IMPLEMENTASI KRIPTOGRAFI ADVANCED ENCRYPTION STANDARD (AES-128) UNTUK PENGAMANAN FILE SOAL BERBASIS WEB PADA SMP GUNUNG JATI KOTA TANGERANG

Muhammad Arrafiqal Maryo[1], Bambang Wisnu Widagdo[2]

[1]Program Studi Teknik Informatika, Universitas Pamulang, JL Puspitek Tangerang Selatan, Indonesia, 15310
e-mail: [1] arrafiqalmaryo@gmail.com

Abstract

Documents are one type of data file that is very important because it functions as a source of information needed by agencies or companies. In this ever-growing digital era, maintaining data confidentiality is very crucial for various agencies, one of which is the Education Agency. Gunung Jati Junior High School (JHS) in Tangerang City has implemented a computer-based examination system (USBK) since 2014. Although this system offers efficiency and convenience, the main problem faced is the weak security system for storing exam question files. This condition creates a significant risk, where important information can be stolen or manipulated, allowing for the leakage of exam questions which negatively impacts the integrity of the exam as well as student fairness. Therefore, in overcoming these problems the author plans to develop a cryptography-based web application by applying the AES-128 algorithm. This research aims to create a web-based application that can protect data by implementing the Advanced Encryption Standard (AES-128) algorithm method into the application to secure the file and provide a more interactive and in-depth learning experience for students through securing school exam data. The results showed that the application of AES-128 as an encryption method has proven effective in increasing the security of question files at Gunung Jati Junior High School and making it the right choice to protect sensitive data.
Keywords: Advanced encryption standard (AES-128), data security, encryption, file security, information security.

Abstrak

Dokumen merupakan salah satu jenis file data yang sangat penting karena berfungsi sebagai sumber informasi yang diperlukan oleh instansi atau perusahaan. Di era digital yang terus berkembang ini, menjaga kerahasiaan data menjadi sangat krusial bagi berbagai instansi salah satunnya, yaitu Instansi Pendidikan. Sekolah Menengah Pertama (SMP) Gunung Jati di Kota Tangerang telah menerapkan sistem ujian berbasis komputer (USBK) sejak tahun 2014. Meskipun sistem ini menawarkan efisiensi dan kemudahan, masalah utama yang dihadapi adalah lemahnya sistem keamanan penyimpanan file soal ujian. Kondisi ini menciptakan risiko yang signifikan, di mana informasi penting dapat dicuri atau dimanipulasi, memungkinkan terjadinya kebocoran soal ujian yang berdampak negative bagi integritas ujian meupun keadilan siswa. Oleh karena itu, dalam mengatasi permasalahan tersebut penulis berencana mengembangkan aplikasi web berbasis kriptografi dengan menerapkan algoritme AES-128. Penelitian ini bertujuan untuk membuat sebuah aplikasi berbasis web yang dapat melindungi data dengan mengimplementasikan metode algoritme Advanced Encryption Standart (AES-128) ke dalam aplikasi untuk pengamanan file tersebut dan memberikan pengalaman belajar yang lebih interaktif dan mendalam bagi siswa melalui pengamanan data ujian sekolah. Hasil penelitian menunjukan bahwa penerapan AES-128 sebagai metode enkripsi telah terbukti efektif dalam meningkatkan keamanan file soal di SMP Gunung Jati dan menjadikannya pilihan yang tepat untuk melindungi data sensitive.
Kata Kunci : Advanced encryption standart (AES-128), enkripsi, keamanan data, pengamanan file, pengamanan informasi

1. PENDAHULUAN

Dokumen merupakan salah satu jenis file data yang sangat penting karena berfungsi sebagai sumber informasi yang diperlukan oleh instansi atau perusahaan. Dalam konteks pendidikan, dokumen dokumen penting seperti soal ujian, laporan, dan data siswa harus dikelola dengan baik dan dilindungi agar tidak jatuh ke tangan yang salah. Di era digital yang terus berkembang ini, menjaga kerahasiaan data menjadi sangat krusial untuk memastikan bahwa informasi yang tersimpan tidak dapat diakses atau dibaca oleh pihak yang tidak berwenang.

Dengan meningkatnya ancaman keamanan siber, seperti pencurian data dan peretasan, institusi mengambil langkah pendidikan harus proaktif untuk melindungi informasi sensitif mereka. Data yang tidak terlindungi dapat disalahgunakan, yang dapat merugikan tidak hanya individu tetapi juga reputasi institusi itu sendiri. Oleh karena itu, institusi pendidikan harus mengadopsi teknologi yang dapat memberikan perlindungan maksimal terhadap data yang dimiliki. Keamanan data bukan hanya tanggung jawab IT, tetapi juga melibatkan seluruh elemen dalam organisasi.

