

**HYBRID KRIPTOGRAFI CIPHER BLOCK CHAINING DAN ELGAMAL  
UNTUK KEAMANAN DATA TEXT**

**SKRIPSI**

**Disusun untuk memenuhi sebagian persyaratan  
mencapai derajat Sarjana**



**Disusun Oleh:**

Rinday Zildjiani Salji

2000018135

**PROGRAM STUDI S1 INFORMATIKA  
FAKULTAS TEKNOLOGI INDUSTRI  
UNIVERSITAS AHMAD DAHLAN**

**2024**

**HALAMAN JUDUL**  
**HYBRID KRIPTOGRAFI *CIPHER BLOCK CHAINING* DAN ELGAMAL**  
**UNTUK KEAMANAN DATA TEXT**  
**SKRIPSI**



**Disusun Oleh:**  
RINDAY ZILDJIANI SALJI  
2000018135

**PROGRAM STUDI S1 INFORMATIKA**  
**FAKULTAS TEKNOLOGI INDUSTRI**  
**UNIVERSITAS AHMAD DAHLAN**

**2024**

**LEMBAR PERSETUJUAN PEMBIMBING  
SKRIPSI**

**HYBRID KRIPTOGRAFI CIPHER BLOCK CHAINING DAN ELGAMAL  
UNTUK KEAMANAN DATA TEXT**

Dipersiapkan dan disusun oleh:

**RINDAY ZILDJIANI SALJI**

**2000018135**



**Program Studi S1 Informatika  
Fakultas Teknologi Industri  
Universitas Ahmad Dahlan**

Telah disetujui oleh:

**Pembimbing**

**Ir. Nur Rochmah Dyah Puji Astuti, S.T., M.Kom.**

**NIP.197608192005012001**

LEMBAR PENGESAHAN  
SKRIPSI

HYBRID KRIPTOGRAFI CIPHER BLOCK CHAINING DAN ELGAMAL UNTUK  
KEAMANAN DATA TEXT

Dipersiapkan dan disusun oleh:  
RINDAY ZILDJANI SALJI  
2000018135

Telah dipertahankan di depan Dewan Penguji  
pada tanggal Hari Bulan Tahun  
dan dinyatakan telah memenuhi syarat

Susunan Dewan Penguji

Ketua : Ir. Nur Rochmah Dyah Puji Astuti, S.T., M.Kom.


NIP. 197608192005012001

Penguji I : Eko Aribowo, S.T., M.Kom.


NIP. 197002062005011001

Penguji II : Ir. Nuril Anwar, S.T., M.Kom.

NIPM. 19890409 201606 111 1228017

 18/4/2024

 18/4/2024

 18/4/2024

Yogyakarta, 20 Maret 2024

Dekan Fakultas Teknologi Industri  
Universitas Ahmad Dahlan



Prof. Dr. Ir. Siti Jamilatun, M.T.

NIP. 19660812 199601 011 0784324

**LEMBAR PERNYATAAN KEASLIAN  
SURAT PERNYATAAN**

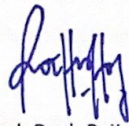
Yang bertanda tangan di bawah ini:

Nama : Rinday Zildjiani Salji  
NIM : 2000018135  
Prodi : Informatika  
Judul TA/Skripsi : *HYBRID KRIPTOGRAFI CIPHER BLOCK CHAINING DAN ELGAMAL*  
UNTUK KEAMANAN DATA TEXT

Dengan ini saya menyatakan bahwa Laporan Tugas Akhir ini tidak terdapat karya yang pernah diajukan untuk memperoleh gelar Ahli Madya/Kesarjanaan di suatu Perguruan Tinggi, dan sepanjang pengetahuan saya juga tidak terdapat karya atau pendapat yang pernah ditulis atau diterbitkan oleh orang lain, kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan dalam daftar pustaka.

