TUGAS AKHIR

ANALISIS PERBANDINGAN KOMPLEKSITAS WAKTU ALGORITMA KRIPTOGRAFI ASIMETRIS (RSA, ECC, DAN ELGAMAL) DALAM PROSES ENKRIPSI, DEKRIPSI, DAN TANDATANGAN DIGITAL

MELINDA UTAMI
17102133

PROGRAM STUDI S1 INFORMATIKA
FAKULTAS INFORMATIKA
INSTITUT TEKNOLOGI TELKOM PURWOKERTO
2022

TUGAS AKHIR

ANALISIS PERBANDINGAN KOMPLEKSITAS WAKTU ALGORITMA KRIPTOGRAFI ASIMETRIS (RSA, ECC, DAN ELGAMAL) DALAM PROSES ENKRIPSI, DEKRIPSI, DAN TANDATANGAN DIGITAL

TIME COMPLEXITY COMPARISON ANALYSIS OF ASYMMETRIC CRYPTOGRAPHY ALGORITHM (RSA, ECC, AND ELGAMAL) IN THE ENCRYPTION, DECRYPTION, AND DIGITAL SIGNATURE PROCESS

Disusun Sebagai Salah Satu Syarat untuk Memperoleh Gelar Sarjana Komputer

MELINDA UTAMI
17102133

PROGRAM STUDI S1 INFORMATIKA
FAKULTAS INFORMATIKA
INSTITUT TEKNOLOGI TELKOM PURWOKERTO
2022

LEMBAR PENGESAHAN PEMBIMBING

ANALISIS PERBANDINGAN KOMPLEKSITAS WAKTU ALGORITMA KRIPTOGRAFI ASIMETRIS (RSA, ECC, DAN *ELGAMAL*) DALAM PROSES ENKRIPSI, DEKRIPSI, DAN TANDATANGAN DIGITAL

TIME COMPLEXITY COMPARISON ANALYSIS OF ASYMMETRIC CRYPTOGRAPHY ALGORITHM (RSA, ECC, AND ELGAMAL) IN THE ENCRYPTION, DECRYPTION, AND DIGITAL SIGNATURE PROCESS

Dipersiapkan dan disusun oleh:
Melinda Utami
17102133
Telah Diujikan dan Dipertahankan dalam Sidang Ujian Tugas Akhir
Pada Kamis, 08 September 2022

Pembimbing I	**Pembimbing II**
(Ipam Fuaddina Adam, S.T., M.Kom.)	**(Trihastuti Yuniati, S.Kom., M.T.)**
NIDN. 0614048403	**NIDN. 0602068902**

Tugas Akhir ini diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 16 September 2022
Kaprodi,

(Amalia Beladinna Arifa, S.Pd., M.Cs)
NIDN. 0606019201

LEMBAR PENETAPAN PENGUJI

ANALISIS PERBANDINGAN KOMPLEKSITAS WAKTU ALGORITMA KRIPTOGRAFI ASIMETRIS (RSA, ECC, DAN *ELGAMAL*) DALAM PROSES ENKRIPSI, DEKRIPSI, DAN TANDATANGAN DIGITAL

TIME COMPLEXITY COMPARISON ANALYSIS OF ASYMMETRIC CRYPTOGRAPHY ALGORITHM (RSA, ECC, AND ELGAMAL) IN THE ENCRYPTION, DECRYPTION, AND DIGITAL SIGNATURE PROCESS

Dipersiapkan dan disusun oleh:

Melinda Utami

17102133

Tugas Akhir Telah diuji dan Dinilai Panitia Penguji Program Studi S1 Informatika

Fakultas Informatika

Institut Teknologi Telkom Purwokerto

Pada Tanggal :8 September 2022

Ketua Penguji

(Muhammad Fajar Sidiq, S.T., M.T.)

NIDN. 0619029102

Anggota Penguji I

(Aditya Wijayanto, S.Kom., M.Cs.)

NIDN. 0608118902

Anggota Penguji II

(Bita Parga Zen, S.Kom., M. Han.)

NIDN. 0603089202

HALAMAN PERNYATAAN KEASLIAN TUGAS AKHIR

Yang bertanda tangan di bawah ini,

Nama : **Melinda Utami**

NIM : **17102133**

Program Studi : **S1 Informatika**

Menyatakan bahwa Tugas Akhir dengan judul:

ANALISIS PERBANDINGAN KOMPLEKSITAS WAKTU ALGORITMA KRIPTOGRAFI ASIMETRIS (RSA, ECC, DAN ELGAMAL) DALAM PROSES ENKRIPSI, DEKRIPSI, DAN TANDATANGAN DIGITAL

Dosen Pembimbing Utama : Ipam Fuaddina Adam, S.T., M. Kom.

Dosen Pembimbing Pendamping : Trihastuti Yuniati, S.Kom., M.T.

