BAB I
PENDAHULUAN

1.1 Latar Belakang

Dalam era digital saat ini, keamanan data menjadi isu yang sangat krusial, terutama dalam konteks informasi penduduk yang bersifat sensitif. Data pribadi, seperti Nomor Induk Kependudukan (NIK), alamat, dan informasi keluarga, rentan terhadap pencurian atau penyalahgunaan jika tidak dilindungi dengan baik. Perkembangan digitalisasi data penduduk telah mengalami kemajuan pesat dalam beberapa tahun terakhir, terutama dengan diterapkannya berbagai sistem berbasis web untuk administrasi kependudukan. Pemerintah Indonesia, melalui Direktorat Jenderal Kependudukan dan Pencatatan Sipil (Dukcapil), telah mengembangkan Sistem Informasi Administrasi Kependudukan (SIAK) yang memungkinkan pengelolaan data penduduk secara terpusat dan online. Selain itu, layanan berbasis web seperti e-KTP Online, BPJS Kesehatan, Dapodik (Data Pokok Pendidikan), dan sistem e-*Government* lainnya telah semakin meningkatkan ketergantungan masyarakat terhadap sistem digital untuk keperluan administrasi dan pelayanan publik. Digitalisasi ini membawa banyak manfaat, termasuk efisiensi layanan dan kemudahan akses, tetapi juga meningkatkan risiko keamanan data yang harus diantisipasi.

Dalam konteks pendataan penduduk di tingkat kelurahan, penggunaan teknologi informasi yang berbasis web telah menjadi solusi yang semakin penting dalam meningkatkan efisiensi dan akurasi data kependudukan. Di banyak kelurahan, metode pengelolaan data yang masih manual sering kali menyebabkan masalah, seperti keterlambatan dalam pencatatan dan pendataan yang tidak akurat. Penelitian oleh (Arip Islahudin & Hadikurniawati, 2022) menunjukkan bahwa penggunaan metode konvensional dalam pelayanan data penduduk di Kelurahan Kalimas mengakibatkan waktu pencatatan yang lama dan kesalahan dalam pengelolaan informasi. Pemerintah Indonesia telah menegaskan pentingnya perlindungan data pribadi melalui Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, hal tersebut tercantum dalam Pasal 35 UU PDP yang

menyatakan bahwa “Pengendali Data Pribadi wajib melindungi dan memastikan keamanan Data Pribadi yang diprosesnya” hal ini termasuk penggunaan teknologi seperti enkripsi. Selain itu pasal 39 mengamanatkan “Pengendali Data Pribadi wajib mencegah Data Pribadi diakses secara tidak sah. Pencegahan dilakukan dengan menggunakan sistem keamanan terhadap data pribadi yang diproses dan atau memproses Data Pribadi menggunakan sistem elektronik secara andal, aman, dan bertanggung jawab” (Undang-undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi, 2022). Dalam konteks ini, penggunaan algoritma enkripsi seperti AES-128 dan Caesar Cipher menjadi solusi yang dapat meningkatkan perlindungan data pada sistem berbasis web.

Secara empiris, kasus kebocoran data di Indonesia semakin meningkat dalam beberapa tahun terakhir. Dikutip dari (BBC News Indonesia, 2023) Lembaga Riset Keamanan Siber (*Communication & Information System Security Research Center)* atau CISSReC menyebutkan terdapat beberapa kebocoran data di Indonesia seperti 1,3 triliun data pendaftaran Kartu SIM telepon, 36 juta data Kendaraan Bermotor, 279 juta data Badan Penyelenggara Jaminan Sosial (BPJS), dua juta data foto dari BPJS. Kemudian 34 juta data paspor Indonesia, 6,9 juta data visa, 186 juta data dari Komisi Pemilihan Umum (KPU), satu triliun data dari Kemendesa, 337 juta data dari Disdukcapil Kemendagri, dan yang terbaru adalah 6,8 juta data DPT Provinsi DKI Jakarta. Oleh karena itu, diperlukan sistem keamanan yang andal untuk menjaga integritas dan kerahasiaan data penduduk.

