



**PENERAPAN ALGORITMA *BLOWFISH* DAN *ELGAMAL* UNTUK
PENGAMANAN DATA SEKUNDER *DATABASE***

SKRIPSI

Harry Darmawan Siregar

1710511009

**PROGRAM STUDI INFORMATIKA, PROGRAM SARJANA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS PEMBANGUNAN NASIONAL VETERAN JAKARTA
2021**



**PENERAPAN ALGORITMA *BLOWFISH* DAN *ELGAMAL* UNTUK
PENGAMANAN DATA SEKUNDER *DATABASE***

SKRIPSI

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

Harry Darmawan Siregar

1710511009

**PROGRAM STUDI INFORMATIKA, PROGRAM SARJANA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS PEMBANGUNAN NASIONAL VETERAN JAKARTA
2021**

PERNYATAAN ORISINALITAS

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

Nama : Harry Darmawan Siregar

NIM : 1710511009

Tanggal : 28 juni 2021

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

Bekasi, 28 Juni 2021

Yang Menyatakan,



(Harry Darmawan Siregar)

PERNYATAAN PERSETUJUAN PUBLIKASI SKRIPSI UNTUK KEPENTINGAN AKADEMIS

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

Nama : Harry Darmawan Siregar
NIM : 1710511009
Fakultas : Ilmu Komputer
Program Studi : Informatika

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

PENERAPAN ALGORITMA BLOWFISH DAN ELGAMAL UNTUK PENGAMANAN DATA SEKUNDER DATABASE

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 data (database), 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 : Bekasi

Pada Tanggal : 28 Juni 2021

Yang Menyatakan,



(Harry Darmawan Siregar)

LEMBAR PENGESAHAN

Dengan ini dinyatakan bahwa Skripsi berikut :

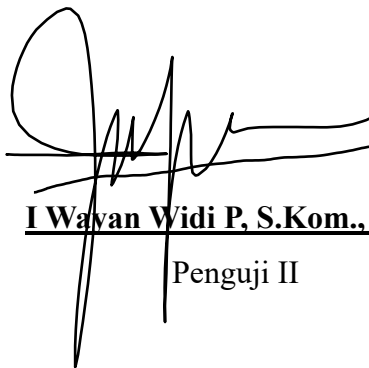
Nama : Harry Darmawan Siregar
NIM : 1710511009
Program Studi : Informatika
Judul Skripsi : Penerapan Algoritma Blowfish Dan Elgamal Untuk Pengamanan Data Sekunder Database.

Telah berhasil dipertahankan di hadapan Tim Penguji dan diterima sebagai bagian persyaratan yang diperlukan untuk memperoleh gelar Sarjana Komputer pada Program Studi S1 Informatika, Fakultas Ilmu Komputer, Universitas Pembangunan Nasional Veteran Jakarta.



Iin Ernawati, S.Kom., M.Si.

Penguji I



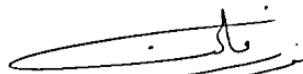
I Wayan Widi P, S.Kom., MTI.

Penguji II



Henki Bayu Seta, S.Kom., MTI.

Pembimbing I



Noor Falih, S.Kom., M.T.

Pembimbing II



Dr. Ermatita, M.Kom.

Dekan



Yuni Widiastiwi, S.Kom., Msi.

Ketua Program Studi

Ditetapkan di : Jakarta
Tanggal Pengesahan : 16 Juli 2021



PENERAPAN ALGORITMA *BLOWFISH* DAN *ELGAMAL* UNTUK PENGAMANAN DATA SEKUNDER *DATABASE*

Harry Darmawan Siregar

ABSTRAK

Perkembangan teknologi mengakibatkan pemanfaatan teknologi informasi salah satunya pemanfaatan pada *E-commerce*. *E-commerce* diterapkan pada berbagai *platform* seperti *personal computer*(PC) dan *mobile smartphone*. Karena banyak berbagai *platform* maka banyak juga penggunaanya. Para pengguna *E-commerce* melakukan *register* yang mengharuskan memasukan nomor telepon, nama dan alamat dimana data-data tersebut adalah data sekunder yang tidak dilindungi keamanan pada *database*. Data tersebut sangatlah penting karena dapat disalahgunakan oleh pihak tidak bertanggung jawab seperti menjual data tersebut. Berdasarkan dari kasus tersebut penelitian ini ingin meneliti untuk meningkatkan keamanan informasi data sekunder dengan penerapan kombinasi algoritma *Blowfish* dan *Elgamal* pada data sekunder *database* agar dapat dilindungi jika terjadi kebocoran data. Pengamanan data dengan melakukan enkripsi dengan *Blowfish* kemudian cipherteks akan kembali dienkripsi lagi dengan *Elgamal* diharapkan dapat meningkatkan keamanan data pada *database* sehingga pengguna *E-commerce* dapat merasa lebih aman saat mempercayakan datanya saat registrasi. Hasil luaran yang didapatkan dari penelitian ini adalah penerapan algoritma *Blowfish* dan algoritma *Elgamal* dapat meningkatkan keamanan data dari serangan *brute force attack* pada cipherteks data sekunder pada *database* dengan penerapan pada perangkat lunak berbasis *website* dengan waktu proses enkripsi dan dekripsi serta penggunaan sumber daya yang cukup efisien.

