

PENGAMANAN PESAN TEKS MENGUNAKAN METODE KRIPTOGRAFI MODIFIED TWOFISH

*Diajukan Sebagai Syarat Untuk Menyelesaikan
Pendidikan Program Strata-1 Pada
Jurusan Teknik Informatika*



Oleh:

Kevin Hidayatullah
NIM: 09021281823043

**JURUSAN TEKNIK INFORMATIKA
FAKULTAS ILMU KOMPUTER UNIVERSITAS SRIWIJAYA
2024**

LEMBAR PENGESAHAN TUGAS AKHIR

**PENGAMANAN PESAN TEKS MENGGUNAKAN METODE
KRIPTOGRAFI MODIFIED TWOFISH**

Oleh:

Kevin Hidayatullah
NIM: 09021281823043

Indralaya, 3 Januari 2024
Pembimbing II,

Pembimbing I,



Al Farissi, S.Kom., M.Cs.
NIP. 198512152014041001



Osvari Arsalan, S.Kom., M.T.
NIP. 198806282018031001

Mengetahui,
Ketua Jurusan Teknik Informatika



Alvi Syahidin Utami, M.Kom.
NIP. 197812222006042003

TANDA LULUS UJIAN SIDANG SKRIPSI

Pada hari kamis tanggal 28 Desember 2023 telah dilaksanakan ujian komprehensif skripsi oleh Jurusan Teknik Informatika Fakultas Ilmu Komputer Universitas Sriwijaya.

Nama : Kevin Hidayatullah
NIM : 09021281823043
Judul : Pengamanan Pesan Teks Menggunakan Metode Kriptografi Modified TwoFish

Dan dinyatakan LULUS

1. Ketua Penguji

Dian Palupi Rini, M.Kom., Ph.D.
NIP.197802232006042002



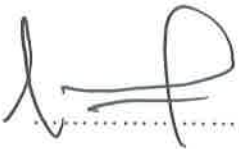
2. Penguji

Mastura Diana Marieska, M.T.
NIP.198603212018032001



3. Pembimbing I

Al Farissi, S.Kom., M.Cs.
NIP. 198512152014041001



4. Pembimbing II

Osvari Arsalan, S.Kom., M.T.
NIP. 198806282018031001



Mengetahui,
Ketua Jurusan Teknik Informatika



Aly Syahrini Utami, M.Kom.
197812222006042003

HALAMAN PERNYATAAN

Yang bertanda tangan di bawah ini:

Nama : Kevin Hidayatullah

Nim : 09021281823043

Prodi : Teknik Informatika

Judul Skripsi : Pengamanan Pesan Teks Menggunakan Metode Kriptografi
Modified Twofish

Hasil pengecekan Software iThenticate/Turnitin: 7%

Menyatakan bahwa laporan proyek saya merupakan hasil karya sendiri dan bukan hasil penjiplakan/plagiat. Apabila ditemukan unsur penjiplakan/plagiat dalam laporan proyek ini, maka saya bersedia menerima sanksi akademik dari Universitas Sriwijaya sesuai dengan ketentuan yang berlaku.

Demikian pernyataan ini saya buat dengan sebenar-benarnya dan tidak ada paksaan oleh siapa pun.



Palembang, 4 Januari 2024



Kevin Hidayatullah
NIM. 09021281823043

MOTTO

"Be yourself; everyone else is already taken."

- Oscar Wilde –

Kupersembahkan Skripsi ini kepada:

1. Allah SWT & Nabi Muhammad SAW
2. Kedua Orangtua dan Keluargaku
3. Teman Seperjuanganku

Securing Text Messages Using Modified Twofish Cryptography Method

By:

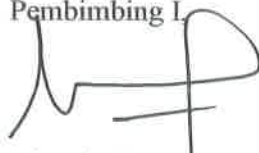
Kevin Hidayatullah (09021281823043)

ABSTRACT

A message is information that is conveyed from one party to another. Messages must also have security that is useful for maintaining confidentiality and avoiding other parties from manipulating the contents of the message. To answer the message security problem, we can use cryptography techniques. This research uses the Twofish algorithm as one of the cryptographic techniques to secure messages. The research is conducted by entering a text message and key, then the software encrypts and produces ciphertext that is unknown to others without a predetermined key. The results in this study show that the bit change is not too significant in the calculation of the avalanche effect so that it produces a small average value depending on the amount of message content. The results of this study used 4 different datasets depending on the number of characters 4803, 9598, 24016 and 48070. And produces an average avalanche effect value of 0.13744%, 0.06973%, 0.02745 and 0.01371%.

