BAB 1
PENDAHULUAN

1.1 Latar belakang

Keamanan data pada website menjadi salah satu aspek krusial dalam pengembangan dan pemeliharaan sistem informasi di era digital. Pertumbuhan signifikan, serta meningkatnya serangan siber, menuntut penerapan mekanisme enkripsi yang andal untuk melindungi informasi sensitif dari akses yang tidak sah. Enkripsi merupakan teknik pengamanan data yang berfungsi mengubah informasi menjadi kode yang tidak dapat dimengerti tanpa proses dekripsi yang benar. Dalam konteks keamanan website, pemilihan algoritma enkripsi yang tepat sangat penting untuk menjaga kerahasiaan, integritas, dan otentikasi data.

Terdapat berbagai algoritma enkripsi yang telah dikembangkan, di antaranya adalah *Advanced Encryption Standard* (*AES*), *Data Encryption Standard* (*DES*), dan *Blowfish*. Masing-masing algoritma ini memiliki keunggulan dan kelemahan yang berbeda dalam hal keamanan, kecepatan, dan kompleksitas implementasi. *AES*, misalnya, dikenal karena tingkat keamanan yang tinggi dan telah menjadi standar enkripsi data oleh pemerintah Amerika Serikat. *DES*, meskipun merupakan salah satu algoritma enkripsi yang lebih tua, masih digunakan dalam beberapa aplikasi karena kesederhanaan dan kecepatannya. *Blowfish*, di sisi lain, menawarkan kecepatan tinggi dan keamanan yang baik dengan fleksibilitas kunci enkripsi yang dapat disesuaikan.

Dalam upaya meningkatkan keamanan data pada website dengan menggunakan kombinasi dari ketiga algoritma ini (*AES*, *DES*, dan *Blowfish*) dapat diterapkan. Pendekatan ini bertujuan untuk memanfaatkan keunggulan masing-masing algoritma, sehingga menciptakan lapisan keamanan yang lebih. Kombinasi ini diharapkan dapat memberikan proteksi yang lebih kuat terhadap berbagai jenis ancaman siber, termasuk serangan brute force, serta memastikan bahwa data pengguna tetap terlindungi dalam lingkungan digital yang terus berkembang.

Latar belakang dalam penulisan ini akan membahas penerapan kombinasi algoritma *AES*, *DES*, dan *Blowfish* dalam konteks keamanan website, serta menganalisis efektivitas dan efisiensi dari pendekatan ini dalam menjaga keamanan data.

Lalu pada Penelitian yang dilakukan oleh Laila Mustika, Implementasi Algoritma AES Untuk Pengamanan *Login* Dan Data *Customer* Pada *E-Commerce* Berbasis *Web* serta mengetahui kendala apa yang dihadapi dalam mengimplementasikan pada *website*. 1[1]

implementasi Algoritma AES maka kerentanan dari serangan XSS dapat diatasi. Algoritma AES mudah untuk diterapkan, memiliki tingkat keamanan yang tinggi serta mengunakan memori yang sedikit dalam pengoperasianya sehingga tidak membebani proses dan ukuran file. Pada pengembangan aplikasi berikutnya agar session disimpan ke dalam database supaya mudah di manajemen dari hasil penelitian yang dilakukan yendi putra. 2 [2]

Hasil dari pengujian dan analisis dari penerapan algoritma kriptografi AES-256 terhadap sistem E-Marketplace Bibit Sriwedari bahwa algoritma tersebut dapat berjalan dengan baik dalam melakukan enkripsi data transaksi pembayaran dari pengguna dan waktu yang relatif cepat. Algoritma AES-256 juga cukup aman dalam pemrosesan enkripsi data dikarenakan memiliki kunci yang panjang dan banyak proses putaran. 3[3]

Penelitian Fikri Prasetyo dengan dibuatnya aplikasi untuk pengamanan data kependudukan menggunakan metode AES-128, maka dapat kesimpulan yaitu aplikasi dapat mengenkripsi file dengan format docx,xlxs,txt dan pdf, algoritma AES-128 dapat diterapkan pada aplikasi keamanan data kependudukan di Desa BogaresKidul, File yang berukuran kecil akan lebih cepat durasi waktu enkripsi dan dekripsinya, Aplikasi dapat mengamankan file data kependudukan. 4[4]

Sistem dapat dimanfaatkan untuk proses enkripsi dan dekripsi file dengan berbagai ukuran dan jenis file, menggunakan algoritma AES. Proses yang dikerjakan pada setiap putaran adalah: SubBytes : substitusi byte dengan menggunakan table substitusi (S- box). ShiftRows : perputaran baris-baris array state secara wrapping. MixColumns : mengacak data di masingmasing kolom array state. AddRoundKey : mengerjakan XOR antara state sekarang round key. Final round: proses untuk putaran terakhir: SubBytes, ShiftRows, AddRoundKey Diskripsi proses enkripsi sebagai berikut : Add Round Key menyatukan chiper teks yang telah ada dengan chiper key yang chiper key dengan ikatantida XOR. Sub Bytes Proses SubBytes () memetakan setiap byte dari array State dengan menggunakan table substitusi S-Box. 5[5]