Kata Kunci : *database*, *Blowfish*, *Elgamal*, data sekunder.

APPLICATION OF BLOWFISH AND ELGAMAL ALGORITHM FOR DATABASE SECONDARY DATA SECURITY

Harry Darmawan Siregar

ABSTRACT

Technological developments have resulted in the use of information technology, one of which is the usage of e-commerce. E-commerce had been applied to various platforms such as personal computers (PCs) and mobile smartphones. Because there are many different platforms, there are also many *users*. The *users* of E-commerce are required to insert their personal data such as phone number, name, and address where those data are called secondary data in a database which is not secured almost on all databases. This kind of data are can be very important too because the irresponsible people who steal and got this data can abuse it to do bad things like selling it. Based on this case, this research wants to research how to improve the security of secondary data information by applying the combination of Blowfish and Elgamal algorithms to the secondary data database so that it can be more secured in case if there is data leakage. Data security by encrypting with Blowfish then ciphertext will be re-encrypted again with Elgamal is expected to improve data security in the database so that E-commerce *users* can feel more secure when entrusting their data during registration. The output obtained from this research are the application of the Blowfish algorithm and the Elgamal algorithm which can improve data security from possibility of brute force attacks on secondary data ciphertext in the database by applying it to website-based software with encryption and decryption process time and efficient use of resources.

Keywords : *database, Blowfish, Elgamal, secondary data.*

KATA PENGANTAR

Pertama-tama penulis ingin memanjatkan puji dan syukur atas kehadiran Allah SWT karena rahmat serta karunia yang diberikan kepada penulis sehingga diberikan kesehatan dan dapat menyelesaikan Skripsi tugas akhir di masa pandemi Covid 19 ini dengan judul: “Penerapan Algoritma Blowfish dan Algoritma Elgamal untuk Mengamankan Data Sekunder Database” yang ditujukan untuk menjadi syarat kelulusan untuk menyelesaikan studi Sarjana Pendidikan Strata Satu program studi Informatika Fakultas Ilmu Komputer Universitas Pembangunan Nasional Jakarta. Kemudian tidak lupa penulis perlu berterima kasih atas dukungan, doa, dan bimbingan dari banyak pihak yaitu kepada :

1. Kedua orang tua penulis yang telah mendukung serta doa-doanya dan memberikan semangat agar Skripsi tugas akhir ini dapat diselesaikan,
2. Bapak Henki Bayu Seta, S.Kom., MTI. selaku Dosen Pembimbing yang telah membimbing penulis dalam menyusun dan menulis Skripsi tugas akhir ini.
3. Noor Falih, S.Kom., M.T. yaitu selaku Dosen Pembimbing yang telah membimbing penulis dalam menyusun dan menulis Skripsi tugas akhir ini.
4. Ibu Iin Ernawati, S.Kom., M.Si. yaitu selaku Dosen Penguji yang telah memberikan masukan dan saran pada saat pengujian skripsi tugas akhir.
5. Bapak I Wayan Widi P, S.Kom., MTI. selaku Dosen Penguji yang telah memberikan masukan dan saran pada saat pengujian skripsi tugas akhir.
6. Bapak/Ibu dosen Informatika Universitas Pembangunan Nasional Veteran Jakarta yang telah memberikan ilmu kepada penulis sehingga mendapatkan ilmu yang bermanfaat.
7. Teman - teman penulis yang telah menyediakan waktu untuk berdiskusi dengan saya mengenai Skripsi tugas akhir.

Penulis menyadari bahwa Skripsi yang ditulis ini masih belum sempurna . Diharapkan semoga skripsi tugas akhir penulis dapat bermanfaat terutama untuk penelitian yang akan dilakukan selanjutnya.

Bekasi, 29 Juni 2021

A handwritten signature in black ink, consisting of stylized cursive letters, likely representing the author's name.

