

SKRIPSI

**ANALISIS PERBANDINGAN HASIL ENKRIPSI RSA DAN *TWOFISH*
DALAM KONTEKS ENKRIPSI *BACKUP DATABASE* DENGAN
PENGUNAAN METODE KOMPRESI DEFLATE**



MUHAMMAD FADHILLAH AKBAR

2010511005

PROGRAM STUDI INFORMATIKA

FAKULTAS ILMU KOMPUTER

UNIVERSITAS PEMBANGUNAN NASIONAL "VETERAN" JAKARTA

2024

SKRIPSI

**ANALISIS PERBANDINGAN HASIL ENKRIPSI RSA DAN *TWOFISH*
DALAM KONTEKS ENKRIPSI *BACKUP DATABASE* DENGAN
PENGUNAAN METODE KOMPRESI DEFLATE**



MUHAMMAD FADHILLAH AKBAR

2010511005

**PROGRAM STUDI INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS PEMBANGUNAN NASIONAL "VETERAN" JAKARTA
2024**

PERNYATAAN ORISINALITAS

Yang bertanda tangan di bawah ini:

Nama : Muhammad Fadhillah Akbar

NIM : 2010511005

Program Studi : S1 Informatika

Judul : Analisis Perbandingan Hasil Enkripsi RSA Dan Twofish Dalam Konteks Enkripsi *Backup Database* Dengan Penggunaan Metode Kompresi Deflate

Menyatakan bahwa skripsi ini adalah hasil harya sendiri, dan semua yang dikutip maupun yang dirujuk telah saya nyatakan dengan benar

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

Jakarta, 20 Juni 2024

Yang Menyatakan,



Muhammad Fadhillah Akbar

NIM 2010.511.005

**PERNYATAAN PERSETUJUAN PUBLIKASI TUGAS AKHIR UNTUK
KEPENTINGAN AKADEMIS**

Sebagai civitas akademik Universitas Pembangunan Nasional “Veteran” Jakarta, saya yang bertanda tangan dibawah ini.

Nama : Muhammad Fadhillah Akbar

NIM : 2010511005

Fakultas : Ilmu Komputer

Program Studi : S1 Informatika

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

“Analisis Perbandingan Hasil Enkripsi RSA Dan Twofish Dalam Konteks Enkripsi Backup Database Dengan Penggunaan Metode Kompresi Deflate”

Dengan Hak Bebas Royalti ini Universitas Pembangunan Nasional “Veteran” Jakarta berhak menyimpan, mengalih media/formatkan, mengelola dalam bentuk pangkalan data (database), merawat, dan mempublikasikan tugas akhir saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.

Demikian pernyataan ini saya buat dengan sebenarnya.

Jakarta 10 Juli 2024

Yang menyatakan,



Muhammad Fadhillah Akbar

LEMBAR PENGESAHAN

Skripsi ini diajukan oleh:

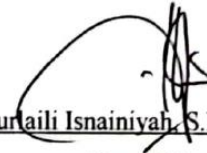
Nama : Muhammad Fadhillah Akbar
NIM : 2010511005
Program Studi : S-1 Informatika
Judul Skripsi/TA : Analisis Perbandingan Hasil Enkripsi RSA Dan Twofish Dalam Konteks Enkripsi *Backup Database* Dengan Penggunaan Metode Kompresi Deflate

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



Jayanta, S.Kom., M.Si.

Penguji 1



Ika Nurtauli Isnainiyah, S.Kom., M.Sc.

Penguji 2



Bayu Hananto, S.Kom., M.Kom.

Dosen Pembimbing I



Hamonangan Kinantan Prabu, S.T., M.T.

Dosen Pembimbing II



Prof. Dr. Ir. Subriyanto, ST., M.Sc., IPM.

Dekan Fakultas Ilmu Komputer



Dr. Widya Cholil, M.I.T.

Kepala Program Studi S1 Informatika

Ditetapkan di : Jakarta

Tanggal Persetujuan : 10 Juli 2024

**ANALISIS PERBANDINGAN HASIL ENKRIPSI RSA DAN TWOFISH
DALAM KONTEKS ENKRIPSI *BACKUP DATABASE* DENGAN
PENGUNAAN METODE KOMPRESI DEFLATE**

