HALAMAN PENGESAHAN

ENKRIPSI GAMBAR MENGGUNAKAN ALGORITMA RC4 DAN ELGAMAL

IRFAN SURYA SULNAS
NIM. 217280150

Telah dipertahankan di depan Komisi Penguji Ujian Skripsi Pada Tanggal 26 Januari 2022 dan dinyatakan telah memenuhi syarat

Komisi Penguji

Muhammad Basri, ST., MT. (*Ketua*) (.....)

Masnur, ST., M.Kom. (*Sekertaris*) (.....)

Ade Hastuty, S.T., S.Kom., M.T. (*Anggota*) (.....)

Marlina, S.Kom., M.Kom. (*Anggota*) (.....)

Mengetahui :

Ketua Program Studi
Teknik Informatika

Marlina, S.Kom., M.Kom.
NBM. 1162 680

Dekan
Fakultas Teknik

Muhammad Basri, ST., MT.
NBM. 959 773

PERNYATAAN KEASLIAN SKRIPSI

Saya yang bertanda tangan di bawah ini:

Nama	: **Irfan Surya Sulnas**
NIM	: **217280150**
Program Studi	: Teknik Informatika
Fakultas	: Teknik Universitas Muhammadiyah Parepare
Judul Skripsi	: Enkripsi Gambar Menggunakan Algoritma RC4 dan Elgamal

Menyatakan dengan sebenarnya bahwa skripsi yang saya tulis ini benar-benar merupakan hasil karya sendiri, bukan merupakan pengambilalihan tulisan atau pemikiran orang lain. Apabila dikemudian hari terbukti atau dapat bahwa sebagian atau keseluruhan skripsi ini hasil karya orang lain, saya bersedia menerima sanksi sesuai dengan aturan yang berlaku.

Parepare, 26 Januari 2022

Yang Menyatakan



Irfan Surya Sulnas

NIM. 217280150

وَيَرْزُقْهُ مِنْ حَيْثُ لَا يَحْتَسِبُ ۚ وَمَن يَتَوَكَّلْ عَلَى ٱللَّهِ فَهُوَ حَسْبُهُۥٓ ۚ إِنَّ ٱللَّهَ بَٰلِغُ أَمْرِهِۦ ۚ قَدْ جَعَلَ ٱللَّهُ لِكُلِّ شَىْءٍ قَدْرًا

Dan dia (Allah) memberinya rezeki dari arah yang tidak disangka-sangkanya. Dan barang siapa yang bertawakkal kepada Allah, niscaya Allah akan mencukupkan (keperluan)nya. Sesungguhnya Allah melaksanakan urusan yang (dikehendaki)Nya. Sungguh Allah telah menjadikan untuk setiap sesuatu menurut takarannya.

(Q.S At-Talaq : 3)

PRAKATA

Bismillahirrahmanirrahim

Alhamdulillahi robbil 'alamiin. Puji syukur ke hadirat Allah *subhanahu wa ta'ala* atas limpahan rahmat-Nya sehingga penulis dapat menyelesaikan skripsi dengan judul Enkripsi Gambar Menggunakan Algoritma RC4 dan Elgamal. Shalawat dan salam senantiasa terkirimkan kepada Nabi Muhammad shallahu 'alaihi wasallam, Beserta para sahabat dan keluarga beliau yang telah memberikan teladan dalam menjalani kehidupan di dunia dan di akhirat.

Terselesainya skripsi ini, tentunya tidak terlepas dari bantuan dari berbagai pihak. Oleh karena itu, pada kesempatan ini penulis mengucapkan banyak terima kasih dengan penuh ketulusan dan penghargaan setinggi-tingginya kepada :

1. Kedua orang tua, ayahanda tercinta Imran Sulnas dan ibunda tersayang Suryati serta kakak Rizal Satria Sulnas dan Sudiman Saputra Sulnas beserta keluarga keluarga yang telah memberikan dukungan baik moril maupun materil serta doa yang tiada henti-hentinya kepada penulis, semoga Allah menjaga mereka semua.
2. Bapak Muhammad Basri, ST., MT. selaku Dekan Fakultas Teknik Universitas Muhammadiyah Parepare.
3. Ibu Marlina, S.Kom., M.Kom. Selaku ketua Program Studi Teknik Informatika Fakultas Teknik Universitas Muhammadiyah Parepare.
4. Bapak Muhammad Basri, ST., MT. Selalu dosen Pembimbing I yang senantiasa memberi dukungan moril serta memberi solusi dari permasalahan dalam pembuatan skripsi ini.

