BAB I
PENDAHULUAN

1.1 Latar Belakang

Dalam dunia digital yang terus berkembang, keamanan informasi sangatlah penting. Untuk melindungi informasi dan data sensitive, enkripsi adalah salah satu Tindakan yang paling umum digunakan. Enkripsi adalah prorses mengubah data menjadi bentuk yang tidak dapat di baca atau di pahami oleh siapa pun kecuali penerima dengan kunci enkripsi yang sesuai.

Algoritma enkripsi kunci simetris adalah salah satu jenis enkripsi yang paling umum digunakan. Algoritma ini menggunakan kunci yang sama untuk enkripsi dan deskripsi. Beberapa algoritma enkripsi kunci simetris telah dikembangkan, antara lain AES (Advanced Encryption Standard) dan DES (Data Encryption Standard). Saat menganalisis perbandingan kinerja algoritma enkripsi kunci simetris AES dan DES dalam keamanan data, beberapa factor penting dapat dipertimbangkan.

Keamanan merupakan faktor penting Ketika algoritma enkripsi. AES telah disetujui AES menggunakan panjang kunci 128, 192, atau 256 bit, sedangkan DES hanya menggunakan kunci 56 bit. Untuk alasan keamanan, AES lebih disukai karena panjang kuncinya yang lebih panjang. Kecepatan enkripsi dan deskripsi merupakan factor penting dalam kinerja algoritma. AES umumnya lebih cepat daripada DES, terutama saat menggunakan Panjang kunci ynag lebih lambat dari DES. Dalam scenario di mana kecepatan sangat penting, DES mungkin merupakan pilihan yang lebih baik. Penggunaan Sumber daya komputasi juga harus diperhitungkan. AES membutuhkan lebih baik banyak sumber daya komputasi daripada DES karena kerumitan algoritmenya. Jika sumber daya terbatas. DES mungkin menjadi pilihan yang lebih baik karena membutuhkan lebih sedikit sumber daya. Ketersediaan implementasi algoritma juga di perhitungkan. AES banyak digunakan dan berbagai platform Bahasa pemrograman implementasi DES bisa lebih terbatas terutama untuk aplikasi yang lebih modern.[1]

1.2 Rumusan Masalah

1. Apa perbedaan utama dalam Panjang kunci antara AES dan DES, dan bagaimana hal ini mempengaruhi tingkat keamanan keduanya ?
2. Bagaimana performa AES dan DES dalam kecepatan Enkripsi daan Dekirpsi data besar ?
3. Bagaimana pemilihan mode operasi penggunaan algoritma ini mempengaruhi keamanan informasi

Dalam konteks praktis ?

1.3 Batasan Masalah

Tujuan dari penelitian ini adalah untuk membandingkan kinerja dua algoritma enkripsi simetris, yaitu Advanced Encryption Standard (AES) dan Data Encryption Standard (DES), dalam konteks keamanan informasi. Beberapa tujuan spesifik dari penelitian ini antara lain:

1. Menganalisis efektivitas dan keamanan AES dan DES dalam melindungi data rahasia.
2. Mengukur kecepatan dan efisiensi kinerja AES dan DES dalam proses enkripsi dan deskripsi data.
3. Mengevaluasi katahanan AES dan DES terhadap serangan kriptoanalisis yang umum.
4. Membandingkan ukuran kunci yang digunakan oleh AES dan DES dalam hal kekuatan keamanan dan kompleksitas.
5. Menentukan pengaruh ukuran blok enkripsi terhadap kinerja dan keamanan AES dan DES.
6. Memberikan rekomendasi atau pertimbangkan penggunaan AES atau DES berdasarkan hasil analisis kinerja dan keamanan.

1.4 Tujuan Penelitian

Fokus pada perbandingan kinerja AES dan DES dalam konteks keamanan informasi. Sebagai Penelitian tidak mempertimbangkan algoritma enkripsi lainnya selain AES dan DES dan Mempertimbangkan aspek keamanan informasi secara umum, termasuk kerahasiaan, integritas, dan autentikasi data.