1. Karya tulis ini adalah benar-benar ASLI dan BELUM PERNAH diajukan untuk mendapatkan gelar akademik, baik di Institut Teknologi Telkom Purwokerto maupun di Perguruan Tinggi lainnya.
2. Karya tulis ini merupakan gagasan, rumusan, dan penelitian Saya Sendiri, tanpa bantuan pihak lain kecuali arahan dari Tim Dosen Pembimbing.
3. Dalam Karya tulis ini tidak terdapat karya atau pendapat orang lain, kecuali secara tertulis dengan jelas dicantumkan sebagai acuan dalam naskah dengan disebutkan nama pengarang dan disebutkan dalam Daftar Pustaka pada karya tulis ini.
4. Perangkat lunak yang digunakan dalam penelitian ini sepenuhnya menjadi tanggung jawab Saya, bukan tanggung jawab Institut Teknologi Telkom Purwokerto.
5. Pernyataan ini Saya buat dengan sesungguhnya, apabila dikemudian hari terdapat penyimpangan dan ketidakbenaran dalam pernyataan ini, maka Saya bersedia menerima Sanksi Akademik dengan pencabutan gelar yang sudah diperoleh serta sanksi lainnya sesuai dengan norma yang berlaku di Perguruan Tinggi.

Purwokerto, 22 Agustus 2022

Yang menyatakan,

(Melinda Utami)

KATA PENGANTAR

Segala puji syukur ke hadirat Tuhan Yang Maha Esa yang telah melimpahkan anugerah dan karunia-Nya sehingga penulis dapat menyelesaikan laporan penelitian ini dengan baik. Selanjutnya penulis mengucapkan terima kasih kepada:

1. Ibu dan seluruh keluarga atas segala dukungan yang diberikan, doa dan dukungan moral maupun materi.
2. Bapak Dr. Arfianto Fahmi, S.T., M.T., IPM, selaku Rektor Institut Teknologi Telkom Purwokerto.
3. Bapak Auliya Burhanuddin, S.Si., M.Kom., selaku Dekan Fakultas Informatika Institut Teknologi Telkom Purwokerto.
4. Ibu Amalia Beladinna Arifa, S.Pd., M.Cs., selaku Kepala Program Studi Teknik Informatika.
5. Bapak Ipam Fuaddina Adam, S.T., M.Kom. selaku Pembimbing I Tugas Akhir yang meluangkan waktunya untuk memberi bimbingan dan masukan dalam penyusunan laporan penelitian.
6. Ibu Trihastuti Yuniati, S.Kom., M.T selaku Pembimbing II Tugas Akhir yang meluangkan waktunya untuk memberi bimbingan dan masukan dalam penyusunan laporan penelitian.
7. Semua pihak yang tidak dapat disebutkan satu per satu yang terlibat dalam penyusunan Laporan Tugas Akhir ini sehingga dapat selesai dengan baik.

Akhir kata, penulis menyadari bahwa penyusunan laporan tugas akhir ini masih belum sempurna. Oleh karena itu, kritik dan saran yang membangun sangat penulis harapkan. Semoga penyusunan laporan ini bermanfaat bagi semua pihak.

Purwokerto, 22 Agustus 2022

Melinda Utami

DAFTAR ISI

COVER i
COVER DALAM ii
LEMBAR PENGESAHAN PEMBIMBING iii
LEMBAR PENETAPAN PENGUJI iv
HALAMAN PERNYATAAN KEASLIAN TUGAS AKHIR v
KATA PENGANTAR vi
DAFTAR ISI vii
DAFTAR TABEL ix
DAFTAR GAMBAR x
DAFTAR ISTILAH xi
ABSTRAK xii
ABSTRACT xiii
BAB I 1
PENDAHULUAN 1
1.1 Latar Belakang Masalah 1
1.2 Rumusan Masalah 5
1.3 Tujuan Penelitian 5
1.4 Batasan Masalah 5
1.5 Manfaat Penelitian 6
BAB II 7
TINJAUAN PUSTAKA 7
2.1 Penelitian Sebelumnya 7
2.2 Dasar Teori 15
2.2.1 Kriptografi 15
2.2.2 Algoritma Kriptografi RSA *(*Rivest-*Shamir-Adleman)* 19
2.2.3 Algoritma Kriptografi ECC (*Elliptic Curve Cryptography*) 22
2.2.4 Algoritma Kriptografi ElGamal 24
2.2.5 Tandatangan Digital 27
2.2.6 Kompleksitas Algoritma 28
2.2.7 Code::Blocks 31
2.2.8 NTL *(Number Theory* Library*)* 32

BAB III 33
METODOLOGI PENELITIAN 33
3.1 Objek dan Subjek Penelitian 33
3.2 Diagram Alir Penelitian 34
3.2.1 Tahapan Pendahuluan 35
3.2.2 Tahapan Studi Pustaka 35
3.2.3 Tahapan Perancangan 35
3.2.4 Tahapan Analisis 36
3.2.5 Tahapan Kesimpulan dan Saran 36
3.2.6 Teknik Pengumpulan Data 36
3.3 Analisis Data 54
BAB IV 55
HASIL DAN PEMBAHASAN 55
4.1 Hasil Pengujian 55
4.2 Analisis 72
BAB V 79
KESIMPULAN DAN SARAN 79
5.1 Kesimpulan 79
5.2 Saran 80
DAFTAR PUSTAKA 81

