UCI University of California, Irvine

MITRE eCTF 2023-24

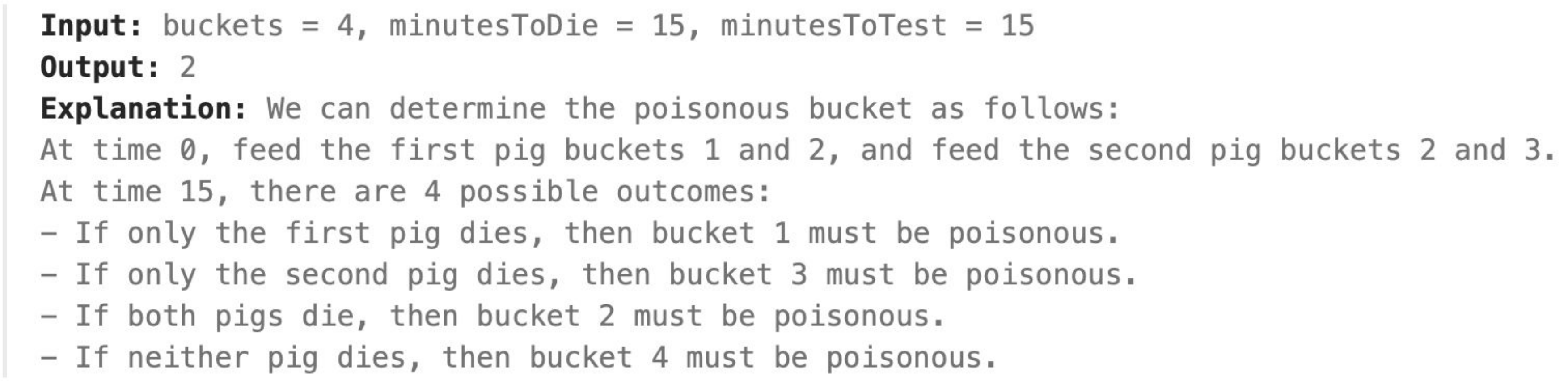
Encryption Libraries & Buffer Overflow Attacks

Jinyao Xu (jinyaox@uci.edu)

Driving Question for the Day (LEETCODE 458)

There are buckets buckets of liquid, where exactly one of the buckets is poisonous. To figure out which one is poisonous, you feed some number of (poor) pigs the liquid to see whether they will die or not. Ignore the time constraint for now.

SAMPLE INPUT:



```
Input: buckets = 4, minutesToDie = 15, minutesToTest = 15
Output: 2
Explanation: We can determine the poisonous bucket as follows:
At time 0, feed the first pig buckets 1 and 2, and feed the second pig buckets 2 and 3.
At time 15, there are 4 possible outcomes:
- If only the first pig dies, then bucket 1 must be poisonous.
- If only the second pig dies, then bucket 3 must be poisonous.
- If both pigs die, then bucket 2 must be poisonous.
- If neither pig dies, then bucket 4 must be poisonous.
```

- What problem can we reduce or mapping it to?
- IDEAS:
    - Induction (My original approach)? What’s even better? O(1) Complexity?

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.

SAT Problem (Karp’s 21 NP Complete)

F=(a V b)(a V -b)(-a V c)(-c V b) --> abc=111

F=(a V b)(a V -b)(-a V c)(-c V -a) --> NO SOLUTION

- *Decision Problem:* Is there an assignment to make it return True?
- *Dual Problem:* Find an assignment to make it return True?
- Both are NP-Complete, solvable with brute force.

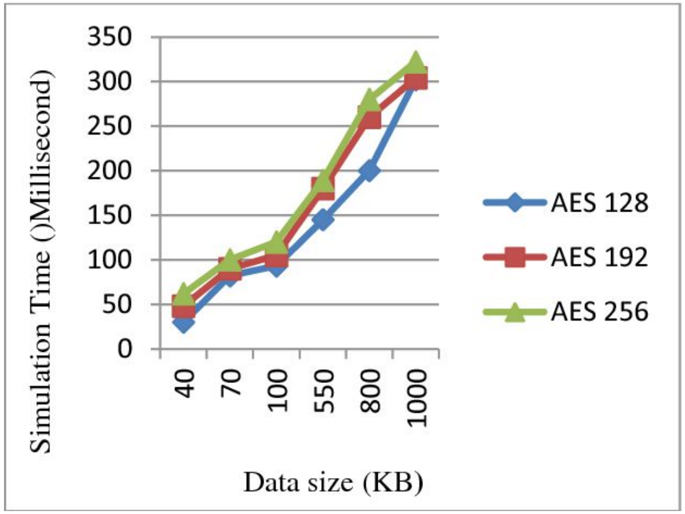
Proof: 1. Show it's NP

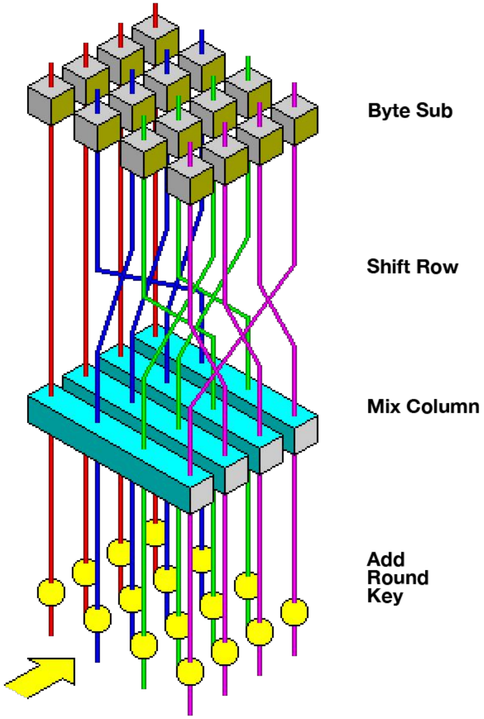
2. Show it's NP-Hard by reducing Circuit-SAT to it

AES (It is Actually NP Complete in BruteForcing)

- ***General Idea*: Linear Mapping and permutations of Data.**
- **Structured Encryption, Varies Length of Keys**
  - **Substitution:** The algorithm replaces the plain text with the encrypted text
  - **Shifting:** All the rows are shifted by one, except the first.
  - **Mixing:** Mix the columns
  - REPEAT THE PROCESS ABOVE

Evaluations:





USE AES ON MCU

- TinyCrypt AES Encryption Library (Produced by a firm called Intel)
- Github Main Page: https://github.com/intel/tinycrypt
- LOAD AND RUN!!

ISSUES REMAINING:

- **How to ensure key safety? How to generate random numbers**
- **How to generate Seeds?**
- **Proof:**
    - **No perfect Randomness (Direct Proof of Polynomial Func)**

LAB ACTIVITY

Goal:

Design a secured system that Reveals its ID only when user enters valid password.

Step 1: Idea Generation (UML, Software Engineering, Documentation Setup)

Step 2: Coding (Starter Code Provided)

Step 3: Security Analysis

* We will be using only 1 final device, it's a group project so let's generate