Metode *blowfish* optimal yang disarankan meningkatkan akurasi keamanan siber untuk semua data yang dirahasiakan sekaligus memerlukan enkripsi, dekripsi, dan waktu kinerja yang lebih sedikit dibandingkan teknik saat ini. Meskipun algoritme berfungsi dengan baik untuk gambar berformat JPEG, efisiensinya perlu diuji untuk jenis gambar lain dan gambar berkualitas HD. Kami berharap dapat memusatkan upayakami pada berbagai jenis aplikasi multimedia, seperti teks, audio, dan video, dengan algoritma yang sesuai. [6]

Perancangan pendekatan steganografi untuk menyembunyikan data rahasia dalam file gambar abu-abu, yang dapat berisi semua jenis bitstream rahasia. Sistem ini memungkinkan pengguna untuk menyembunyikan dan menyimpan informasi rahasia di perangkat lokal atau global mereka. Tujuan dari pekerjaan ini adalah untuk melindungi data rahasia. Teknologi ini juga dapat membantu mencegah akses tidak sah dan menjamin keamanan pesan selama transmisi. 14[7]

Algoritma enkripsi *blowfish* adalah salah satu algoritma kriptografi yang paling terkenal. Namun, masing-masing algoritma yang ada saat ini memiliki kelebihan dan kekurangannya masing-masing. Namun, ada beberapa kelemahan dalam menggunakan algoritma ini, termasuk operasi komputasi yang kompleks, masalah tetap (S-Box) dan pola, yang dapat muncul saat menangani data yang lebih kompleks, termasuk teks. 15[8]

Penelitian ini di ambil karena pentingnya keamanan *website* tidak hanya bergantung pada algoritma kriptografi, tetapi juga pada implementasi yang baik, manajemen kunci yang aman, pembaruan sistem secara teratur, dan langkah-langkah keamanan yang komprehensif. Kombinasi algoritma kriptografi adalah salah satu aspek dari strategi keamanan yang lebih luas.

1.2 Rumusan masalah

Rumusan ini berfokus pada evaluasi keunggulan kombinasi algoritma dibandingkan penggunaan algoritma tunggal dalam melindungi data pada website mengeksplorasi efisiensi kinerja kombinasi algoritma ketika digunakan untuk mengamankan data dengan format yang berbeda, yang merupakan kebutuhan umum pada website serta mengidentifikasi potensi kendala dalam penerapan kombinasi algoritma pada website.

Berikut ini rumusan masalah yang diambil dari penelitian terkait dari :

1. Bagaimana cara mengintegrasikan algoritma kriptografi AES, DES, dan Blowfish dalam sistem deteksi keamanan website untuk meningkatkan tingkat perlindungan data?
2. Apa keunggulan dan kelemahan dari penggunaan kombinasi algoritma AES, DES, dan Blowfish dibandingkan dengan pendekatan yang hanya menggunakan satu algoritma?
3. Bagaimana mengukur dan mengevaluasi efektivitas kombinasi algoritma AES, DES, dan Blowfish dalam mendeteksi dan mencegah serangan terhadap keamanan website?

1.3 Tujuan

Tujuan dari penelitian ini untuk mengimplementasikan kombinasi dari algoritma AES, DES, dan Blowfish untuk digunakan dalam proses enkripsi dan dekripsi data pada website guna menciptakan lapisan keamanan yang lebih kompleks dan sulit ditembus oleh serangan siber. Mengukur dan menganalisis kinerja kombinasi algoritma tersebut dalam hal waktu enkripsi dan dekripsi (seperti waktu pemrosesan yang lebih lama) untuk berbagai jenis data (teks, gambar, dan file PDF) , serta membandingkannya dengan penggunaan algoritma secara individu atau dalam kombinasi yang lebih sederhana. penelitian diharapkan dapat memberikan kontribusi dalam bidang keamanan siber, khususnya dalam pengembangan metode enkripsi yang lebih aman dan efisien untuk perlindungan data pada website.

1.4 Manfaat

Manfaat dari penelitian ini bertujuan untuk membantu pengembang website dalam meningkatkan keamanan data dengan menerapkan kombinasi algoritma yang lebih kuat, sehingga melindungi informasi sensitif dari ancaman siber seperti pencurian data, manipulasi, dan penyadapan. Mengidentifikasi kombinasi algoritma yang tidak hanya aman tetapi juga efisien dalam hal waktu pemrosesan, sehingga memungkinkan implementasi keamanan yang kuat tanpa mengorbankan performa website secara keseluruhan serta meningkatkan kesadaran akan pentingnya keamanan data di kalangan pengembang, pengguna, dan penerapan praktik-praktik keamanan yang lebih baik dalam pengelolaan website.

1.5 Batasan masalah

Batasan masalah pada penelitian ini Pengujian kombinasi algoritma *AES, DES,* dan *Blowfish* akan dilakukan dalam lingkungan yang terkontrol dengan data simulasi uji coba dalam sistem website yang sebenarnya tidak

akan dilakukan sebagai bagian dari penelitian ini dan analisis kinerja sistem akan terbatas pada waktu enkripsi dan dekripsi data.