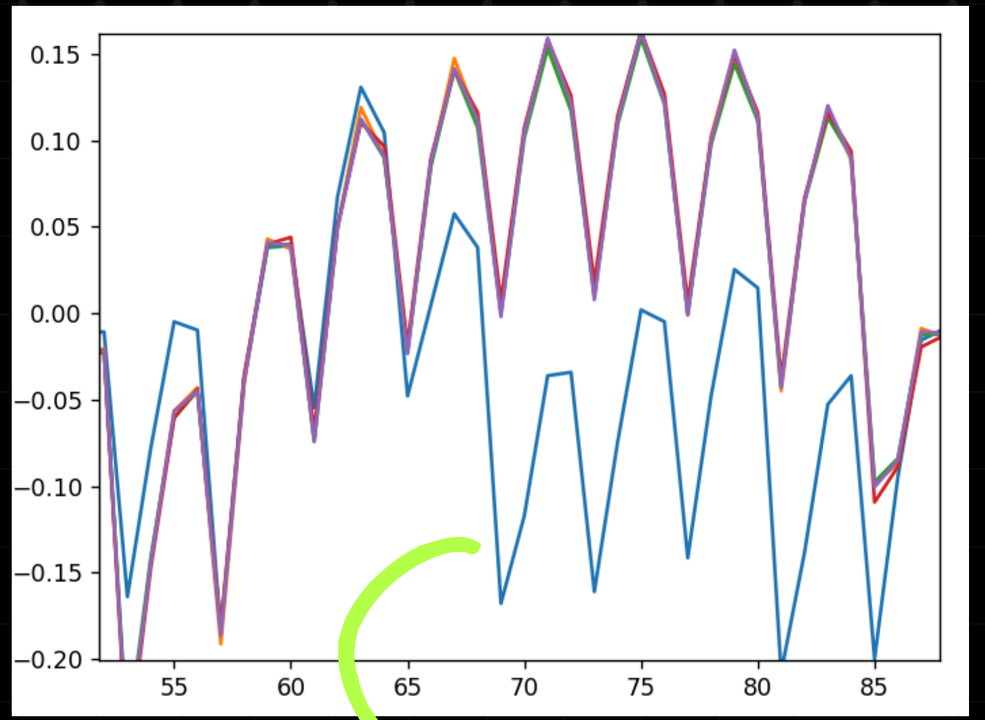


oscilloscope + Probes + Target device

How are they useful?

