BAB 1
PENDAHULUAN

1.1 Latar Belakang

Seiring perkembangan zaman perkembangan teknologi informasi akan terus berkembang semakin pesat. Perkembangan teknologi informasi yang sangat pesat ini telah membantu banyak manusia dalam melakukan kegiatan aktivitas sehari-hari mereka. Selain banyak memberikan dampak positif yang membantu aktivitas manusia, perkembangan teknologi juga memberikan dampak buruk juga. Dengan perkembangan teknologi informasi semakin pesat maka persebaran informasi akan semakin cepat dan mudah dapat diakses dan digunakan oleh banyak kalangan pengguna teknologi. Semakin banyak pengguna teknologi maka semakin banyak data tersebar. Saat ini penggunaan teknologi sudah memiliki banyak jenis *platform* yaitu *platform personal computer* (PC) dan *mobile smartphone*. Penggunaan teknologi tersebut memberikan perkembangan teknologi informasi yang sangat pesat, salah satunya adalah *mobile smartphone*. Perkembangan teknologi informasi tersebut membuat semakin banyak data informasi tersebar di internet seperti *E-commerce* yang saat ini sangat popular. Pada masa pandemi *covid-19* ini masyarakat memilih untuk tidak keluar rumah untuk berbelanja dan memilih belanja secara *online* di *E-commerce*. Dikarenakan perkembangan teknologi tersebut semakin banyak pengguna *E-commerce* pada masa pandemi ini maka persebaran data semakin luas. Persebaran data informasi penting ini merupakan incaran bagi pihak yang tidak bertanggung jawab pada masa pandemi ini. Berdasarkan artikel berita (Trio Hamdani 2020, hlm 1) pada tahun 2020 lebih tepatnya setelah pandemi sudah banyak *E-commerce* yang mengalami kebocoran data yaitu Tokopedia dan juga Bukalapak Data yang bocor pada *E-Commerce* tersebut antara lain adalah data pengguna aplikasi *E-commerce* baik pada *platform personal computer*(PC) dan *mobile smartphone*. Berdasarkan artikel berita (Arif Rafman 2020, hlm. 1) data yang telah bocor dan berhasil dicuri yaitu data berasal

dari *database E-commerce* tersebut yaitu seperti *username, password,* dan data sekunder lain seperti nama, tempat tanggal lahir, alamat, dan nomor telepon. Beberapa data seperti *password* seharusnya sudah memiliki sistem keamanan data informasi yaitu dengan enkripsi dimana pada *E-commerce* Tokopedia telah menerapkan keamanan data pada *password* dengan *hash* dan perlindungan 2FA. Namun bagaimana dengan keamanan data pada data sekundernya ? Data sekunder memiliki nilai yang sangat penting dan harus dilindungi. Beberapa kasus yang diakibatkan bocornya data sekunder adalah *phising* masal. Mungkin pembaca dan penulis telah merasakan dampak bocornya data sekunder dan tidak sadar bahwa data sekundernya telah bocor dan dimanfaatkan seperti dijual. Dampak tersebut yaitu bocornya data sekunder kita yaitu nomor telepon dimana kita sering mendapatkan pesan singkat pada perangkat *mobile smartphone* seperti iklan promosi, dan pesan singkat penipuan *phising*. Data-data sekunder tersebut merupakan data yang memiliki tipe data teks. Maka dari itu penulis ingin menerapkan algoritma kriptografi untuk mengamankan data sekunder tersebut.

Untuk mengamankan data sekunder maka pengamanan data dapat digunakan penerapan algoritma kriptografi. Algoritma kriptografi merupakan algoritma yang berfungsi untuk mengamankan data dengan dua proses yakni enkripsi dan dekripsi. Proses tersebut mengubah data asli plainteks menjadi cipherteks yang memiliki keamanan data. Algoritma kriptografi dipilih yakni algoritma *Blowfish* dan algoritma *Elgamal* Dari kedua algoritma kriptografi tersebut akan diterapkan algoritma kriptografi ganda yaitu pertama data plainteks akan dienkripsi oleh algoritma kriptografi *Blowfish* kemudian hasil cipherteks akan menjadi plainteks lagi dan dienkripsi lagi dengan algoritma *Elgamal* dan menghasilkan data cipherteks.