Muhammad Fadhillah Akbar

ABSTRAK

Dalam era digital yang terus berkembang pesat, perlindungan data menjadi sangat krusial. Data yang tersimpan dalam basis data cadangan seringkali mencakup informasi yang sangat sensitif dan kritis, sehingga diperlukan metode enkripsi yang kuat untuk menjaga kerahasiaan dan integritasnya. Penelitian ini bertujuan untuk menganalisis dan membandingkan kinerja dua algoritma enkripsi, yaitu RSA dan Twofish, dalam konteks enkripsi *Backup Database* dengan metode kompresi Deflate. RSA adalah algoritma enkripsi asimetris yang terkenal dengan tingkat keamanannya yang tinggi, sementara Twofish adalah algoritma enkripsi simetris yang efisien dalam hal waktu komputasi dan penggunaan memori. Penelitian ini mengungkap kelebihan dan kekurangan masing-masing algoritma dalam aplikasi spesifik, serta bagaimana metode kompresi Deflate mempengaruhi efisiensi enkripsi dan dekripsi. Hasil penelitian menunjukkan bahwa RSA, meskipun memiliki keamanan yang tinggi, memerlukan waktu pemrosesan yang lebih lama dibandingkan Twofish. Sebaliknya, Twofish menawarkan waktu komputasi yang lebih cepat dan penggunaan memori yang lebih efisien, namun memiliki kerentanan terhadap kunci yang digunakan. Kombinasi kedua algoritma dengan metode kompresi Deflate tidak terlalu efisien dalam meningkatkan efisiensi penyimpanan dan transfer data dalam sistem *Backup Database*.

Kata Kunci: Kriptografi, Enkripsi, Kompresi, *Backup Database*, RSA, Twofish, Deflate.

**COMPARATIVE ANALYSIS OF THE RESULTS OF RSA AND TWOFISH
ENCRYPTION IN THE CONTEXT OF DATABASE BACKUP ENCRYPTION
USING THE DEFLATE COMPRESSION METHOD**

Muhammad Fadhillah Akbar

ABSTRACT

In the rapidly evolving digital era, data protection has become crucial. Data stored in backup databases often includes highly sensitive and critical information, necessitating robust encryption methods to ensure confidentiality and integrity. This research aims to analyze and compare the performance of two encryption algorithms, namely RSA and Twofish, in the context of Backup Database encryption using the Deflate compression method. RSA is an asymmetric encryption algorithm known for its high level of security, while Twofish is a symmetric encryption algorithm efficient in terms of computational time and memory usage. This study reveals the advantages and disadvantages of each algorithm in specific applications, as well as how the Deflate compression method affects the efficiency of encryption and decryption. The results show that RSA, despite its high security, requires longer processing times compared to Twofish. Conversely, Twofish offers faster computation times and more efficient memory usage but has vulnerabilities related to the keys used. The combination of both algorithms with the Deflate compression method is not very efficient in enhancing storage efficiency and data transfer in Backup Database systems.

Keyword: *Cryptography, Encryption, Compression, Backup Database, RSA, Twofish, Deflate.*

KATA PENGANTAR

Puji syukur ke hadirat Allah SWT atas segala limpahan Rahmat dan Karunia-Nya, serta Shalawat beserta salam kepada Nabi Muhammad SAW sehingga penulis dapat menyelesaikan proposal skripsi ini dengan judul “**Analisis Perbandingan Hasil Enkripsi RSA Dan *Twofish* Dalam Konteks Enkripsi *Backup Database* Dengan Penggunaan Metode Kompres Deflate**” yang mana ditunjukkan sebagai salah satu langkah untuk menyelesaikan Program Studi Informatika Fakultas Ilmu Komputer Universitas Pembangunan Nasional “Veteran” Jakarta.

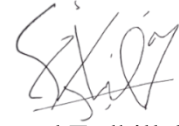
Dalam penyusunan dan penulisan skripsi ini tak lepas dari bantuan, dukungan, serta doa dari berbagai pihak. Oleh karena itu, dalam kesempatan kali ini penulis senantiasa menyampaikan rasa terima kasih yang sebesar-besarnya kepada pihak yang sudah membantu dalam penyusunan skripsi ini terutama kepada:

1. Ibu, bapak, dan adik saya atas semua doa-doanya, perhatian, semangat serta dukungan yang selalu diberikan kepada saya dalam menyelesaikan proposal skripsi ini sampai selesai.
2. Bapak Bayu Hananto, S.Kom., M.Kom. selaku dosen pembimbing 1 dan Bapak Hamonangan Kinantan Prabu S.T., M.T. selaku dosen pembimbing 2 yang telah bersedia dalam meluangkan waktu untuk memberikan bimbingan, masukan, dan dukungan.
3. Ibu Dr. Widya Cholil, M.I.T. selaku Ketua Program Studi Informatika Fakultas Ilmu Komputer Universitas Pembangunan Nasional Veteran Jakarta.
4. Seluruh dosen Fakultas Ilmu Komputer Universitas Pembangunan Nasional Veteran Jakarta yang telah mendidik dan memberikan ilmu yang bermanfaat kepada penulis.
5. Sahabat saya, terutama Ronald, Mamen, Febriani dan Natasya yang selalu mendoakan, memberi semangat, serta bantuan selama saya menyelesaikan skripsi ini hingga selesai.

