BAB I
PENDAHULUAN

1.1 Latar Belakang

Kemajuan dalam bidang teknologi informasi memberikan banyak keuntungan bagi kehidupan manusia, tetapi keuntungan yang ditawarkan juga menimbulkan kejahatan seperti pencurian data. Sehingga perkembangan ilmu untuk mengamankan data semakin ditingkatkan agar pengguna teknologi selalu merasa aman. Aktivitas penyimpanan data dan pertukaran informasi secata digital mempunyai resiko dan tentunya harus disertai dengan keamanan informasi. Hal ini jelas terlihat apabila dalam aktivitas tersebut terdapat informasi penting yang sifatnya privasi dapat diakses oleh orang lain yang tidak berkepentingan. Maka diperlukan pengamanan untuk melakukan pencegahan atas sampainya informasi ke tangan yang tidak berhak. Agama Islam telah mengatur dengan jelas tentang pentingnya menjaga privasi. Berikut salah satu firman *Allah Subhanahu Wa Ta'ala* tentang ayat *Al-Qur'an* yang berkaitan dengan pentingnya menjaga privasi:

يَا أَيُّهَا الَّذِينَ آمَنُوا لَا تَدْخُلُوا بُيُوتًا غَيْرَ بُيُوتِكُمْ حَتَّى تَسْتَأْنِسُوا وَتُسَلِّمُوا عَلَى أَهْلِهَا ذَلِكُمْ خَيْرٌ لَّكُمْ لَعَلَّكُمْ تَذَكَّرُونَ

Artinya : *"Wahai orang-orang yang beriman! Janganlah kamu memasuki rumah yang bukan rumahmu sebelum meminta izin dan memberi salam kepada penghuninya. Yang demikian itu lebih baik bagimu, agar kamu selalu ingat."*
(QS. An-Nur : 27)

Privasi adalah hal-hal yang berkaitan dengan hak milik pribadi yang memiliki bentuk berupa dokumen, foto, video, pesan, lokasi, ataupun data-data penting lain yang dimiliki seseorang (Soediro, 2018). Demi menjaga privasi, lebih baik untuk selalu minta izin untuk melihat, membuka, atau menggunakan seluruh hal yang berkaitan dengan privasi. yang sebagaimana dalam *hadist* Abu Daud nomor 1485 :

عن محمد بن كعب القرظي حدثني عبد الله :أن رسول الله صلى الله عليه و سلم قال ”لا تستروا الجدر من نظر في كتاب أخيه بغير إذنه فإنما ينظر في النار سلوا الله [عزوجل] ببطون أكفكم ولا تسألوه بظهورها فإذا فرغتم فامسحوا بها وجوهكم “

Artinya : *“Dari Muhammad bin Ka’ab al Qurazhi, Abdullah bercerita kepadaku bahwa Rasulullah shallallahu ‘alaihi wa sallam bersabda, “Janganlah kalian menutupi tembok. Siapa saja yang melihat buku kawannya tanpa seizinnya maka sebenarnya dia hanyalah memandang api neraka. Berdoalah meminta kepada Allah dengan menggunakan bagian dalam telapak tangan kalian dan janganlah kalian menggunakan bagian luar telapak tangan. Jika kalian selesai berdoa maka usapkanlah tangan kalian ke wajah” (HR Abu Daud no 1485).*

Berbagai cara dilakukan untuk menjaga keamanan data seperti menyembunyikan data dengan teknik steganografi atau dengan cara menyandikan data menjadi suatu kode-kode yang tidak dimengerti, sehingga apabila dicuri atau disadap oleh orang lain akan kesulitan untuk mengetahui dan memahami informasi yang sebenarnya. Proses penyandian yang dilakukan adalah dengan menggunakan kriptografi. Kriptografi melingkupi proses transformasi informasi menjadi suatu bentuk yang tidak dapat dipahami, sehingga orang-orang yang tidak berhak tidak mungkin mengerti. Proses transformasi tersebut terdiri dari enkripsi dan dekripsi. Enkripsi adalah sebuah proses penyandian yang mengubah sebuah kode pesan yang mudah dimengerti (*plaintext*) menjadi sebuah kode pesan yang tidak bisa dimengerti (*ciphertext*). Dekripsi adalah kebalikan dari enkripsi yaitu proses penyandian yang mengubah sebuah kode pesan yang tidak bisa dimengerti (*ciphertext*) menjadi kode pesan yang mudah dimengerti (*plaintext*).

Meningkatkan keamanan kriptosistem merupakan tantangan yang menarik banyak pihak peneliti untuk mengusulkan dan mengembangkan kriptosistem baru

untuk mencapai tujuan kriptografi. Selain menerapkan algoritma kriptografi yang baru, maka cara yang dapat dilakukan adalah dengan memodifikasi suatu algoritma kriptografi, namun hal ini bukanlah suatu pekerjaan yang mudah. Oleh karena itu mengkombinasikan dua algoritma kedalam satu proses merupakan cara lain untuk meningkatkan algoritma kriptografi yang sudah ada. Proses penyandian yang dilakukan secara ganda bertujuan untuk menghasilkan teks yang benar-benar acak serta tidak memperlihatkan pola-pola keterhubungannya dengan teks asli, sehingga dapat meningkatkan kerahasiaan hasil enkripsi serta mempersulit pihak-pihak yang tidak berwenang yang berusaha untuk memecahkan dan mengetahui makna asli dari teks yang bersifat rahasia.