Algoritma kriptografi yang dipilih yaitu dengan pertimbangan kedua algoritma harus memiliki jenis algoritma kriptografi yang berbeda yaitu simetris dan asimetris. Dengan perbedaan jenis algoritma kriptografi tersebut diharapkan dapat memberikan keuntungan dan keunggulan dari masing-masing jenis algoritma tersebut. Algoritma simetris merupakan algoritma kriptografi yang memiliki proses

enkripsi dan dekripsi cukup cepat, namun algoritma jenis ini memiliki kelemahan yaitu memerlukan kunci yang perlu didistribusikan. Maka dari itu algoritma kedua yang diperlukan yaitu algoritma dengan jenis asimetris dimana algoritma kriptografi asimetris menerapkan kunci yang berbeda pada setiap tahap enkripsi dan dekripsi pesan, kunci tersebut diketahui dengan nama kunci publik dan untuk proses dekripsi menggunakan kunci yang bersifat rahasia yaitu kunci privat.

Algoritma kriptografi yang digunakan yaitu algoritma *Blowfish*. Algoritma kriptografi *Blowfish* dipilih karena algoritma kriptografi ini berjenis simeteris dan algoritma *Blowfish* cepat dalam melakukan proses enkripsi dan dekripsi dan memiliki kompatibilitas dan efisiensi dalam penerapannya lalu algoritma *Blowfish* tidak ada hak patennya dan bersifat *open source* (Suhandinata 2019, hlm. 5).

Algoritma kriptografi asimeteris yang digunakan yaitu algoritma *Elgamal.* Algoritma ini memiliki keamanan yang cukup tinggi karena keamanan algoritma ini ada pada sulitnya menghitung logaritma diskrit tetapi dengan kekurangan pada komputasi yang besar dan hasilnya akan lebih besar dari plainteksnya (Himawan dkk. 2016, hlm. 696). Algoritma *Elgamal* merupakan probabilistik yaitu plainteks tunggal dapat dienkripsi menjadi beberapa cipherteks yang mungkin sehingga dapat menghasilkan peningkatan ukuran hingga dua kali lipat pada cipherteks. Maka dari itu pada penelitian ini penulis berusaha menggabungkan kecepatan dan efisiensi dari *Blowfish* dengan algoritma *Elgamal* ini.

Pada penelitian ini, kedua algoritma kriptografi tersebut akan dikombinasikan untuk pengamanan data dua algoritma. Pada penelitian sebelumnya (Sadli dan Painem, 2018 hlm. 366-372) untuk mengamankan data pada *database* digunakan algoritma *Blowfish* dan *AES* untuk mengamankan *database*. Dari solusi penelitian sejenis tersebut saya menggunakan algoritma *Blowfish* juga tetapi untuk algoritma keduanya yaitu algoritma *Elgamal.* Untuk enkripsi tahap awal menggunakan algoritma kriptografi simetris yang lebih cepat yaitu *Blowfish* dan kemudian dilanjutkan dengan algoritma asimetris *Elgamal* yang memberikan keamanan yang lebih baik. Dengan dilakukannya penelitian ini akan menguji

keberhasilan pengamanan dengan algoritma kriptografi ganda pada data sekunder yang berupa teks dan diharapkan dapat bermanfaat dan berhasil digunakan untuk memenuhi aspek keamanan dan kerahasiaan data sekunder teks dan apakah hasilnya bisa diterapkan pada *database*.

1.2 Rumusan Masalah

Dari latar belakang yang dipaparkan di atas, maka dapat dirancang rumusan masalah yang dibahas yakni :

1. Apakah proses enkripsi data sekunder dengan algoritma kriptografi simeteris *Blowfish* dan algoritma asimetris *Elgamal* dapat berhasil mengamankan data ?
2. Apakah proses dekripsi data sekunder dengan algoritma kriptografi simetris *Blowfish* dan algoritma asimetris *Elgamal* dapat berhasil mengembalikan data menjadi plainteks ?
3. Bagaimana efisiensi waktu dan sumber daya komputer pada penerapan algoritma *Blowfish* dan *Elgamal* dalam mengamankan data sekunder *database* ?