Salah satu solusi yang dapat diterapkan adalah penggunaan teknologi Kriptografi. Kriptografi adalah seni dan ilmu untuk menjaga kerahasiaan informasi melalui metode enkripsi yang kompleks. Dengan kriptografi, pesan asli (plaintext) dapat diubah menjadi pesan terenkripsi (ciphertext) yang aman, dan kemudian dapat dikembalikan ke bentuk aslinya melalui proses dekripsi. Ini sangat membantu dalam melindungi data sensitif dari akses yang tidak sah, sehingga memberikan rasa aman bagi pengguna. Implementasi kriptografi dapat membantu meningkatkan kepercayaan antara pihak pihak yang terlibat dalam proses pendidikan.

Sekolah Menengah Pertama (SMP) Gunung Jati di Kota Tangerang telah menerapkan sistem ujian berbasis komputer (USBK) sejak tahun 2014. Meskipun sistem ini menawarkan efisiensi dan kemudahan, masalah utama yang dihadapi adalah lemahnya sistem keamanan penyimpanan file soal ujian. Saat ini, file soal ujian masih disimpan dalam komputer tanpa perlindungan tambahan, yang membuatnya rentan terhadap akses tidak sah, baik dari pihak luar maupun orang-orang di dalam institusi tersebut. Hal ini menciptakan tantangan baru dalam pengelolaan data yang aman.

Kondisi ini menciptakan risiko yang signifikan, di mana informasi penting dapat dicuri atau dimanipulasi. Selain itu, lemahnya sistem keamanan juga dapat menyebabkan kebocoran soal ujian, yang akan berdampak negatif pada integritas ujian dan keadilan bagi siswa. Oleh karena itu, ada kebutuhan mendesak untuk menerapkan solusi yang lebih efektif dalam mengamankan data tersebut. Dalam hal ini, pemahaman tentang pentingnya keamanan data harus ditanamkan kepada seluruh stakeholder, termasuk siswa dan guru.

Dalam konteks ini, penggunaan teknologi kriptografi relevan. Penulis menjadi sangat berencana mengembangkan aplikasi web berbasis kriptografi dengan menerapkan algoritme AES-128. Algoritme ini, yang juga dikenal sebagai cipher, adalah serangkaian aturan atau langkah-langkah untuk melakukan enkripsi dan dekripsi data dengan parameter bilangan yang dirahasiakan. Algoritme AES-128 adalah algoritme enkripsi simetris yang menggunakan kunci 128-bit untuk proses enkripsi dan dekripsi data, menjadikannya salah satu standar yang diakui secara internasional untuk keamanan data.

Dengan mengimplementasikan kriptografi menggunakan AES-128, diharapkan file soal ujian di SMP Gunung Jati Kota Tangerang dapat terlindungi secara maksimal. Ini tidak hanya akan meningkatkan keamanan data, tetapi juga memberikan kepercayaan kepada siswa, orang tua, dan pihak terkait lainnya terhadap pengelolaan informasi di institusi pendidikan. Di samping itu, aplikasi ini juga diharapkan dapat memberikan kemudahan dalam proses pengelolaan dan distribusi soal ujian.

Melalui penerapan sistem ini, tidak hanya keamanan data yang ditingkatkan, tetapi juga integritas proses pendidikan secara keseluruhan. Dengan adanya sistem yang aman, diharapkan dapat mendorong inovasi dalam metode evaluasi dan pengajaran. Inovasi ini akan membawa dampak positif terhadap kualitas pendidikan yang diberikan kepada siswa.

Akhirnya, penelitian ini diharapkan dapat memberikan kontribusi signifikan dalam pengembangan sistem keamanan informasi di institusi pendidikan, serta menjadi model bagi sekolah-sekolah lain dalam mengadopsi teknologi keamanan informasi yang lebih baik. Dengan langkah-langkah yang tepat, institusi pendidikan dapat menciptakan lingkungan yang aman dan terpercaya bagi semua pihak yang

terlibat. Melalui penelitian ini, penulis berharap dapat menunjukkan betapa pentingnya keamanan data di era digital dan mendorong lebih banyak institusi untuk berinvestasi dalam solusi yang efektif.