Penulis

DAFTAR ISI

PENERAPAN ALGORITMA <i>BLOWFISH</i> DAN <i>ELGAMAL</i> UNTUK PENGAMANAN DATA SEKUNDER <i>DATABASE</i>	ii
PERNYATAAN ORISINALITAS	iii
PERNYATAAN PERSETUJUAN PUBLIKASI SKRIPSI UNTUK KEPENTINGAN AKADEMIS	iv
LEMBAR PENGESAHAN	v
ABSTRAK	vi
ABSTRACT	vii
KATA PENGANTAR	viii
DAFTAR ISI	x
DAFTAR GAMBAR	xv
DAFTAR TABEL	xvi
BAB 1 PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah	4
1.3 Batasan Masalah	4
1.4 Tujuan Penelitian	5
1.5 Manfaat Penelitian	5
1.6 Luaran yang diharapkan	5
1.7 Sistematika Penulisan	5
BAB 2 LANDASAN TEORI	7
2.1 Kriptografi	7
2.2 Plainteks	7

2.3 Cipherteks	7
2.5 Kriptografi Simetris	8
2.6 Kriptografi Asimetris	8
2.7 <i>Blowfish</i>	8
2.7.1 Enkripsi-Dekripsi <i>Blowfish</i>	8
2.8 <i>Elgamal</i>	10
2.8.1 Pembentukan Kunci	10
2.8.2 Proses Enkripsi	11
2.8.3 Proses Dekripsi	11
2.9 <i>Database</i>	13
2.10 Data	13
2.11 <i>Blowfish</i> ECB	13
2.12 ASCII	13
2.13 Pengujian Metode <i>Black box</i>	15
2.14 Pengujian Metode <i>Load Testing</i>	15
2.15 Penelitian Terkait	15
BAB 3 METODE PENELITIAN	19
3.1 Kerangka Pikir	19
3.1.1 Identifikasi Masalah	20
3.1.2 Studi Literatur	20
3.1.3 Analisis Perancangan Perangkat Lunak	21
3.1.4 Perancangan Perangkat Lunak	21
3.1.5 Implementasi	24
3.1.6 Pengujian Sistem	24
3.1.7 Analisis Hasil	24

3.1.8 Kesimpulan.....	25
3.1.9 Dokumentasi.....	25
3.2 Alat Bantu Penelitian	25
3.3 Jadwal Penelitian.....	26
BAB 4 HASIL DAN PEMBAHASAN.....	27
4.1 Data.....	27
4.2 Kebutuhan Perancangan Perangkat Lunak	28
4.3 Analisis Perancangan Proses Enkripsi dan Dekripsi Perangkat Lunak	28
4.3.1 Analisis Perancangan Cara Kerja Proses Enkripsi.....	28
4.3.2 Analisis Perancangan Proses Dekripsi.....	36
4.3.3 Analisis Proses Pembangkitan Kunci <i>Blowfish-Elgamal</i>	39
4.3.4 Analisis Perhitungan Proses Enkripsi Algoritma <i>Blowfish-Elgamal</i>	43
4.3.5 Analisis Perhitungan Proses Dekripsi Algoritma <i>Blowfish-Elgamal</i>	62
4.4 Perancangan Perangkat Lunak Enkripsi-Dekripsi Algoritma <i>Blowfish</i> dan <i>Elgamal</i>	80
4.4.1 <i>Flowchart</i> Enkripsi-Dekripsi	81
4.4.2 Use Case Enkripsi-Dekripsi	85
4.5 Implementasi Enkripsi-Dekripsi Algoritma <i>Blowfish</i> dan <i>Elgamal</i>	87
4.5.1 Implementasi Proses Enkripsi	88
4.5.2 Implementasi Proses Dekripsi	89
4.6 Pengujian Perangkat Lunak.....	94
4.6.1 Pengujian Fungsionalitas Perangkat Lunak(<i>Black box Testing</i>)....	94
4.6.2 Pengujian Waktu Proses Perangkat Lunak	97

4.7 Analisis Hasil Luaran Perangkat Lunak.....	98
4.7.1 Analisis hasil luaran	98
4.7.2 Analisis Hasil Waktu Proses Enkripsi-Dekripsi	103
4.7.3 Analisis Perbandingan Waktu Enkripsi <i>Blowfish</i> dan Enkripsi <i>Elgamal</i> dengan Waktu Kombinasi <i>Blowfish</i> dan <i>Elgamal</i>	104
4.7.4 Analisis Penggunaan Sumber Daya Komputer Penerapan Algoritma <i>Blowfish</i> dan <i>Elgamal</i>	105
4.7.5 Analisa Hasil Pengujian Efisiensi Proses Enkripsi Penerapan Algoritma <i>Blowfish</i> dan <i>Elgamal</i> Pada Dua Perangkat Keras Berbeda.	110
BAB 5 KESIMPULAN DAN SARAN	113
5.1 Kesimpulan	113
5.2 Saran.....	114
DAFTAR PUSTAKA	116
DAFTAR RIWAYAT HIDUP	119
LAMPIRAN.....	120
Lampiran 1.....	121
Lampiran 2.....	124
Lampiran 3.....	125
Lampiran 4.....	129
Lampiran 5.....	161
Lampiran 6.....	223
Lampiran 7.....	228
Lampiran 8.....	234
Lampiran 9.....	239
Lampiran 10.....	245

