BAB I
PENDAHULUAN

1.1 Latar Belakang

Indonesia saat ini sedang menerapkan konsep Society 5.0, yang menekankan pada aktivitas masyarakat yang terpusat pada teknologi informasi (Wijayanti dkk., 2022). Meskipun teknologi canggih ini membantu banyak aspek kehidupan masyarakat, seperti pekerjaan dan aktivitas sehari-hari, namun juga membawa risiko yang seringkali tidak disadari, seperti masalah keamanan dan privasi data pengguna. Salah satu cara untuk mengatasi masalah ini adalah dengan menggunakan metode kriptografi, yang merupakan salah satu metode penting dalam menjaga keamanan data digital.

Kriptografi telah menjadi bagian penting dalam sejarah teknologi informasi sejak awal. Di masa lalu, kriptografi digunakan untuk mengamankan pesan militer dan diplomatis. Namun, dengan perkembangan teknologi, kriptografi menjadi semakin penting dalam melindungi data elektronik yang disimpan dan dikirim melalui jaringan. Dengan munculnya internet, pertukaran informasi menjadi lebih mudah, tetapi juga meningkatkan risiko keamanan (Tantimin dan Anugerah, 2022).

Keamanan data adalah aspek yang krusial, terutama ketika berbicara tentang akun *online*, seperti *e-commerce*, dompet digital, dan perbankan *online*. Untuk melindungi informasi yang disimpan di dalamnya, diperlukan lapisan keamanan yang kuat. Salah satu langkah penting adalah melindungi akun dengan menggunakan *password* yang dapat diandalkan. Namun, penggunaan *password* statis dapat memungkinkan risiko pencurian oleh pihak yang tidak bertanggung jawab (Azhar dkk., 2020). Inilah mengapa penerapan ilmu kriptografi menjadi sangat penting untuk melindungi akun dari serangan *hacker*. Selain itu, dengan menerapkan algoritma kriptografi pengelola *database* atau administrator pun bahkan tidak akan mengetahui *password* pengguna. Dengan mengintegrasikan kriptografi ke dalam sistem keamanan,

dapat memastikan bahwa data sensitif tetap aman dan terlindungi, mengurangi risiko pencurian informasi yang berharga. Menurut Mustika (2020), secara umum *website* yang menyimpan informasi dan data penting menerapkan algoritma kriptografi untuk meningkatkan keamanannya. Implementasi algoritma kriptografi terbukti membuat *website* lebih aman, yang pada akhirnya dapat meningkatkan kepercayaan pengguna serta menarik lebih banyak pelanggan. Salah satu *e-commerce* yang menerapkan kriptografi, yaitu Lazada menerapkan AES-128 pada penyimpanan data yang sensitif. Selain itu, Bank BCA Indonesia juga menerapkan teknologi kriptografi melalui penggunaan protokol SSL/TLS guna mengamankan komunikasi antara pengguna dan server, sehingga data login maupun transaksi tetap terlindungi dari pihak yang tidak berwenang.

Pada penelitian ini dipilih algoritma *Advance Encryption Standard* 256 (AES-256) karena algoritma ini telah menunjukkan efektivitas yang tinggi dalam melindungi data dari serangan *brute force* (Gunawan, 2023). Selain itu, AES-256 menjadi algoritma yang lebih baru karena menggantikan algoritma sebelumnya, yaitu *Data Encryption Standard* (DES) yang sudah diketahui kelemahannya (Munir, 2019). Menurut Asriyanik (2017), salah satu potensi kelemahan AES-256 adalah bentuk serangan *Extended Sparse Linearization* (b) yaitu sebuah serangan terhadap cipher blok dan serangan ini tidak dapat dibuktikan tidak efektif terhadap AES-256. Selain itu, kelemahan AES-256 adalah apabila berhasilnya dipecahkan persamaan matematis yang mendasarinya secara otomatis seluruh sistem di dalam AES-256 dapat ditembus. Dengan demikian, akan lebih baik jika AES-256 dikombinasikan dengan algoritma lain. Pada penelitian sebelumnya, yaitu yang dilakukan Nurjaman dan Turnip (2024), penggabungan AES-256 dan SHA-512 dapat diandalkan karena menjamin integritas dan kerahasiaan dokumen secara efektif. Sedangkan pada penelitian ini akan mengombinasikan AES-256 dengan algoritma *Secure Hash Algorithm* 256 (SHA-256) dan menambahkan metode *Cipher Block Chain* (CBC) ke dalam AES-256.

