BAB I
PENDAHULUAN

1.1 Latar Belakang Penelitian

Kemajuan pesat dalam teknologi informasi dan komunikasi dalam dua dekade terakhir telah mentransformasi beragam aspek kehidupan, khususnya ranah pendidikan yang semakin bergantung pada sistem digital berbasis web. Menurut, Subroto et al., (2023) digitalisasi dalam sektor pendidikan Indonesia mengalami akselerasi signifikan, terutama pasca situasi pandemi COVID-19 yang menuntut lembaga pendidikan beralih pada pembelajaran dan evaluasi daring. Salah satu dampak langsung dari transformasi ini adalah munculnya sistem ujian berbasis *website* yang memungkinkan fleksibilitas, efisiensi, dan aksesibilitas yang lebih tinggi bagi peserta didik di seluruh wilayah. Akan tetapi, di balik kemudahan ini, terdapat tantangan serius dalam aspek keamanan data, terutama terhadap kebocoran soal ujian, manipulasi data hasil ujian, serta akses ilegal oleh pihak tak berwenang Utama et al., (2023). Masalah ini menjadi semakin krusial mengingat integritas akademik dan kepercayaan publik terhadap institusi pendidikan bergantung pada validitas proses evaluasi. Teknologi kriptografi, khususnya *Advanced Encryption Standard* (AES), telah banyak digunakan sebagai solusi dalam mengamankan data sensitif. Penelitian terdahulu oleh Irawan et al., (2023) dan Oktavani et al., (2023) menunjukkan efektivitas algoritma AES dalam menjaga kerahasiaan dan integritas data pada berbagai platform digital. Dalam konteks pendidikan, penggunaan AES-256 secara khusus diyakini mampu memberikan perlindungan tingkat tinggi terhadap data ujian daring Setiadi et al., (2024). Oleh karena itu, penelitian ini menjadi penting untuk menjawab tantangan tersebut melalui pengembangan sistem keamanan berbasis kriptografi yang relevan dengan kebutuhan lokal dan standar internasional.

Seiring meningkatnya penggunaan sistem ujian daring di lingkungan pendidikan tinggi, berbagai ancaman terhadap keamanan data kian bermunculan. Salah satu isu krusial adalah kebocoran soal ujian dan manipulasi data hasil ujian yang berpotensi merusak kredibilitas institusi serta mengurangi kepercayaan publik. Studi yang dilakukan Setiadi et al., (2024) mengindikasikan bahwa soal ujian yang tidak dilindungi secara kriptografis rentan terhadap akses tidak sah yang

dapat menyebabkan penggandaan dan penyebaran ilegal sebelum ujian berlangsung. Sementara itu, Ramadhintia & Bisma (2021) mencatat bahwa risiko kerusakan perangkat lunak akibat serangan virus serta gangguan jaringan dapat mengakibatkan kegagalan sistem secara menyeluruh pada pelaksanaan ujian daring.

Urgensi perlindungan soal ujian juga diperkuat melalui regulasi resmi, yakni Permendikbud Nomor 57 Tahun 2015 Pasal 19 ayat (5) yang menyatakan bahwa naskah soal Ujian Nasional (UN) sebelum dan sesudah pelaksanaan UN termasuk dalam klasifikasi dokumen negara yang bersifat rahasia(Kementerian Pendidikan dan Kebudayaan Republik Indonesia, 2015). Kebocoran soal ujian tidak hanya menurunkan kredibilitas sistem pendidikan, tetapi juga dapat menimbulkan konsekuensi hukum. Dengan demikian, dibutuhkan mekanisme pengamanan yang andal guna melindungi kerahasiaan soal, khususnya dalam pelaksanaan ujian berbasis teknologi informasi.