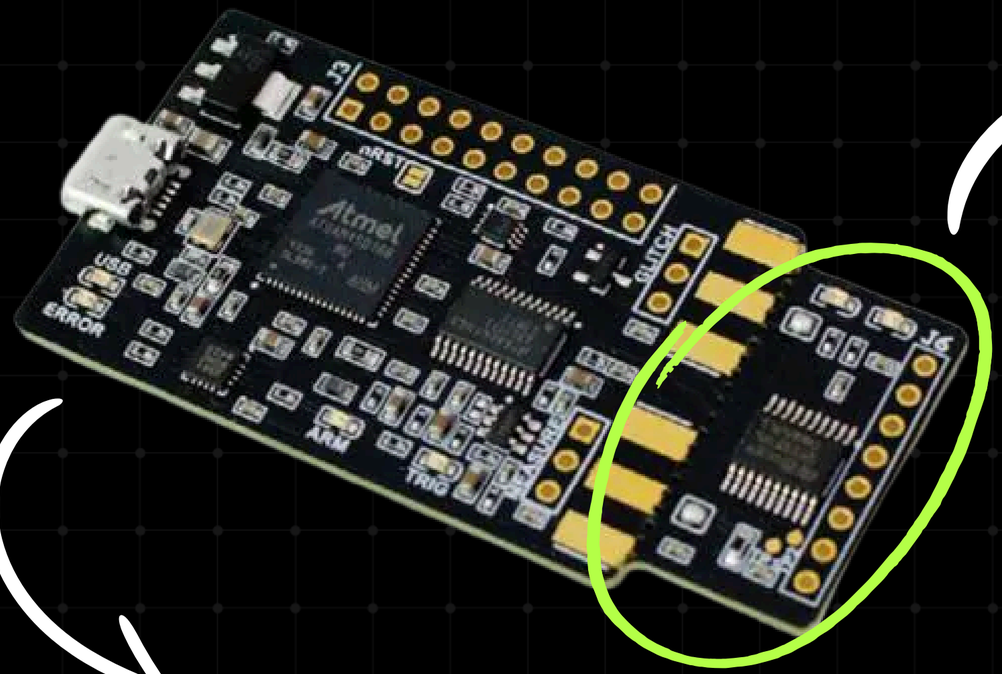


zoom



outlier

CHIPWHISPERER-NANO

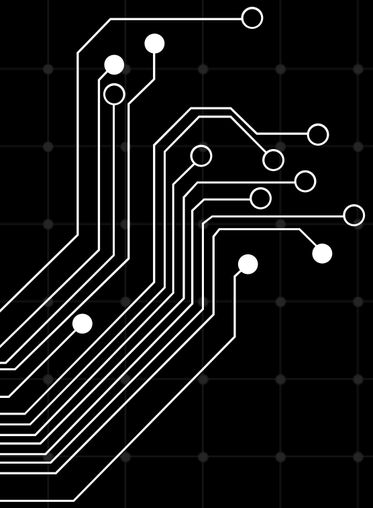


STM32
(Target Device)

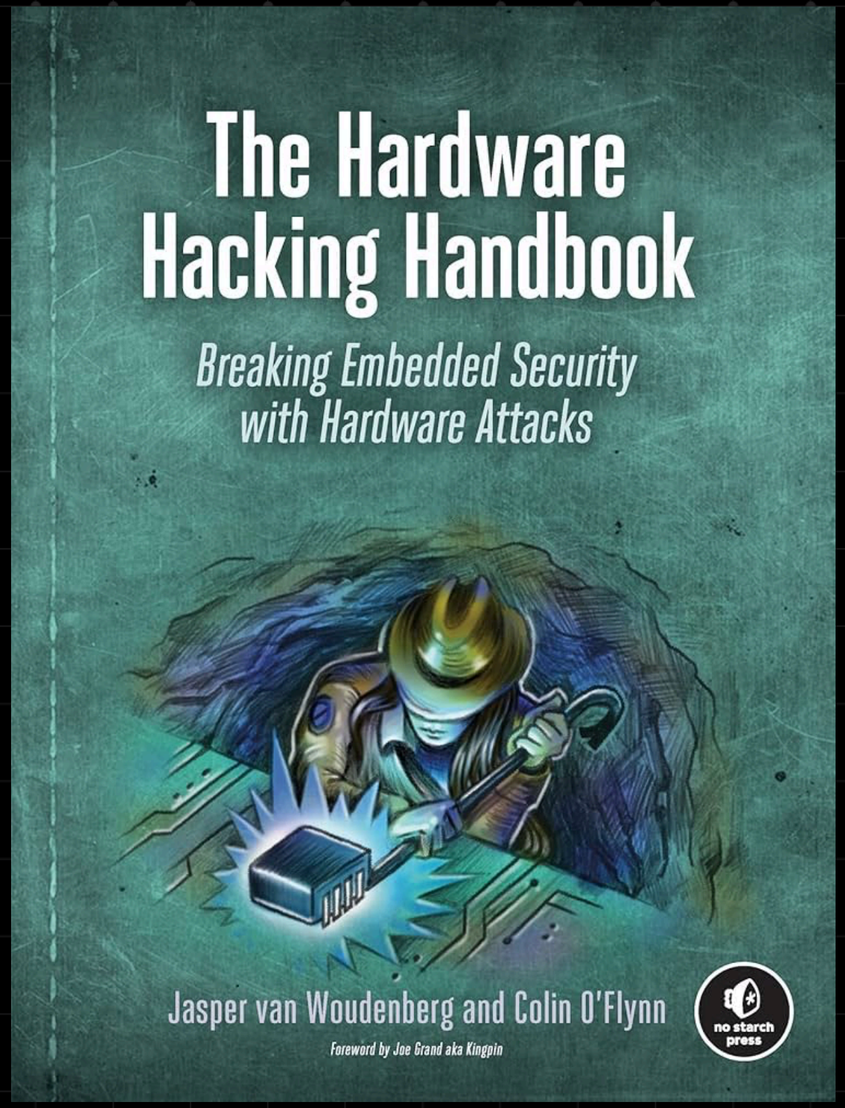
Measurement Section , which has a **microcontroller** for sampling and **ADC** for observing the power traces

NOTEBOOK LINK

tinyurl.com/2x5xe5j2



REFERENCES


The Hardware Hacking Handbook
Breaking Embedded Security with Hardware Attacks
Jasper van Woudenberg and Colin O'Flynn
Foreword by Joe Grand aka Kingpin
no starch press

HardHack - Day2

WhatsApp group