BAB I
PENDAHULUAN

1.1 Latar Belakang

Dalam era digital saat ini, internet telah menjadi salah satu media komunikasi dan transaksi yang sangat populer. Dalam lingkungan perkuliahan, banyak universitas dan perguruan tinggi yang menggunakan *website* untuk memudahkan mahasiswa dalam mengakses informasi, seperti jadwal kuliah, nilai, dan lain sebagainya.

Maka dari itu, diperlukan tindakan preventif untuk meningkatkan keamanan data yang tersimpan pada *website*, salah satunya dengan menerapkan teknologi kriptografi. *Advanced Encryption Standard (*AES*)* merupakan salah satu teknik kriptografi yang dapat digunakan untuk meningkatkan keamanan URL. Dengan menerapkan AES pada URL, maka informasi yang dikirim melalui URL akan terenkripsi dan sulit untuk dibaca.

Beberapa penelitian terdahulu yang menjadi acuan penelitian ini antara lain penelitian yang dilakukan oleh Dede Rusman[1] pada tahun 2021 yang berjudul "Implementasi Enkripsi Keamanan URL (*Uniform Resource Locator*) Menggunakan Algoritma AES" menghasilkan kesimpulan URL masih dalam bentuk plainteks dan tidak menjadi *cipher*teks, sistem sudah aman dari serangan SQL *Injection*, sedangkan untuk kecepatan hasil percobaan dari 100 pengguna di dapat 16.1/detik dengan waktu terima rata-rata 200.84 kb/detik dan waktu kirim rata-rata 3.11 kb/detik.

Penelitian serupa juga pernah dilakukan oleh Ridwan Andriyanto, dkk.[2] pada tahun 2020 yang berjudul "Penerapan Kriptografi AES *Class* Untuk Pengamanan URL *Website* Dari Serangan SQL Injection" menghasilkan kesimpulan Algoritma AES dapat mengenkripsi dan mendekripsi data URL sebuah *website* dengan panjang kunci yang bervariasi, yaitu 128 bit, 192 bit, dan 256 bit, sehingga dapat menyamarkan informasi yang terdapat pada URL. Enkripsi URL

menghasilkan keluaran berupa URL yang tidak menampilkan variabel asli melainkan *cipher*teks hasil enkripsi.

Selain itu, penelitian yang dilakukan oleh Aghistina Kartikadewi, dkk.[3] pada tahun 2021 yang berjudul "Implementasi Kriptografi dengan Algoritma *Advanced Encryption Standard* (AES) 128 Bit dan Steganografi menggunakan Metode *End of File* (EOF) Berbasis Java Desktop pada Dinas Pendidikan Kabupaten Tangerang" menghasilkan kesimpulan tindakan pencurian, penyalahgunaan dan manipulasi data tidak dapat terjadi karena isi file dokumen sudah teracak, dengan menggunakan kunci yang berbeda saat enkripsi dan dekripsi maka keamanan data rahasia semakin terjaga dan aman. Proses dekripsi dengan kunci yang asli akan mengembalikan *file* menjadi *file* semula tanpa mengalami perubahan sedikitpun. Waktu yang digunakan untuk melakukan proses enkripsi dan dekripsi berbanding lurus dengan ukuran file yang diproses (semakin kecil ukuran *file* yang diproses, semakin cepat proses enkripsi dan dekripsi dilakukan, semakin besar ukuran file yang diproses, semakin lama proses enkripsi dan dekripsi dilakukan).

Penelitian Aprizaldi., dkk.[4] pada tahun 2023 yang berjudul "Aplikasi Keamanan Data Berbasis Web Menggunakan Algoritma AES 128 Untuk Enkripsi Dan Dekripsi Data" menghasilkan kesimpulan dengan adanya sistem keamanan dalam penguncian data dan file dapat menghindari terjadinya penipuan dalam pembocoran data proses dan produksi. Selain itu, mengenkripsi file dan menyimpannya ke dalam *database* dalam suatu program dapat membantu melindungi program dari pengguna yang tidak bertanggung jawab.

Penelitian Yusuf Jordan El Anwar, dkk.[5] pada tahun 2022 yang berjudul "Penerapan Metode Kriptografi AES Untuk Mengamankan File Dokumen" menghasilkan kesimpulan sistem pengamanan dokumen elektronik berbasis web dapat mengenkripsi dan mendekripsi dokumen menggunakan metode AES.

Oleh karena itu, penelitian ini bertujuan untuk menerapkan AES pada URL untuk meningkatkan keamanan *website* mahasiswa Atma Luhur. Penelitian ini diharapkan dapat memberikan solusi yang tepat dalam meningkatkan keamanan data akademik terkait mahasiswa pada *website* tersebut. Selain itu, penerapan AES pada URL juga dapat memberikan manfaat lainnya, seperti meningkatkan privasi

data akademik mahasiswa dan mencegah akses yang tidak sah ke informasi yang terdapat pada *website*.

1.2 Rumusan Masalah

Rumusan masalah pada penelitian ini adalah "Bagaimana cara menerapkan algoritma AES untuk keamanan URL yang digunakan pada *website* Mahasiswa Atma Luhur?"

1.3 Batasan Masalah

Batasan masalah yang akan dibahas meliputi aspek-aspek berikut:

1. Fokus penelitian pada penerapan algoritma *Advanced Encryption Standard (*AES*)* sebagai enkripsi URL *website* mahasiswa Atma Luhur.
2. Studi kasus *website* mahasiswa Atma Luhur dengan *domain* utama https://mahasiswa.atmaluhur.ac.id sebagai objek penelitian.

1.4 Tujuan dan Manfaat Penelitian

Tujuan dari penelitian ini adalah menerapkan algoritma AES untuk keamanan URL yang digunakan pada *website* Mahasiswa Atma Luhur. Setelah tujuan penelitian ini tercapai, diharapkan dapat memberikan manfaat sebagai berikut:

1. Meningkatkan kerahasiaan file yang diakses pada suatu halaman *website*.
2. Menyamarkan informasi yang dikirimkan pada URL *website*.

1.5 Sistematika Penulisan

Sistematika penulisan pada penelitian ini akan disusun sebagai berikut:

BAB I PENDAHULUAN

Pada bab pendahuluan, terdapat latar belakang masalah, rumusan masalah, batasan masalah, tujuan dan manfaat penelitian, serta sistematika penulisan.

BAB II LANDASAN TEORI

Pada bab ini, disampaikan teori-teori yang berkaitan dengan topik penelitian, seperti model *iterative*, metode pengembangan berorientasi obyek, alat bantu pemodelan sistem dengan UML, teori dasar URL, keamanan data, kriptografi, AES, dan penelitian terdahulu.

BAB III METODOLOGI PENELITIAN

Bab ini menjelaskan tentang metodologi penelitian yang digunakan, seperti model *iterative*, metode pengembangan berorientasi obyek, dan alat bantu pemodelan sistem dengan UML, serta algoritma AES.

BAB IV PEMBAHASAN

Pada bab ini, disampaikan pembahasan terkait masalah dari sistem yang berjalan, solusi yang diusulkan, penerapan algoritma AES ke URL website mahasiswa Atma Luhur, dan pengujian fungsionalitas sistem.

BAB V PENUTUP

Pada bab ini disampaikan kesimpulan dari penelitian dan saran yang dapat diberikan untuk penelitian lebih lanjut.