2. METODE

Data Penelitian

Data yang akan digunakan pada penelitian ini yaitu dokumen soal dengan format docx atau pdf yang ada pada SMP Gunung Jati Tangerang. Pada tahap ini penulis mengumpulkan data secara langsung file soal pada SMP Gunung Jati Tangerang.

Perancangan Pengujian

Rancangan pengujian yang digunakan menggunakan metode Blackbox testing dan Whitebox testing.

Penerapan Metode

Metode yang digunakan pada penelitian ini adalah metode *waterfall*, yang dimulai dari perumusan masalah, studi literatur, metode ini digunakan sebagai pedoman untuk melakukan penelitian agar hasil yang diperoleh tidak menyimpang dari tujuan yang telah ditetapkan dari penelitian sebelumnya.

Pengumpulan Data

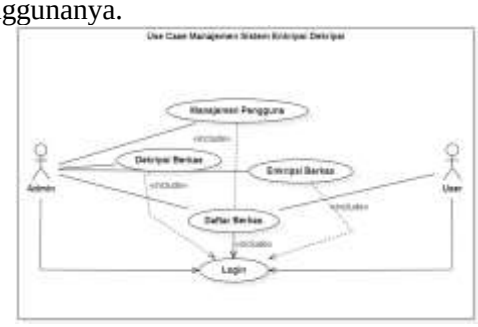
Pada tahap ini dilakukan pengumpulan data dari semua data yang diatas. Tahapan proses pengumpulan data didapat melalui wawancara dan observasi.

Perancangan Basis Data

Perancangan basis data mencakup beberapa komponen penting sebelum proses pembuatan program. Adapun komponen tersebut adalah *usecase diagram*, *activity diagram*, *sequence diagram*, *entity relationship diagram* dan struktur database.

Use Case Diagram

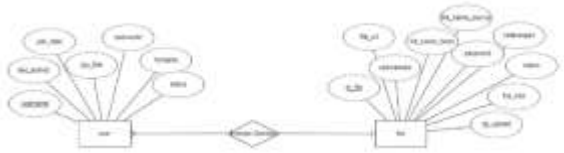
Pada Gambar 3. 1 merupakan gambar *use case* manajemen sistem *enkripsi dekripsi* yang menjelaskan akses fitur pengguna dan siapa saja penggunanya.



Gambar 4. 1 Use Case Diagram Manajemen Sistem Enskripsi Data

ERD (*Entity Relationship Diagram*)

Entity Relationship Diagram adalah suatu model untuk menjelaskan hubungan antar data dalam basis data berdasarkan suatu persepsi yang terdiri dari beberapa object yang mempunyai relasi hubungan.



Gambar 4. 2 *Entity Relationship Diagram*

3. HASIL

Berikut adalah hasil implementasi dari algoritme *Advanced Encryption Standard* (AES-128) untuk pengamanan file soal berbasis web pada SMP Gunung Jati Kota Tangerang. Dalam implementasi ini, sistem keamanan data dirancang untuk melindungi file soal yang bersifat rahasia dan hanya dapat diakses oleh pihak yang berwenang. Sistem ini menggunakan algoritme kriptografi *Advanced Encryption Standard* (AES-128), yang dikenal sebagai salah satu metode enkripsi paling aman dan efisien. AES-128 bekerja dengan panjang kunci 128-bit, memberikan tingkat keamanan tinggi terhadap keamanan file UNBK.

Halaman Login

Gambar 5. 1 Halaman untuk login

Halaman Admin

Gambar 5. 2 Halaman *Dasboard* Admin

Halaman Enkripsi

Gambar 5. 3 Halaman *Enkripsi*

Halaman Deskripsi

Gambar 5. 4 Halaman *Deskripsi*

Halaman Daftar Berkas

Gambar 5. 5 Halaman Data Berkas

4. PEMBAHASAN

Halaman Login

Halaman *login* berfungsi sebagai pintu masuk utama bagi pengguna yang telah memiliki akun untuk mengakses sistem. Pada halaman ini, pengguna diminta memasukkan nama pengguna (*username*) dan kata sandi (*password*) yang telah terdaftar sebelumnya. Sistem kemudian akan menjalankan proses autentikasi dengan mencocokkan data login yang dimasukkan dengan informasi yang tersimpan di basis data. Untuk menjaga keamanan, kata sandi dienkripsi selama proses ini. Setelah proses login berhasil, pengguna akan diarahkan ke halaman utama untuk mengakses berbagai fitur yang tersedia dalam sistem.