Sejalan dengan urgensi tersebut, sejumlah penelitian sebelumnya telah mengkaji penerapan algoritma kriptografi dalam upaya meningkatkan keamanan data, khususnya pada konteks sistem ujian dan pengelolaan informasi sensitif. (Wicaksana & Setiawan (2020) menerapkan algoritma Advanced Encryption Standard (AES) untuk melindungi berkas soal ujian dari akses tidak sah, menghasilkan tingkat kerahasiaan yang tinggi dan memastikan hanya pihak berwenang yang dapat mengakses data tersebut. Priambudi & Mufti (2023) mengimplementasikan AES-128 pada aplikasi pengamanan file berbasis web untuk SMP Yapipa, menunjukkan bahwa metode ini efektif mengenkripsi file berformat PDF, XLS, DOC, dan TXT dengan waktu pemrosesan yang relatif cepat, serta mempertahankan ukuran file setelah proses dekripsi kembali ke bentuk semula. Wiharto & Mufti (2022) menerapkan AES-128 untuk mengamankan basis data obat di apotek berbasis web, dengan hasil pengujian menunjukkan bahwa data sensitif seperti nama obat, harga, dan stok dapat terenkripsi sepenuhnya di dalam database, sehingga tidak dapat diakses tanpa kunci yang sah. Sementara itu, Hariyanto et al., (2018) mengembangkan aplikasi enkripsi dan dekripsi soal ujian menggunakan algoritma RSA berbasis Java Desktop, yang mampu mengenkripsi file dokumen DOC dan PDF secara efektif, serta mengembalikannya ke bentuk asli melalui kunci privat yang sesuai. Di sisi lain, Basim & Painem (2020) memadukan RC4 dan 3DES

dengan steganografi EOF untuk melindungi soal ujian berbasis desktop, menunjukkan bahwa kombinasi metode kriptografi dan steganografi mampu meningkatkan keamanan melalui pengaburan data ganda. Berdasarkan perbandingan algoritma kriptografi yang dilakukan oleh (Meko, 2018), AES terbukti memiliki performa terbaik dengan kecepatan enkripsi mencapai 48% dan dekripsi 45%, mengungguli DES, Blowfish, dan IDEA. Keunggulan ini, ditambah kemampuan mendukung panjang kunci hingga 256 bit, menjadikan AES sebagai pilihan ideal untuk menjaga keamanan data yang memerlukan keseimbangan antara tingkat perlindungan tinggi dan efisiensi pemrosesan.

Pendekatan yang digunakan dalam penelitian-penelitian sebelumnya juga menunjukkan adanya kelebihan dan kelemahan yang perlu diperhatikan. AES-128 dan AES-256 memiliki keunggulan pada kecepatan enkripsi serta kekuatan keamanan, namun penerapannya pada platform berbeda memerlukan penyesuaian teknis terkait integrasi dan manajemen kunci. Penerapan AES-128 seperti pada penelitian Wiharto & Mufti (2022) efektif untuk sistem berbasis web, namun belum memanfaatkan panjang kunci maksimum yang ditawarkan AES-256. RSA, sebagaimana digunakan pada penelitian Hariyanto et al. (2018), memiliki keunggulan dalam manajemen kunci asimetris, tetapi umumnya lebih lambat dibandingkan AES jika digunakan untuk data berukuran besar. Metode berbasis desktop sebagaimana pada penelitian Basim & Painem (2020) menawarkan keamanan ganda melalui kriptografi dan steganografi, namun kurang fleksibel untuk integrasi pada sistem berbasis web. Dengan demikian, masih terdapat ruang penelitian untuk mengembangkan sistem keamanan data yang menggabungkan kekuatan AES-256 dengan mekanisme autentikasi yang tangguh, dioptimalkan untuk sistem ujian berbasis *website*, sehingga dapat menjawab tantangan keamanan sekaligus menjaga kinerja dan kemudahan integrasi lintas platform.

Penelitian ini bertujuan menganalisis dan mengimplementasikan algoritma kriptografi AES-256 dalam sistem ujian berbasis website guna meningkatkan keamanan data dan integritas proses evaluasi pendidikan digital. Fokus penelitian mencakup pengembangan model implementasi yang optimal, evaluasi performa sistem, serta validasi efektivitas keamanan. Prototipe pengembangan web dibuat menggunakan Next.js (front-end) dan Express.js (back-end), dengan enkripsi–

dekripsi di sisi client. Evaluasi mencakup pengujian laboratorium, monitoring traffic menggunakan Wireshark, uji black-box, serta simulasi serangan untuk memastikan ketahanan sistem. Dengan demikian, penelitian ini diharapkan dapat menjadi rujukan akademis maupun praktis dalam pengembangan standar keamanan sistem ujian berbasis web di Indonesia.