Yogyakarta, 15 Maret 2024

Mengetahui,  
Dosen Pembimbing



Ir. Nur Rochmah Dyah Puji Astuti, S.T., M.Kom.  
NIP.197608192005012001

Yang menyatakan,



Rinday Zildjiani Salji  
NIM. 2000018135

## PERNYATAAN TIDAK PLAGIAT

Saya yang bertanda tangan di bawah ini:

Nama : Rinday Zildjiani Salji  
NIM : 2000018135  
Email : [rinday2000018135@webmail.uad.ac.id](mailto:rinday2000018135@webmail.uad.ac.id)  
Program Studi : S1 Informatika  
Fakultas : Teknologi Industri  
Judul Tesis : *HYBRID KRIPTOGRAFI CIPHER BLOCK CHAINING DAN ELGAMAL*  
UNTUK KEAMANAN DATA TEXT

Dengan ini menyatakan bahwa:

1. Hasil karya yang saya serahkan ini adalah asli dan belum pernah diajukan untuk mendapatkan gelar kesarjanaan baik di Universitas Ahmad Dahlan maupun di institusi pendidikan lainnya.
2. Hasil karya saya ini bukan saduran/terjemahan melainkan merupakan gagasan, rumusan, dan hasil pelaksanaan penelitian/implementasi saya sendiri, tanpa bantuan pihak lain, kecuali arahan pembimbing akademik dan narasumber penelitian.
3. Hasil karya saya ini merupakan hasil revisi terakhir setelah diujikan yang telah diketahui dan disetujui oleh pembimbing.
4. Dalam karya saya ini tidak terdapat karya atau pendapat yang telah ditulis atau dipublikasikan orang lain, kecuali yang digunakan sebagai acuan dalam naskah dengan menyebutkan nama pengarang dan dicantumkan dalam daftar pustaka.

Pernyataan ini saya buat dengan sesungguhnya. Apabila di kemudian hari terbukti ada penyimpangan dan ketidakbenaran dalam pernyataan ini maka saya bersedia menerima sanksi akademik berupa pencabutan gelar yang telah diperoleh karena karya saya ini, serta sanksi lain yang sesuai dengan ketentuan yang berlaku di Universitas Ahmad Dahlan.

Yogyakarta, 15 Maret 2024

Yang Menyatakan



Rinday Zildjiani Salji

## LEMBAR PERSETUJUAN AKSES

Saya yang bertanda tangan di bawah ini:

Nama : Rinday Zildjiani Salji  
NIM : 2000018135  
Email : [rinday2000018135@webmail.uad.ac.id](mailto:rinday2000018135@webmail.uad.ac.id)  
Program Studi : S1 Informatika  
Fakultas : Teknologi Industri  
Judul Tesis : *HYBRID KRIPTOGRAFI CIPHER BLOCK CHAINING DAN  
ELGAMAL UNTUK KEAMANAN DATA TEXT*

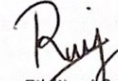
Dengan ini Saya menyerahkan hak sepenuhnya kepada Perpustakaan Universitas Ahmad Dahlan untuk menyimpan, mengatur akses serta melakukan pengelolaan terhadap karya saya ini dengan mengacu pada ketentuan akses tesis elektronik sebagai berikut (beri tanda pada kotak):

Saya (~~tidak mengizinkan~~ *mengizinkan*) \* karya tersebut diunggah ke dalam aplikasi Repository Perpustakaan Universitas Ahmad Dahlan.

Demikian pernyataan ini Saya buat dengan sebenarnya.

Yogyakarta, 15 Maret 2024

Menyatakan



Rinday Zildjiani Salji

Mengetahui,

Dosen Pembimbing Skripsi



Ir. Nur Rochmah Dyah Purnastuti, S.T., M.Kom.  
NIP.197608192005012001

## KATA PENGANTAR

Assalamualaikum Wr.Wb.

Puji Syukur penulis panjatkan ke hadirat Allah SWT atas segala karunia-Nya, yang telah melimpahkan nikmat-Nya sehingga penulis dapat menyelesaikan penulisan skripsi ini dengan judul “Hybrid Kriptografi *Cipher Block Chaining* (CBC) dan Elgamal Untuk Keamanan Data Text”.