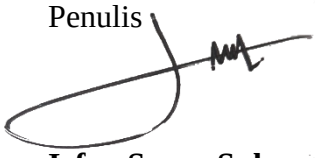
5. Bapak Masnur S.T., M.Kom. Selaku dosen Pembimbing II yang telah memberi saran dan tambahan ilmu serta solusi dari permasalahan dalam pembuatan skripsi ini.
6. Ibu Ade Hastuty, S.T., S.Kom., M.Kom. Selaku Penguji I yang telah memberi masukan dan arahan.
7. Ibu Marlina, S.Kom., M.Kom. Selaku Penguji II yang telah memberi masukan dan arahan.
8. Para Dosen FT UM Parepare yang telah banyak memberikan pengetahuan pada penulis, selama menimba ilmu di FT UM Parepare ini.
9. Teman saya, Yusril Anwar, Taufiq Hidayat, Selpi R, Muhammad Farid Fatwa yang bersama-sama berjuang.
10. Semua pihak yang membantu dalam pembuatan skripsi ini yang tidak dapat saya tuliskan.

Akhirnya penulis berharap semoga amal baik dari semua pihak yang telah membantu penulis dalam menyelesaikan skripsi ini mendapatkan balasan pahala dari rahmat Allah ta'ala. Semoga apa yang telah ditulis dalam skripsi ini dapat bermanfaat bagi semua pihak. *Amin ya Rabbal a'lamin*.

Subahanakallahumma wabihamdika asyhadu alla ilaha illa anta astagfiruka waatubuu ilaika.

Parepare, 26 Januari 2022

Penulis



Irfan Surya Sulnas

NIM. 217280150

ABSTRAK

IRFAN SURYA SULNAS. *Enkripsi Gambar Menggunakan Algoritma RC4 Dan Elgamal* (dibimbing oleh Muhammad Basri dan Masnur).

Kriptografi adalah ilmu ataupun seni yang mempelajari bagaimana membuat suatu pesan yang dikirim oleh pengirim dapat disampaikan kepada penerima dengan aman. Kriptografi merupakan bagian dari suatu cabang ilmu matematika yang disebut *kriptologi*. Didalam suatu pesan dapat berisi teks maupun gambar. Bila informasi penting ini jatuh ke tangan orang yang salah, maka akan menyebabkan hal yang tidak diinginkan, seperti manipulasi gambar dengan bentuk yang negatif yang dapat merugikan pemilik gambar. Pada tulisan ini akan dijelaskan mengenai pembuatan aplikasi yang menerapkan kriptografi untuk mengamankan gambar dengan cara mengenkripsi nilai-nilai pada tiap piksel gambar. Dalam aplikasi ini akan menggunakan algoritma RC4 dan Elgamal untuk mengenkripsi nilai-nilai pada tiap piksel gambar.

Kata Kunci : *Enkripsi, Kriptografi, Gambar, Algoritma, RC4, Elgamal.*

ABSTRACT

IRFAN SURYA SULNAS. *Image Encryption Using RC4 and Elgamal Algorithms* (*suvervised by* Muhammad Basri *and* Masnur).

Cryptography is the science or art of learning how to make a message sent by the sender securely deliverable to the recipient. Cryptography is part of a branch of mathematics called cryptology. In a message can contain text or images. When this important information falls into the hands of the wrong person, it will cause unwanted things, such as manipulation of images with negative shapes that can harm the owner of the image. In this article will be explained about the creation of applications that apply cryptography to secure images by encrypting the values on each pixel of the image. The app uses rc4 and elgamal algorithms to encrypt the values of each pixel of the image.

Keywords: Encryption, Cryptography, Images, Algorithm, RC4, Elgamal.

DAFTAR ISI

	Halaman
HALAMAN PENGESAHAN	ii
PERNYATAAN KEASLIAN SKRIPSI	iii
HALAMAN INSPIRASI	iv
PRAKATA	v
ABSTRAK	vii
ABSTRACT	viii
DAFTAR ISI	ix
DAFTAR TABEL	xi
DAFTAR GAMBAR	xiv
DAFTAR LAMPIRAN	xvii
BAB I PENDAHULUAN	1
A. Latar Belakang	1
B. Rumusan Masalah	2
C. Batasan Masalah	2
D. Tujuan Penelitian	3
E. Manfaat Penelitian	3
F. Sistematika Penulisan	3
BAB II TINJAUAN PUSTAKA	5
A. Tinjauan Penelitian Terdahulu	5
B. Kriptografi	6
C. Citra Digital	12
D. Matlab	17

E. Algoritma RC4 23
F. Algoritma Elgamal 26
G. Flowchart 29
H. *Unified Modelling Language* (UML) 30
I. Kerangka Pikir 34
BAB III METODE PENELITIAN 35
A. Jenis Penelitian 35
B. Waktu dan Tempat Penelitian 35
C. Alat dan Bahan 35
D. Perancangan Sistem 36
E. Metode Pengumpulan Data 45
F. Metode Pengujian 45
BAB IV HASIL DAN PEMBAHASAN 47
A. Hasil 47
B. Pembahasan 59
BAB V TUTUP 140
A. Kesimpulan 140
B. Saran 141
DAFTAR PUSTAKA 142
DAFTAR LAMPIRAN 143

