BAB I
PENDAHULUAN

1.1. Latar Belakang

Kemajuan teknologi internet sebagai media penghantar informasi telah diadopsi oleh hampir semua orang dewasa ini. Dimana informasi telah menjadi sesuatu yang sangat berharga. Bagi pelaku usaha, informasi bisa dianggap sebagai senjata untuk meningkatkan daya saing. Bagi militer, informasi bisa menjadi penentu kemenangan dalam perang. Bagi para wartawan, informasi menjadi sesuatu yang memiliki daya jual yang sangat mahal. Bagi perorangan, informasi menjadi sesuatu yang sangat pribadi. Bahkan informasi pun dapat menjadi alat untuk mempengaruhi perpolitikan bagi suatu negara [1].

Perkembangan penyembunyian *file* itu sendiri semakin hari semakin pesat. Dengan kata lain *file* yang disembunyikan tersebut sudah barang tentu banyak orang sudah mengetahui cara untuk membukanya hal ini membuat setiap orang yang akan menyembunyikan *file* merasa bahwa ini sudah tidak aman lagi. Sehingga apabila berbicara mengenai sebuah pengamanan pasti tidak akan jauh dari apa yang disebut kriptografi. Penyembunyian *file* tidaklah terjamin dan selalu ada resiko terbuka untuk umum, dalam artian semua isinya dapat dibaca oleh orang yang tidak berhak [2] . Begitu banyak kasus penyadapan terhadap suatu informasi telah membuat para peneliti berfikir keras untuk mengamankannya. Dengan kriptografi, informasi yang dianggap rahasia dapat disembunyikan dengan teknik penyandian, sehingga tidak dimengerti oleh orang lain, selain oleh pembuat dan penerimanya saja [1].

Untuk menjaga kerahasiaan suatu data salah satu nya adalah enkripsi (*encryption*). Enkripsi adalah suatu proses yang dilakukan untuk mengubah pesan asli menjadi *ciphertext*. Sedangkan suatu proses yang dilakukan untuk mengubah pesan asli tersembunyi menjadi pesan biasa (yang mudah dibaca) disebut deskripsi. Pesan biasa atau pesan asli disebut *plaintext* sedangkan pesan yang

telah diubah atau disandikan supaya tidak mudah dibaca disebut dengan *chipertext* [3].

Adapun beberapa metode penelitian terkait yang telah dilakukan sebelumnya untuk mengamankan data, diantara nya Hamzah (2011) menggunakan metode RSA dan *blowfish* untuk enkripsi dan dekripsi data. Maulida (2015) menggunakan metode *Affine Cipher* dan RSA. Pada penelitian kali ini penulis menggunakan metode RSA dan *Vigenere Cipher*.

Berdasarkan kunci yang digunakan, algoritma kriptografi dapat dibedakan atas dua jenis, yaitu algoritma kriptografi simetris dan asimetris. Algoritma kriptografi simetris atau disebut juga algoritma kriptografi konvensional adalah algoritma yang menggunakan kunci untuk proses enkripsi sama dengan kunci untuk proses dekripsi. Algoritma kriptografi Asimetris adalah algoritma yang menggunakan kunci yang berbeda untuk proses enkripsi dan dekripsinya. Algoritma ini disebut juga algoritma kunci umum *(public key algorithm)* karena kunci untuk enkripsi dibuat umum *(public key)* atau dapat diketahui oleh setiap orang, tapi kunci untuk dekripsi hanya diketahui oleh orang yang berwenang mengetahui data yang disandikan atau sering disebut kunci pribadi *(private key).* [4].

Metode RSA termasuk di jenis kriptografi asimetris. Metode kriptografi RSA yang ditemukan pada tahun 1976 oleh Peneliti MIT (*Massachussets Institute of Technology*) oleh Ron (R)ivest , Adi (S)hamir dan Leonard (A)dleman. Metode RSA menggunakan 2 kunci untuk melakukan proses persandian data yang dimana kunci pertama *(public key)* yang digunakan untuk melakukan persandian dan kunci kedua *(private key)* yang digunakan untuk menterjemahkan bahasa yang sudah disandikan menjadi bahasa yang dapat dibaca oleh manusia. Penelitian ini meneliti metode yang aman dalam menjaga keamanan pesan dari serangan *cryptonalyst.* [5].

Vigenere cipher termasuk di jenis kriptografi simetris. *Vigenere chiper* merupakan salah satu algoritma kriptografi klasik untuk menyandikan suatu *plaintext* dengan menggunakan teknik substitusi. *Vigenere cipher* pada dasarnya cukup rumit untuk dipecahkan. Meskipun begitu, *Vigenere cipher* tetap memiliki

kelemahan. Salah satunya adalah dapat diketahui panjang kuncinya. Hal ini disebabkan karena umumnya terdapat frasa yang berulang-ulang pada *ciphertext* yang dihasilkan [6]. Pada penelitian ini penulis menggunakan metode *Vigenere Cipher* dengan ukuran bilangan ASCII 0-255 agar lebih sulit dipecahkan.