Lampiran 11.....	248
Lampiran 12.....	251

DAFTAR GAMBAR

Gambar 1 Proses Algoritma Kriptografi	7
Gambar 2 Jaringan Feistel Blowfish dan S-Box	9
Gambar 3 Tabel ASCII	14
Gambar 4 Tabel Extended ASCII	14
Gambar 5 Kerangka Pikir.....	19
Gambar 6 Gambaran Umum Flowchart Enkripsi	21
Gambar 7 Perancangan Flowchart Enkripsi.....	22
Gambar 8 Gambaran Umum Flowchart Dekripsi	23
Gambar 9 Perancangan Flowchart Dekripsi	23
Gambar 10 Perancangan Cara Kerja Proses Enkripsi	29
Gambar 11 Jaringan Feistel Algoritma Blowfish	30
Gambar 12 Flowchart enkripsi Blowfish	32
Gambar 13 Flowchart enkripsi Elgamal	35
Gambar 14 Flowchart Dekripsi Elgamal.....	37
Gambar 15 Flowchart Dekripsi Blowfish	38
Gambar 16 Perancangan Enkripsi-Dekripsi Perangkat Lunak.....	81
Gambar 17 Perancangan Enkripsi Perangkat Lunak.....	82
Gambar 18 Flowchart Perancangan Dekripsi Perangkat Lunak	84
Gambar 19 Use Case Perangkat Lunak Enkripsi Dekripsi	86
Gambar 20 Halaman Implementasi Proses Enkripsi.....	88
Gambar 21 Luaran daftar Kunci setelah Enkripsi.....	89
Gambar 22 Halaman <i>User</i> Login Page	90
Gambar 23 Halaman <i>User</i> setelah Login	91
Gambar 24 Hasil Dekripsi Menampilkan Data Plainteks Asli	92
Gambar 25 Halaman <i>Admin</i>	92
Gambar 26 Dekripsi Data <i>User</i> oleh <i>Admin</i>	93
Gambar 27 Hasil Dekripsi Menampilkan Data Asli	94

DAFTAR TABEL

Tabel 1 Penelitian Terkait	17
Tabel 2 Jadwal Kegiatan Penelitian	26
Tabel 3 Konversi Kunci Blowfish ke Hexadesimal	39
Tabel 4 Hasil Pembangkitan Kunci	41
Tabel 5 Konversi Karakter Plainteks menjadi Hexadesimal data Alamat	43
Tabel 6 Konversi Hexadesimal menjadi Desimal data Alamat	59
Tabel 7 Pembagian Blok M dan Kunci k data Alamat	60
Tabel 8 Konversi Desimal ke Hexadesimal plainteks Elgamal data Alamat.....	64
Tabel 9 Konversi Hex Plainteks menjadi Karakter data Alamat	79
Tabel 10 Pengujian Perangkat Lunak <i>Black box</i>	95
Tabel 11 Hasil pengujian 100 Data waktu Enkripsi dan Dekripsi	98
Tabel 12 Peningkatan Panjang Plainteks dan Cipherteks Data Nama	100
Tabel 13 Peningkatan Panjang Plainteks dan Cipherteks Data Alamat.....	101
Tabel 14 Peningkatan Panjang Plainteks dan Cipherteks Data Nomor Telepon	102
Tabel 15 Waktu Enkripsi dan Dekripsi dalam Milisekon.....	103
Tabel 16 Perbandingan Waktu Enkripsi Blowfish dan Elgamal dengan Kombinasi Kedua Algoritma.....	104
Tabel 17 Pengujian Penggunaan Sumber Daya Komputer <i>Load Testing</i> Penerapan Kombinasi Enkripsi <i>Blowfish</i> dan <i>Elgamal</i>	106
Tabel 18 Pengujian Penggunaan Sumber Daya Komputer Dekripsi	109
Tabel 19 Pengujian Efisiensi Proses Enkripsi Penerapan Algoritma Blowfish dan Elgamal Pada Dua Perangkat Keras Berbeda.	112