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 ZILDJIANI 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. ..... 18/4 2024.

NIP. 197608192005012001

Penguji I : Eko Aribowo, S.T., M.Kom. 26/3/24

NIP. 197002062005011001

Penguji II : Ir. Nuril Anwar, S.T., M.Kom. ..... 29-3-2024.

NIPM. 19890409 201606 111 1228017

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	Yang menyatakan,
Ir. Nur Rochmah Dyah Puji Astuti, S.T., M.Kom.	Rinday Zildjiani Salji
NIP.197608192005012001	NIM. 2000018135

PERNYATAAN TIDAK PLAGIAT

Saya yang bertanda tangan di bawah ini:

Nama	:	Rinday Zildjiani Salji
NIM	:	2000018135
Email	:	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

y Zildjiani Salji

LEMBAR PERSETUJUAN AKSES

Saya yang bertanda tangan di bawah ini:

Nama	:	Rinday Zildjiani Salji
NIM	:	2000018135
Email	:	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 (**mengijinkan/~~tidak mengijinkan~~**)* 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 Rochman Dyah Puji Astuti, 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-Syarh:6)-

“Apabila sesuatu yang kau senangi tidak terjadi maka senangilah apa yang terjadi”
-Ali bin Abi Thalib-

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR KODE PROGRAM

DAFTAR RUMUS

DAFTAR LAMPIRAN

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 kerahasian 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.