



DAFTAR ISI

| | |
|--|-------------|
| HALAMAN JUDUL | i |
| HALAMAN PENGESAHAN | ii |
| HALAMAN PERNYATAAN | iii |
| HALAMAN PERSEMBAHAN | iv |
| HALAMAN MOTTO | v |
| PRAKATA | vi |
| DAFTAR ISI | ix |
| DAFTAR TABEL | xii |
| DAFTAR GAMBAR | xiii |
| DAFTAR LAMBANG | xiv |
| DAFTAR LAMBANG | xv |
| INTISARI | xvi |
| ABSTRACT | xvii |
| 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. Ideal dan Ring Faktor | 12 |
| 2.1.3. Ring Polinomial dan Lapangan Hingga | 18 |
| 2.1.4. Siklik dan <i>Centered Lift</i> | 26 |
| 2.2. Ruang Vektor | 29 |
| 2.3. Konsep Dasar Modul | 37 |
| 2.3.1. Modul dan Submodul | 37 |
| 2.3.2. Modul Faktor | 42 |
| 2.3.3. Pembangun Modul | 44 |
| 2.4. Jarak Hamming dan Berat Hamming | 45 |
| III SISTEM KRIPTOGRAFI NTRU DAN MATRU | 49 |
| 3.1. Kriptografi | 49 |



| | | |
|---|---|------------|
| 3.2. | Sistem Kriptografi NTRU | 54 |
| 3.2.1. | Sistem Kriptografi NTRU | 54 |
| 3.2.2. | Cara Kerja NTRU | 57 |
| 3.3. | Sistem Kriptografi MaTRU | 58 |
| 3.3.1. | Sistem Kriptografi MaTRU | 59 |
| 3.3.2. | Cara Kerja MaTRU | 64 |
| 3.3.3. | Pemilihan Parameter MaTRU | 65 |
| 3.3.3.1 | Pemilihan Parameter Pasangan (f, g) dan (Φ, Ψ) . . | 66 |
| 3.3.3.2 | Pemilihan Matriks A dan B | 67 |
| 3.3.3.3 | Pemilihan Matriks w | 69 |
| 3.3.4. | Pilihan Parameter untuk Sistem Kriptografi MaTRU | 69 |
| 3.4. | Perbandingan Sistem Kriptografi MaTRU dan NTRU | 69 |
| IV ANALISIS DAN PENINGKATAN SISTEM KRIPTOGRAFI MATRU | | 71 |
| 4.1. | Latar Belakang Analisis Sistem Kriptografi MaTRU | 71 |
| 4.2. | Analisis dan Peningkatan Parameter p Pada Sistem Kriptografi Ma- TRU | 72 |
| 4.2.1. | Analisis Parameter p Pada Sistem Kriptografi MaTRU | 72 |
| 4.2.1.1 | Nilai parameter $p = 2$ dan df bernilai genap | 73 |
| 4.2.1.2 | Nilai parameter $p = 2$ dan df bernilai ganjil | 77 |
| 4.2.1.3 | Nilai Parameter $p = 3$ | 77 |
| 4.2.1.4 | Nilai parameter $p = 3$ | 82 |
| 4.2.1.5 | Nilai parameter $p = 2$ | 84 |
| 4.2.2. | Ringkasan Analisis Parameter p Pada Sistem Kriptografi MaTRU | 85 |
| 4.2.3. | Peningkatan Parameter p Pada Sistem Kriptografi MaTRU | 86 |
| 4.3. | Analisis dan Peningkatan Parameter q Pada Sistem Kriptografi Ma- TRU | 91 |
| 4.4. | Analisis dan Peningkatan Parameter n Pada Sistem Kriptografi Ma- TRU | 93 |
| 4.4.1. | Nilai Parameter $n = 6$ | 94 |
| 4.4.2. | Nilai Parameter $n = 8$ | 94 |
| 4.4.3. | Nilai Parameter $n = 11$ | 95 |
| 4.4.4. | Nilai Parameter $n = 16$ | 95 |
| 4.4.5. | Nilai Parameter $n = 18$ | 96 |
| 4.5. | Ringkasan Modifikasi dari Sistem Kriptografi MaTRU | 97 |
| V PENUTUP | | 100 |
| 5.1. | Kesimpulan | 100 |



| | |
|--|------------|
| 5.2. Saran | 101 |
| DAFTAR PUSTAKA | 102 |
| A SKRIP PROGRAM MENGKONVERSI BINARI KE STRING | 103 |
| B SKRIP PROGRAM MENGKONVERSI STRING KE BINARI | 105 |