



**ANALISIS PERBANDINGAN ALGORITMA KRIPTO-  
GRAFI RSA DAN EIGAMAL UNTUK PENGAMANAN  
CITRA DIGITAL MEDIS COVID-19**

**SKRIPSI**

**R IRHAM NURFI SATRIO**

**1810511086**

**UNIVERSITAS PEMBANGUNAN NASIONAL VETERAN JA-  
KARTA  
FAKULTAS ILMU KOMPUTER  
PROGRAM STUDI INFORMATIKA  
2022**



**ANALISIS PERBANDINGAN ALGORITMA KRIPTO-  
GRAFI RSA DAN EIGAMAL UNTUK PENGAMANAN  
CITRA DIGITAL MEDIS COVID-19**

**SKRIPSI**

**Diajukan Sebagai Salah Satu Syarat untuk Memperoleh Gelar  
Sarjana Komputer**

**R IRHAM NURFI SATRIO**

**1810511086**

**UNIVERSITAS PEMBANGUNAN NASIONAL VETERAN JA-  
KARTA**

**FAKULTAS ILMU KOMPUTER  
PROGRAM STUDI INFORMATIKA**

**2022**

## PERNYATAAN ORISINALITAS

Skripsi ini adalah hasil karya sendiri, dan semua sumber yang dikutip maupun dirujuk telah saya nyatakan benar.

Nama : R. Irham Nurfi Satrio

NIM : 1810511086

Tanggal : 26 Juli 2022

Bilamana dikemudian hari ditemukan ketidaksesuaian dengan pernyataan saya ini, maka saya bersedia dituntut dan diproses sesuai dengan ketentuan yang berlaku.

Jakarta, 26 Juli 2022

Yang menyatakan,



R. Irham Nurfi Satrio

## LEMBAR PERSETUJUAN PUBLIKASI

Sebagai civitas akademik Universitas Pembangunan Nasional Veteran Jakarta, saya yang bertanda tangan di bawah ini:

Nama : R. Irham Nurfi Satrio

NIM : 1810511086

Fakultas : Ilmu Komputer

Program Studi : S1 Informatika

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Universitas Pembangunan Nasional Veteran Jakarta Hak Bebas Royalti Non-Eksklusif (*Non-Exclusive Royalty Free Right*) atas karya ilmiah saya yang berjudul:

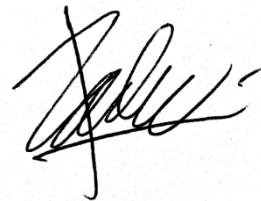
### **ANALISIS PERBANDINGAN ALGORITMA KRIPTOGRAFI RSA DAN EIGAMAL UNTUK PENGAMANAN CITRA DIGITAL MEDIS COVID-19**

Beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti ini Universitas Pembangunan Nasional Veteran Jakarta berhak menyimpan, mengalih media/formatkan, mengelola dalam bentuk pangkalan kata (basis data), merawat dan mempublikasikan Skripsi saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta. Demikian pernyataan ini saya buat dengan sebenarnya.

Dibuat di : Jakarta

Pada Tanggal : 26 Juli 2022

Yang menyatakan,



R. Irham Nurfi Satrio

# LEMBAR PENGESAHAN

Dengan ini dinyatakan bahwa Tugas Akhir berikut :

Nama : R. Irham Nurfi Satrio

NIM : 1810511086

Program Studi : S-1 Informatika

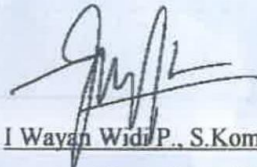
Judul : ANALISIS PERBANDINGAN ALGORITMA KRIPTOGRAFI  
RSA DAN ELGAMAL UNTUK PENGAMANAN CITRA DIGI-  
TAL MEDIS COVID-19

Telah berhasil dipertahankan di hadapan Tim Penguji dan diterima sebagai per-  
syaratan yang diperlukan untuk memperoleh gelar Sarjana Komputer pada Pro-  
gram Studi Informatika Fakultas Ilmu Komputer, Universitas Pembangunan Na-  
sional Veteran Jakarta.



Hengki Bayu Seta, S.Kom, M.TI.

Dosen Penguji 1



I Wayan Widi P., S.Kom, M.Kom.