Dengan semakin meningkatnya ancaman keamanan siber, implementasi metode kriptografi yang kuat dalam proteksi data penduduk menjadi langkah penting untuk menjaga kepercayaan publik dan memastikan bahwa informasi pribadi tetap aman dari akses yang tidak sah. Kriptografi merupakan teknik mengubah data asli menjadi format yang tidak dapat dibaca. Beberapa algoritma kriptografi telah dikembangkan untuk meningkatkan keamanan data, di antaranya adalah *Advanced Encryption Standard* (AES) dan Caesar Cipher. AES-128 dikenal sebagai algoritma kriptografi yang kuat dengan kunci sepanjang 128 bit, yang banyak digunakan dalam berbagai aplikasi keamanan tingkat tinggi (Wicaksana & Mufti, 2024). Sementara itu, Caesar Cipher adalah salah satu bentuk kriptografi

klasik yang sederhana namun tetap memberikan tingkat perlindungan tambahan jika dikombinasikan dengan metode kriptografi lain (Ardiansyah dkk., 2023).

Penelitian sebelumnya telah menunjukkan efektivitas implementasi algoritma AES-128 dalam mengamankan data sensitif. Misalnya, studi oleh (Prameshwari & Sastra, 2018) yang mengimplementasikan AES-128 untuk enkripsi dan dekripsi file dokumen, menunjukkan bahwa algoritma ini memiliki tingkat keamanan yang tinggi dalam pertukaran informasi. Selain itu, kombinasi antara algoritma enkripsi modern dan klasik, seperti AES dan Caesar Cipher, telah diuji untuk meningkatkan keamanan data. (Nuraeni dkk., 2020) mengimplementasikan kombinasi Caesar Cipher dan AES untuk pengamanan data pajak bumi dan bangunan, menghasilkan *ciphertex*t yang lebih kuat dan sulit dipecahkan. Pada perbandingan antar varian AES, AES-128 memerlukan 10 putaran (rounds), sedangkan AES-256 memerlukan 14 putaran, sehingga AES-128 lebih efisien dari sisi waktu dan penggunaan sumber daya (Hakim, 2018). Penelitian lain oleh (Chandra dkk., 2019) juga menunjukkan bahwa AES-128 mampu mengenkripsi file dengan baik, meskipun membutuhkan waktu komputasi yang lebih lama untuk file berukuran besar. Sementara itu, Caesar Cipher dipilih meskipun sederhana karena nilai edukatifnya. Walaupun tidak cukup aman untuk aplikasi modern jika berdiri sendiri, Caesar Cipher memiliki peran penting dalam membantu memahami dasar-dasar kriptografi serta menambah kerumitan sederhana ketika digabungkan dengan algoritma modern.

Dalam penelitian ini, akan diimplementasikan kombinasi metode AES-128 dan Caesar Cipher dalam sebuah aplikasi berbasis web yang berfungsi untuk melindungi data penduduk. Pemilihan aplikasi berbasis web ini karena kemudahan akses, pembaruan efisien, dan keamanan data. Aplikasi web, yang dirancang untuk dapat diakses melalui berbagai perangkat yang terhubung ke internet, menghilangkan kebutuhan untuk instalasi spesifik pada masing-masing perangkat pengguna, yang berarti aksesibilitas ini sangat penting dalam konteks penggunaan luas di berbagai wilayah (Mikelsone dkk., 2021). Seiring dengan permintaan yang meningkat untuk solusi yang dapat diakses secara fleksibel, aplikasi berbasis web menawarkan kemudahan yang signifikan bagi pengguna untuk terlibat dengan

layanan tanpa batasan teknis. Dengan menggunakan pendekatan ini, diharapkan sistem mampu memberikan perlindungan ganda terhadap informasi sensitif, sehingga meningkatkan keamanan dan mengurangi risiko kebocoran data.

1.2 Rumusan Masalah

Berdasarkan paparan latar belakang sebelumnya, peneliti merumuskan beberapa rumusan masalah yaitu:

1. Bagaimana mengimplementasikan algoritma AES-128 dan Caesar Cipher untuk pengamanan data penduduk pada sistem berbasis web?
2. Bagaimana kinerja keamanan AES 128 dan Caesar Chiper pada sistem data penduduk berbasis web?