1.5 Manfaat Penelitian

Berdasarkan paparan dari tujuan di atas, Adapun manfaat yang diberikan dalam penelitian ini antara lain:

1. Mengetahui bagaimana karakteristik, kekuatan, dan kelemahan masing-masing algoritma untuk membantu Anda memilih algoritma enkripsi yang tepat untuk melindungi data Anda.
2. Memberikan keputusan tentang pilihan algoritma yang sesuai dengan persyaratan system dan tingkat perlindungan yang diinginkan. Dengan melakukan analisis komparatif kinerja AES dan DES.
3. Refernsi penelitian ini dapat memberikan wawasan baru, pemahaman yang lebih dalam dan update terkait perbandingan algoritma enkripsi simetris yang poputer.

1.6 Metode Penelitian

Pada penulisan penelitian ini, ada beberapa metode penelitian yang digunakan sebagai bahan penyusun penelitian. Metode-metode yang digunakan antara lain:

1. Studi Pustaka

   Membaca berbagai informasi yang berkaitan dengan penelitian yang sedang dilakukan dengan membaca jurnal ilmiah, artikel, buku dan dokumen.

2. Studi Korelasional

   Mengamati hubungan dua variable dan mengukur kekuatan tersebut. Studi korelasional biasanya dilakukan menggunakan kriptografi simetris

1.7 Sistematika Penulisan

Pada bagian ini, akan dijelaskan sistematika penulisan skripsi ini. Sistematika penulisan akan menjelaskan struktur dan isi dari setiap bab, termasuk bab-bab berikutnya yang akan membahas pendahuluan, Tinjauan pustaka, Metode penelitian, hasil dan analisis, dan kesimpulan.

Penjelasan mengenai struktur penulisan skripsi pada setiap bab, termasuk isi dan tujuan masing-masing bab.

Penulisan skripsi ini dibagi dalam beberapa bab dengan masing-masing bab terdiri dari sub-sub tertentu yang saling berkaitan. Untuk lebih jelasnya sistematika pembahasan tiap-tiap bab adalah sebagai berikut :

BAB I Pendahuluan

Dalam bab pendahuluan materinya sebagian besar berupa penguraian dari latar belakang, rumusan masalah, Batasan masalah, tujuan penelitian, manfaat penelitian, dan sistematika penulisan.

BAB II Tinjauan Pustaka

Dalam bab merupakan tinjauan pustaka berupa tema yang pernah diteliti sebelumnya. Uraian teori-teori yang mendasari pembahasan terperinci yang berhubungan dengan

metode penelitian. meliputi pembahasan singkat mengenai Analisis Perbandingan kriptografi, AES, DES Dan sebagainya.

BAB III Metodologi Penelitian

Dalam bab ini akan diuraikan mengenai hasil penelitian, mulai dari tahapan analisis, desain, hasil testing dan implementasi. Selain itu juga akan dijelaskan mengenai proses kerja sistem dan pengujian sistem serta analisis kesalahan. mengtahui cara dan langkah serta tools yang digunakan dalam penelitian ini, serta penelitian – penelitian yang terkait dengan penelitian ini.

BAB IV Implementasi dan Pembahasan

Bab implementasi dan pembahasan berisi tentang papara implementasi dan analisis hasil uji coba program. Bab IV ini akan memaparkan hasil-hasil dari tahapan penelitian, dari tahapan analisis, desain dan implementasi desain.

BAB V Penutup

Bab ini berisi kesimpulan dan saran dari pembahasan yang telah dibuat. Dalam pembuatan kesimpulan diperkuat dengan bukti-bukti yang ditemukan pada saat melakukan penelitian.

Pada bab ini diuraikan tentang kesimpulan dari hasil yang didapat dari penelitian dan juga saran yang digunakan untuk pengembangan penelitian ke arah yang lebih baik lagi di masa yang akan datang.