SHA-256 adalah fungsi *hash* kriptografis, yang berarti algoritma ini mengambil input (pesan atau data) dan menghasilkan nilai *hash* unik yang bersifat tetap panjangnya. SHA-256 mengharutsilkan nilai *hash* yang terdiri dari 256 bit atau 64 karakter heksadesimal. Panjang ini memberikan tingkat keamanan yang lebih tinggi dibandingkan dengan varian *hash* dengan panjang yang lebih pendek (Munir, 2019). Dengan demikian, dengan menggunakan SHA-256 saat pesan dengan sepanjang apapun ketika dilakukan algoritma kriptografi akan memiliki hasil yang tetap, yaitu 64 karakter dan nantinya akan lebih memudahkan enkripsi pada algoritma AES-CBC-256. Menurut Fredianto dkk. (2019), fungsi *hash* bersifat satu arah yang artinya setelah suatu dokumen, teks, ataupun data dilakukan algoritma SHA-256, maka data tersebut tidak bisa dikembalikan atau dilihat lagi data aslinya. Sifat pada fungsi *hash* inilah yang akan diterapkan sehingga administrator *database* tidak mampu untuk melihat *password* pengguna. Selain itu, kelebihan algoritma ini adalah belum ditemukan kolisinya (belum dapat diretas atau dua input berbeda menghasilkan output *hash* yang sama) dan terbukti aman hingga sampai saat ini (Munir, 2019). Menurut Manankova dkk (2022), SHA-256 bisa saja tidak efektif apabila input yang diberikan tidak kompleks dan pendek. Penyerangan ini dapat dilakukan dengan cara *Brute Force*. Algoritma *Brute Force* melakukan serangan dengan menebak kombinasi kunci secara sistematis dan acak untuk membajak serta menemukan kode secara langsung (Gunawan, 2023). Dengan demikian akan lebih baik lagi jika SHA-256 digabungkan dengan algoritma lain apabila inputnya tidak kompleks.

Pada tahun 2001, *U.S. National Institute of Standards and Technology* (NIST) memasukkan AES (termasuk varian AES-256) untuk digunakan dalam berbagai mode operasi block cipher, salah satunya adalah *Cipher Block Chaining* (CBC). Pada mode CBC, setiap blok *plaintext* dioperasikan dengan *ciphertext* dari blok sebelumnya menggunakan operasi XOR sebelum dienkripsi. Dengan cara ini, setiap blok *ciphertext* sangat bergantung pada blok *plaintext* yang telah diproses sebelumnya, sehingga meningkatkan difusi (Perubahan kecil dalam input akan menyebabkan perubahan

besar) dan keamanan enkripsi. Untuk membuat setiap pesan adalah unik, maka sebuah *initialization vector* (nilai awal dalam mode operasi CBC) wajib digunakan pada blok pertama (Warkim dan Lewelusa, 2015).

Berdasarkan latar belakang yang telah dijelaskan, penulis tertarik untuk mengkaji autentikasi dan integrasi data dengan memanfaatkan algoritma SHA-256 dan AES- CBC 256, yang diimplementasikan pada program berbasis *website* (aplikasi yang dijalankan melalui *website* browser menggunakan jaringan internet**)**. Selain itu, sistem ini juga didukung oleh manajemen *Firestore database*, yaitu layanan *database* dari platform *google Firebase* yang memungkinkan penyimpanan dan sinkronisasi data secara *real-time* serta menyediakan fleksibilitas dan keamanan tinggi. Dengan demikian, penulis mengambil judul penelitian "Implementasi Keamanan Data Berbasis *Website* Menggunakan Kombinasi Algoritma SHA-256 dan AES-CBC-256 dengan Manajemen *Database Firestore* pada akun *Website*".

Pemilihan kombinasi algoritma ini didasarkan pada kenyataan bahwa password pengguna biasanya relatif pendek, umumnya minimal 8 karakter sesuai standar keamanan yang umum diterapkan. Sementara itu, AES-CBC-256 memproses data dalam blok dan membutuhkan minimal 2 blok (32 karakter). Jika hanya ada 1 blok, proses berantai tidak berjalan penuh karena blok kedua membutuhkan hasil enkripsi dari blok pertama. Oleh karena itu, password dengan panjang bervariasi perlu diubah terlebih dahulu agar sesuai dengan ukuran 32 karakter. Disinilah fungsi *hash* seperti SHA-256 digunakan. SHA-256 memiliki sifat menghasilkan *output* dengan panjang tetap, yaitu 32 byte (256 bit), terlepas dari panjang input yang dimasukkan. Hal ini memungkinkan *password* pengguna yang relatif pendek tetap dapat digunakan dalam algoritma enkripsi AES-CBC-256.