Skripsi ini disusun sebagai salah satu syarat untuk memperoleh gelar Strata Satu (S1) pada Program Studi Informatika di Universitas Ahmad Dahlan. Skripsi ini terselesaikan atas bantuan banyak pihak, penulis ingin mengucapkan rasa terima kasih yang sebesar-besarnya kepada:

1. Orang tua saya ibu Erda Ayu dan Ayah Riduan yang selalu memberikan doa, perhatian, dukungan moral dan materi, serta nasehat sehingga saya dapat menyelesaikan skripsi ini dengan baik.
2. Bapak Jefree Fahana, S.T., M.Kom selaku Dosen Pembimbing Akademik.
3. Ibu Nur Rochmah Dyah Puji Astuti, S.T., M.Kom. selaku Dosen Pembimbing yang telah memberikan arahan, serta dengan tabah dalam membimbing skripsi saya.
4. Bapak Eko Aribowo, S.T., M.Kom. dan Bapak Ir. Nuril Anwar, S.T., M.Kom. selaku Dosen Penguji Skripsi.
5. Kepada Almarhumah Adik perempuan saya Rainnisa Wardah, yang selalu turut serta memberikan dukungan, doa, dan semangat.
6. Sahabat Seperjuangan saya Akbar, Aan, Akmal, Elinda, Dhani yang menjadi teman saya sejak awal masuk kuliah hingga dapat menyelesaikan skripsi.
7. Semua pihak yang telah membantu dan tidak bisa di sebutkan satu persatu.

Akhir kata, penulis menyadari bahwa skripsi ini masih memiliki kekurangan, penulis menerima segala kritik, saran, dan masukan dari pembaca guna perbaikan dan pengembangan penelitian dimasa yang akan datang. Semoga skripsi ini dapat memberikan manfaat dan kontribusi dalam bidang ilmu yang diteliti.

Wassalamualaikum Wr. Wb.

Yogyakarta, 15 Maret 2024

Penulis



## **MOTTO**

“Sesungguhnya bersama kesulitan ada Kemudahan”

**-(Qr. Asy-Syarah:6)-**

“Apabila sesuatu yang kau senangi tidak terjadi maka senangilah apa yang terjadi”

**-Ali bin Abi Thalib-**

## DAFTAR ISI

HALAMAN JUDUL .....	II
LEMBAR PERSETUJUAN PEMBIMBING .....	III
LEMBAR PENGESAHAN.....	IV
LEMBAR PERNYATAAN KEASLIAN.....	V
PERNYATAAN TIDAK PLAGIAT .....	VI
LEMBAR PERSETUJUAN AKSES .....	VII
KATA PENGANTAR.....	VIII
MOTTO.....	IX
DAFTAR ISI.....	X
DAFTAR GAMBAR.....	XII
DAFTAR TABEL.....	XIII
DAFTAR KODE PROGRAM.....	XIV
DAFTAR RUMUS .....	XV
DAFTAR LAMPIRAN .....	XVI
ABSTRAK.....	XVII
BAB I.....	1
1.1 Latar Belakang .....	1
1.2 Batasan Masalah .....	2
1.3 Rumusan Masalah .....	2
1.4 Tujuan Penelitian.....	2
1.5 Manfaat Penelitian .....	3
BAB II.....	4
2.1 Kajian Penelitian Terdahulu.....	4
2.2 Landasan Teori .....	11
1. Keamana Data .....	11
2. Kriptografi .....	11
3. Algoritma Elgamal .....	12
4. Algoritma <i>Cipher Block Chaining</i> .....	16
5. <i>Hybrid</i> Kriptografi .....	19
6. <i>White Box</i> .....	20
7. <i>Black Box</i> .....	20
BAB III.....	22
3.1 Pengumpulan Data .....	22
3.2 Alat dan Bahan .....	22
1 Perangkat Keras ( <i>Hardware</i> ).....	22
2 Perangkat Lunak ( <i>Software</i> ).....	22
3.3 Tahapan Penelitian.....	23
1 Studi Literatur.....	23
2 Desain <i>Hybrid Cryptosystem</i> .....	23
3 <i>Software</i> dan <i>Hardware</i> .....	24
4 Analisis .....	24
5 Perancangan.....	24
6 Implementasi.....	24

