UNIVERSITAS
GADJAH MADA
Serangan Reduksi Latis LLL (Lenstra-Lenstra-Lovasz) pada Sistem Kriptografi NTRU (Nth Degree Truncated Polynomial Ring)
SAIFULLAH ALI, Prof. Dr.rer.nat. Indah Emilia Wijayanti, M.Si.
Universitas Gadjah Mada, 2021 | Diunduh dari http://etd.repository.ugm.ac.id/

DAFTAR ISI

HALAMAN JUDUL . . . . . **i**
HALAMAN PENGESAHAN . . . . . **ii**
HALAMAN PERNYATAAN . . . . . **iii**
HALAMAN PERSEMBAHAN . . . . . **iv**
HALAMAN MOTTO . . . . . **v**
PRAKATA . . . . . **vi**
DAFTAR ISI . . . . . **ix**
DAFTAR TABEL . . . . . **xi**
DAFTAR GAMBAR . . . . . **xii**
DAFTAR LAMBANG . . . . . **xiii**
INTISARI . . . . . **xv**
ABSTRACT . . . . . **xvi**
I PENDAHULUAN **1**
1.1. Latar Belakang Masalah 1
1.2. Tujuan dan Manfaat Penelitian 2
1.3. Tinjauan Pustaka 3
1.4. Metodologi Penelitian 4
1.5. Sistematika Penulisan 5
II DASAR TEORI **6**
2.1. Konsep Dasar Ring 6
2.1.1. Ring dan Subring 6
2.1.2. Pembentukan Ring Faktor dari Suatu Ideal 13
2.1.3. Ring Polinomial dan Lapangan Hingga 14
2.1.4. Siklik dan *Centered Lift* 26
2.2. Ruang Vektor 29
III Latis **38**
3.1. Konsep Dasar Latis 38
3.2. Permasalahan Latis 52
3.3. Vektor Terpendek 54
IV Sistem Kriptografi NTRU **61**
4.1. Kriptografi 61
4.2. Deskripsi Sistem Kriptografi NTRU 65
4.2.1. Sistem Kriptografi NTRU 65

UNIVERSITAS
GADJAH MADA
Serangan Reduksi Latis LLL (Lenstra-Lenstra-Lovasz) pada Sistem Kriptografi NTRU (Nth Degree Truncated Polynomial Ring)
SAIFULLAH ALI, Prof. Dr.rer.nat. Indah Emilia Wijayanti, M.Si.
Universitas Gadjah Mada, 2021 | Diunduh dari http://etd.repository.ugm.ac.id/

4.2.2. Cara Kerja NTRU 68
4.3. Latis NTRU 74
V Serangan Sistem Krptografi NTRU dengan Reduksi Latis 80
5.1. Reduksi Latis 80
5.1.1. Reduksi Latis LLL 83
5.1.2. Algoritma Babai 88
5.1.3. Serangan Sistem Kriptografi NTRU dengan LLL 91
5.2. Estimasi Waktu Pemecahan NTRU 251 dengan Simulasi 94
VI PENUTUP 97
6.1. Kesimpulan 97
6.2. Saran 98
DAFTAR PUSTAKA 100
A SKRIP PROGRAM PYTHON POLINOMIAL 101
B SKRIP PROGRAM PYTHON NTRU 107
C SKRIP PROGRAM PYTHON EKSEKUTOR NTRU 111
D HASIL RUNNING PROGRAM EKSEKUTOR NTRU 113
E SKRIP PROGRAM PYTHON LLL 114
F SKRIP PROGRAM PYTHON EKSEKUTOR LLL 122
G HASIL RUNNING PROGRAM EKSEKUTOR LLL 124