MysteryTwister C3

THE CRYPTO CHALLENGE CONTEST

Lightweight Introduction to Lattices – Part 3

Author: M. Dimitrov, B. Esslinger

July 2020

Introduction (1/2)

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.

This challenge introduces an encryption scheme which uses systems of linear equations. Can you decrypt a message without knowing the key?

Introduction (2/2)

In the previous parts of this challenge series you learned how to solve a system of linear equations with the use of *SageMath* [2]. Now you can apply your knowledge to break an encryption scheme which we introduce on the following slides.

Challenge (1/3)

Alice and Bob established an "interesting" (but insecure) encryption scheme. Alice creates n equations with n variables and sends them to Bob over an insecure channel using two packets. The first packet consists of all the coefficients used in the equations in form of a matrix without any changes. However, the second packet consists of all the right sides of the equations in scrambled order. Their shared secret key consists of the original indexes of the scrambled right sides of the equations.

Challenge (2/3)

Having the secret key, Bob can unscramble the right sides of the equations and recover the unknown variables. Then, he multiplies all the recovered variables and the product is the decrypted message and also our solution.

Hint: They were using `leet` language to create or read the final number. For example, the word `sage` in leet language is `5463`.

Please hand in only the number (the product) as the solution.

Challenge (3/3)

Eve captured the following two packets P_1 and P_2:

$$P_1 = \begin{pmatrix} 33 & 79 & 29 & 41 & 47 \\ 79 & 27 & 39 & 79 & 44 \\ 90 & 83 & 58 & 1 & 90 \\ 38 & 32 & 13 & 15 & 96 \\ 72 & 82 & 88 & 83 & 23 \end{pmatrix}$$

$$P_2 = [\,73300,\ 167887,\ 243754,\ 254984,\ 458756\,]$$

Can you recover the original message?

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/`