Terdapat banyak algoritma kriptografi yang sudah ada dengan kelebihan dan kekurangannya. Pada penelitan ini akan mengimplementasikan kombinasi algoritma *Beaufort Cipher* dan algoritma RSA (*Rivest Shamir Adleman*) untuk pengamanan *file* teks. Alasan menggunakan algoritma RSA berdasarkan penelitian terdahulu yang dilakukan oleh (Kurniawan, 2017) menjelaskan bahwa sampai saat ini algoritma RSA sangat sulit untuk dipecahkan dan akan membutuhkan waktu yang sangat lama. Sedangkan alasan menggunakan algoritma *Beaufort Cipher* berdasarkan penelitian terdahulu yang dilakukan oleh (Fadlan et al., 2019) menjelaskan bahwa kelebihan dari algoritma *Beaufort Cipher* adalah jumlah kunci yang digunakan memiliki panjang yang sama dengan jumlah karakter pesan asli (*plaintext*). Hal inilah yang dapat membuat pesan hasil enkripsi menjadi sulit untuk diketahui oleh pihak lain, karena tiap-tiap karakter *plaintext* akan memiliki pasangan kunci yang berbeda dengan karakter *plaintext* lainnya.

Berdasarkan permasalahan yang telah telah diuraikan serta penjelasan dari hasil penelitian terdahulu, maka pembaruan yang dilakukan dalam penelitian ini adalah terletak pada konsep dan algoritma yang digunakan. Jika pada penelitian yang dilakukan oleh (Kurniawan, 2017) hanya menggunakan satu algoritma kriptografi yaitu RSA, maka pada penelitian ini akan menggabungkan dua algoritma. Jika pada penelitian yang dilakukan oleh (Irawan et al., 2020) dengan menggabungkan dua algoritma kriptografi, namun hanya menggunakan algoritma kriptografi kunci simetris yaitu *Beaufort Cipher* dan Transposisi Kolom, maka

pada penelitian ini akan menggabungkan algoritma kriptografi kunci simetris dan kunci asimetris.

Berdasarkan uraian yang dikemukakan diatas, maka penulis mencoba mengangkat topik tugas akhir dengan judul penelitian "Implementasi Kombinasi Algoritma *Beaufort Cipher* dan Algoritma RSA dalam Skema Super Enkripsi untuk Pengamanan *File* Teks".

1.2 Rumusan Masalah

Berdasarkan latar belakang diatas, maka secara umum permasalahan yang akan dibahas dalam penelitian ini adalah sebagai berikut:

1. Bagaimana proses enkripsi dan dekripsi pesan teks menggunakan skema super enkripsi.
2. Bagaimana mengkombinasikan algoritma *Beaufort Cipher* dan algoritma RSA dalam skema super enkripsi untuk pengamanan *file* teks.
3. Bagaimana merancang aplikasi dalam mengamankan *file* teks dengan mengkombinasikan algoritma *Beaufort Cipher* dan algoritma RSA.

1.3 Batasan Masalah

Dalam melaksanakan penelitian ini, peneliti membatasi ruang masalah yang akan diteliti. Batasan-batasan masalah yang dipergunakan yaitu:

1. Penelitian ini hanya fokus untuk melakukan pengamanan isi *file* teks dalam format **.txt* dengan maksimal *size* (ukuran) 169 KB (*kilo bytes*) serta hanya mengenkripsi berupa *string* dan tidak mengenkripsi komponen lain yang terdapat pada *file* teks seperti tabel, grafik maupun gambar.
2. Algoritma kriptografi yang dikombinasikan dalam skema super enkripsi yaitu algoritma *Beaufort Cipher* dan algoritma RSA, dengan menggabungkan dua jenis kunci yang berbeda yaitu kunci simetris dan kunci asimetris.
3. Bilangan prima *p* dan *q* untuk membangkitkan kunci publik dan kunci privat algoritma RSA hanya menggunakan maksimal tiga digit angka. Hal ini dilakukan untuk mempermudah dalam proses perhitungan enkripsi/dekripsi serta mempermudah dalam pengimplementasiannya.

4. Proses enkripsi/dekripsi algoritma *Beaufort Cipher* menggunakan penyandian karakter A-Z dan karakter a-z yang terdapat dalam tabel ASCII dengan *modulo* 26 dan hanya menggunakan kunci dengan karakter *alphabet*.
5. Implementasi dari penelitian ini berbasis *web* dengan menggunakan bahasa pemrograman *php*.

1.4 Tujuan Penelitian

Berdasarkan rumusan masalah, maka tujuan dari penelitian ini adalah sebagai berikut:

1. Untuk mengetahui proses enkripsi dan dekripsi pesan teks menggunakan skema super enkripsi.
2. Untuk menerapkan kombinasi algoritma *Beaufort Cipher* dan algoritma RSA dalam skema super enkripsi untuk pengamanan *file* teks.
3. Untuk merancang sebuah aplikasi dalam mengamankan *file* teks dengan mengkombinasikan algoritma *Beaufort Cipher* dan algoritma RSA.

1.5 Manfaat Penelitian

Hasil dari penelitian ini diharapkan dapat memberikan manfaat bagi peneliti dan pembaca. Adapun manfaat yang diharapkan dari hasil penelitian ini adalah sebagai berikut:

1. Penelitian ini menghasilkan sebuah aplikasi berbasis *web* yang dapat memudahkan untuk menjaga kerahasiaan isi *file* teks dengan menerapkan skema super enkripsi menggunakan kombinasi algoritma simetris *Beaufort Cipher* dan algoritma asimetris RSA.
2. Menambah wawasan dan pengetahuan tentang proses pengamanan *file* teks dalam skema super enkripsi menggunakan kombinasi algoritma simetris *Beaufort Cipher* dan algoritma asimetris RSA.
3. Hasil penelitian ini juga diharapkan dapat menambah bahan referensi yang bermanfaat bagi Universitas Islam Negeri Sumatera Utara (UINSU), khusunya pada Program Studi Ilmu Komputer Fakultas Sains dan Teknologi (FST).