DAFTAR TABEL

		Halaman
Tabel 2.1	Operator Aritmetika	20
Tabel 2.2	Operator Rasional	20
Tabel 2.3	Operator Logika	21
Tabel 2.4	Operator Kelas Integer	21
Tabel 2.5	Format Gambar	22
Tabel 2.6	*Flowchart*	29
Tabel 2.7	*Symbol Use Case Diagram*	31
Tabel 2.8	*Symbol Class Diagram*	32
Tabel 2.9	*Symbol Sequence Diagram*	33
Tabel 2.10	*Symbol State Chart Diagram*	33
Tabel 2.11	*Symbol Activity Diagram*	33
Tabel 3.1	Spesifikasi Perangkat Keras	36
Tabel 3.2	Spesifikasi Perangkat Lunak	36
Tabel 3.3	Keterangan *Use Case Diagram* Sistem Yang Berjalan	37
Tabel 3.4	Keterangan *Use Case Diagram* Sistem Yang Diusulkan	38
Tabel 4.1	Penjelasan *Use Case Diagram* Umum	49
Tabel 4.2	Hasil Percobaan Menggunakan RC4	85
Tabel 4.3	Ukuran Piksel Hasil Percobaan Menggunakan	87
Tabel 4.4	Hasil Percobaan Menggunakan Elgamal percobaan 1	88