1.3 Batasan Masalah

Sedangkan agar pembahasan permasalahan tetap berada pada dalam batasan yang diinginkan dan tidak menyimpang terlalu jauh, maka pembahasan terbatas pada beberapa pembahasan sebagai berikut:

1. Algoritma yang akan digunakan adalah algoritma kriptografi simetris *Blowfish* dan algoritma asimetris *Elgamal*.
2. Data yang akan digunakan untuk proses enkrip dan dekrip adalah data sekunder seperti alamat, nomor telepon, dan nama.
3. Parameter hasil penelitian adalah keberhasilan proses enkripsi dan dekripsi, waktu proses , penggunaan sumber daya komputer pada proses enkripsi dan dekripsi dan apakah cipherteks bisa dimasukan ke dalam *database*.
4. Program dibuat dalam bentuk aplikasi berbasis *website* yang melakukan simulasi fungsional proses enkripsi dan dekripsi data sekunder.

1.4 Tujuan Penelitian

Tujuan dilakukan penelitian ini adalah untuk menguji penerapan algoritma kriptografi *Blowfish* dan *Elgamal* pada data sekunder dan apakah hasil cipherteksnya bisa diterapkan pada *database* dan apakah dengan efisiensi penerapan ini dapat meningkatkan keamanan informasi data pada *database*.

1.5 Manfaat Penelitian

Dari hasil penelitian ini diharapkan dapat memberikan manfaat yaitu antara lain :

1. Untuk penulis sendiri dapat menambah pengetahuan dan pengalaman dalam penelitian algoritma kriptografi.
2. Untuk pihak *E-commerce* yaitu dapat mengamankan data sekunder pengguna aplikasinya dengan lebih baik lagi dari ancaman serangan kebocoran data.
3. Untuk para pengguna aplikasi *E-commerce* dapat lebih merasa aman dengan datanya yang telah diberikan saat mendaftar pada aplikasi *E-commerce*.

1.6 Luaran yang diharapkan

Hasil luaran yang diharapkan dari penelitian ini yaitu untuk mengetahui apakah penerapan algoritma kriptografi algoritma *Blowfish* dan algoritma *Elgamal* berhasil diterapkan dan apakah bisa meningkatkan keamanan informasi data sekunder dan penerapannya bisa efisien pada perangkat lunak berbasis *website*.

1.7 Sistematika Penulisan

Sistematika penulisan pada penelitian ini yaitu tersusun dan terdiri dari lima bab dan daftar pustaka. Dengan sistematika penulisan ini diharapkan dapat mempermudah pembaca untuk mengetahui alur dan isi dari penelitian ini. Sistematika penulisan sebagai berikut:

BAB 1 PENDAHULUAN

Pada bab ini menjelaskan latar belakang masalah, batasan masalah, rumusan masalah , tujuan penelitian, manfaat dari penelitian, luaran yang diharapkan.

BAB 2 LANDASAN TEORI

Pada Bab ini menjelaskan teori – teori yang diperlukan untuk membantu penelitian – penelitian, lalu bab ini juga dijelaskan mengenai penelitian terkait yang digunakan pada penelitian ini.

BAB 3 METODE PENELITIAN

Pada bab ini menjelaskan mengenai kerangka pikir dalam melakukan penelitian dan juga tahap perencanaan dalam membangun perangkat lunak , dan jadwal dalam penelitian.

BAB 4 HASIL DAN PEMBAHASAN

Pada bab ini akan menjelaskan mengenai Perancangan yang sudah direncanakan pada metodologi penelitian dan penerapannya serta hasil dan pembahasan dari penelitian. Kemudian hasil analisis hasil dari penelitian.

BAB 5 KESIMPULAN DAN SARAN

Pada bab ini menjelaskan hasil kesimpulan yang didapatkan dari penelitian yang telah dilakukan dan saran untuk penelitian selanjutnya.

DAFTAR PUSTAKA