UCI University of California, Irvine

MITRE eCTF 2023-24

TIVA Programming & Soldering

Jinyao Xu (jinyaox@uci.edu)

Read Specification Sheet

1. Identify the System

2. Identify the Constraints (sizes, times, etc)

3. Identify the Requirements

BrainStorm

Driving Questions for the Day

1. LEETCODE 877 Medium:

Alice and Bob play a game with piles of stones. There are an **even** number of piles arranged in a row, and each pile has a **positive** integer number of stones piles[i]. The objective of the game is to end with the most stones. The **total** number of stones across all the piles is **odd**, so there are no ties.

2. Blackboard-Collaboration Question:

What are some key features for a 2 party encryption algorithm?

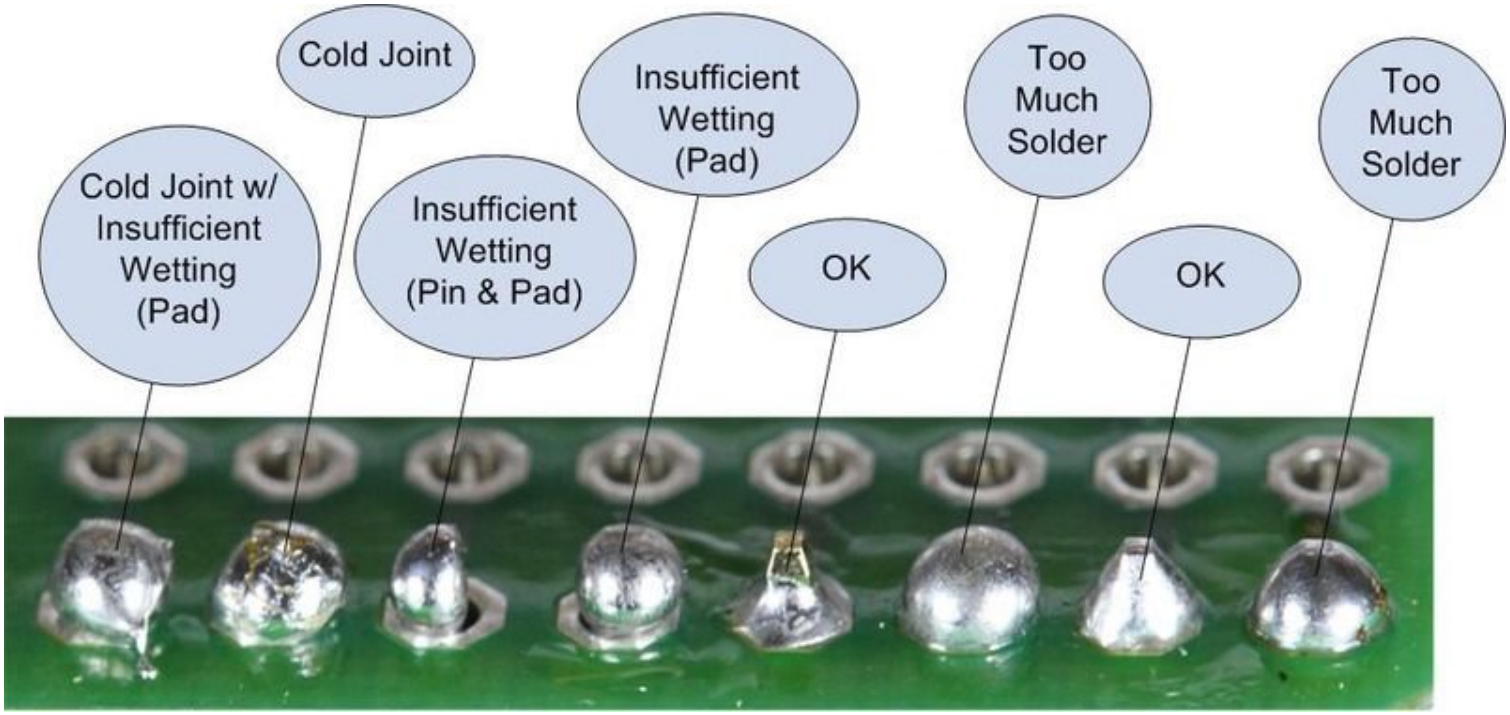
How to ensure these Features?

