BAB I PENDAHULUAN

1.1 Latar Belakang

Semakin meningkatnya teknologi yang semakin canggih membawa sebuah perubahan yang cukup signifikan. Perubahan tersebut dikenal dengan istilah Revolusi Industri 4.0 yang merupakan sebuah kemajuan teknologi yang sering digunakan oleh banyak orang. Revolusi industri 4.0 adalah sebuah data yang digerakkan dengan adanya campur tangan komputer menggunakan metode *machine learning* atau *AI* (Alimuddin et al., 2023). Menurut Klaus Schawab revolusi Industri 4.0 memiliki tantangan yang harus dihadapi salah satunya seperti keamanan *cyber* dan privasi data.

Maka dari itu, dengan semakin pesatnya informasi teknologi maka perlunya untuk mengamankan data atau *file*. Keamanan data atau *file* merupakan salah satu langkah yang mudah untuk melindungi sebuah informasi bersifat penting yang berasal dari akses tidak sah. Keamanan *file* ini sangat diperlukan pada era Revolusi Industri 4.0, karena maraknya serangan *cyber* dan peretasan komputer yang bisa mengganggu keberlangsungan suatu industri. Menurut Mulyana (2016, dalam Soesanto, 2023), keamanan *file* merupakan salah satu aksi pencegahan dari sebuah penganggu pengguna *file* atau pengguna yang memakai jaringan yang tidak berkewajiban memiliki akses (Soesanto et al., 2023). Dengan semakin pesatnya dunia teknologi ini membuat keamanan *file* menjadi sangat penting karena untuk melindungi privasi dan informasi dari pihak yang tidak memiliki akses.

Keamanan *file* adalah serangkaian metode atau teknik yang untuk melindungi *file* dari akses yang tidak sah, seperti pencurian atau kerusakan. Tujuannya untuk menjaga informasi dalam *file* tetap rahasia, aman, dan hanya dapat di akses oleh pihak yang berwenang. Oleh karena itu, upaya untuk memastikan agar *file* terjaga dengan menggunakan metode ChaCha20 dan *Advanced Encryption Standard* (*AES*). ChaCha20 merupakan metode enkripsi yang cepat dan aman. ChaCha20 dipopulerkan oleh Daniel J. Bernstein sebagai varian dari algoritma. Algoritma ChaCha20 sangat populer dalam pengimplementasi enkripsi dikarenakan percampuran antara kecepatan dan keamanannya yang dapat diunggulkan. Chaca20 mempunyai desain yang hampir sama dengan Salsa20, pada algoritma ChaCha20

menggunakan kunci 256-bit yang mempunyai 8 putaran (Kebande, 2023). Sedangkan *AES* (*Advanced Encryption Standard)* adalah sebuah algoritma yang melakukan transformasi terhadap blok data yang menggunakan kunci enkripsi yang sama. *AES* bekerja pada sistem yang melibatkan operasi matematika dengan level tingkat sulit (Saripa, 2023). Proses kerja enkripsi dasar *AES* adalah *subbytes* (menggunakan tabel S-Box untuk menggabungkan *byte* pada blok matriks), *shift row* (digunakan untuk menggeser baris matriks), *MixColumns* (melakukan pergeseran dari kanan ke kiri), dan *AddRoundkey* (blok di XOR kan dengan kunci yang diperluas) (Aryanto et al., 2023). Pada proses dekripsi *AES* terdapat tahap-tahapan kebalikan dari proses enkripsi. Dengan memakai kunci yang sama untuk dekripsi, blok data yang telah terenkripsi dapat dipulihkan kembali ke bentuk awalnya. algoritma *AES* adalah jenis *block chipper* yang memiliki panjang kunci 128 bit, 192 bit dan 256 bit (Surbakti & Purwanto, 2024).

Algoritma Chacha20 dan *AES* merupakan suatu enkripsi yang dapat di digunakan dalam menjaga keamanan *file*. Pada algoritma *AES* terdapat kelebihan salah satunya adalah sifat karakteristiknya yang di mana selalu ada bidang khusus untuk bilangan prima, memicu kekuatan *AES* (Surbakti & Purwanto, 2024). *AES* juga memiliki sebuah kelemahan, salah satunya yaitu algoritma kriptografi yang menggunakan kunci simetris dalam proses pengiriman dan penerimanya data. Namun, penggunaan kunci simetris ini memiliki risiko lebih tinggi terhadap kebocoran, terutama seiring waktu (Hidayatulloh et al., 2023). Pada algoritma ChaCha20 terdapat keunggulan, yaitu menggunakan teknik kriptografi *ARX* (*addition, rotation*, dan XOR) yang memberikan performa lebih cepat, kompleksitas lebih rendah, dan mampu menghilangkan serangan waktu (Alyas & Abdullah, 2021a).