Keywords: Cryptography, Twofish Algorithm, Avalanche Effect, Message Security

Pembimbing I



Al Farissi, S.Kom., M.Cs.

NIP. 198512152014041001

Palembang, 3 Januari 2024

Pembimbing II,



Osvari Arsalan, S.Kom., M.T.

NIP. 198806282018031001

Mengetahui,
Ketua Jurusan Teknik Informatika



Alvi Syahriz Utami, M.Kom.
NIP. 197812222006042003

Pengamanan Pesan Teks Menggunakan Metode Kriptografi Modified Twofish

Oleh:

Kevin Hidayatullah (09021281823043)

ABSTRAK

Pesan merupakan sebuah informasi yang disampaikan dari satu pihak ke pihak yang lain. Pesan juga harus memiliki keamanan yang berguna untuk menjaga kerahasiaan dan terhindar dari pihak lain untuk memanipulasi isi pesan tersebut. Untuk menjawab permasalahan keamanan pesan tersebut kita dapat menggunakan teknik kriptografi. Penelitian ini menggunakan algoritma Twofish sebagai salah satu teknik kriptografi untuk mengamankan pesan. Penelitian dilakukan dengan cara memasukan sebuah pesan teks dan kunci, lalu perangkat lunak mengenkripsi dan menghasilkan cipherteks yang tidak diketahui oleh orang lain tanpa kunci yang sudah ditentukan. Hasil pada penelitian ini menunjukkan perubahan bit yang tidak terlalu signifikan pada perhitungan *avalanche effect* sehingga menghasilkan nilai rata-rata yang kecil bergantung pada banyaknya isi pesan. Hasil penelitian ini menggunakan 4 dataset yang berbeda tergantung pada banyaknya jumlah karakter 4803, 9598, 24016 dan 48070. Dan menghasilkan rata-rata nilai avalanche effect sebesar 0.13744%, 0,06973%, 0,02745 dan 0,01371%.

Kata Kunci: Kriptografi, Algoritma Twofish, *Avalanche Effect*, Pengamanan Pesan

Pembimbing I,



Al Farissi, S.Kom., M.Cs.
NIP. 198512152014041001

Palembang, 3 Januari 2024

Pembimbing II,



Osvari Arsalan, S.Kom., M.T.
NIP. 198806282018031001



KATA PENGANTAR

Alhamdulillah, puji dan syukur kehadiran Allah SWT atas rahmat dan karunia-nya, sehingga penulis dapat menyelesaikan tugas akhir yang berjudul “Pengamanan Pesan Teks Menggunakan Metode Kriptografi Modified TwoFish”. Adapun tugas akhir ini disusun untuk memenuhi salah satu persyaratan kelulusan tingkat sarjana pada jurusan Teknik Informatika Fakultas Ilmu Komputer Sriwijaya.

Pada kesempatan ini, penulis ingin menyampaikan ucapan terima kasih sebanyak-banyaknya kepada banyak pihak yang telah memberikan semangat, dukungan, motivasi, doa dan bimbingan dalam menyelesaikan tugas akhir ini, pihak tersebut antara lain:

1. Kedua orang tua saya beserta keluarga yang telah memberikan semangat dan motivasi dalam menyelesaikan tugas akhir ini.
2. Bapak Prof. DR. Erwin, S.Si., M.Si. selaku Dekan Fakultas Ilmu Komputer Universitas Sriwijaya.
3. Ibu Alvi Syahrini Utami, M.Kom, selaku Ketua Jurusan Teknik Informatika Fakultas Ilmu Komputer Universitas Sriwijaya.
4. Bapak Al Farissi, M. Cs, dan Bapak Osvari Arsalan, M.T. sebagai pembimbing Tugas Akhir yang mengarahkan dan memberi motivasi dalam proses pengerjaannya.