Dosen Penguji 2



Helena Nurramdhani Irmada, S.Pd, M.Kom.

Dosen Pembimbing 2



Bayu Hananto, S.Kom, M.Kom.

Dosen Pembimbing 1



Dr. Ermanita, M.Kom

Dekan



Desta Sandya Prasvita, S. Komp., M.Kom.

Ketua Program Studi SI Informatika

Ditetapkan pada di : Jakarta

Tanggal Persetujuan : 26 Juli 2022



# **ANALISIS PERBANDINGAN ALGORITMA KRIPTOGRAFI RSA DAN EIGAMAL UNTUK PENGAMANAN CITRA DIGITAL MEDIS COVID-19**

**R. Irham Nurfi Satrio**

## **ABSTRAK**

Seiring dengan perkembangan teknologi, kebutuhan dalam pertukaran informasi yang aman dan terjamin pun semakin cepat. Dengan adanya penyimpanan informasi tersebut maka dibutuhkan sistem keamanan yang baik pula agar terhindar dari kejahatan dan pembobolan pada informasi yang disimpan. Salah satu bentuk untuk mengamankan informasi yang ada ialah dengan mengenkripsi data tersebut. Terdapat banyak teknik dan jenis enkripsi salah satunya ialah dengan menggunakan metode algoritma kriptografi RSA dan ElGamal. Pada *Open-Source Database* situs Kaggle terdapat kumpulan dataset yang dapat peneliti gunakan untuk memenuhi tujuan penelitiannya, salah satunya ialah citra rekam medis MRI pasien yang terdampak penyakit COVID-19. Pada penelitian ini akan menerapkan enkripsi citra medis MRI dengan menggunakan algoritma kriptografi RSA dan membandingkannya dengan algoritma kriptografi ElGamal untuk melihat efisiensi dari kedua algoritma tersebut dilihat dari kecepatan enkripsi dan dekripsi serta nintegritas dari citra digital tersebut apakah berubah atau tidak. Penelitian ini diharapkan mendapatkan manfaat dan luaran berupa bahan pertimbangan bagi pemilik citra digital untuk menggunakan metode algoritma yang lebih efisien pada penelitian ini dan membuka wawasan terkait efisiensi penerapan kedua enkripsi.

**Kata Kunci : keamanan data, enkripsi, kriptografi, algoritma elgamal, algoritma rsa, citra digital, mri, covid-19**

**COMPARATIVE ANALYSIS OF THE RSA AND ELGAMAL CRYPTO-  
GRAPHIC ALGORITHMS FOR SECURING COVID-19 MEDICAL DIGITAL  
IMAGES**

**R. Irham Nurfi Satrio**

**ABSTRACT**

*Along with the development of technology, the need for safe and secure information exchange is also getting faster. With this information storage, a good security system is also needed to avoid crime and break-ins in the stored information. One form of securing existing information is to encrypt the data. There are many techniques and types of encryption, one of which is to use the RSA and ElGamal cryptographic algorithm methods. On the Open-Source Database on the Kaggle site, there is a collection of datasets that researchers can use to fulfill their research objectives, one of which is the MRI medical record images of patients affected by COVID-19. In this study, we will apply MRI medical image encryption using the RSA cryptographic algorithm and compare it with the ElGamal cryptographic algorithm to see the efficiency of the two algorithms seen from the encryption and decryption speed and the integrity of the digital image whether it changes or not. This research is expected to get benefits and outcomes in the form of consideration for digital image owners to use a more efficient algorithm method in this study and open insights regarding the efficiency of the implementation of both encryptions.*

**Keywords : data security, encryption, cryptography, elgamal algorithm, rsa algorithm, digital image, mri, covid-19**

## KATA PENGANTAR

Puji syukur saya panjatkan kepada Allah Swt. atas segala karunia dan nikmat-Nya sehingga skripsi ini dapat berhasil diselesaikan dengan judul: “*Analisis Perbandingan Algoritma Kriptografi RSA dan ElGamal untuk Pengamanan Citra Digital Covid-19*” yang ditujukan untuk menjadi syarat kelulusan untuk menyelesaikan perkuliahan pada Program Studi Informatika Fakultas Ilmu Komputer Universitas Pembangunan Nasional Veteran Jakarta. Dan ucapan terima kasih juga penulis ucapkan kepada:

