



**APLIKASI PENGAMANAN DOKUMEN MENGGUNAKAN  
ALGORITMA KUNCI PUBLIK ELGAMAL**

**REZA DWI FAUZAN**

**1414.203.19**

**Skripsi ini diajukan sebagai syarat memperoleh gelar Sarjana  
Komputer di Universitas Bina Darma**

**PROGRAM STUDI INFORMATIKA  
FAKULTAS ILMU KOMPUTER  
UNIVERSITAS BINADARMA**

**2020**


**HALAMAN PENGESAHAN**

**APLIKASI PENGAMANAN DOKUMEN MENGGUNAKAN  
ALGORITMA KUNCI PUBLIK ELGAMAL**

**REZA DWI FAUZAN  
1414.203.19**

**Skripsi ini diajukan sebagai syarat memperoleh gelar Sarjana  
Komputer di Universitas Bina Darma**

**Pembimbing**

  
**Nyimas Sopiha, M.M., M.Kom.**

**Palembang, Maret 2020  
Fakultas Ilmu Komputer  
Universitas Bina Darma  
Dekan**

  
**Dedy Syamsuar, S.Kom., M.I.T., Ph.D.**

## HALAMAN PERSETUJUAN

Skripsi Berjudul "APLIKASI PENGAMANAN DOKUMEN MENGGUNAKAN ALGORITMA KUNCI PUBLIK ELGAMAL" Oleh "REZA DWI FAUZAN" telah dipertahankan didepan komisi penguji pada hari jumat tanggal 21 Februari 2020.

### Komisi Penguji

- |                      |                                 |         |
|----------------------|---------------------------------|---------|
| 1. Ketua Tim Penguji | Nyimas Sopiah, M.M., M.Kom.     | (.....) |
| 2. Anggota Penguji   | Eka Puji Agustini, M.M., M.Kom. | (.....) |
| 3. Anggota Penguji   | R.M. Nasrul Halim D, M.Kom.     | (.....) |

**Mengetahui**  
**Program Studi Informatika**  
**Fakultas Ilmu Komputer**  
**Universitas Bina Darma**

**Ketua Program Studi**  
Universitas **Bina Darma**  
Fakultas Ilmu Komputer  
**Dr. Widya Cholil, S.KOM., M.I.T.**

## SURAT PERNYATAAN

Saya yang bertanda tangan di bawah ini :

Nama : Reza Dwi Fauzan

Nim : 141420319

Dengan ini menyatakan bahwa :

1. Skripsi ini adalah asli dan belum pernah di ajukan untuk mendapatkan gelar sarjana di Universitas Bina Darma atau perguruan tinggi lain;
2. Skripsi ini murni gagasan, rumusan dan penelitian saya sendiri dengan arahan tim pembimbing;
3. Di dalam Skripsi ini tidak terdapat karya atau pendapat yang telah di tulis atau di publikasikan orang lain, kecuali secara tertulis dengan jelas di kutip dengan mencantumkan nama pengarang dan memasukkan ke dalam daftar rujukan;
4. Saya bersedia Skripsi yang saya hasilkan di cek keasliannya menggunakan plagiarism checker serta di unggah ke internet, sehingga dapat di akses public secara daring;
5. Surat Pernyataan ini saya tulis dengan sungguh-sungguh dan apabila terbukti melakukan penyimpangan atau ketidakbenaran dalam Pernyataan ini, saya bersedia menerima sanksi sesuai dengan peraturan dan perundang-undangan yang berlaku.

Demikianlah Surat Pernyataan ini saya buat agar dapat dipergunakan sebagaimana mestinya.

Palembang, 07 Maret 2020



Yang membuat pernyataan,

Reza Dwi Fauzan

NIM: 141420319

## MOTTO DAN PERSEMBAHAN

*Motto :*

- *“Jangan pernah menyerah ketika menghadapi rintangan dalam hidup”*
- *“Berlari dari masalah hanya akan memperpanjang masalah yang dihadapi”*
- *“Kerja keras dan usaha akan selalu membuahkan hasil”*
- *“Allah tidak akan meninggalkan hamba-Nya yang tetap yakin dan berusaha”*
- *“Jika tidak tahu cara melakukan sesuatu, maka belajar lah agar bisa”*
- *“Jangan pernah putus asah, berdoa dan minta tolong lah kepada Allah SWT dan tetap yakin”*

*Persembahan :*

- *Allah SWT yang telah memberi jalan dan kelancaran serta sehat jasmani dan rohani dalam penulisan skripsi ini.*
- *Ayah dan Ibu yang telah mendukung baik secara moral dan material selama penulisan skripsi ini.*
- *Saudara – saudara saya.*
- *Teman – teman yang telah membantu dalam kesusahan.*
- *Ibu Nyimas Sopiah, M.M., M.Kom. yang telah memberikan bimbingan selama proses penulisan skripsi*
- *Ibu Dr.Widya Cholil, S.Kom., M.I.T. Ketua Program Studi Informatika.*