Diharapkan hasilnya dapat memberikan kontribusi signifikan bagi praktisi teknologi pendidikan dalam mengembangkan sistem ujian yang aman dan efisien. Implikasi praktis dari penelitian ini meliputi tersedianya panduan implementasi yang dapat diadopsi oleh institusi pendidikan untuk meningkatkan keamanan sistem evaluasi digital mereka. Dari sisi akademis, temuan ini memperkaya pengetahuan tentang aplikasi kriptografi dalam pendidikan dan dapat menjadi landasan untuk riset lanjutan di bidang keamanan sistem ujian. Selain itu, hasil penelitian juga mendukung pengembangan regulasi dan standar keamanan data dalam sistem pendidikan digital di Indonesia. Bagi industri pengembang perangkat lunak pendidikan, hasil studi ini dapat menjadi acuan dalam mengintegrasikan fitur keamanan tingkat tinggi tanpa mengorbankan performa sistem. Dalam jangka panjang, kontribusinya diharapkan menciptakan ekosistem ujian yang lebih aman dan terpercaya, yang pada akhirnya meningkatkan kualitas serta integritas evaluasi pendidikan di era digital. Dampak positif yang diharapkan mencakup peningkatan kepercayaan stakeholder pendidikan terhadap sistem ujian dan pengurangan risiko kebocoran data maupun manipulasi hasil evaluasi.

1.2 Rumusan Masalah Penelitian

Merujuk pada latar belakang yang sudah diuraikan, maka permasalahan pokok yang menjadi sorotan penelitian ini dapat dirumuskan sebagai berikut:

1. Bagaimana merancang dan mengimplementasikan algoritma kriptografi AES-256 pada sistem ujian berbasis web untuk melindungi data ujian agar tetap aman selama proses pengiriman dan penyimpanan?
2. Bagaimana hasil pengujian keamanan data terenkripsi yang dikirim melalui jaringan, berdasarkan analisis paket menggunakan Wireshark dan pengujian fungsionalitas menggunakan metode *Black box*?

3. Bagaimana tingkat hubungan antara data asli (*plaintext*) dan data terenkripsi (*ciphertext*) berdasarkan perhitungan Korelasi Pearson sebagai salah satu indikator efektivitas enkripsi?

1.3 Tujuan Penelitian

Berdasarkan Rumusan masalah yang telah diuraikan, maka tujuan dari penelitian ini antara lain.

1. Merancang dan mengimplementasikan algoritma kriptografi AES-256 pada sistem ujian berbasis web untuk melindungi data ujian agar tetap aman selama proses pengiriman dan penyimpanan.
2. Melakukan pengujian keamanan data terenkripsi yang dikirim melalui jaringan menggunakan analisis paket dengan Wireshark serta pengujian fungsionalitas sistem menggunakan metode Black box.
3. Menganalisis tingkat hubungan antara data asli (*plaintext*) dan data terenkripsi (*ciphertext)* dengan perhitungan Korelasi Pearson sebagai salah satu indikator efektivitas enkripsi.

1.4 Manfaat Penelitian

Manfaat dari penelitian ini diklasifikasikan ke dalam dua aspek, yakni aspek teoritis dan aspek praktis.

1.4.1 Manfaat Teoritis

1. Memberikan kontribusi terhadap pengembangan ilmu pengetahuan di bidang kriptografi, khususnya penerapan algoritma AES-256 dalam sistem informasi berbasis web.
2. Menambah referensi literatur terkait implementasi AES-256 dalam konteks keamanan data sistem ujian daring, termasuk analisis keamanan menggunakan Wireshark dan Korelasi Pearson.
3. Menjadi dasar bagi penelitian lanjutan yang ingin membandingkan efisiensi dan keamanan berbagai algoritma kriptografi pada sistem berbasis web.

1.4.2 Manfaat Praktis

1. Menyediakan solusi bagi pengembang sistem ujian berbasis web untuk meningkatkan keamanan data dengan menggunakan algoritma kriptografi AES-256 yang telah diuji secara fungsional dan keamanan jaringannya.

2. Mengurangi risiko kebocoran dan manipulasi data pada proses ujian berbasis web melalui penerapan enkripsi di sisi *frontend* yang telah dibuktikan efektivitasnya dengan pengujian langsung.
3. Memberikan kontribusi bagi institusi pendidikan dalam membangun sistem ujian berbasis web yang lebih aman, efisien, dan terpercaya.