Penulis menyadari bahwa proposal skripsi ini belum sempurna, baik dari segi materi maupun penyajiannya. Oleh karena itu, saran dan kritik yang membangun sangat diharapkan dalam penyempurnaan skripsi ini.

Jakarta, 10 Juli 2024

Penulis,



Muhammad Fadhillah Akbar

DAFTAR ISI

LEMBAR JUDUL	i
PERNYATAAN ORISINALITAS	ii
PERNYATAAN PERSETUJUAN PUBLIKASI TUGAS AKHIR UNTUK KEPENTINGAN AKADEMIS	iii
LEMBAR PENGESAHAN	iv
ABSTRAK	v
ABSTRACT	vi
KATA PENGANTAR	vii
DAFTAR ISI	ix
DAFTAR TABEL	xii
DAFTAR GAMBAR	xiii
DAFTAR LAMPIRAN	xv
BAB I	1
PENDAHULUAN	1
1.1 Latar Belakang Masalah.....	1
1.2 Rumusan Masalah	2
1.3 Tujuan Penelitian	3
1.3.1 Bagi Penulis	3
1.3.2 Bagi Peneliti Lain.....	3
1.4 Manfaat Penelitian	3
1.5 Ruang Lingkup Penelitian.....	4
1.6 Luaran yang Diharapkan	4
BAB II	6
TINJAUAN PUSTAKA	6
2.1 Keamanan Data	6
2.2 Database	7
2.2.1 Backup Database.....	7
2.3 Bahasa Pemrograman Python	8

2.3.1	Tkinter	9
2.4	Kriptografi.....	10
2.4.1	Terminologi.....	10
2.4.2	Algoritma Kriptografi	11
2.5	Algoritma Enkripsi.....	12
2.5.1	Algoritma Enkripsi RSA.....	12
2.5.2	Algoritma Enkripsi Twofish	14
2.6	Kompresi Data	17
2.7	Message Digest Algoritma 5 (MD5).....	18
2.8	Metode Deflate.....	18
2.9	Review Penelitian Relevan	20
BAB III	24
METODOLOGI PENELITIAN	24
3.1	Kerangka Berpikir.....	24
3.2	Metode Penelitian.....	25
3.2.1	Identifikasi Masalah	25
3.2.2	Analisis Kebutuhan	25
3.2.3	Perancangan Aplikasi.....	26
3.2.4	Implementasi	26
3.2.5	Pengujian.....	27
3.2.6	Analisis Hasil	28
3.3	Alat dan Bahan Penelitian.....	28
3.3.1	Alat Penelitian.....	28
3.3.2	Bahan Penelitian.....	29
3.4	Jadwal Penelitian.....	30
BAB IV	31
HASIL DAN PEMBAHASAN	31
4.1	Analisis Sistem.....	31
4.2	Flowchart, Activity Diagram, dan Use Case Diagram.....	33
4.2.1	Flowchart Enkripsi Algoritma RSA.....	33

4.2.2	Flowchart Dekripsi Algoritma RSA	34
4.2.3	Flowchart Enkripsi Algoritma Twofish	35
4.2.4	Flowchart Dekripsi Algoritma Twofish	36
4.2.5	Flowchart Kompresi Deflate	37
4.2.6	Flowchart Dekompresi Deflate	39
4.2.7	Use Case Diagram.....	40
4.2.8	Activity Diagram Enkripsi dan Dekripsi Algoritma RSA	42
4.2.9	Activity Diagram Enkripsi dan Dekripsi Algoritma Twofish.....	44
4.2.10	Activity Diagram Kompresi dan Dekompresi Metode Deflate.....	46
4.3	Rancang Bangun Aplikasi.....	48
4.3.1	Rancangan Aplikasi (Wireframe)	48
4.3.2	Tampilan Antarmuka	51
4.4	Analisis Hasil	55
4.7.1	Interpretasi Variabel.....	55
4.7.2	Hasil Algoritma Enkripsi RSA	56
4.7.3	Hasil Algoritma Enkripsi Twofish	65
4.7.4	Hasil Algoritma Kompresi Deflate	73
BAB V	89
KESIMPULAN DAN SARAN	89
5.1	Kesimpulan	89
5.2	Saran.....	90
DAFTAR PUSTAKA	viii