## ABSTRAK

Penelitian ini memaparkan mengenai penelitian perancangan aplikasi pengamanan algoritma kriptografi (enkripsi dan dekripsi) yang menerapkan algoritma kunci publik asimetri Elgamal. Algoritma Elgamal ini di pilih karena algoritma ini merupakan salah satu dari algoritma asimetri yang cukup baru dan yang patennya baru dibuka pada tahun 1997. Suatu instansi atau perusahaan-perusahaan saat ini pasti memiliki suatu dokumen atau berkas yang tidak boleh di ganggu atau di rusak oleh pihak yang tidak bertanggung jawab, oleh sebab itu suatu instansi atau perusahaan tersebut pastilah sangat membutuhkan suatu aplikasi sistem untuk mengamankan dokumen penting. Dokumen yang banyak digunakan sekarang menggunakan dekstop seperti dokumen dari *microsoft office*, dan tidak sedikit pihak yang bertujuan untuk merusak atau mencuri dokumen dari suatu instansi atau perusahaan. Untuk itu peneliti ingin merancang suatu aplikasi yang dapat berguna bagi pengguna dalam perlindungan dokumen-dokumen yang di anggap perivasi. Untuk proses pengembangan sistem ini sendiri peneliti akan menggunakan metode RUP (*Rational Unified Process*) untuk membantu dalam proses penelitian dan pengembangan sistem. Hasil perancangan aplikasi ini sangat diharapkan dan ditujukan untuk mendasari penelitian-penelitian berikutnya tentang analisis algoritma kriptografi asimetri yang khususnya pada algoritma kunci publik elgamal. Selain itu hasil pengembangan ini juga ditujukan untuk pengajaran praktikum dalam mata kuliah kriptografi di program studi Informatika.

Kata kunci: Aplikasi, algoritma, asimetri, Elgamal.

## KATA PENGANTAR

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

Puji dan syukur kehadiran Allah SWT atas berkat, rahmat dan Karunia-Nya lah, Skripsi ini dapat diselesaikan guna untuk memenuhi syarat dalam menyelesaikan tugas akhir dan bisa lulus dari perkuliaan agar bisa memperoleh gelar sarjana. Disadari penulisan skripsi ini masih jauh untuk bisa dikatakan sempurna, telah dilakukan revisi dan perbaikan lebih dari satu kali agar akhirnya bisa diterima benar, hal tersebut dikarenakan penulis memiliki kemampuan yang terbatas, oleh karena itulah dibutuhkan bimbingan agar bisa menyelesaikan penulisan skripsi ini.

Pada kesempatan yang baik ini, penulis ingin menyampaikan rasa syukur dan ucapan terima kasih kepada pihak – pihak yang telah memberikan dukungan, bimbingan dan nasihat – nasihat selama penulisan skripsi berlangsung. Penulis mengucapkan terima kasih kepada:

1. Dr. Sunda Ariana, M.Pd, M.M. Selaku Rektor Universitas Bina Darma Palembang.
2. Dedy Syamsuar, S.Kom, MIT. Selaku Dekan Fakultas Ilmu Komputer.
3. Dr.Widya Cholil, S.Kom,MIT. Selaku Ketua Program Studi Informatika.
4. Nyimas Sopiah M.M., M.Kom. Selaku Pembimbing Utama yang telah memberikan arahan dan dukungan dalam penulisan skripsi.
5. Bapak dan Ibu saya yang telah memberikan dukungan moril dan materil kepada saya selama proses penulisan skripsi. Dan juga teman – teman dan saudara saya.

Palembang, Maret 2020  
Penulis

Reza Dwi Fauzan

## DAFTAR ISI

	<b>Halaman</b>
Cover Dalam.....	i
Halaman Pengesahan.....	ii
Halaman Persetujuan.....	iii
Pernyataan.....	iv
Motto Dan Persembahan.....	v
Abstrak.....	vi
Kata Pengantar.....	vii
Daftar Isi.....	viii
Daftar Gambar.....	xi
Daftar Table...../.....	xii
<b>BAB I PENDAHULUAN.....</b>	<b>1</b>
1.1 Latar Belakang.....	1
1.2 Rumusan Masalah.....	3
1.3 Batasan Masalah.....	3
1.4 Tujuan dan Manfaat Penelitian.....	3
1.4.1 Tujuan Penelitian.....	3
1.4.2 Manfaat Penelitian.....	3
1.5 Waktu dan Tempat.....	4
1.5.1 Waktu Penelitian.....	4
1.5.2 Tempat Penelitian.....	4
1.6 Metodologi.....	5
1.6.1 Metode Penelian.....	5
1.6.2 Metode Pengembangan Perangkat Lunak.....	5
1.6.3 Alat Penelitian.....	7
1.7 Sistematika Penulisan.....	7
<b>BAB II TINJAUAN PUSTAKA.....</b>	<b>9</b>