1.5 Ruang Lingkup Penelitian

Ruang lingkup penelitian ini diperlukan untuk memperjelas ruang lingkup serta fokus penelitian agar tidak melebar dari tujuan utama. Adapun batasan penelitian ini adalah sebagai berikut:

1. Penelitian difokuskan pada pengembangan dan pengujian sistem ujian berbasis *website* yang menerapkan algoritma kriptografi AES-256 untuk enkripsi dan dekripsi data penting seperti data user, soal, jawaban, dan hasil ujian.
2. Pengujian keamanan sistem dilakukan melalui pemantauan paket data menggunakan Wireshark untuk memastikan bahwa data telah terenkripsi dengan benar selama transmisi, pengujian fungsionalitas dilakukan menggunakan metode *Black box* guna mengevaluasi apakah seluruh fitur sistem berfungsi sesuai dengan spesifikasi, serta pengujian hubungan antara *plaintext* dan *ciphertext* menggunakan Korelasi Pearson untuk mengukur efektivitas enkripsi.
3. Data yang dienkripsi di sisi *frontend* mencakup informasi sensitif seperti data siswa, seluruh konten soal beserta pilihan jawabannya, serta hasil ujian yang diperoleh setiap peserta. Proses enkripsi dilakukan langsung di perangkat pengguna sebelum data dikirim ke server.
4. Data yang dienkripsi di sisi *backend* mencakup informasi penting terkait data guru dan data admin, yang dienkripsi di server untuk melindungi keamanan pada penyimpanan maupun pengelolaan data.
5. Data yang tidak dienkripsi meliputi informasi umum seperti data kelas dan daftar siswa di dalam kelas, karena data tersebut tidak mengandung informasi yang tergolong rahasia atau berdampak besar jika diakses oleh pihak luar.

6. Ujian disajikan dalam bentuk pilihan ganda (maksimal enam opsi, satu jawaban benar) dengan dukungan fitur timer, navigasi soal, penanda (flag), dan unggah gambar.
7. Sistem ujian yang dikembangkan pada penelitian ini masih dijalankan dalam lingkungan local server (belum diimplementasikan secara luas pada jaringan publik/online), sehingga pengujian difokuskan pada aspek fungsionalitas dan keamanan dalam skala terbatas.

1.6 Struktur Organisasi Skripsi

Sistematika penulisan skripsi pada peneltian ini mengacu pada Pedoman Penulisan Karya Ilmiah UPI Tahun 2024. Skripsi disusun dalam 5 bab, setiap bab memiliki fokus penulisan sebagai berikut:

1. BAB I PENDAHULUAN

   Bab ini menguraikan latar belakang penelitian, rumusan masalah, tujuan penelitian, manfaat penelitian, dan struktur organisasi skripsi. Pendahuluan memberikan dasar pemahaman mengenai topik penelitian serta menjelaskan urgensi penerapan algoritma AES-256 dalam meningkatkan keamanan data pada sistem ujian berbasis web.
2. BAB II TINJAUAN PUSTAKA

   Bab ini menguraikan latar belakang penelitian, rumusan masalah, tujuan penelitian, manfaat penelitian, dan struktur organisasi skripsi. Pendahuluan memberikan dasar pemahaman mengenai topik penelitian serta menjelaskan urgensi penerapan algoritma AES-256 dalam meningkatkan keamanan data pada sistem ujian berbasis web.
3. BAB III METODE PENELITIAN

   Bab ini menjelaskan pendekatan dan prosedur penelitian yang digunakan untuk mencapai tujuan penelitian. Di dalamnya mencakup desain penelitian, perangkat keras dan perangkat lunak yang digunakan, tahapan implementasi sistem ujian berbasis web dengan enkripsi AES-256 di sisi *frontend*, metode pengujian (*Black box*, Wireshark, Korelasi Pearson), serta teknik analisis data.
4. BAB IV HASIL DAN PEMBAHASAN

Bab ini menyajikan hasil perancangan dan implementasi sistem yang telah dibangun, pengujian fungsional menggunakan metode *Black box*, pengujian keamanan menggunakan Wireshark, serta analisis hubungan *plaintext* dan *ciphertext* menggunakan Korelasi Pearson. Temuan dianalisis untuk menjawab rumusan masalah dan dievaluasi berdasarkan tujuan penelitian.

5. BAB V SIMPULAN DAN SARAN

   Bab ini merangkum temuan utama penelitian, memberikan implikasi dari hasil yang diperoleh terhadap pengembangan sistem ujian berbasis web yang aman, serta menawarkan saran untuk penelitian atau pengembangan lebih lanjut. Simpulan di sini menjadi jawaban dari tujuan penelitian yang telah dirumuskan pada bab pertama.

Struktur ini dirancang agar skripsi tersusun secara sistematis, memberikan alur yang jelas, dan mempermudah pembaca untuk memahami setiap tahap penelitian.