Penelitian ini memiliki kebaruan dibandingkan penelitian Nurjaman dan Turnip (2024), yang menggunakan SHA untuk menyimpan *hash* kunci di *database* tanpa keterkaitan langsung dengan proses enkripsi AES-256. Dalam penelitian ini, kombinasi algoritma SHA-256 dan AES-256-CBC diterapkan untuk mengamankan akun *website*,

di mana *password* pengguna di-*hash* dengan SHA-256 untuk menghasilkan *message digest* yang berfungsi sebagai kunci sekaligus *plaintext* untuk enkripsi AES-256-CBC, dengan hasil enkripsi disimpan di *Firestore database*. Untuk pemulihan *password*, SHA-256 hanya digunakan sebagai kunci enkripsi AES-256-CBC. Kebaruan penelitian ini meliputi penggunaan mode CBC pada AES-256, yang meningkatkan keamanan melalui difusi antar-blok (Warkim dan Lewelusa, 2015), serta fokus pada autentikasi *website*, berbeda dari penelitian Nurjaman yang mengamankan dokumen PDF. Selain itu, penelitian ini menerapkan keamanan berlapis dengan mengintegrasikan SHA-256 dan AES-256-CBC dalam satu rangkaian enkripsi, dan memanfaatkan *Firestore database* yang sangat aman, dibandingkan penyimpanan online biasa seperti pada penelitian sebelumnya. Namun, penelitian ini belum menyertakan pengujian keamanan spesifik seperti *avalanche effect*, yang dilakukan Nurjaman dan Turnip.

Kombinasi algoritma ini bertujuan untuk meningkatkan keamanan data pengguna dan mengantisipasi potensi kelemahan pada AES-256, seperti serangan terhadap *cipherblock* pada AES-256. Dengan meng-*hash password* dan kunci menggunakan SHA-256 sebelum enkripsi, data yang diproses AES-256-CBC menjadi *hash* satu arah yang tidak dapat dikembalikan ke bentuk asli. Hal ini memastikan bahwa meskipun penyerang berhasil mendekripsi *ciphertext*, informasi asli tetap terlindungi, sehingga menambah lapisan keamanan yang signifikan pada sistem.

1.2 Rumusan Masalah

Berdasarkan latar belakang, maka permasalahan yang dirumuskan adalah sebagai berikut:

1. Bagaimana proses implementasi pengamanan *password* menggunakan algoritma SHA-256 dan AES-CBC-256 pada sistem *login* aplikasi *website* ?
2. Bagaimana konstruksi program aplikasi pengamanan *password* dalam sistem *login website* menggunakan AES-CBC-256 dengan kunci *hash*-ing SHA-256 ?

1.3 Tujuan Penelitian

Berdasarkan rumusan masalah, terdapat beberapa tujuan dari penelitian ini yaitu sebagai berikut.

1. Merancang sistem dan skema aplikasi *website* yang menerapkan SHA-256 dan AES-CBC-256 pada *password* pengguna.
2. Mengonstruksi *prototype* program aplikasi *website* yang mengimplementasikan SHA-256 dan AES-CBC-256.

1.4 Manfaat Penelitian

1. Manfaat Teoritis

   Penelitian ini diharapkan dapat mengimplementasikan sistem keamanan akun pada *website*, khususnya melalui penggunaan kombinasi algoritma SHA-256 dan AES-CBC-256, dan untuk memberikan pemahaman mengenai algoritma kriptografi SHA-256 dan AES-CBC-256.

2. Manfaat Praktis

   Penelitian ini secara praktis akan memberikan alternatif pengamanan *website* dengan sistem keamanan akun yang menggunakan kombinasi algoritma SHA-256 dan AES-CBC-256. Dengan pendekatan ini, akun pengguna menjadi sangat sulit diretas, bahkan pengelola atau pembuat *website* tidak akan memiliki akses langsung ke akun pengguna