5. Bapak Danny Matthew Saputra, M.SC. selaku dosen pembimbing akademik yang telah membimbing dan memberikan masukan sehingga penulis dapat menyelesaikan tugas akhir ini dengan baik.
6. Ibu Mastura Diana Marieska, M.T. selaku dosen penguji yang telah memberikan koreksi dan masukan untuk Tugas Akhir ini.
7. Genta Agsal Valendri, Argha Novan, serta semua anggota kelas TI REG A 2018, yang telah memberi bantuan dan informasi dalam proses pengerjaan tugas akhir ini.
8. Teman-teman jurusan Teknik Informatika yang selalu berbagi informasi dan dukungan dalam menyelesaikan tugas akhir ini.

Penulis menyadari dalam penyusunan tugas akhir ini masih terdapat banyak kekurangan dan jauh dari kata sempurna. Untuk itu penulis mengharapkan kritikan dan saran yang membangun untuk kesempurnaan tugas akhir ini. Akhir kata semoga tugas akhir yang penulis buat memberikan manfaat bagi kita semua.

Indralaya, 3 Januari 2024

Kevin Hidayatullah

DAFTAR ISI

	Halaman
HALAMAN JUDUL	i
LEMBAR PENGESAHAN SKRIPSI	ii
TANDA LULUS UJIAN KOMPREHENSIF SKRIPSI	iii
HALAMAN PERNYATAAN	iv
MOTTO DAN PERSEMBAHAN	v
ABSTRACT	vi
ABSTRAK	vii
KATA PENGANTAR	viii
DAFTAR ISI	x
DAFTAR GAMBAR	xv
DAFTAR TABEL	xvi
BAB I PENDAHULUAN	I-1
1.1 Pendahuluan	I-1
1.2 Latar Belakang	I-1
1.3 Rumusan Masalah	I-2
1.4 Tujuan.....	I-3
1.5 Manfaat.....	I-3
1.6 Batasan Masalah.....	I-3
1.7 Sistematika Penulisan.....	I-3
1.8 Kesimpulan.....	I-5
BAB II LANDASAN TEORI	II-1
2.1 Pendahuluan	II-1
2.2 Landasan Teori	II-1
2.2.1 Kriptografi	II-1
2.2.2 Algoritma Twofish	II-1
2.2.3 Avalanche Effect	II-4

2.3 Penelitian Lain Yang Relevan	II-5
2.4 Kesimpulan.....	II-6
BAB III METODOLOGI PENELITIAN	III-1
3.1 Pendahuluan	III-1
3.2 Pengumpulan Data	III-1
3.2.1 Jenis Data.....	III-1
3.2.2 Sumber Data	III-1
3.3 Tahapan Penelitian	III-1
3.3.1 Kerangka Kerja.....	III-2
3.3.2 Kriteria Pengujian.....	III-3
3.3.3 Format Data Pengujian	III-4
3.3.4 Alat yang digunakan dalam Pelaksanaan Penelitian	III-4
3.3.5 Pengujian Penelitian	III-4
3.3.6 Analisis Hasil Pengujian dan Membuat Kesimpulan	III-4
3.4 Metode Pengembangan Perangkat Lunak	III-5
BAB IV PENGEMBANGAN PERANGKAT LUNAK	IV-1
4.1 Pendahuluan	IV-1
4.2 Algoritma Modified Twofish	IV-1
4.3 Fase Insepsi	IV-1
4.3.1 Kebutuhan Perangkat Lunak	IV-1
4.3.2 Perancangan Perangkat Lunak	IV-3
4.4 Fase Elaborasi.....	IV-8
4.4.1 Pemodelan Bisnis	IV-8
4.4.2 Perancangan Interface	IV-9
4.4.3 Kebutuhan Perangkat Lunak	IV-10
4.4.4 Diagram Aktivitas	IV-11
4.4.5 Sequence Diagram.....	IV-14
4.5 Fase Kontruksi.....	IV-17