DAFTAR TABEL

Tabel 2. 1 S*tate of the Art* 11
Tabel 2. 2 Pengelompokan Algoritma Berdasarkan Notasi O-Besar[18] 30
Tabel 3. 1 Spesifikasi minimum Code::Blocks 33
Tabel 3. 2 spesifikasi komponen penelitian 33
Tabel 3. 3 Pseudocode enkripsi dan Dekripsi Algoritma RSA 38
Tabel 3. 4 Pseudocode Tanda Tangan Digital Algoritma RSA 39
Tabel 3. 5 pseudocode Enkripsi dan Dekripsi algoritma ECC 42
Tabel 3. 6 tanda tangan digital algoritma ECC 45
Tabel 3. 7 pseudocode enkripsi dan dekripsi algoritma ElGamal 50
Tabel 3. 8 pseudocode tanda tangan digital algoritma ElGamal 52
Tabel 4. 1 Pengujian Algoritma RSA 192 bit 55
Tabel 4. 2 Pengujian Algoritma RSA 512 bit 56
Tabel 4. 3 Pengujian Algoritma RSA 1024 bit 56
Tabel 4. 4 Pengujian Algoritma ECC 192 bit 57
Tabel 4. 5 Pengujian Algoritma ElGamal 192 bit 57
Tabel 4. 6 Pengujian Algoritma ElGamal 512 bit 58
Tabel 4. 7 Pengujian Algoritma ElGamal 1024 bit 58
Tabel 4. 8 data hasil pengujian 59
Tabel 4. 9 Kompleksitas Waktu RSA 60
Tabel 4. 10 Kompleksitas waktu ECC 61
Tabel 4. 11 Komplekistas waktu ElGamal 63
Tabel 4. 12 Kompleksitas waktu Tandatangan Digital RSA 65
Tabel 4. 13 Kompleksitas waktu Tandatangan Digital ECC 66
Tabel 4. 14 Kompleksitas waktu Tandatangan Digital ElGamal 69

DAFTAR GAMBAR

Gambar 2. 1 Proses Enkripsi dan dekripsi 16
Gambar 2. 2 Proses Pembuatan Tandatangan Digital 28
Gambar 3. 1 Flowchart Enkripsi dan Dekripsi Algoritma RSA 37
Gambar 3. 2 Flowchart Tanda Tangan Digital Algoritma RSA 39
Gambar 3. 3 Flowchart Enkripsi dan Dekripsi algoritma ECC 41
Gambar 3. 4 flowchart tanda tangan digital algoritma ECC 45
Gambar 3. 5 flowchart enkripsi dan dekripsi algoritma ElGamal 49
Gambar 3. 6 flowchart tanda tangan digital algoritma ElGamal 51
Gambar 4. 1 Grafik perbandingan waktu pembangkitan kunci 72
Gambar 4. 2 Perbandingan waktu enkripsi 73
Gambar 4. 3 Perbandingan Waktu Dekripsi 73
Gambar 4. 4 Perbandingan Waktu Pembangkitan Kunci Tanda tangan Digital ... 74
Gambar 4. 5 Perbandingan Waktu Pembuatan Tanda tangan Digital 75
Gambar 4. 6 Perbandingan Waktu keseluruhan proses enkripsi dan dekripsi 75
Gambar 4. 7 Perbandingan Waktu keseluruhan proses pembuatan tandatangan digital 76
Gambar 4. 8 Kurva Perbandingan Kompleksitas Enkripsi dan Dekripsi 77
Gambar 4. 9 Kurva Perbandingan Kompleksitas Tandatangan Digital 78

DAFTAR ISTILAH

Algoritma kunci Asimetris	Menggunakan kunci yang berbeda untuk proses enkripsi – dekripsi.
Algoritma kunci Simetris	Menggunakan kunci yang sama untuk proses enkripsi – dekripsi.
Block Ciphers	Proses penyandiannya berorientasi pada sekumpulan bit/*byte* data (per blok).
Ciphertext	Pesan yang telah enkripsi.
Dekripsi	Proses untuk mengubah ciphertext kembali ke plaintext.
Enkripsi	Proses yang dilakukan untuk mengubah plaintext ke dalam ciphertext.
Flowchart	Diagram yang menampilkan langkah-langkah dan keputusan untuk melakukan sebuah proses dari suatu program.
Key(kunci)	Kunci yang digunakan untuk melakukan enkripsi dan dekripsi.
Plaintext	Suatu pesan yang tidak disandikan ataupun dapat disebut juga sebagai pesan asli.
Pseudocode	Algoritma pemrograman yang dituliskan secara sederhana dibandingkan dengan sintaksis bahasa pemrograman.
Stream Ciphers	Proses penyandiannya akan beriorientasi pada satu bit/*byte* data.