Setiap metode kriptografi mempunyai kelebihan dan kelemahannya masing-masing baik dari segi kecepatan enkripsi dan dekripsi maupun dari segi keamanannya. Kelebihan kriptografi simetris adalah pada segi kecepatan untuk proses enkripsi dan dekripsi yang tinggi, namun memiliki kelemahan dalam segi pendistribusian kuncinya. Sedangkan kelebihan kriptografi asimetris adalah kemudahan dalam pertukaran kunci, namun lemah dalam segi kecepatannya. Untuk mengatasi kelemahan masing-masing algoritma kriptografi tersebut, maka dipadukan kedua sistem algoritma kriptografi tersebut. Perpaduan atau penggabungan sistem ini disebut kriptografi *hybrid* [7]. Oleh karena itu penulis menggabungkan dua metode yaitu RSA dan *Vigenere Cipher* agar dapat menutupi kelemahan pada masing-masing metode dan memperkuat keamanan agar dapat terhindar dari pihak-pihak yang tidak berhak mengakses data. Untuk itu kali ini penulis membahas tentang **"PENGAMANAN DOKUMEN MENGGUNAKAN KOMBINASI METODE *RSA (RIVEST SHAMIR ADLEMAN)* DAN *VIGENERE CHIPER"***

1.2. Rumusan Masalah

Keamanan dokumen merupakan suatu hal yang sangat penting bagi seseorang ataupun kelompok. Ada suatu data yang sifatnya pribadi dan rahasia sehingga tidak boleh diakses oleh sembarang orang. Untuk menghindari pembobolan dan pencurian dokumen, dibutuhkan suatu pengamanan terhadap dokumen agar suatu dokumen dapat tersimpan dengan aman dan tidak semua orang dapat mengakses dokumen tersebut kecuali orang-orang yang berhak.

1.3. Tujuan penelitian

Adapun tujuan dari penelitian ini ialah :

1. Untuk mengamankan data *file* menggunakan kombinasi metode RSA dan *vigenere cipher*.
2. Membuat aplikasi pengamanan dokumen yang bermanfaat untuk kepentingan kelompok atau individu.

1.4. Manfaat Penelitian

Adapun manfaat yang dapat diperoleh dari penelitian ini adalah :

1. Merahasiakan pesan agar dapat terjaga keamanan nya.
2. Menambah pengetahuan baru tentang kombinasi metode RSA dan *Vigenere Cipher* untuk mengamankan dokumen.
3. Penulis dapat mengetahui kelemahan dan kelebihan masing-masing metode dari RSA dan *Vigenere Chiper* untuk pengamanan data.
4. Menjadi referensi untuk penelitian selanjutnya.

1.5. Batasan masalah

Dalam tugas akhir ini batasan masalah yang dipergunakan ialah :

1. Format *file* yang digunakan pada uji coba ini ialah tipe dokumen *text* (doc,docx,xls,ppt,pdf).
2. Untuk memperkuat kunci dari *Vigenere cipher* penulis menggunakan bilangan ASCII.
3. Aplikasi digunakan di Program Studi Teknik Telekomunikasi Politeknik Negeri Sriwijaya.
4. Ukuran *file* maksimal 500KB
5. Aplikasi ini dapat digunakan oleh dosen, admin, mahasiswa.
6. Menggunakan bahasa pemrograman *PHP*.

1.6. Metodologi Penelitian

Penulis akan merancang dengan tahapan-tahapan metodologi penelitian sebagai berikut :

a. Studi Literatur

Studi literatur dilakukan dengan pengumpulan bahan referensi mengenai pengamanan data, dari buku-buku dan jurnal ilmiah yang dapat membantu memecahkan masalah dari penelitian, maupun informasi yang diakses melalui internet.

b. Metode Analisis

Pada tahap ini dilakukan analisa terhadap bahan referensi yang telah dikumpulkan untuk mendapatkan pemahaman tentang metode yang akan diterapkan yaitu algoritma *hybird* RSA dan *vigenere cipher.*

c. Metode Pengumpulan Data

Metode ini dilakukan beberapa macam data file yang berformat doc,docx,txt,ppt,pdf dan xls yang nanti nya akan di enkripsi.

d. Implementasi

Pada tahapan ini dilakukan implementasi algoritma RSA dan *vigenere cipher* untuk penyelesaian masalah pengamanan data file menggunakan data yang telah dikumpulkan sebelumnya.

e. Evaluasi dan Analisis Hasil

Pada tahap ini dilakukan evaluasi serta analisis terhadap hasil yang didapatkan melalui implementasi algoritma RSA dan *vigenere cipher* dalam penyelesaian masalah pengamanan data *file.*

f. Dokumentasi dan Pelaporan

Pada tahap ini dilakukan dokumentasi dan penyusunan laporan hasil evaluasi dan analisis serta implementasi algoritma RSA dan *vigenere cipher* dalam pengamanan data.

1.7. Sistematika Penulisan

Tugas akhir ini disusun dalam lima bab dengan sistematika penulisan sebagai berikut.

BAB I PENDAHULUAN

Bab pendahuluan ini berisi tentang hal-hal yang mendasari dilakukannya penelitian serta pengidentifikasian masalah penelitian. Bagian-bagian yang terdapat dalam bab pendahuluan ini meliputi latar belakang masalah, perumusan masalah, batasan masalah, tujuan penelitian, dan manfaat penelitian.

BAB II TINJAUAN PUSTAKA

Pada bab tinjauan pustaka menguraikan landasan teori, penelitian terdahulu, kerangka pikir dan hipotesis yang diperoleh dari acuan yang mendasari dalam melakukan kegiatan penelitian pada tugas akhir ini.

BAB III METODOLOGI PENELITIAN

Bab ini membahas analisis dan penerapan algoritma RSA dan *Vigenere Cipher* untuk melakukan pengamanan pada data. Pada bab ini dijabarkan proses yang dilakukan serta cara kerja algoritma yang digunakan.

BAB IV HASIL DAN PEMBAHASAN

Pada bab ini penulis akan memaparkan hasil dan pembahasan terhadap uji coba sistem algoritma yang telah dilakukan dalam meyelesaikan permasalahan pengamanan data.

BAB V KESIMPULAN DAN SARAN

Bab ini berisi tentang kesimpulan dari hasil penelitian serta saran-saran mengenai apa saja yang harus ditambahkan yang berkaitan untuk penelitian selanjutnya.