4.5.1	Diagram Kelas	IV-17
4.5.2	Implementasi Diagram Kelas	IV-20
4.5.3	Implementasi Antarmuka	IV-21
4.6	Fase Transisi.....	IV-21
4.6.1	Pemodelan Bisnis	IV-23
4.6.2	Rencana Pengujian	IV-23
4.6.3	Implementasi	IV-24
4.7	Kesimpulan.....	IV-25
BAB V HASIL DAN ANALISIS PENELITIAN.....		V-1
5.1	Pendahuluan	V-1
5.2	Data Hasil Penelitian	V-1
5.2.1	Konfigurasi Percobaan	V-1
5.2.2	Skenario Pengujian	V-1
5.2.3	Analisi Hasil Pengujian Waktu Proses Eksekusi.....	V-4
5.2.4	Analisis Hasil Pengujian Avalanche Effect.....	V-5
5.3	Kesimpulan.....	V-6
BAB VI KESIMPULAN DAN SARAN.....		VI-1
6.1	Kesimpulan.....	VI-1
6.2	Saran	VI-1
DAFTAR PUSTAKA		xv
LAMPIRAN.....		xvii

DAFTAR GAMBAR

Gambar II-1 Skema Algoritma Twofish	II-2
Gambar III-1 Kerangka kerja	III-2
Gambar IV-1 Diagram Use Case	IV-3
Gambar IV-2 Rancangan Antarmuka Encrypt.....	IV-9
Gambar IV-3 Rancangan Antarmuka Decrypt.....	IV-10
Gambar IV-4 Diagram aktivitas enkripsi.....	IV-12
Gambar IV-5 Diagram aktivitas dekripsi	IV-13
Gambar IV-6 Diagram aktivitas avalanche effect.....	IV-14
Gambar IV-7 Sequence Diagram enkripsi	IV-15
Gambar IV-8 Sequence Diagram dekripsi	IV-16
Gambar IV-9 Sequence Diagram Avalanche Effect	IV-17
Gambar IV-10 Class Diagram.....	IV-19
Gambar IV-11 Implementasi Tampilan Antarmuka Enkripsi.....	IV-21
Gambar IV-12 Implementasi Tampilan Antarmuka Dekripsi	IV-22
Gambar V-1 Waktu Eksekusi Enkripsi	V-4
Gambar V-2 Waktu Eksekusi Dekripsi.....	V-4

DAFTAR TABEL

Tabel II-1 Jangkauan Kriteria Avalanche Effect	II-5
Tabel IV-1 Kebutuhan Fungsional Perangkat Lunak.....	IV-2
Tabel IV-2 Kebutuhan Non Fungsional Perangkat Lunak.....	IV-2
Table IV-3 Definisi Aktor.....	IV-3
Table IV-4 Definisi Use Case	IV-4
Tabel IV-5 Skenario Use Case Proses Enkripsi Pesan.....	IV-4
Tabel IV-6 Skenario Use Case Proses Dekripsi Pesan	IV-6
Tabel IV-7 Skenario Use Case Proses Pengujian Avalanche Effect	IV-7
Tabel IV-8 Implementasi Diagram Kelas	IV-20
Tabel IV-9 Rencana Pengujian	IV-23
Tabel IV-10 Hasil Implementasi Rencana Pengujian	IV-24
Tabel V-1 Hasil Waktu Eksekusi.....	V-1
Tabel V-2 Hasil Avalanche Effect	V-3

BAB I

PENDAHULUAN

1.1 Pendahuluan

Bab pendahuluan ini memaparkan latar belakang, rumusan masalah, tujuan penelitian, manfaat penelitian, batasan masalah, dan sistematika penulisan . Bab ini memberikan informasi tentang keseluruhan dari penelitian.

1.2 Latar Belakang

Pesan memiliki banyak manfaat salah satunya adalah untuk berkomunikasi sesama manusia. Pesan itu sendiri sudah berkembang dari waktu ke waktu. Yang awalnya pesan disampaikan secara tatap muka, mengirim melalui surat di kantor pos, lalu mengirim pesan melalui email dengan menggunakan komputer dan sekarang dengan perkembangan zaman seperti ini pesan bisa disampaikan menggunakan handphone atau smartphone.

Pesan juga memiliki informasi yang sangat penting. Tetapi tetap ada kemungkinan informasi dari pesan itu bisa disadap oleh orang-orang yang tidak seharusnya mengetahui isi informasi dari pesan tersebut. Kriptografi (cryptography) berasal dari Bahasa Yunani: “cryptos” artinya “secret” (rahasia), sedangkan “gráphein” artinya “writing” (tulisan). Jadi, kriptografi berarti secret writing (tulisan rahasia) (Munir, 2006).