7	Pengujian.....	24
BAB IV	.....	25
4.1	Perancangan Proses <i>Hybrid Cryptosystem</i> .....	25
1	Pembentukan Kunci Elgamal .....	26
2	Enkripsi <i>Hybrid CBC</i> .....	28
3	Dekripsi <i>Hybrid CBC</i> .....	31
4.2	Implementasi <i>Hybrid Cryptosystem</i> .....	32
1	<i>Use Case Diagram</i> .....	32
2	<i>Activity Diagram</i> .....	33
3	Rancangan <i>Frontpage</i> .....	37
4	<i>Source Code</i> .....	40
4.3	Pengujian <i>Hybrid Cryptosystem</i> .....	59
1	<i>White Box</i> .....	59
2	<i>Black Box</i> .....	72
3	Kecepatan <i>Hybrid</i> .....	73
BAB V	.....	75
5.1	Kesimpulan.....	75
5.2	Saran.....	75
DAFTAR PUSTAKA	.....	76
LAMPIRAN	.....	78

## DAFTAR GAMBAR

Gambar 2. 1 Diagram Enkripsi CBC.....	16
Gambar 2. 2 Diagram Dekripsi CBC .....	18
Gambar 2. 3 Diagram Hybrid Kriptografi .....	20
Gambar 3. 1 Diagram Tahapan Penelitian .....	23
Gambar 4. 1 Diagram Hybrid Cryptosystem CBC dan elgamal .....	26
Gambar 4. 2 Diagram Pembangkit Kunci Elgamal .....	27
Gambar 4. 3 Diagram Enkripsi Cipher Block Chaining .....	28
Gambar 4. 4 Diagram Dekripsi hybrid .....	31
Gambar 4. 5 Use Case Hybrid Kriptografi .....	33
Gambar 4. 6 Activity diagram Pembangkitan kunci elgamal .....	34
Gambar 4. 7 Activity diagram Enkripsi Hybrid .....	35
Gambar 4. 8 Activity Diagram Dekripsi Elgamal x CBC.....	36
Gambar 4. 9 Rancangan Frontpage halaman Tentang .....	37
Gambar 4. 10 Rancangan Frontpage halaman Tutorial .....	38
Gambar 4. 11 Rancangan Frontpage halaman pembangkitan kunci elgamal .....	39
Gambar 4. 12 Rancangan Frontpage halaman enkripsi.....	39
Gambar 4. 13 Rancangan Frontpage halaman dekripsi.....	40
Gambar 4. 14 Halaman About .....	41
Gambar 4. 15 Halaman Tutorial .....	44
Gambar 4. 16 Halaman pembangkitan kunci elgamal .....	47
Gambar 4. 17 Halaman Enkripsi .....	49
Gambar 4. 18 Halaman Dekripsi.....	55
Gambar 4. 19 Flow Graph Pengujian Elgamal .....	62
Gambar 4. 20 Flow Graph Pengujian CBC.....	66
Gambar 4. 21 Flow Graph Pengujian Dekripsi .....	70

## DAFTAR TABEL

Tabel 2. 1 Kajian penelitian terdahulu .....	7
Tabel 2. 2 Plaintext Perhitungan elgamal .....	14
Tabel 2. 3 Hasil Enkripsi ELgamal.....	14
Tabel 2. 4 Hasil Dekripsi Elgamal .....	15
Tabel 2. 5 Plaintext Enkripsi CBC .....	17
Tabel 2. 6 Kunci CBC .....	17
Tabel 2. 7 Inital Vektor CBC .....	17
Tabel 2. 8 Block Plaintext CBC .....	17
Tabel 2. 9 Ciphertext CBC .....	19
Tabel 2. 10 Hasil Perhitungan Dekripsi CBC.....	19
Tabel 4. 1 Kunci Elgamal .....	27
Tabel 4. 2 Enkripsi Kunci.....	28
Tabel 4. 3 konversi kunci elgamal ke biner.....	29
Tabel 4. 4 block plaintext .....	29
Tabel 4. 5 Initia vektor.....	29
Tabel 4. 6 Hasil perhitungan Enkripsi CBC.....	30
Tabel 4. 7 Hasil Ciphertext.....	30
Tabel 4. 8 Warpping Ciphertext.....	31
Tabel 4. 9 Hasil Akhri Dekripsi Hybrid.....	32
Tabel 4. 10 Hasil Plaintext .....	32
Tabel 4. 11 Matriks Graf Algoritma Elgamal .....	63
Tabel 4. 12 Hasil Pengujian Elgamal .....	64
Tabel 4. 13 graph matrix hybrid Enkripsi .....	67
Tabel 4. 14 Hasil dari pengujia white box Hybrid .....	68
Tabel 4. 15 Matriks Graf CBC.....	71
Tabel 4. 16 hasil pengujian Whitebox dekripsi Hybrid .....	72
Tabel 4. 17 Skenario Pengujian Black Box .....	72
Tabel 4. 18 Kecepatan Proses Hybrid .....	73

