

BAB V

KESIMPULAN DAN SARAN

5.1 Kesimpulan

Penelitian ini berfokus pada penerapan dan evaluasi dua algoritma enkripsi, yaitu RSA dan Twofish, serta metode kompresi Deflate, dalam rangka mengamankan data *Backup Database*. Proses pengujian dilakukan secara menyeluruh untuk memahami dampak kombinasi metode ini terhadap ukuran *file*, waktu proses, dan integritas data. Dari hasil pengujian yang dilakukan, beberapa kesimpulan utama dapat ditarik.

Algoritma RSA membutuhkan waktu yang lebih lama untuk proses enkripsi dan dekripsi dibandingkan dengan Twofish meskipun pada ukuran *file* yang sama. Hal ini menjadikan Twofish lebih cocok untuk aplikasi yang membutuhkan efisiensi waktu dan kecepatan pemrosesan, seperti dalam lingkungan *Database* yang memerlukan *Backup* dan pemulihan data yang cepat, akan tetapi RSA juga memiliki kelebihan yaitu lebih baik dari segi keamanan dikarenakan RSA merupakan bagian dari enkripsi asimetrik yang memiliki 2 kunci terpisah untuk melakukan enkripsi dan dekripsi sehingga lebih sulit untuk dipecahkan.

Terkait proses kompresi dan dekompresi, ditemukan bahwa hasilnya bervariasi. Dalam proses kompresi *file* enkripsi RSA terjadi peningkatan ukuran setelah dienkripsi dan dikompresi. Hal ini menunjukkan bahwa algoritma kompresi Deflate pada *file* RSA tidak efektif dalam mengurangi ukuran *file* yang sudah dienkripsi. Sedangkan pada *file* enkripsi Twofish proses kompresi lebih efektif karena dapat mengurangi ukuran *file* sebelum di kompresi akan tetapi saat dilakukan pada *file* dengan ukuran yang besar, proses ini tidak terlalu efektif karena hanya mengurangi sedikit bahkan ada yang bertambah ukuran datanya setelah di kompresi.

Dari integritas data, nilai *Checksum* MD5 pada proses enkripsi dan dekripsi RSA yang dihasilkan sebelum dan sesudah proses kompresi serta enkripsi tetap sama. Hal ini menunjukkan bahwa data tidak mengalami perubahan selama proses tersebut dan untuk memastikan bahwa data yang dipulihkan adalah data yang sama dengan yang di-*Backup*. Sedangkan pada proses enkripsi dan dekripsi menggunakan Twofish, nilai *Checksum* mengalami perubahan, hal ini dikarenakan proses perubahan yang signifikan dari enkripsi Twofish terhadap *file* yang di enkripsi. Meskipun demikian hal tersebut tidak mempengaruhi data di dalamnya.

Pemilihan algoritma enkripsi dan metode kompresi yang tepat sangat penting untuk memastikan efisiensi proses dan efektivitas pengurangan ukuran *file*. Selain itu, pengujian lebih lanjut dengan berbagai jenis dan ukuran *file* diperlukan untuk mendapatkan gambaran yang lebih komprehensif mengenai kinerja algoritma yang diuji dalam berbagai skenario penggunaan. Dengan mempertimbangkan kesimpulan ini, implementasi enkripsi dan kompresi data *Backup Database* dapat dioptimalkan untuk memastikan keamanan, integritas, dan efisiensi penyimpanan data secara keseluruhan.

5.2 Saran

Berdasarkan hasil penelitian, beberapa saran untuk implementasi lebih lanjut adalah:

1. Untuk sistem yang membutuhkan kecepatan dan konsistensi dalam kompresi dan dekompresi, algoritma Twofish lebih direkomendasikan dibandingkan RSA. Twofish menunjukkan performa yang lebih baik dalam hal kecepatan dan konsistensi waktu.
2. Untuk sistem yang membutuhkan keamanan data terbaik, lebih direkomendasikan menggunakan algoritma RSA dibanding algoritma Twofish.
3. Metode kompresi tidak selalu mengurangi ukuran *file* apalagi pada *file* terenkripsi RSA. Diperlukan evaluasi lebih lanjut untuk menemukan metode

kompresi yang lebih efisien atau memilih untuk tidak mengkompresi *file* yang sudah dienkripsi jika ukuran tidak berkurang signifikan.

4. Melakukan pengujian lebih lanjut dengan berbagai jenis dan ukuran *file* untuk mendapatkan gambaran yang lebih komprehensif mengenai kinerja kedua algoritma dalam skenario yang lebih beragam.

Dengan mempertimbangkan kesimpulan dan saran di atas, implementasi enkripsi dan kompresi data *Backup Database* dapat dioptimalkan untuk memastikan keamanan, integritas, dan efisiensi penyimpanan data.