BAB I

PENDAHULUAN

1.1 Latar Belakang

Keamanan data digunakan agar data yang kita miliki terlindungi dan terjamin, terdapat tiga perspektif pada keamanan data yaitu kerahasian data,keutuhan data, dan ketersediaan data [1]. Kerahasian data pada era teknologi informasi saat ini perlu diimplementasikan, karena terdapat data-data rahasia yang tidak semua orang boleh mengetahuinya seperti email dan password[2]. kerahasiaan informasi penting untuk mencegah pihak yang tidak berwenang dapat memahaminya. [3]. Kebocoran data dapat terjadi karena kurangnya pengamanan pada sistem informasi terutama pada data berupa text, seperti nama, email, password dan username. Data yang telah bocor jika jatuh pada orang yang salah beresiko identitas dan keamanan terancam, kerugian finansial dan kerusakan reputasi. Metode yang biasa digunakan untuk mengamankan data adalah kriptografi.

Ilmu kriptografi berisi tentang menjaga keamanan data informasi menggunakan teknik matematika untuk pesan rahasia yang hanya dipahami oleh pemilik dan penerima pesan [4]. Kriptografi bertujuan agar pesan rahasia dapat terjaga privasi, keaslian dan keutuhan dari pesan tersebut [5]. Kriptografi berdasarkan kunci terdapat dua yaitu kunci simetri dan kunci asimetri. Kriptografi dengan kunci simetri salah satu nya adalah kriptografi Cipher Block Chaining (CBC) . Kriptografi CBC menggunakan blok bit, pada proses enkripsi dan dekripsi. Proses enkripsi menggunakan blok bit yang digunakan pada proses pengamanan data text akan membagi data menjadi ukuran yang sama dengan blok-blok biner yang telah ditentukan, lalu dengan menggunakan XOR untuk nilai blok dan nilai blok sebelumnya [6]. Untuk proses dekripsi, menggunakan chipertext yang telah ada kemudian di XOR dan akan menghasilkan plaintext. Kelebihan dari algoritma Cipher Block Chaining dapat menyembunyikan pola dari plaintext, mampu mencegah serangan brute-force dan linear cryptanalysis karena Cipher Block Chaining mempunyai sifat non linear yang membuatnya sulit untuk di serangan. Cipher Block Chaining memiliki kelemahan pada proses dekripsi ciphertext sebelumnya akan berakibat pada deskripsi selanjutnya, jika terjadi kesalahan maka chipertext setelahnya akan mengalami kesalahan juga [7].

Kriptografi elgamal merupakan kriptografi asimetri, karena pada kriptografi ini terdapat dua kunci yang akan digunakan. Kunci public yang berisi tiga bilangan dan kunci privat yang berisi dua bilangan [8]. Algoritma kriptografi ElGamal, yang menggunakan kunci publik, bekerja seperti mesin sandi untuk melindungi pesan. Ia mengubah setiap blok teks biasa menjadi blok teks teracak, yang kemudian dapat dikembalikan menjadi teks biasa. Keamanan algoritma ini berasal dari kesulitan menghitung logaritma pada bilangan prima besar, membuatnya sulit untuk disusupi. Keunggulan ElGamal termasuk dalam cara dia membuat kunci serta proses enkripsi dan dekripsinya yang melibatkan komputasi besar, menghasilkan pesan terenkripsi dengan ukuran dua kali lipat dari pesan aslinya[9].

Untuk meningkatkan kekuatan algoritma maka pada penelitian ini akan dilakukan proses hybrid dua algoritma yaitu CBC dan elgamal. CBC digunakan karena mempunyai kelebihan proses block yang saling berkaitan antara satu block dengan lainnya, elgamal digunakan untuk meningkatkan kekuatan kunci pada CBC. Dengan demikian, data text dapat dijaga kerahasiaannya dan integrasinya terjaga secara baik.

1.2 Batasan Masalah

Dari konteks latar belakang yang telah dijelaskan sebelumnya, terdapat rumusan masalah yang dapat diidentifikasi, yaitu:

1. Pada pengujian yang akan dilakukan menggunakan data *text*.
2. Algoritma yang digunakan untuk proses *hybrid* kriptografi *Cipher Block Chaining* dan elgamal Pengujian proses *hybrid* menggunakan *white box*, *black box* dan kecepatan proses enkripsi dan dekripsi.
3. Bilangan acak pada algoritma elgamal ditentukan dengan nilai 2.
4. Initial vector (C0) pada proses CBC ditentukan dengan nilai 0 sebanyak kunci.

1.3 Rumusan Masalah

Dari konteks latar belakang dan batasan masalah yang telah dijelaskan sebelumnya, terdapat rumusan masalah yang dapat diidentifikasi, yaitu:

1. Bagaimana proses hybrid kriptografi *Cipher Block Chaining* dan elgamal untuk meningkatan algoritma.
2. Bagaimana pengujian algoritma hybrid dalam proses enkripsi dan dekripsi.

1.4 Tujuan Penelitian

Berdasarkan rumusan masalah yang telah diidentifikasi, berikut tujuan yang ingin dicapai dalam penelitian:

1 Implementasi proses hybrid kriptografi *Cipher Block Chaining* dan elgamal untuk meningkatkan algoritma tersebut.

2 Algoritma hybrid kriptografi mampu mengembalikan *ciphertext* dengan proses dekripsi ke *plaintext* semula.

3 Menghasilkan alur hybrid yang sesuai dengan algoritma yang digunakan.

1.5 Manfaat Penelitian

Berdasarkan tujuan dari penelitian yang sudah dijabarkan, berikut manfaat yang akan dicapai dalam penelitian :

1. Dengan algoritma hybrid maka kekuatan algortimanya meningkat
2. Meningkatkan keamanan data dengan menggunakan algoritma hybrid.
3. Menghasilkan alur algoritma baru.