1. Kedua orang tua atas segala doa, dukungan, nasihat dan kasih sayangnya sehingga saya dapat menjalankan studi hingga saat ini
2. Bapak Bayu Hananto, S.Kom, M.Kom. selaku dosen pembimbing I
3. Ibu Helena Nurramdhani Irmada, S.Pd, M.Kom. selaku dosen pembimbing II
4. Andini Rizki Aulia, Sahabat OVE: Fauzan, Cahyo, Dinda, Oca, dan AHM: Arini, Adham, Nung, Alief, yang selalu menemani dan mendukung penulis selama masa dan kegiatan aktif perkuliahan, dan selalu memberi masukan serta semangat kepada penulis.
5. Keluarga besar Pohon Ajaib dan VIMAVEJA yang selalu ada dan memberikan hiburan, canda dan tawa di luar aktivitas perkuliahan.
6. Teman – teman Informatika 2018 yang tidak dapat saya sebutkan satu per satu yang selalu menemani perkuliahan dan memberikan dukungan selama masa perkuliahan terhadap penulis.

Akhir kata, semoga skripsi ini dapat bermanfaat bagi para pembacanya.

Jakarta, 27 Juli 2022

Penulis



## DAFTAR ISI

PERNYATAAN ORISINALITAS .....	i
LEMBAR PERSETUJUAN PUBLIKASI.....	ii
LEMBAR PENGESAHAN .....	iii
ABSTRAK .....	iv
<i>ABSTRACT</i> .....	v
KATA PENGANTAR .....	vi
DAFTAR ISI.....	vii
DAFTAR GAMBAR .....	x
DAFTAR TABEL.....	xi
BAB I.....	1
PENDAHULUAN .....	1
1.1. Latar Belakang .....	1
1.2. Rumusan Masalah .....	2
1.3. Tujuan.....	3
1.4. Manfaat Penelitian.....	3
1.5. Batasan Masalah.....	3
1.6. Luaran yang Diharapkan .....	4
1.7. Sistematika Penulisan.....	4
BAB II.....	6
TINJAUAN PUSTAKA .....	6
2.1. Kriptografi .....	6
2.1.1. Symmetric Key.....	6
2.1.2. Asymmetric Key .....	7
2.1.3. Enkripsi .....	8
2.1.4. Dekripsi .....	8

2.1.5.	Algoritma ElGamal .....	9
2.1.6.	Pembangkitan Kunci ElGamal .....	9
2.1.7.	Enkripsi ElGamal .....	10
2.1.8.	Dekripsi El Gamal .....	11
2.1.9.	Algoritma kriptografi <i>Rivest-Shamir-Adleman (RSA)</i> .....	11
2.1.10.	Pembangkitan Kunci RSA .....	11
2.1.11.	Enkripsi RSA .....	13
2.1.12.	Dekripsi RSA .....	14
2.2.	Citra Digital .....	15
2.3.	Magnetic Resonance Imaging (MRI) .....	15
2.4.	Rekam Medis ( <i>Medical Records</i> ) .....	16
2.5.	Daftar Riset yang Relevan .....	16
BAB III .....		19
METODOLOGI PENELITIAN .....		19
3.1.	Diagram Alur Penelitian .....	19
3.1.1.	Identifikasi Masalah .....	19
3.1.2.	Studi Literatur .....	20
3.1.3.	Pengumpulan Data .....	20
3.1.4.	Rancang Bangun Sistem .....	20
3.1.5.	Implementasi dan Analisis .....	21
3.1.6.	Pengujian .....	23
3.1.7.	Evaluasi & Dokumentasi .....	23
3.2.	Alat Bantu Penelitian .....	23
3.3.	Jadwal Kegiatan Penelitian .....	24
BAB IV .....		26
PEMBAHASAN .....		26