Halaman Admin

Pada halaman *dashboard* admin ini menampilkan tampilan *dashboard* dari sebuah sistem *Enkripsi* dan *Dekripsi* UNBK sekolah (SMP Gunung Jati Tangerang). Pada bagian atas terdapat tiga buah kotak informasi yang menunjukkan total pengguna, total *enkripsi*, dan total *dekripsi*.Pada bagian kiri terdapat menu navigasi yang terdiri dari Berkas, Daftar Berkas, dan Data Pengguna. Secara keseluruhan, tampilan ini memberikan informasi dasar tentang aktivitas dan status sistem di SMP Gunung Jati Tangerang.

Halaman Enkripsi

Untuk melakukan *enkripsi* file pada sistem ini, pengguna terlebih dahulu memilih menu "Berkas" pada navigasi di sisi kiri. Selanjutnya, dari sub-*menu* yang tersedia, pengguna akan memilih opsi "*Enkripsi* Berkas". Setelah masuk ke form enkripsi berkas, pengguna akan diminta untuk melakukan beberapa langkah. Pertama, pengguna harus memilih file yang akan dienkripsi. Kedua, pengguna diminta untuk memasukkan *password* atau kunci yang akan digunakan untuk mengamankan file tersebut. Ketiga, pengguna juga dapat menambahkan keterangan tambahan untuk file yang akan dienkripsi. Setelah pengguna melakukan langkah-langkah tersebut, sistem akan memproses *enkripsi* terhadap file yang telah dipilih oleh pengguna.

Halaman Deskripsi

Dalam proses dekripsi file pada sistem ini, pengguna dapat mengembalikan file yang sebelumnya telah dienkripsi. Pada tampilan dekripsi berkas, jika pengguna ingin melakukan dekripsi, pertama, pengguna harus memilih file yang telah terenkripsi sebelumnya. Setelah itu, pengguna akan memilih opsi "*Dekripsi* Berkas" pada menu yang tersedia. Selanjutnya, pengguna diminta untuk memasukkan password yang sesuai dengan proses *enkripsi* file yang dilakukan sebelumnya. Setelah memasukkan password yang benar, pengguna dapat memilih tombol "*Dekripsi* Berkas" untuk memulai proses pengembalian file ke bentuk aslinya. Dengan mengikuti langkah-langkah ini, pengguna dapat mendekripsi file yang telah diamankan melalui proses enkripsi sebelumnya.

Halaman Daftar Berkas

Pada halaman ini, terdapat tiga baris data yang menunjukkan rincian tiga berkas yang telah diproses. Setiap baris menampilkan ID, nama pengguna, nama berkas asli, nama berkas yang

telah dienkripsi, ukuran berkas, tanggal proses, dan status apakah berkas tersebut telah terdekripsi atau masih terenkripsi. Halaman ini memungkinkan pengguna untuk melihat dan memantau status *enkripsi* dan *dekripsi* berkas-berkas yang dikelola oleh sistem. Fitur pencarian juga disediakan untuk memudahkan pengguna menemukan berkas yang diinginkan. Selain itu, terdapat navigasi untuk berpindah halaman jika terdapat lebih banyak data yang ditampilkan. Secara keseluruhan, halaman ini menyediakan antarmuka yang terstruktur dan informatif untuk mengelola proses *enkripsi* dan *dekripsi* berkas dalam sistem manajemen berkas.

5. KESIMPULAN

Berdasarkan hasil penelitian yang dilakukan, maka kesimpulan yang diperoleh adalah sebagai berikut :

Keamanan penyimpanan file soal ujian di SMP Gunung Jati, Kota Tangerang, sangat kurang, yang dapat menyebabkan potensi kebocoran atau penyalahgunaan data.

1. Soal ujian hanya disimpan di komputer tanpa perlindungan yang cukup, sehingga meningkatkan risiko akses tidak sah dan kehilangan informasi.
2. File soal ujian memiliki risiko tinggi untuk hilang karena pengawas dapat dengan mudah mengakses komputer, menjadikannya rentan terhadap pencurian atau penghapusan.

6. DAFTAR PUSTAKA

Journal Article

[1] F. A. Sitorus, N. B. Nugroho, and U. F. S. S. Pane, "Implementasi Algoritma Advanced Encryption Standard (AES) 128 Bit untuk Keamanan Data Transaksi Penjualan Pada PT. Mitsubishi Electric Indonesia," *J. CyberTech*, no. x, pp. 1–15, 2020, [Online]. Available: https://ojs.trigunadharma.ac.id/

[2] A. Aprizald, M. A. Hasan, and D. Setiawan, "Aplikasi Keamanan Data Berbasis Web Menggunakan Algoritma AES 128 Untuk Enkripsi Dan Dekripsi Data," *JEKIN - J. Tek. Inform.*, vol. 2, no. 2, pp. 85–95, 2023, doi: 10.58794/jekin.v2i2.225.