2.1 Landasan Teori.....	9
2.1.1 Aplikasi.....	9
2.1.2 Algoritma Kriptografi Elgamal.....	10
2.1.3 HTML.....	15
2.1.4 JavaScript.....	16
2.1.5 Metode Pengembangan Sistem.....	17
2.2 Penelitian Sebelumnya.....	20
2.3 Kerangka Berfikir.....	22
<b>BAB III ANALISIS DAN PERANCANGAN.....</b>	<b>24</b>
3.1 <i>Inception</i> (Permulaan).....	24
3.1.1 Definisi Kegiatan.....	24
3.1.2 Analisis Batasan Kegiatan.....	26
3.1.3 Analisis Kebutuhan Fungsional.....	26
3.1.4 Analisis Kebutuhan Sistem.....	27
3.2 <i>Elaboration</i> (Perluasaan).....	27
3.2.1 Desain Sistem.....	27
3.2.2 Perancangan antarmuka (Interface).....	30
<b>BAB IV HASIL DAN IMPLEMENTASI.....</b>	<b>34</b>
4.1 Hasil Penelitian.....	34
4.1.1 Menu Halaman Utama.....	35
4.1.2 Menu Halaman Enkripsi.....	36
4.1.3 Menu Halaman Dekripsi.....	39
4.2 Implementasi.....	42
4.2.1 Enkripsi Dengan Metode Elgamal.....	42
4.2.2 Dekripsi Dengan Metode Elgamal.....	42
4.2.3 Implementasi Algoritma Elgamal.....	43
4.2.4 Perbandingan Sebelum dan Setelah Enrkripsi.....	45
<b>BAB V KESIMPULAN DAN SARAN.....</b>	<b>47</b>

5.1 Kesimpulan.....	47
5.2 Saran.....	48
<b>DAFTAR PUSTAKA.....</b>	<b>49</b>
<b>LAMPIRAN.....</b>	<b>50</b>

## DAFTAR GAMBAR

	<b>Halaman</b>
<b>Gambar 2.1</b> Skema Kriptografi Asimetri.....	11
<b>Gambar 2.2</b> Skema Kriptografi Kunci Publik Elgamal.....	13
<b>Gambar 2.3</b> Struktur Penulisan <i>Javascript</i> .....	17
<b>Gambar 2.4</b> Arsitektur <i>Rational Unified Process</i> .....	18
<b>Gambar 2.5</b> Kerangka Berfikir.....	22
<b>Gambar 3.1</b> <i>Uce Case Diagram</i> .....	28
<b>Gambar 3.2</b> <i>Activity Diagram</i> .....	29
<b>Gambar 3.3</b> <i>Class Diagram</i> .....	30
<b>Gambar 3.4</b> Rancangan Halaman Utama.....	31
<b>Gambar 3.5</b> Rancangan Halaman <i>Privatekey</i> .....	31
<b>Gambar 3.6</b> Rancangan Halaman Enkripsi.....	32
<b>Gambar 3.7</b> Rancangan Halaman Dekripsi.....	32
<b>Gambar 4.1</b> Tampilan Halaman Utama.....	35
<b>Gambar 4.2</b> Tampilan Menu Enkripsi.....	36
<b>Gambar 4.3</b> Proses Memilih <i>Plaintext</i> .....	37
<b>Gambar 4.4</b> Menu <i>Input Password</i> Enkripsi.....	37
<b>Gambar 4.5</b> Menu Download Hasil Enkripsi.....	38
<b>Gambar 4.6</b> Hasil Enkripsi.....	38
<b>Gambar 4.7</b> Tampilan Menu Dekripsi.....	39
<b>Gambar 4.8</b> Proses Memilih <i>Chipertext</i> .....	40
<b>Gambar 4.9</b> Menu <i>Input Password</i> Dekripsi.....	40
<b>Gambar 4.10</b> Menu <i>Download</i> Hasil Dekripsi.....	41
<b>Gambar 4.11</b> Contoh Dokumen <i>Plaintext</i> .....	41
<b>Gambar 4.12</b> <i>Source Code</i> Proses Enkripsi.....	42
<b>Gambar 4.13</b> <i>Source Code</i> Proses Dekripsi.....	43

## DAFTAR TABLE

	<b>Halaman</b>
<b>Table 2.1</b> Tabel Enkripsi.....	15
<b>Tabel 2.2</b> Tabel Dekripsi.....	15
<b>Tabel 4.1</b> Persentase Keberhasilan Enkripsi File.....	43
<b>Tabel 4.2</b> Persentase Keberhasilan Dekripsi File.....	44
<b>Tabel 4.3</b> Persentase Sebelum dan Setelah Enkripsi.....	45