1.3 Tujuan Penelitian

Berdasarkan rumusan masalah yang telah disusun, penelitian ini bertujuan untuk:

1. Mengimplementasikan algoritma AES-128 dan Caesar Cipher dalam sistem berbasis web guna meningkatkan keamanan data penduduk.
2. Mengevaluasi kinerja keamanan data terenkripsi yang dihasilkan oleh algoritma AES-128 dan Caesar Cipher pada sistem data penduduk berbasis web melalui pengujian dengan Wireshark, serta analisis hubungan linear plaintext dan ciphertext menggunakan metode Korelasi Pearson.

1.4 Manfaat Penelitian

Penelitian ini diharapkan dapat memberikan manfaat baik secara teoritis maupun praktis, antara lain:

1.4.1 Manfaat Teoritis

1. Menambah wawasan dalam bidang kriptografi khususnya dalam penerapan AES-128 dan Caesar Cipher untuk perlindungan data penduduk.
2. Memberikan referensi bagi penelitian selanjutnya mengenai kombinasi algoritma enkripsi dalam keamanan data berbasis web.
3. Menyediakan studi kasus mengenai penerapan dua algoritma enkripsi dalam sistem keamanan data berbasis web.

1.4.2 Manfaat Praktis

1. Menghasilkan sistem berbasis web yang mampu melindungi data penduduk dari ancaman pencurian atau penyalahgunaan data.
2. Membantu pengembang perangkat lunak memahami cara mengintegrasikan AES-128 dan Caesar Cipher dalam proses enkripsi dan dekripsi data.
3. Memberikan solusi keamanan bagi organisasi atau instansi yang memerlukan proteksi data penduduk dalam sistem informasi mereka.
4. Meningkatkan kesadaran akan pentingnya keamanan data pribadi serta perlindungannya dalam database berbasis web.

1.5 Ruang Lingkup Penelitian

Penelitian ini ditetapkan dengan tujuan untuk mengarahkan fokus penelitian agar tetap terarah sehingga menghindari risiko meluasnya ruang lingkup penelitian. Berikut ruang lingkup penelitian ini:

1. Data yang dienkripsi terbatas pada data penduduk seperti nik, nama, alamat, tanggal lahir, jenis kelamin, agama, status perkawinan, dan pekerjaan. Data yang di enkripsi berupa teks bukan foto.
2. *Role* pengguna hanya *administrator.*
3. Hanya terdapat 5 surat (domisili, tidak mampu, usaha, kelakuan baik, belum menikah).
4. Algoritma enkripsi yang digunakan hanya aes-128 dan caesar cipher, tanpa membandingkan dengan algoritma enkripsi lainnya.
5. Implementasi sistem berbasis website, tidak mencakup aplikasi berbasis mobile.
6. Pengujian dilakukan menggunakan data uji (data *dummy*), bukan data asli dari instansi pemerintahan atau lembaga terkait.
7. Pengujian fungsional menggunakan *black box testing*.
8. Pengujian keamanan menggunakan wireshark dan korelasi *pearson*
9. Aplikasi web diimplementasikan dan dijalankan pada *area local host*

1.6 Struktur Organisasi Skripsi

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

Bab I berupa Pendahuluan yang berisi latar belakang penelitian, rumusan masalah, tujuan penelitian, manfaat penelitian, dan ruang lingkup penelitian.

Bab II berupa Tinjauan Pustaka yang berisi uraian teori dan penelitian terdahulu yang relevan sebagai dasar untuk mendukung penelitian. Bagian ini juga mencakup kerangka teori dan konsep yang menjadi landasan penelitian.

Bab III pada bab ini menjelaskan metode penelitian, Langkah-langkah, serta desain penelitian yang digunakan dalam proses pengembangan sistem.

Bab IV berisi uraian Hasil dan Pembahasan untuk menyajikan temuan atau hasil penelitian dalam bentuk teks, tabel, atau grafik, serta memberikan interpretasi dan pembahasan terhadap hasil tersebut. Pada bagian ini, hasil penelitian dikaitkan dengan teori atau penelitian terdahulu.

Bab V berupa Simpulan dan Saran yang menyajikan ringkasan dari hasil penelitian serta menjawab rumusan masalah. Bagian ini juga memberikan saran untuk penelitian selanjutnya atau implikasi praktis dari temuan penelitian.