[3] Melenia Bayu Aryanto, Muhlis Tahir, Silvia Irma Devita, Zuda Nuril Mustofa, Qurrotun Ainiyah, and Shelviatus Sundoro, "Implementasi Enkrip Dan Dekrip File Menggunakan Metode Advance Encryption Standard (AES-128)," *J. Ilm. Sist. Inf. dan Ilmu Komput.*, vol. 3, no. 1, pp. 89–104, 2023, doi: 10.55606/juisik.v3i1.434.

[4] Simbolon Rohani Asih Imelda, Indra Gunawan, Kirana Okta Ika, Dewi Rafiqa, and Solikhun S, "Penerapan Algoritma AES 128-Bit dalam Pengamanan Data Kependudukan pada Dinas Dukcapil Kota Pematangsiantar," *J. Comput. Syst. Informatics*, vol. 1, no. 2, pp. 54–60, 2020.

[5] M. Hidayat, M. Tahir, A. Sukriyadi, A. Sulton, C. A. S. A, and S. A. F, "Penerapan kriptografi," vol. 2, no. 3, pp. 35–41, 2023.

[6] H. Herman, R. Wijaya, S. Miharja, and Wilson, "Implementasi Algoritma Aes-128 Dan Sha-256 Dalam Perancangan Aplikasi Pengamanan File Dokumen," *J. TIMES*, vol. 10, no. 2, pp. 80–87, 2022, doi: 10.51351/jtm.10.2.2021666.

[7] R. Firdaus and R. R. Santika, "Penerapan Algoritma AES-128 Untuk Enkripsi Dokumen Di PT Caveo Biometric Security," *Semin. Nas. Mhs. Fak. Teknol. Inf. Univ. Budi Luhur*, no. September, pp. 111–120, 2022.

[8] R. Maulana and R. M. Simanjorang, "Implementasi Kriptografi Pengamanan Data Pribadi Siswa SMA Swasta Jaya Krama Beringin Dengan Algoritma RC4," *J. Nas. Komputasi dan Teknol. Inf.*, vol. 4, no. 6, pp. 377–383, 2021, doi: 10.32672/jnkti.v4i6.3533.

[9] Nahar Mardiyantoro and M. Listiani, "Implementasi Algoritma AES Pada QR-Code Sebagai Parameter Keaslian Data Dalam Pembuatan KTA," *SATESI J. Sains Teknol. dan Sist. Inf.*, vol. 1, no. 1, pp. 26–31, 2021, doi: 10.54259/satesi.v1i1.5.

[10] D. Nurnaningsih and A. A. Permana, "Rancangan Aplikasi Pengamanan Data Dengan Algoritma Advanced Encyption Standard (Aes)," *J. Tek. Inform.*, vol. 11, no. 2, pp. 177–186, 2018, doi: 10.15408/jti.v11i2.7811.

[11] R. Oktafiani, E. I. H. Ujianto, and R. Rianto, "Kombinasi Algoritma Kriptografi Vigenere Cipher dan SHA256 untuk Keamanan Basis Data," *J. Sist. Komput. dan Inform.*, vol. 4, no. 3, p. 433, 2023, doi: 10.30865/json.v4i3.5583.

[12] Rina Noviana, "Pembuatan Aplikasi Penjualan Berbasis Web Monja Store Menggunakan Php Dan Mysql," *J. Tek. dan Sci.*, vol. 1, no. 2, pp. 112–124, 2022, doi: 10.56127/jts.v1i2.128.

[13] W. Siregar, I. Irvan, and E. Rahayu, "Sistem Informasi Pembayaran Iuran Keamanan Dan Kebersihan Pada Perumahan Berbasis Website Menggunakan Metode Design Thinking," *JiTEKH*, vol. 8, no. 2, pp. 50–58, 2020, doi: 10.35447/jitekh.v8i2.204.

[14] A. Yasinta Permana and A. Voutama, "Pemodelan UML Pada Sistem Penjualan Sembako Di Toko Amshop," *Inf. Manag. Educ. Prof.*, vol. 7, no. 1, pp. 41–50, 2022.

[15] Abdulloh, R. (2022). 7 Materi Pemrograman Web Untuk Pemula 1 : HTML, CSS, &MariaD (cara cepat menjadi Web programmer)) (As.pratisto@gmail.com (ed.)).PT Elex MediaKomputindo.