UNIVERSITAS
GADJAH MADA
Enkripsi dan Dekripsi Citra Digital Grayscale Menggunakan Kriptografi Kurva Eliptik Diffie-Hellman
RESTI ANISA LESTARI, Dr. Aluysius Sutjijana, M.Sc.
Universitas Gadjah Mada, 2022 | 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 . . . . . **viii**
DAFTAR TABEL . . . . . **x**
DAFTAR LAMBANG . . . . . **xi**
INTISARI . . . . . **xii**
ABSTRACT . . . . . **xiii**
I PENDAHULUAN **1**
1.1. Latar Belakang Masalah 1
1.2. Tujuan dan Manfaat Penelitian 2
1.3. Tinjauan Pustaka 2
1.4. Metodologi Penelitian 3
1.5. Sistematika Penulisan 3
II DASAR TEORI **5**
2.1. Struktur Aljabar 5
2.1.1. Grup 5
2.1.2. Ring dan Lapangan 13
2.2. Kriptografi 20
2.2.1. Pendahuluan 20
2.2.2. Enkripsi 21
2.2.3. Dekripsi 21
2.2.4. Kriptosistem Sederhana 21
2.2.5. Kriptosistem Kompleks 23
2.2.6. Algoritma Simetris 25
2.2.7. *Diffie-Hellman Key Exchange Algorithm* 26
2.3. Citra Digital 28
III Kurva Eliptik **31**
3.1. Basis Teori 31
3.1.1. Persamaan Weierstrass 31

UNIVERSITAS
GADJAH MADA
Enkripsi dan Dekripsi Citra Digital Grayscale Menggunakan Kriptografi Kurva Eliptik Diffie-Hellman
RESTI ANISA LESTARI, Dr. Aluysius Sutjijana, M.Sc.
Universitas Gadjah Mada, 2022 | Diunduh dari http://etd.repository.ugm.ac.id/

3.2. Kurva Eliptik Atas Lapangan Bilangan Real 31
3.2.1. Aturan Grup Pada Kurva Eliptik Atas Lapangan Bilangan Real 33
3.3. Kurva Eliptik Atas Lapangan Bilangan Bulat Modulo p 45
3.4. Endomorfisma Grup Kurva Eliptik dan Teorema Hasse 50
3.5. Order Grup $E(\mathbb{Z}_p)$ 58
3.5.1. Algoritma Naive 58
3.5.2. Algoritma Shank 62
IV SKEMA KRIPTOGRAFI KURVA ELIPTIK DIFFIE-HELLMAN . . 66
4.1. Perancangan Kurva Eliptik di Bidang $\mathbb{Z}_p$ 66
4.1.1. Pembuatan Semua Titik (x, y) 66
4.2. Matrik yang Dibentuk dari Citra dengan Format .jpg 68
4.3. Representasi Piksel Pada Kurva Eliptik 70
4.4. Pertukaran Kunci Diffie-Hellman 74
4.5. Perancangan Sistem Enkripsi *Elliptic Curve Diffie-Hellman* (ECDH) 75
4.6. Perancangan Sistem Dekripsi *Elliptic Curve Diffie-Hellman* (ECDH) 77
V UJI COBA MANUAL ENKRIPSI DAN DEKRIPSI CITRA DIGITAL *GRAYSCALE* 78
VI PENUTUP 85
6.1. Kesimpulan 85
6.2. Saran 85
DAFTAR PUSTAKA 87
A KODE PROGRAM MATLAB CITRA DIGITAL KE MATRIKS PIKSEL 88
B KODE PROGRAM MATLAB MATRIKS PIKSEL KE CITRA DIGITAL 89