DAFTAR ISI

HALAMAN JUDUL . . . . . **i**
HALAMAN PENGESAHAN . . . . . **ii**
HALAMAN PERNYATAAN BEBAS PLAGIASI . . . . . **iii**
HALAMAN PERSEMBAHAN . . . . . **iv**
HALAMAN MOTTO . . . . . **v**
PRAKATA . . . . . **vi**
DAFTAR ISI . . . . . **vii**
DAFTAR TABEL . . . . . **ix**
DAFTAR GAMBAR . . . . . **x**
DAFTAR LAMBANG . . . . . **xi**
INTISARI . . . . . **xiii**
ABSTRACT . . . . . **xiv**
I PENDAHULUAN **1**
1.1. Latar Belakang Masalah 1
1.2. Rumusan Masalah 3
1.3. Tujuan dan Manfaat Penelitian 3
1.4. Tinjauan Pustaka 4
1.5. Metodologi Penelitian 5
1.6. Sistematika Penulisan 6
II LANDASAN TEORI **8**
2.1. Bilangan Bulat 8
2.1.1. Relasi Habis Membagi 8
2.1.2. Faktor Persekutuan Terbesar dan Algoritma Euclid 10
2.1.3. Kongruensi 13
2.1.4. Algoritma Perluasan Euclid 15
2.1.5. Teorema Wilson dan Teorema Kecil Fermat 18
2.1.6. Representasi Bilangan Bulat 20
2.2. Struktur Aljabar 23
2.2.1. Relasi Biner 23
2.2.2. Grup 26
2.2.3. Ring dan Lapangan 32
2.3. Kriptografi 37
III KURVA ELIPTIK **40**

3.1. Kurva Eliptik atas Lapangan Bilangan Real 40
3.2. Kurva Eliptik atas Lapangan Bilangan Bulat Modulo p 54
3.3. Endomorfisma Grup Kurva Eliptik dan Teorema Hasse 62
3.4. Order Grup $E(\mathbb{Z}_p)$ 72
3.4.1. Algoritma Naive 72
3.4.2. Algoritma Shank 78
IV SKEMA TANDA TANGAN DIGITAL 90
4.1. Masalah Logaritma Diskrit 92
4.1.1. Algoritma Pollard-Rho 94
4.1.2. Algoritma Pohlig-Hellman 99
4.2. Fungsi Hash Kriptografik 105
4.2.1. Secure Hash Algorithm (SHA) 108
4.2.2. Masalah Ulang Tahun 113
4.3. Algoritma Tanda Tangan Digital Kurva Eliptik 118
V IMPLEMENTASI DAN UJI COBA 125
5.1. Sarana Implementasi 125
5.2. Implementasi Skema Tanda Tangan Digital Kurva Eliptik 126
5.3. Uji Coba 130
5.3.1. Perbandingan dari Algoritma Naive dan Algoritma Shank . 130
5.3.2. Uji Coba Algoritma Tanda Tangan Digital Kurva Eliptik . . 132
VI KESIMPULAN DAN SARAN 136
6.1. Kesimpulan 136
6.2. Saran 137
DAFTAR PUSTAKA 139
A TABEL PERBANDINGAN WAKTU DARI ALGORITMA NAIVE DAN ALGORITMA SHANK 141
B SKRIP PROGRAM MATLAB 144
C SKRIP PROGRAM PYTHON 146