JURNAL SITEBA
Volume 2, No. 1, 2023
https://journal.iteba.ac.id/index.php/jurnalsiteba/index

STUDI ALGORITMA KRIPTOGRAFI KUNCI SIMETRIS PADA KEAMANAN DATA DENGAN METODE KOMPARASI

Rahmaniah 1, Mhd Firman Aditya 2, Widya Arfanda 3, Veren Ndika purnama 4,Cicilia Dara5
Institut Teknologi Batam
Rahmaniah230@gmail.com

Abstrak

Masalah keamanan merupakan salah satu aspek paling penting dalam dunia teknologi informasi, seperti keamanan data. Keamanan data merupakan isu krusial dalam era informasi yang semakin maju untuk melindungi data dari ancaman dan serangan siber, diperlukanlah penggunaan algoritma kriptografi yang efektif dan andal. Oleh karena itu, Penelitian tentang algoritma keamanan data menjadi sangat penting untuk melindungi integritas, kerahasiaan, dan ketersediaan informasi. Penelitian ini bertujuan untuk melakukan studi algoritma kriptografi yang umum digunakan pada keamanan data. Metode yang digunakan adalah Metode Komparasi dengan cara studi literatur dan analisis terhadap algoritma kriptografi modern, Dalam melakukan studi literatur, Peneliti mengumpulkan dan menganalisis publikasi, Penelitian, makalah, atau referensi lain yang relevan tentang algoritma kriptografi keamanan data yang memiliki kategori algoritma kriptografi kunci simetris seperti, Advanced Encryption Standard (AES), Data Encryption Standard (DES), 3DES, Blowfish, beberapa algoritma ini memiliki kelebihan dan kekurangan oleh karena itu, pemilihan algoritma kriptografi harus disesuaikan dengan jenis data yang akan dienkripsi dan level keamanan yang dibutuhkan.

Key Words: Keamanan Data, Algoritma Kriptografi Kunci Simetris, Metode Komparasi

1. PENDAHULUAN

Keamanan Data (Data Security) adalah sebuah prosedur dengan dukungan regulasi dan teknologi untuk melindungi data dari kerusakan data, modifikasi data, serta penyebaran data baik yang disengaja maputun tidak. Dengan adanya Keamanan Data pemilik dapat mencegah akses yang tidak diinginkan terhadapat perangkat keras ataupun perangkat lunak seperti komputer, database, website yang berusaha mengambil data

digital yang bersifat personal. Keamanan data menjadi salah satu aspek kritis dalam era informasi yang terus berkembang pesat. Oleh karena itu, perlunya algoritma keamanan data yang kuat dan efisien menjadi sangat penting untuk menjaga kerahasiaan dan integritas data. Jurnal ini bertujuan untuk melakukan studi komparatif terhadap empat algoritma kriptografi yang umum digunakan dalam keamanan data. Algoritma kriptografi sendiri memiliki due kategori yaitu algoritma kriptografi klasik dan algoritma kriptografi modern, Kami sendiri memilih algoritma kriptografi modern, jenis algoritma yang dikembangkan secara lebih kompleks dan canggih dalam menghadapi tantangan keamanan data yang semakin kompleks. Algoritma ini didasarkan pada matematika dan komputasi yang rumit untuk mengamankan data dan informasi. Algoritma kriptografi modern memiliki keamanan yang lebih tinggi dan lebih sulit untuk dipecahkan dengan teknik serangan yang umum digunakan seperti Brute Force. Sehingga kami memiliH kategori algoritma kriptografi dengan kunci simetris yaitu, AES (Advanced Encryption Standard), DES (Data Encryption Standard), 3DES (Triple Data Encryption Standard), dan Blowfishh. Kunci simetris sendiri adalah jenis kunci yang sama digunakan untuk mengenkripsi dan mendekripsi data. Dalam algoritma kriptografi dengan kunci simetris, pihak yang terlibat dalam proses enkripsi dan dekripsi harus memiliki akses ke kunci yang sama. Oleh karena itu, tingkat keamanan kunci simetris sangat tergantung pada kerahasiaan dan keamanan kunci itu sendiri.