Salah satu algoritma yang terkenal dan sudah banyak digunakan dalam aplikasi keamanan data adalah algoritma blowfish yang dikembangkan oleh Bruce Schneier. Algoritma blowfish adalah algoritma enkripsi simetris. Algoritma blowfish lebih lambat mengamankan data yang besar jika dibandingkan dengan

algoritma kriptografi yang lebih modern saat ini. Maka Bruce Schneier dan beberapa peneliti lainnya mengembangkan blowfish ini untuk menjadi algoritma yang lebih aman dan lebih efisien yang dinamakan dengan algoritma twofish. Algoritma twofish memiliki tingkat keamanan yang lebih tinggi jika dibandingkan dengan blowfish. Pada tahun 1997 algoritma twofish mengikuti sayembara yang diselenggarakan oleh National Institute of Standards and Technology (NIST) untuk menggantikan Data Encryption Standard (DES) yang dinamakan dengan Advanced Encryption Standard (AES). Dan twofish berhasil memasuki 5 besar finalis kandidat yang mengikuti kompetisi AES. Walaupun twofish tidak memenangkan sayembara tersebut tetapi twofish memiliki potensi yang tinggi untuk mengamankan data.

Dengan latar belakang ini, algoritma Twofish dapat digunakan untuk meningkatkan keamanan pesan teks. Penelitian ini kami ingin menguji coba modified algoritma twofish ini pada kecepatan enkripsi dan dekripsi. Dan kami akan melakukan pengujian avalanche effect pada modified algoritma twofish.

1.3 Rumusan Masalah

Berdasarkan latar belakang yang telah penulis uraikan diatas, rumusan masalah pada penelitian ini adalah:

1. Bagaimana membangun perangkat lunak menggunakan kriptografi *modified twofish* pada pengamanan teks?
2. Bagaimana tingkat kinerja kriptografi *modified twofish* pada pengamanan teks dengan mengukur kecepatan dan pengujian *avalanche effect*?

1.4 Tujuan Penelitian

Tujuan penelitian ini adalah:

1. Mengaplikasikan pengamanan teks menggunakan kriptografi *modified twofish*.
2. Mengembangkan perangkat lunak yang bekerja sebagai pengamanan teks.
3. Menilai tingkat kinerja kriptografi *modified twofish* terhadap pengamanan teks.

1.5 Manfaat Penelitian

Manfaat penelitian ini adalah:

1. Dapat menolong masyarakat umum untuk mengamankan pesan yang bersifat rahasia.
2. Hasil dari penelitian ini bisa dijadikan landasan berpikir untuk penelitian selanjutnya.

1.6 Batasan Masalah

Batasan masalah penelitian ini adalah:

1. Tipe data yang akan *encrypt* dan *decrypt* adalah plainteks bertipe file .txt dengan karakter ASCII.
2. Penelitian menguji dan menilai *avalanche effect* pengamanan teks serta kecepatan *encrypt* dan *decrypt* dari kriptografi *modified twofish*.

1.7 Sistematika Penulisan

BAB I. PENDAHULUAN

Bab ini menguraikan pokok-pokok pikiran yang mendasari penelitian, meliputi latar belakang, rumusan masalah, tujuan dan manfaat penelitian, batasan atau ruang lingkup masalah, dan sistematika penulisan.

BAB II. KAJIAN LITERATUR

Bab ini menguraikan landasan teori yang akan diaplikasikan dalam penelitian, meliputi penjelasan tentang cipher, Twofish yang di modifikasi, dan berbagai literatur karya lain yang terkait dengan penelitian ini.

BAB III. METODOLOGI PENELITIAN

Bab ini menjelaskan proses penelitian. Setiap program penelitian akan dijelaskan secara rinci dengan menggunakan kerangka kerja. Bab ini diakhiri dengan rancangan panduan manajemen proyek untuk melaksanakan penelitian.