DAFTAR TABEL

Tabel 2.1 Hitungan Rumus RSA.....	13
Tabel 2.2 Karakteristik Twofish	16
Tabel 2.3 Review Penelitian Relevan	21
Tabel 3.1 Jadwal Penelitian.....	30
Tabel 4.1 Hasil Enkripsi dan Dekripsi RSA	57
Tabel 4.2 Rata-Rata Kecepatan Enkripsi dan Dekripsi RSA.....	59
Tabel 4.3 Waktu Enkripsi RSA.....	59
Tabel 4.4 Waktu Dekripsi RSA	61
Tabel 4.5 Checksum MD5 File Enkripsi dan Dekripsi RSA	64
Tabel 4.6 Hasil Enkripsi dan Dekripsi Twofish.....	65
Tabel 4.7 Rata-Rata Kecepatan Enkripsi dan Dekripsi Algoritma Twofish.....	67
Tabel 4.8 Waktu Enkripsi Twofish	67
Tabel 4.9 Waktu Dekripsi Twofish.....	69
Tabel 4.10 Checksum MD5 File Enkripsi dan Dekripsi Twofish.....	72
Tabel 4.11 Hasil Kompresi dan Dekompresi File RSA	73
Tabel 4.12 Rata-Rata Kecepatan Kompresi File RSA	75
Tabel 4.13 Waktu Kompresi File RSA	75
Tabel 4.14 Waktu Dekompresi File RSA	77
Tabel 4.15 Checksum MD5 File Kompresi dan Dekompresi RSA	80
Tabel 4.16 Hasil Kompresi dan Dekompresi File Twofish.....	81
Tabel 4.17 Rata-Rata Kecepatan Kompresi dan Dekompresi File Twofish	83
Tabel 4.18 Waktu Kompresi File Twofish.....	83
Tabel 4.19 Waktu Dekompresi Twofish	85
Tabel 4.20 Checksum MD5 File Kompresi dan Dekompresi Twofish.....	88

DAFTAR GAMBAR

Gambar 2.1 Proses Enkripsi dan Dekripsi	10
Gambar 2.2 Flowchart Key Generate RSA.....	12
Gambar 2.3 Flowchart Algoritma Twofish.....	15
Gambar 2.4 Alur Proses Kompresi dan Dekompresi Dokumen	17
Gambar 2.5 Alur Kompresi Metode Deflate.....	20
Gambar 3.1 Alur Kerangka Berpikir.....	24
Gambar 3.2 Skema Proses Implementasi RSA.....	27
Gambar 3.3 Skema Proses Implementasi Twofish	27
Gambar 4.1 Flowchart Proses Enkripsi RSA.....	33
Gambar 4.2 Flowchart Proses Dekripsi RSA.....	34
Gambar 4.3 Flowchart Proses Enkripsi Twofish	35
Gambar 4.4 Flowchart Proses Dekripsi Twofish	36
Gambar 4.5 Flowchart Proses Kompresi Deflate.....	38
Gambar 4.6 Flowchart Proses Dekompresi Deflate	39
Gambar 4.7 Use Case Diagram Aplikasi	40
Gambar 4.8 Activity Diagram Enkripsi Dekripsi RSA.....	42
Gambar 4.9 Activity Diagram Dekripsi RSA	43
Gambar 4.10 Activity Diagram Dekripsi Twofish.....	44
Gambar 4.11 Activity Diagram Dekripsi Twofish.....	45
Gambar 4.12 Activity Diagram Kompresi Deflate	46
Gambar 4.13 Activity Diagram Dekripsi Twofish.....	47
Gambar 4.14 Wireframe Menu Utama.....	48
Gambar 4.15 Wireframe Enkripsi RSA	49
Gambar 4.16 Wireframe Enkripsi Twofish.....	49
Gambar 4.17 Wireframe Kompresi Deflate	50
Gambar 4.18 Wireframe Dekompresi Deflate	50
Gambar 4.19 Menu Utama.....	51
Gambar 4.20 Halaman Enkripsi Dekripsi RSA	52

Gambar 4.21 Halaman Enkripsi Dekripsi Twofish.....	53
Gambar 4.22 Halaman Kompresi Deflate	54
Gambar 4.23 Halaman Dekompresi Deflate	55
Gambar 4.24 Grafik Standar Deviasi Waktu Enkripsi dan Dekripsi RSA	63
Gambar 4.25 Grafik Standar Deviasi Waktu Enkripsi dan Dekripsi Twofish.....	71
Gambar 4.27 Grafik Standar Deviasi Waktu Kompresi dan Dekompresi File RSA ..	78
Gambar 4.29 Grafik Standar Deviasi Waktu Kompresi dan Dekompresi File Twofish	86

DAFTAR LAMPIRAN

Lampiran 1 Surat Riset Mahasiswa.....	A
Lampiran 2 Dokumentasi Kode Program	B
Lampiran 3 Daftar Riwayat Hidup.....	C
Lampiran 4 Hasil Turnitin.....	D