Penelitian ini menggunakan metode komparasi berbasis studi literatur dan analisis terhadap sumber-sumber terpercaya yang membahas keempat algoritma tersebut. Melalui pendekatan ini, Penelitian ini menyajikan rangkuman teoritik tentang prinsip kerja, kelebihan, kelemahan, serta tingkat keamanan masing-masing algoritma.

2. METODELOGI PENELITIAN

Berdasarkan pembahasan yang telah disampaikan, Penelitian ini termasuk Penelitian kualitatif Karena di dalam jurnal ini, Peneliti melakukan studi literatur untuk memahami prinsip kerja, keamanan, dan karakteristik algoritma kriptografi kunci simetris AES, DES, 3DES, dan Blowfishh.

Berikut adalah penjelasan rinci dan jelas tentang tahapan metode komparasi yang digunakan:

A. Pengumpulan Data

Dalam tahap pengumpulan data, peneliti melakukan studi literatur secara mendalam tentang algoritma kriptografi kunci simetris AES, DES, 3DES, dan Blowfishh. Data

dikumpulkan dari berbagai sumber tepercaya seperti jurnal ilmiah, buku, konferensi, dan makalah penelitian terkait. Informasi yang dikumpulkan mencakup prinsip kerja masing-masing algoritma, kompleksitas, panjang kunci, tingkat keamanan, dan kelemahan yang dimiliki oleh setiap algoritma.

B. Penentuan Kriteria Komparasi

Penentuan kriteria komparasi merupakan langkah penting dalam metode komparasi. Peneliti menentukan kriteria atau faktor-faktor yang relevan dan signifikan untuk membandingkan keempat algoritma. Beberapa kriteria yang mungkin dipertimbangkan meliputi:

Tingkat keamanan: Evaluasi sejauh mana algoritma tersebut tahan terhadap serangan kriptanalisis atau serangan lainnya.

Kecepatan enkripsi dan dekripsi: Analisis tentang seberapa cepat algoritma dapat mengamankan dan mendekripsi data.

Efisiensi: Evaluasi tentang seberapa efisien penggunaan sumber daya komputasi yang dibutuhkan oleh masing-masing algoritma.

Panjang kunci: Penilaian tentang seberapa panjang kunci yang digunakan untuk mengamankan data.

C. Pengolahan Data

Setelah data dikumpulkan, peneliti akan mengolah data secara sistematis. Data dari studi literatur dianalisis untuk mendapatkan pemahaman yang mendalam tentang kekuatan dan kelemahan masing-masing algoritma. Proses ini dapat melibatkan perbandingan statistik atau analisis kualitatif untuk mengidentifikasi perbedaan dan kesamaan antara algoritma.

D. Pembandingan

Pembandingan adalah langkah utama dalam metode komparasi. Berdasarkan data yang telah diolah, peneliti akan membandingkan keempat algoritma kriptografi kunci simetris (AES, DES, 3DES, dan Blowfishh) berdasarkan kriteria komparasi yang telah ditentukan. Perbandingan dilakukan untuk setiap kriteria dan dapat diilustrasikan dalam bentuk tabel, grafik, atau narasi yang jelas.

E. Penarikan Kesimpulan

Dari hasil pembandingan, peneliti akan menarik kesimpulan tentang keefektifan dan kinerja masing-masing algoritma dalam mengamankan data. Penelitian akan menyajikan temuan berdasarkan analisis kritis tentang kekuatan dan kelemahan dari masing-masing algoritma. Penarikan kesimpulan akan memberikan gambaran menyeluruh tentang algoritma mana yang lebih sesuai digunakan dalam berbagai skenario keamanan data.

F. Rekomendasi

Selain penarikan kesimpulan, peneliti juga dapat memberikan rekomendasi tentang algoritma mana yang lebih sesuai untuk digunakan dalam konteks keamanan data tertentu. Rekomendasi ini didasarkan pada hasil pembandingan dan kesimpulan yang telah ditarik dari penelitian ini. Rekomendasi ini dapat memberikan panduan berharga bagi para ahli keamanan data dan praktisi dalam memilih algoritma yang paling sesuai untuk melindungi data sensitif dalam berbagai skenario keamanan yang berbeda.