4.1.	Pencarian dan Pengumpulan Data .....	26
4.1.1.	Sumber Data Citra Digital.....	26
4.2.	Pembuatan Program Enkripsi – Dekripsi Algoritma RSA .....	28
4.2.1.	Proses Pembangkitan Kunci Enkripsi RSA .....	28
4.2.2.	Proses Enkripsi Citra dengan RSA .....	33
4.2.3.	Proses Dekripsi Citra dengan RSA .....	38
4.3.	Pembuatan Program Enkripsi – Dekripsi Algoritma ElGamal .....	42
4.3.1.	Proses Pembangkitan Kunci Enkripsi ElGamal.....	42
4.3.2.	Enkripsi Citra dengan ElGamal .....	43
4.3.3.	Dekripsi Citra dengan Elgmal.....	46
4.4.	Pengujian Citra Digital.....	49
4.4.1.	Analisis Perbandingan Perubahan Ukuran Citra.....	49
4.4.2.	Analisis Perbandingan Waktu Enkripsi – Dekripsi Citra.....	51
4.4.3.	Analisis Perbandingan Nilai Checksum Citra.....	53
4.4.4.	Analisis Perbandingan Histogram Citra.....	54
BAB V.....		63
KESIMPULAN.....		63
5.1.	Kesimpulan.....	63
5.2.	Saran.....	64
DAFTAR PUSTAKA .....		65
DAFTAR RIWAYAT HIDUP.....		66
LAMPIRAN.....		67

## DAFTAR GAMBAR

Gambar 1 flow kunci simetris .....	7
Gambar 2 flow kunci asimetris .....	8
Gambar 3 Alur pembangkitan kunci ElGamal.....	10
Gambar 4 Alur pembuatan kunci RSA .....	12
Gambar 5 flow enkripsi RSA.....	13
Gambar 6 flow dekripsi RSA.....	14
Gambar 7 Citra MRI .....	16
Gambar 8 Flow diagram penelitian.....	19
Gambar 9 Alur rancang bangun sistem penelitian .....	21
Gambar 10 Alur pembuatan kunci, enkripsi dan dekripsi algoritma RSA .....	22
Gambar 11 Alur pembuatan kunci, enkripsi dan dekripsi algoritma ElGamal ....	22
Gambar 12 Alur pengujian penelitian .....	23
Gambar 13 Grafik perbandingan ukuran hasil enkripsi .....	49
Gambar 14 Grafik perbandingan rata - rata perubahan ukuran dalam bentuk persentase .....	50
Gambar 15 Grafik perbandingan perubahan rata - rata keseluruhan ukuran .....	50
Gambar 16 Grafik perbandingan waktu enkripsi kedua algoritma .....	51
Gambar 17 Grafik perbandingan rata - rata waktu enkripsi & dekripsi kedua algoritma .....	52
Gambar 18 Grafik perbandingan waktu dekripsi kedua algoritma .....	52

## DAFTAR TABEL

Tabel 1 Daftar riset yang relevan .....	16
Tabel 2 Jadwal Kegiatan Penelitian .....	24
Tabel 3 Citra digital yang diuji .....	26
Tabel 4 nilai RGB blok piksel pertama sampel citra 'a' .....	33
Tabel 5 nilai RGB hasil enkripsi .....	36
Tabel 6 konversi decimal ke biner dan pengambilan nilai MSB dan LSB nya ....	36
Tabel 7 nilai cipher RGB hasil enkripsi RSA blok pertama citra 'a' .....	37
Tabel 8 Enkripsi Citra dengan RSA.....	37
Tabel 9 nilai cipher RGB blok piksel pertama citra 'b' .....	38
Tabel 10 konversi nilai cipher ke bentuk biner .....	38
Tabel 11 Hasil penggabungan MSB dan LSB .....	39
Tabel 12 Hasil konversi biner ke bentuk decimal .....	39
Tabel 13 nilai RGB hasil dekripsi RSA blok pertama citra 'b'.....	41
Tabel 14 Dekripsi Citra dengan RSA.....	41
Tabel 15 nilai RGB blok pertama piksel citra 'a' .....	43
Tabel 16 nilai cipher RGB hasil enkripsi .....	45
Tabel 17 Enkripsi Citra dengan ElGamal .....	46
Tabel 18 nilai cipher blok piksel pertama citra 'b' .....	47
Tabel 19 nilai RGB hasil dekripsi ElGamal blok pertama citra 'b' .....	48
Tabel 20 Dekripsi Citra dengan ElGamal .....	48
Tabel 21 Perbandingan nilai Checksum SHA256.....	53
Tabel 22 Perbandingan Histogram Citra.....	55