Fundamental of Soldering

1. Don't burn the house down

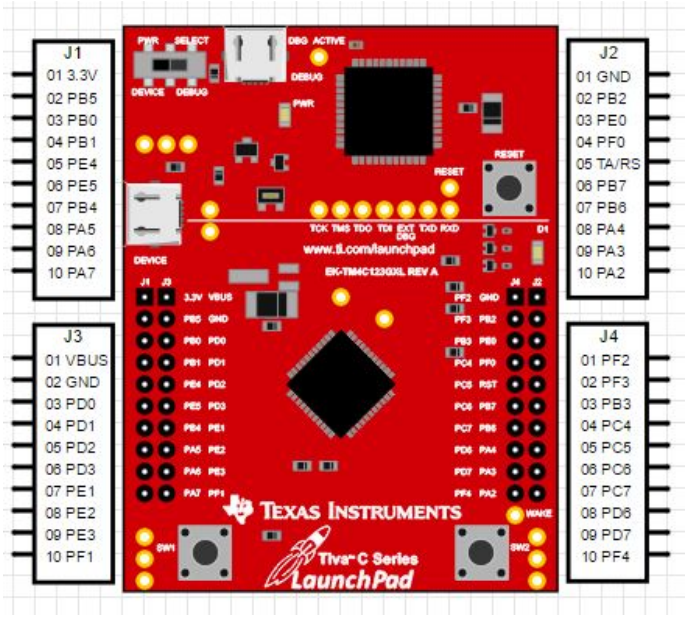
2. Avoid Short Circuit (VERY IMPORTANT)

3. Clean your hand afterwards



TIVA-C First Program (LED & GPIO)

1. Let's Test With LED FIRST (J101)



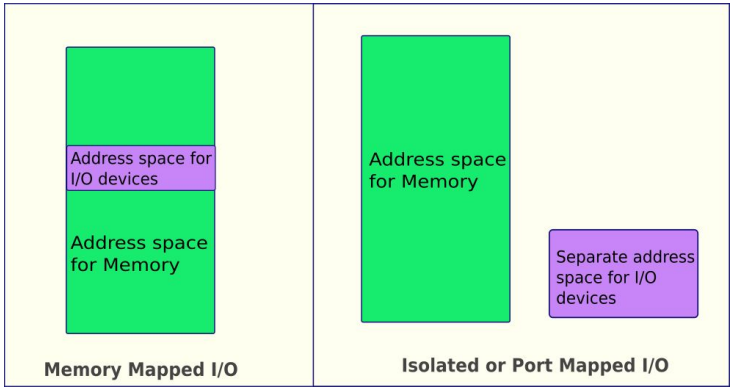
2. Memory Mapped Input-Output (IO)

   - let's take a look at the data sheet

   - or header file

3. TIME TO PROGRAM!

https://microcontrollerslab.com/use-gpio-pins-tm4c123g-tiva-launchpad/



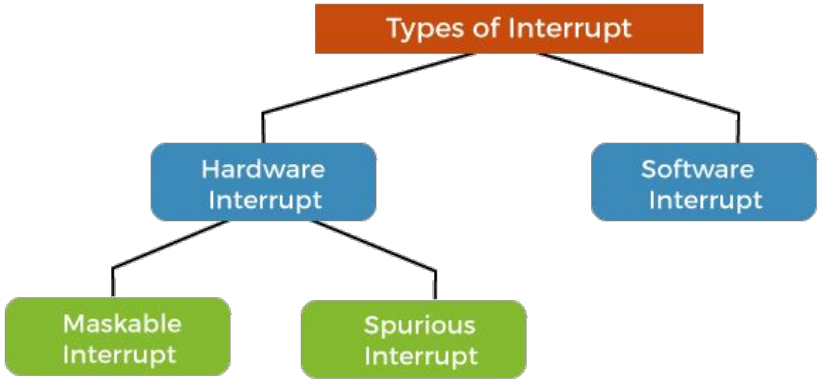
What are Interrupts? FOR MCU

Analogy: Clock Alarm

Advantages?

- Efficient

- No Time Delay (comp to query)



Disadvantages?

- Hard to program (with priority level)

https://microcontrollerslab.com/gpio-interrupts-tm4c123-tiva-launchpad-edge-level-triggered/

Fundamentals Of Encryption

- It's old, been there for a while.

- **It's a process, not a simple protocol**

    1. Key generation (key_space {all possible generated value})

    2. Encryption Algorithm

    3. Decrypt Algorithm (Necessary?)

A Bijective Function (XOR as an example, proof by Induction)

- Injective

- Surjective

Kerckhoffs Principle

The security of a cryptosystem must lie in the choice of its keys only; everything else (including the algorithm itself) should be considered public knowledge.