Meskipun algoritma *AES* dan Chacha20 telah efektif untuk menjaga peningkatan keamanan *file* dan implementasinya yang cukup rumit sehingga membuat orang yang tidak memiliki akses tidak dapat mengakses *file* tersebut. Hal ini tidak dapat dipungkiri bahwa semakin pesatnya dunia teknologi membuat banyak orang berbondong-bondong menciptakan pembaruan yang lebih efektif. Metode *double encrypt* ini menawarkan kombinasi yang mampu mengurangi kelemahan dari setiap algoritma jika digunakan secara bersamaan, serta meningkatkan ketahanan terhadap berbagai jenis serangan kriptografi. *Double encrypt* merupakan teknik kriptografi

yang melibatkan proses enkripsi secara dua kali, yang di mana memiliki dua kunci yang berbeda untuk lebih meningkatkan keamanan. *Double encrypt* ini bertujuan untuk meningkatkan keamanan *file* lebih tinggi dibandingkan hanya 1 metode saja (Pangestu et al., 2022).

Pada penelitian terlebih dahulu yang berjudul "Implementasi Sistem Keamanan *File* Menggunakan Algoritma *AES* untuk Mengamankan *File* Pribadi" yang diteliti oleh Saripa di Universitas Negeri Makassar, menjelaskan tentang keamanan *file* dengan menggunakan metode algoritma *AES*, di mana hasil penelitian ini menunjukkan bahwa algoritma *AES* telah berhasil mengamankan *file,* yaitu dokumen Word, PDF, Excel, dan Power Point. *File* yang dienkripsi menjadi tidak terbaca oleh pihak yang tidak memiliki akses sehingga dapat menjaga kerahasiaan data dan *AES* mampu menjaga keamanan data dengan baik.

Dalam perbedaan penelitian terdahulu dan penelitian ini akan menggunakan *double encrypt* untuk keamanan *file* dan juga pada penelitian ini akan menggunakan *AES* dengan menambahkan metode ChaCha20 dan melakukan modifikasi pada bagian *AES*. Modifikasi menggunakan penambahan *AddRoundkey* sebelumnya bertujuan agar proses enkripsi akan lebih susah untuk dipecahkan. Dalam algoritma *AES*, langkah *AddRoundKey* merupakan komponen krusial yang menggabungkan data dengan kunci enkripsi menggunakan operasi XOR. Penelitian yang dilakukan oleh Luong pada tahun 2023 menunjukkan bahwa memodifikasi transformasi *AddRoundKey* dapat meningkatkan keamanan algoritma dengan menciptakan hubungan yang lebih kompleks antara *plaintext* dan *ciphertext* (Luong, 2023). Penelitian ini menyoroti pentingnya penyesuaian langkah *AddRoundKey* untuk meningkatkan ketahanan algoritma *AES* terhadap serangan kriptografi, seperti *differential cryptanalysis* dan linear *cryptanalysis*.

Dengan mendasarkan pada penelitian tersebut, modifikasi algoritma *AES* melalui penambahan langkah *AddRoundKey* sebelum *MixColumns* bertujuan untuk lebih memperkuat difusi data pada tahap awal enkripsi. Penambahan ini diharapkan dapat meningkatkan ke-*random*-an hasil enkripsi dan mengurangi kemungkinan eksploitasi pola oleh pihak yang tidak berwenang sehingga keamanan algoritma menjadi lebih optimal. Berdasarkan dari latar belakang di atas, penelitian ini

memiliki tujuan untuk meningkatkan keamanan *file* agar lebih sulit untuk diretas atau diakses pihak yang tidak berwenang. Oleh karena itu, penelitian ini dianggap penting karena maraknya kasus peretasan data oleh oknum yang tidak memiliki akses.

