

Introduction to LLL “Cryptography”

Di Santi Giovanni

May 10, 2021

Contents

1	Introduction to Lattices	2
1.1	Vector Spaces	2
1.2	Lattices	2
2	LLL	3
2.1	Purpose	3
2.2	Algorithm	3
3	Applications	4
3.1	Attack Knapsack	4
3.2	Attack RSA	4

Chapter 1

Introduction to Lattices

1.1 Vector Spaces

Definition 1.1.1 *Vector spaces.*

A vector space V is a subset of \mathbb{R}^m with the property that

$$\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_k v_k \text{ with } \alpha_1, \dots, \alpha_k \in \mathbb{R}$$

1.2 Lattices

Chapter 2

LLL

2.1 Purpose

2.2 Algorithm

Chapter 3

Applications

3.1 Attack Knapsack

3.2 Attack RSA

End of Paper

gg^2

Bibliography