## DAFTAR KODE PROGRAM

Kode Program 4. 1 Halaman About .....	41
Kode Program 4. 2 Halaman Tutorial .....	44
Kode Program 4. 3 Halaman Pembangkitan Kunci Elgamal .....	48
Kode Program 4. 4 Halaman Enkripsi .....	50
Kode Program 4. 5 Halaman Deskripsi .....	56
Kode Program 4. 6 Algoritma Pengujian Kunci Elgamal .....	60
Kode Program 4. 7 Pengujian algoritma hybrid Enkripsi .....	64
Kode Program 4. 8 Algoritma hybrid Dekripsi .....	68

## DAFTAR RUMUS

<i>Rumus 2.1 Mencari Nilai y</i> .....	12
<i>Rumus 2.2 Enkripsi elgamal nilai a</i> .....	13
<i>Rumus 2.3 Enkripsi elgamal nilai b</i> .....	13
<i>Rumus 2.4 Dekripsi elgamal nilai a</i> .....	13
<i>Rumus 2.5 Dekripsi elgamal nilai b</i> .....	13
<i>Rumus 2.6 Enkripsi CBC</i> .....	17
<i>Rumus 2.7 Dekripsi CBC</i> .....	19

## DAFTAR LAMPIRAN

Lampiran 1 Hasil pengujian Black Box .....	78
Lampiran 2 Hasil pengujian Black Box .....	78
Lampiran 3 Hasil pengujian Black Box .....	79
Lampiran 4 Hasil pengujian Black Box .....	79
Lampiran 5 Hasil pengujian Black Box .....	79
Lampiran 6 Hasil pengujian Black Box .....	80
Lampiran 7 Hasil pengujian Black Box .....	80
Lampiran 8 Hasil pengujian Black Box .....	80
Lampiran 9 Hasil pengujian Black Box .....	81
Lampiran 10 Hasil pengujian Black Box .....	81
Lampiran 11 Hasil pengujian Black Box .....	81



## ABSTRAK

Dalam pertukaran pesan, menjaga kerahasiaan informasi penting untuk mencegah pihak yang tidak berwenang memahaminya. Keamanan data digunakan agar data yang kita miliki terlindungi dan terjamin, terdapat tiga perspektif pada keamanan data yaitu kerahasiaan data, keutuhan data, dan ketersediaan data. Kebocoran data dapat terjadi karena kurangnya pengamanan pada sistem informasi, kriptografi merupakan upaya untuk melakukan keamanan data text.

Algoritma kriptografi yang digunakan dalam penelitian adalah algoritma cipher block chaining yang merupakan kriptografi simetris dan algoritma elgamal yang merupakan kriptografi asimetri. Metode yang akan dilakukan adalah hybrid pada kedua algoritma pada pengamanan data text.

Pengujian terhadap hybrid kriptografi menggunakan metode white box dengan hasil proses hybrid berjalan sesuai dengan alur, Dari hasil perhitungan black box terbukti bahwa pengujian black box terhadap fungsi aplikasi *Hybrid Kriptografi Cipher Block Chaining* dan Elgamal mendapatkan persentase penerimaan sebesar 100%, pengujian kecepatan yang sudah diterapkan menggunakan 5 data dengan panjang *plaintext* yang berbeda proses enkripsi membutuhkan waktu yang lebih lama dibandingkan dengan proses dekripsi.

**Kata Kunci** : Kriptografi, Algoritma Hybrid, Elgamal, Cipher Block Chaining, Data text.