3. ANALISA DAN PERANCANGAN

Berdasarkan studi literatur dan analisis terhadap karakteristik dan keamanan data yang dimiliki oleh masing-masing algoritma kunci simetris, yaitu AES, DES, 3DES, dan Blowfishh. Berikut adalah hasil dan pembahasan yang didasari dari data landasan teori dan metode yang digunakan:

A. Hasil Studi Literatur tentang Algoritma Kriptografi Kunci Simetris:

a) AES (Advanced Encryption Standard):

- AES merupakan salah satu algoritma kriptografi yang paling banyak digunakan dan dianggap sebagai standar de facto dalam keamanan data.
- AES menggunakan blok ukuran 128 bit dan kunci dengan panjang 128, 192, atau 256 bit.
- Algoritma ini menggunakan struktur blok substitusi dan permutasi yang kompleks untuk mengamankan data dengan tingkat keamanan yang tinggi.

b) DES (Data Encryption Standard):

- DES adalah salah satu algoritma kriptografi kunci simetris yang pertama kali digunakan secara luas.
- Namun, saat ini DES kurang umum digunakan karena panjang kuncinya hanya 56 bit, yang terbukti kurang aman terhadap serangan Brute Force.

c) 3DES (Triple Data Encryption Standard):

- 3DES merupakan pengembangan dari DES yang menggunakan tiga kali operasi DES untuk meningkatkan keamanan.
- Proses enkripsi menggunakan tiga kunci yang berbeda dan dapat diulang beberapa kali.
- Meskipun lebih aman daripada DES, 3DES memiliki kelemahan yaitu kecepatan yang lebih lambat karena pengulangan proses enkripsi.

d) Blowfishh

- Blowfishh adalah algoritma kriptografi kunci simetris blok yang dikembangkan oleh Bruce Schneier pada tahun 1993.
- Blowfishh menggunakan ukuran blok 64 bit dan dapat menggunakan kunci dengan panjang 32 hingga 448 bit.
- Algoritma ini terkenal karena kecepatan dan efisiensinya dalam mengamankan data, sehingga sering digunakan dalam aplikasi dengan kebutuhan tinggi akan keamanan dan kinerja.

B. Pembahasan Hasil Metode Komparasi:

Berdasarkan studi literatur dan analisis terhadap empat algoritma kriptografi kunci simetris, berikut adalah pembahasan hasil metode komparasi:

a) Tingkat Keamanan:

- AES: AES dianggap sebagai algoritma dengan tingkat keamanan yang sangat tinggi, terutama jika menggunakan kunci 256 bit. Algoritma ini telah menggantikan DES karena dianggap lebih aman dan tahan terhadap serangan kriptanalisis yang canggih.
- DES: DES saat ini dianggap sudah tidak aman karena panjang kunci yang terbatas, sehingga dapat dipecahkan dengan mudah menggunakan serangan Brute Force.
- 3DES: 3DES memberikan tingkat keamanan yang lebih baik daripada DES karena penggunaan tiga kali operasi DES, namun kecepatannya lebih lambat dibandingkan AES.
- Blowfishh: Blowfishh menawarkan tingkat keamanan yang cukup baik dengan ukuran kunci yang dapat dipilih hingga 448 bit.

b) Kecepatan Enkripsi dan Dekripsi:

- AES: AES cenderung lebih cepat dalam proses enkripsi dan dekripsi jika menggunakan kunci 128 bit atau 192 bit. Namun, ketika menggunakan kunci 256 bit, kinerja AES dapat sedikit menurun.
- DES: Meskipun DES adalah algoritma yang kurang aman, kecepatan enkripsi dan dekripsinya lebih cepat daripada AES karena panjang kuncinya yang lebih pendek.

- 3DES: Kecepatan 3DES lebih lambat daripada AES karena melibatkan tiga kali operasi DES. Namun, dapat memberikan tingkat keamanan yang lebih tinggi tergantung pada panjang kunci yang digunakan.
- Blowfishh: Blowfishh menonjolkan kecepatan dan efisiensinya dalam proses enkripsi dan dekripsi data.

c) Efisiensi:

- AES: AES biasanya efisien dalam penggunaan sumber daya komputasi dan memerlukan sedikit ruang memori untuk operasionalnya.
- DES: Karena desainnya yang lebih tua, DES memiliki efisiensi yang baik dalam penggunaan sumber daya komputasi.
- 3DES: Efisiensi 3DES lebih rendah dibandingkan AES karena melibatkan tiga kali operasi DES.
- Blowfishh: Blowfishh juga menawarkan efisiensi yang baik dalam penggunaan sumber daya komputasi.