BAB IV. PENGEMBANGAN PERANGKAT LUNAK

Bab ini menjelaskan tentang analisis dan perancangan perangkat lunak yang Anda buat. Kami memulai dengan analisis kebutuhan, merancang dan membangun perangkat lunak, kemudian melakukan pengujian untuk memastikan bahwa sistem yang dikembangkan sesuai dengan desain dan persyaratan yang dibuat.

BAB V. HASIL DAN ANALISAN PENELITIAN

Bab ini menjelaskan hasil tes sesuai rencana. Hasil pengujian dan tabel analisis menjadi tolak ukur kesimpulan penelitian ini.

BAB VI. KESIMPULAN DAN SARAN

Bab ini membahas kesimpulan dari seluruh pembahasan pada bab-bab sebelumnya dan saran-saran yang disampaikan dalam temuan penelitian.

1.8 Kesimpulan

Pada bab ini telah dipaparkan pokok pikiran dalam penelitian yang dilakukan, seperti latar belakang, rumusan masalah, tujuan penelitian, manfaat penelitian, batasan masalah dan sistematika penulisan.

DAFTAR PUSTAKA

- A. M. Qadir and N. Varol. (2019). A Review Paper on Cryptography. 2019 7th International Symposium on Digital Forensics and Security (ISDFS), Barcelos, Portugal, 2019, pp. 1-6, <https://doi.org/10.1109/ISDFS.2019.8757514>.
- Anil G. Sawant, Dr. Vilas N. Nitnaware, Pranali Dengale, Sayali Garud, & Akshay Gandewar. (2019). TWOFISH ALGORITHM FOR ENCRYPTION AND DECRYPTION. JETIR, 6(1), 288-291.
- Ariyus, D. (2008). Pengantar Ilmu Kriptografi: Teori, Analisis dan Implementasi. ANDI: Yogyakarta.
- Elsa Elvira Awal, E. Haodudin E. Haodudin Nurkifli, Tesa Nur Tesa Nur Padilah. (2022). ANALISIS PERBANDINGAN HASIL ENKRIPSI DAN DESKRIPSI ALGORITMA KRIPTOGRAFI RIJNDAEL DAN TWOFISH UNTUK PENYANDIAN DATA. Jurnal JMIK, 3(1), 260-265.
- H. K. Hoomod and A. M. Hussein. (2019). New Modified Twofish For Data Protection Using Salsa20 and Lü system. International Conference on Intelligent Computing and Control Systems (ICCS). Madurai, India, 2019, pp. 1189-1195. <https://doi.org/10.1109/ICCS45141.2019.9065573>.
- Munir, Rinaldi. (2006). Kriptografi. Informatika: Bandung.
- Muslih, Muslih., & Handoko, Lekso Budi. (2022). PENGUJIAN AVALANCHE EFFECT PADA KRIPTOGRAFI TEKS MENGGUNAKAN AUTOKEY CIPHER, 2(1), 127-134. <https://garuda.kemdikbud.go.id/documents/detail/3842091>

- Mycielski. (2021). Twofish-in-java. <https://github.com/mycielski/twofish-in-java>
- Purnima GehlotS, R. BiradarB, P. Singh. (2013). Implementation of Modified Twofish Algorithm using 128 and 192-bit keys on VHDL. Jurnal IJCA, 70(13), 37-42. <https://doi.org/10.5120/12024-8087>.
- Rahman, Z., Hasanuddin, T., & Abdullah, S. (2020). Implementasi Metode Enkripsi dan Deskripsi File menggunakan Algoritma Twofish. Buletin Sistem Informasi dan Teknologi Islam (BUSITI), 1(2), 66-70. <https://doi.org/10.33096/busiti.v1i2.741>.
- Siswanto, Anggun Saputro, Gunawan Pria Utama, Basuki Hari Prasetyo. (2021). Penerapan Algoritma Kriptografi Twofish Untuk Mengamankan Data File. Jurnal Budi luhur, 18(1), 09-18. <https://dx.doi.org/10.36080/bit.v18i1.1446>.
- Sry Yunarti. (2014). APLIKASI ENKRIPSI DAN DEKRIPSI FILE MENGGUNAKAN ALGORITMA TWOFISH. Jurnal Informatika Progres, 6(2), 13-25. <https://doi.org/10.56708/progres.v6i2.39>.