Tabel 4.5 Ukuran Piksel Hasil Percobaan Menggunakan Elgamal Percobaan 1 89

Tabel 4.6 Hasil Percobaan Menggunakan Elgamal Percobaan 2 90

Tabel 4.7 Ukuran Piksel Hasil Percobaan Menggunakan Elgamal Percobaan 2 91

Tabel 4.8 Hasil Percobaan Menggunakan Gabungan RC4 dan Elgamal 98

Tabel 4.9 Ukuran Piksel Hasil Percobaan Menggunakan Gabungan RC4 dan Elgamal 100

Tabel 4.10 Menekan Tombol Enkripsi Pada Saat Data Kosong 104

Tabel 4.11 Ukuran Gambar Terlalu Besar 104

Tabel 4.12 Menekan Tombol Piksel dan Histogram Saat Gambar Kosong 115

Tabel 4.13 Menekan Tombol Enkripsi Saat Nilai g Lebih Besar Dari 257 106

Tabel 4.14 Menekan Tombol Enkripsi Saat Nilai x Lebih Besar Dari g 106

Tabel 4.15 Menekan Tombol Enkripsi Saat Nilai k Lebih besar Dari x 107

Tabel 4.16 Proses Enkripsi Berhasil 107

Tabel 4.17 Menekan Tombol Simpan Saat Data Masih Kosong 108

Tabel 4.18 Menekan Tombol Simpan Saat Nama *File* Masih Kosong 108

Tabel 4.19 Berhasil Menyimpan Gambar 109

Tabel 4.20 Menekan Tombol Dekripsi Saat Data Masih Kosong 109

Tabel 4.21 Menekan Tombol Piksel dan Histogram Saat Gambar Kosong 110

Tabel 4.22 Proses Dekripsi Berhasil 110

Tabel 4.23 Menekan Tombol Simpan Saat Data Masih Kosong 111

Tabel 4.24 Menekan Tombol Simpan Saat Nama *File* Masih Kosong 111

Tabel 4.25 Berhasil Menyimpan Gambar 112

Tabel 4.26 Grafik Matriks Enkripsi RC4 115

Tabel 4.27 Grafik Matriks Dekripsi RC4 118

Tabel 4.28 Grafik Matriks Enkripsi Elgamal 124

Tabel 4.29 Grafik Matriks Dekripsi Elgamal 128

Tabel 4.30 Grafik Matriks Enkripsi Gabungan 133

Tabel 4.31 Grafik Matriks Dekripsi Gabungan 138

Tabel 4.32 Hasil Pengujian 139

DAFTAR GAMBAR

Halaman

Gambar 2.1	Skema Proses Enkripsi dan Dekripsi Menggunakan Kunci	7
Gambar 2.2	*Pseudo-code* KSA	25
Gambar 2.3	*Pseudo-code* PRGA	26
Gambar 3.1	*Use Case Diagram* Sistem Yang Berjalan	37
Gambar 3.2	*Use Case Diagram* Sistem Yang Diusulkan	38
Gambar 3.3	*Flowchart* Enkripsi Algoritma RC4	39
Gambar 3.4	*Flowchart* Dekripsi *Algoritma RC4*	40
Gambar 3.5	*Flowchart* Enkripsi Algoritma Elgamal	41
Gambar 3.6	*Flowchart* Dekripsi Algoritma Elgamal	42
Gambar 3.7	*Flowchart* Enkripsi Gabungan Algoritma RC4 Dan Elgamal	43
Gambar 3.8	*Flowchart* Dekripsi Gabungan Algoritma RC4 Dan Elgamal	44
Gambar 4.1	*Use Case Diagram* Umum	48
Gambar 4.2	*Activity Diagram* Menu	50
Gambar 4.3	*Activity Diagram* Gabungan RC4 dan Elgamal	51
Gambar 4.4	*Activity Diagram* Algoritma RC4	52
Gambar 4.5	*Activity Diagram* Algoritma Elgamal	53
Gambar 4.6	*Sequence Diagram* Gabungan RC4 dan Elgamal	54
Gambar 4.7	*Sequence Diagram* RC4	55
Gambar 4.8	*Sequence Diagram* Elgamal	56
Gambar 4.9	Halaman Awal	56

Gambar 4.10 Profil 57

Gambar 4.11 Gabungan RC4 dan Elgamal 58

Gambar 4.12 Algoritma RC4 dan Elgamal 58

Gambar 4.13 Gambar Sampel 59

Gambar 4.14 Nilai Piksel Pada Gambar Sampel 60

Gambar 4.15 Baris dan Kolom 66

Gambar 4.16 *Cipher* Nilai Piksel Pada Gambar Sampel Dengan RC4 70

Gambar 4.17 Gambar *Cipher* Secara Keseluruhan 70

Gambar 4.18 Dekripsi Secara Keseluruhan 74

Gambar 4.19 *Cipher* Nilai Piksel Pada Gambar Sampel Dengan Elgamal 77

Gambar 4.20 *Cipher* Secara Keseluruhan 77

Gambar 4.21 Dekripsi Secara Keseluruhan 80

Gambar 4.22 *Cipher* Nilai Piksel Pada Gambar Sampel Dengan Gabungan 83

Gambar 4.23 *Cipher* Secara Keseluruhan 83

Gambar 4.24 Dekripsi Secara Keseluruhan 85

Gambar 4.25 Nilai Awal Pada Piksel Gambar Nomor 1 93

Gambar 4.26 Nilai Piksel Pada *Cipherimage* nomor 1 95

Gambar 4.27 Nilai Piksel *Plainimage* nomor 1 96

Gambar 4.28 Histogram Perbandingan Nilai Piksel Gambar nomor 1 97

Gambar 4.29 Histogram Perbandingan Nilai Piksel Gambar nomor 9 98

Gambar 4.30 Histogram Perbandingan Nilai Piksel Gambar nomor 10 98

Gambar 4.31 Histogram Perbandingan Nilai Piksel Gambar nomor 1 101

Gambar 4.32 Histogram Perbandingan Nilai Piksel Gambar nomor 4 101

Gambar 4.33 Histogram Perbandingan Nilai Piksel Gambar nomor 6 102

Gambar 4.34 Histogram Perbandingan Nilai Piksel Gambar nomor 7 102

Gambar 4.35 Histogram Perbandingan Nilai Piksel Gambar nomor 9 103

Gambar 4.36 Histogram Perbandingan Nilai Piksel Gambar nomor 10 103

Gambar 4.37 *Flowchart* enkripsi RC4 113

Gambar 4.38 *Flowgraph* enkripsi RC4 114

Gambar 4.39 *Flowchart* dekripsi RC4 116

Gambar 4.40 *Flowgraph* dekripsi RC4 117

Gambar 4.41 *Flowchart* enkripsi Elgamal 120

Gambar 4.42 *Flowgraph* enkripsi Elgamal 121

Gambar 4.43 *Flowchart* dekripsi Elgamal 125

Gambar 4.44 *Flowgraph* dekripsi Elgamal 126

Gambar 4.45 *Flowchart* enkripsi gabungan 129

Gambar 4.46 *Flowgraph* enkripsi gabungan 130

Gambar 4.47 *Flowchart* dekripsi gabungan 134

Gambar 4.48 *Flowgraph* dekripsi gabungan 135

DAFTAR LAMPIRAN

		Halaman
Lampiran – 1	*Listing Program* Halaman Utama	143
Lampiran – 2	*Listing Program* Menu Profil	144
Lampiran – 3	*Listing Program* Proses KSA, PRGA, dan Menu Keluar	145
Lampiran – 4	*Listing Program* Menu Enkripsi Gabungan	147
Lampiran – 5	*Listing Program* Menu Algoritma RC4 dan Elgamal	150