d) Panjang Kunci:

- AES: AES menawarkan tiga varian panjang kunci, yaitu 128 bit, 192 bit, dan 256 bit, yang memberikan fleksibilitas dalam memilih tingkat keamanan yang diinginkan.
- DES: DES hanya menggunakan kunci dengan panjang 56 bit, yang membuatnya kurang aman dalam mengamankan data saat ini.
- 3DES: Panjang kunci 3DES dapat dipilih hingga 168 bit, yang meningkatkan tingkat keamanan dari DES.
- Blowfishh: Blowfishh memiliki fleksibilitas dalam panjang kunci, mulai dari 32 hingga 448 bit, yang memungkinkan tingkat keamanan yang beragam.

4. KESIMPULAN

Berdasarkan hasil metode komparasi yang telah dilakukan, AES merupakan pilihan yang lebih unggul dalam hal keamanan data, kecepatan enkripsi dan dekripsi, serta efisiensi penggunaan sumber daya komputasi dibandingkan dengan algoritma lainnya. AES juga menawarkan fleksibilitas dalam memilih tingkat keamanan berdasarkan panjang kunci yang digunakan. DES, 3DES, dan Blowfishh tetap menjadi pilihan jika ada kebutuhan khusus atau implementasi khusus yang memerlukan fitur-fitur yang unik dari masing-masing algoritma.

Rekomendasi:

Berdasarkan hasil metode komparasi, rekomendasi yang dapat diberikan adalah:

- AES direkomendasikan sebagai pilihan utama dalam implementasi keamanan data karena tinggi dan kinerja yang baik.
- DES sebaiknya tidak digunakan lagi karena keamanannya yang sudah terbukti lemah.
- 3DES dapat dipertimbangkan jika ada batasan sistem yang mengharuskan penggunaan algoritma dengan panjang kunci yang lebih besar.
- Blowfishh cocok digunakan dalam aplikasi yang memerlukan kinerja yang tinggi dan tingkat keamanan yang memadai.

REFERENSI

Angga Syahputra, J. P. (2020). Implementasi Algoritma AES(Advanced Encryption Standard) Untuk Mengamankan File Soal Ujian Sekolah Dengan Kunci Algoritma 3Des (Triple DES). Jurnal CyberTech, 1673 - 1681.

Busran, J. W. (2021). ANALISA KOMPUTASI ALGORITMA DES DENGAN RC4 UNTUK KEAMANAN DATA. Jurnal Teknologi Terpadu, 20 - 23.

Ghosh, A. (2020). PERBANDINGAN ALGORITMA ENKRIPSI: AES, BLOWFISHH DAN TWOFISH UNTUK KEAMANAN JARINGAN NIRKABEL. Jurnal Riset Internasional Teknik dan Teknologi (IRJET), 4656 - 4659.

Novelius Buulolo, A. S. (2020). ANALISIS DAN PERANCANGAN KEAMANAN DATA TEKS MENGGUNAKAN ALGORITMA KRIPTOGRAFI DES (DATA ENCRYPTION STANDARD). Jurnal Teknologi Informasi, 61 - 65.

Nuniek Fahriani, H. R. (2018). IMPLEMENTASI TEKNIK ENKRIPSI DAN DEKRIPSI DI FILE VIDEO MENGGUNAKAN ALGORITMA BLOWFISHH. Jurnal Teknologi Informasi dan Ilmu Komputer (JTIIK), 697 -702.

Rizaldi. (2020). KOMPARASI ALGORITMA SEQUENTIAL SEARCHING DAN INTERPOLATION SEARCHING PADA STUDI KASUS PENCARIAN DATA TILANG PENGADILAN NEGERI SAMARINDA. JURTI, 86 - 92.

Siregar, N. (2019). PERANCANGAN APLIKASI KEAMANAN PESAN TEKS DENGAN MENGGUNAKAN ALGORITMA TRIPLE DES. Jurnal Teknik Informatika Kaputama (JTIK), 11 -17.

Syafmi Giffari Sipayng, G. L. (2019). ANALISA KEAMANAN URL YANG MENGGUNAKAN ALGORITMA 3DES. KOMIK (Konferensi Nasional Teknologi Informasi dan Komputer), 349 - 354.