1.2 Rumusan Masalah

1. Bagaimana implementasi dari modifikasi *AES* dengan penambahan *AddRoundkey* sebelum *MixColumns* dalam meningkatkan keamanan *file*?
2. Bagaimana performa kombinasi antara *AES* modifikasi dan ChaCha20 dalam hal waktu enkripsi, waktu dekripsi , kecepatan enkripsi, dan kecepatan dekripsi?

1.3 Tujuan Penelitian

1. Mampu mengidentifikasi *AddRoundkey* yang akan digunakan dalam menjaga keamanan *file* dan mengimplementasi kemampuan Chacha20 dan *AES* yang telah dimodifikasi dalam proses menjaga keamanan *file*.
2. Mampu mengevaluasi performa algoritma ChaCha20 dan *AES* yang telah dimodifikasi berdasarkan waktu enkripsi, waktu dekripsi, kecepatan enkripsi, dan kecepatan dekripsi untuk menentukan efisiensi dan efektivitas kombinasi kedua algoritma tersebut dalam menjaga keamanan *file*.

1.4 Batasan dan Asumsi Penelitian

1. Penelitian ini berfokus pada jurnal atau artikel ilmiah dengan batasan tahun 2021-2024 yang membahas tentang:
   - Keamanan *file*
   - Algoritma ChaCha20
   - *Advanced Encryption Standard* (*AES*)
   - *Double encryption*
2. Penelitian dilakukan dengan pengujian pada *file* dengan ukuran dan format sebagai berikut :
   a. Format PDF dan Word dengan variasi ukuran *file* 100 KB-100MB.
   b. Format *file* teks (TXT) dengan ukuran maksimal 300 *byte*. Batasan ukuran *file* digunakan untuk memastikan pengujian dilakukan secara efektif tanpa mengurangi kinerja proses enkripsi dan dekripsi.

1.5 Manfaat Penelitian

1.5.1 Manfaat Akademis

1. Memberikan inovasi terbaru mengenai pelindungan keamanan *file* dengan menambahkan *AddRoundkey* pada algoritma *AES.*
2. Memudahkan peneliti lainnya dalam kinerja *AddRoundkey* pada algoritma *AES* yang berfungsi untuk keamanan *file***.**

1.5.2 Manfaat Ilmiah

1. Menjadi sumber acuan dan sumber referensi bagi peneliti lainnya yang akan meneliti topik ChaCha20 dan *AES* modifikasi, terutama dalam konteks keamanan data dan performa enkripsi.
2. Membuktikan hipotesis apakah *AES* yang dimodifikasi dengan tambahan *AddRoundkey* dapat meningkatkan performa keamanan dan efisiensi dibandingkan dengan *AES* standar, dan sekaligus menunjukkan kinerja kombinasi ChaCha20 dan *AES* dalam pengamanan *file* berbagai format dan ukuran.

1.6 Sistematika Penulisan

BAB 1 PENDAHULUAN

Menjelaskan latar belakang penelitian, rumusan masalah, tujuan penelitian, batasan penelitian, manfaat penelitian, serta sistematika penulisan secara umum.

BAB 2 LANDASAN TEORI

Membahas teori-teori yang relevan dengan penelitian, termasuk algoritma ChaCha20, *AES*, konsep kriptografi, Serta tinjauan terhadap penelitian terdahulu yang terkait.

BAB 3 METODOLOGI PENELITIAN

Menjelaskan metode yang digunakan dalam penelitian, termasuk algoritma yang diterapkan (modifikasi *AES* dan ChaCha20 dengan enkripsi ganda). Diuraikan juga alat dan bahan yang digunakan, serta tahapan penelitian yang meliputi implementasi algoritma, pengujian parameter kinerja (waktu dan kecepatan enkripsi, dekripsi, serta analisis entropi), dan evaluasi hasil pengujian pada berbagai jenis *file* (PDF, Word, TXT).

BAB 4 HASIL DAN PEMBAHASAN

Menyajikan proses implementasi algoritma AES standar, AES modifikasi, ChaCha20, dan *Double encrypt*, serta hasil pengujian dan analisis performa

berdasarkan berbagai parameter (entropi, waktu, kecepatan) terhadap *file* beragam jenis dan ukuran.

BAB 5 KESIMPULAN DAN SARAN

Merangkum temuan utama dari penelitian, serta memberikan saran untuk pengembangan dan perbaikan metode di masa mendatang.