MysteryTwister C3

THE CRYPTO CHALLENGE CONTEST

Lightweight Introduction to Lattices – Part 1

Author: M. Dimitrov, B. Esslinger

May 2020

Introduction (1/5)

This challenge series accompanies the basic theory from a chapter called "LIGHTWEIGHT INTRODUCTION TO LATTICES". The chapter is part of the CrypTool Book [1].

Some lattice-based cryptography schemes are secure against quantum computers. Therefore, these constructions are relevant for current post-quantum cryptography research.

In this part of the challenge series we introduce systems of linear equations to find a hidden message in a picture.

Introduction (2/5)

A system of linear equations is set of linear equations, e.g.:

$$\begin{aligned} 2x + y &= 15 \\ x + y + z &= 20 \\ 3z &= 30 \end{aligned}$$

This system can easily be solved by pen and paper only – as shown in the next slide.

Introduction (3/5)

The last equation reveals the value of $z = 10$. Eliminating the variable z by replacing its value in the previous equations, we reduce the system to system of two unknown variables:

$$\begin{aligned} 2x + y &= 15 \\ x + y &= 10 \\ z &= 10 \end{aligned}$$

We can now subtract the second equation from the first one to receive x. Then, we end up with the following solution.

$$x = 5 \qquad y = 5 \qquad z = 10$$

Introduction (4/5)

Another way to solve the system of linear equation on slide 3 is to use *SageMath* (a computer-algebra system (CAS), which uses Python as scripting language)[2].

```
sage: x = var(’x’, domain=ZZ)
sage: y = var(’y’, domain=ZZ)
sage: z = var(’z’, domain=ZZ)
sage: solve([2*x + y == 15, x+y+z == 20,
      3*z == 30], (x,y,z))
[[x == 5, y == 5, z == 10]]
```

Introduction (5/5)

The following figure can also represent the system of linear equations on slide 3 .

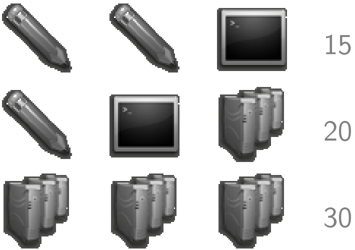

Figure: Visual Puzzle

Challenge (1/2)

Can you recover the hidden message in the picture puzzle in the figure on the following slide? Each symbol represents a distinct decimal digit. There is a balance that each left side equals the corresponding right side. Automate the process by using *SageMath*.

Hint: ASCII (American Standard Code for Information Interchange) is involved. The solution consists of 7 letters.

Challenge (2/2)

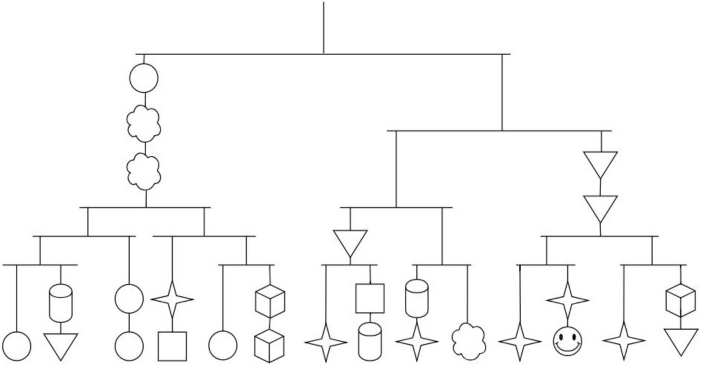

Figure: Puzzle Challenge (picture created by the author)

References

1. The CrypTool Book, Chapter 12.
   https://www.cryptool.org/en/ctp-documentation/ctbook
2. SageMath can either be downloaded or used online.
   - Download SageMath: https://www.sagemath.org/
   - SageMathCell: https://sagecell.sagemath.org/
   - CoCalc: https://cocalc.com/