BAB I

PENDAHULUAN

I.1 Latar Belakang

Model pengamanan berkas adalah suatu model yang mengimplementasikan satu atau lebih algoritma keamanan, dalam hal ini kriptografi, untuk melindungi keabsahan, integritas, dan keamanan berkas. Sudah banyak penelitian yang mengusung model pengamanan berkas guna memenuhi kebutuhan akan perlindungan keamanan.

Terdapat sekelompok peneliti yang melakukan sebuah penelitian berjudul *Analisis Performa Kriptografi Hybrid Algoritma Blowfish dan Algoritma RSA*, penelitian ini menghasilkan suatu aplikasi yang menerapkan algoritma *Blowfish* dan RSA dalam mengamankan data. Dari penelitian ini didapat suatu model pengamana yang lebih aman karena gabungan kekuatan dari algoritma RSA dan algoritma *blowfish* untuk untuk menanggulangani kelemahan RSA dalam waktu pemrosesan. Namun, kecepatan algoritma gabungan dalam mengenkripsi dan mendekripsi data tidak lebih cepat dibanding algoritma pembentuknya, yaitu RSA atau *Blowfish*.

Lalu pada tahun 2018 terdapat suatu penelitian yang berjudul *Implementasi Algoritma Prediction by Partial Matching (PPM) Pada Kompresi File Teks Terenkripsi Elgamal*. Dari penelitian ini didapatkan kesimpulan berupa algoritma PPM baik digunakan untuk mengompresi *file* berbentuk teks, dengan hasil akhiran kompresi lebih kecil dibanding *file* awal dan algoritma *ElGamal* dapat membantu mengamankan informasi yang berada dalam *file* teks.

Selain dari dua penelitian tersebut, terdapat penelitian yang membandingkan beberapa algoritma kriptografi asimetris berdasarkan performanya. Dari membandingkan performa tiga algoritma asimetris paling terkenal yaitu RSA, ECC, dan *ElGamal*, RSA terbukti unggul dalam penyandian data, keamanan, serta lebih cepat dan valid.

Berdasarkan referensi penelitian yang telah peneliti temukan, peneliti mengusung untuk menggunakan kriptografi asimetris RSA, dimana RSA merupakan kriptografi asimetris yang paling aman dengan tingkat kesulitan pemecahan kunci yang tinggi. Lalu peneliti mengusung untuk menggunakan algoritma kompresi *Prediction by Partial Matching* atau PPM, dimana algoritma efektif untuk mengurangi ukuran berkas, sehingga dapat meningkatkan performa algoritma RSA.

Peneliti mengusung untuk menggunakan berkas *Curriculum Vitae* (CV) sebagai objek dari penelitian ini sebagaimana CV merupakan berkas yang berisi data diri pribadi yang bersifat privasi yang membutuhkan pengamanan, yang mana hal ini dibahas dalam Permenkominfo No. 20 tahun 2016 dimana tiap warga negara berhak atas perlindungan data pribadi dalam sistem elektronik.

Berdasarkan paparan yang sudah diuraikan, maka penulis akan mengusulkan penggunaan algoritma RSA dan algoritma kompresi PPM dalam melindungi berkas dan mengukur performanya dari segi keamanan, waktu pemrosesan, dan ukuran berkas yang dihasilkan. Sehingga penelitian ini akan mengangkat judul "Model Pengamanan Berkas Menggunakan Kriptografi Asimetris RSA dan Algoritma Kompresi PPM Pada File Curriculum Vitae (CV)".

I.2 Rumusan Masalah

Berdasarkan latar belakang yang telah penulis kemukakan, dapat disimpulkan rumusan masalah sebagai berikut :

a. Bagaimana hasil implementasi algoritma kompresi PPM dan kriptografi asimetris RSA terhadap *file* yang diamankan?
b. Apakah implementasi penerapan algoritma kompresi PPM dan kriptografi asimetris RSA dapat menghasilkan hasil akhir yang lebih baik dibandingkan dengan model pengamanan yang sudah ada pada penelitian terdahulu yang menggunakan kompresi LZW dan kriptografi *Twofish*?

I.3 Tujuan Penelitian

Berdasarkan latar belakang dan rumusan masalah yang telah dipaparkan, penilitian ini bertujuan :

1. Mengetahui hasil akhir penerapan kriptografi asimetris RSA dan algoritma kompresi PPM pada *file* yang dilindungi.
2. Mengukur hasil akhir penerapan kriptografi asimetris RSA dan algoritma kompresi PPM dibandingkan dengan model pengamanan berkas yang sudah ada di penelitian terdahulu yang menggunakan kompresi LZW dan kriptografi *Twofish*.

I.4 Manfaat Penelitian

Berdasarkan latar belakang dan tujuan yang telah dipaparkan, manfaat penelitian ini dapat dirumuskan sebagai berikut:

Penelitian ini dapat dijadikan pertimbangan dalam pembuatan model pengamanan berkas yang diharapkan memiliki hasil akhir lebih baik dari sisi keamanan, waktu, dan ukuran, serta dapat digunakan sebagai referensi bagi penelitian selanjutnya tentang model pengamanan berkas.

I.5 Ruang Lingkup Penelitian

Ruang lingkup dari penelitian ini penulis batasi agar penelitian mendapatkan hasil yang optimal, adapaun batasan-batasan tersebut antara lain:

a. Sistem yang dikembangkan berbasis web.
b. Kriptografi yang digunakan adalah kriptografi asimetris RSA dan algoritma kompresi PPM.
c. Penelitian menggunakan bahasa pemrograman *Node.Js* dan *framework React*.
d. *File* yang akan diamankan berformat .doc, .docx, .pdf, dan .txt.
e. Data *file* yang akan diamankan hanya berupa data *string*.
f. Data pribadi yang terdapat dalam berkas CV adalah sebagai berikut :
    i. Nama
    ii. Nomor telepon
    iii. Alamat email
    iv. Alamat rumah

v. Riwayat pendidikan

I.6 Luaran yang Diharapkan

Luaran yang diharapkan dalam penelitian ini adalah *website* yang dapat mengamankan berkas menggunakan algoritma RSA dan algoritma kompresi PPM dengan performa yang lebih unggul dari sisi keamanan, waktu pemrosesan, dan ukuran berkas yang dihasilkan.

I.7 Sistematika Penulisan

Berikut penulis paparkan sistematika penulisan agar pembaca mendapatkan gambaran yang jelas akan penelitian :

BAB I PENDAHULUAN

Bab ini memaparkan latar belakang, rumusan masalah, tujuan penelitian, manfaat penelitian, ruang lingkup penelitian, luaran yang diharapkan, dan sistematika penulisan penelitian ini.

BAB II TINJAUAN PUSTAKA

Bab ini memaparkan teori-teori berkaitan dengan topik penelitian yang akan digunakan sebagai dasar penelitian.

BAB III METODE PENELITIAN

Bab ini memaparkan rancangan sistem, kebutuhan sistem, pengumpulan data, eksperimen sistem terhadap data yang dikumpulkan, dan desain sistem.

BAB IV HASIL DAN PEMBAHASAN

Bab ini berisi hasil yang di dapat dari penggunaan sistem yang dibuat, analisis perancangan sistem berdasarkan hipotesa untuk menjawab rumusan masalah yang ada, serta analisis tingkat keamanan yang dihasilkan sistem.

BAB V PENUTUP

Bab ini membahas kesimpulan yang didapat dari penelitian ini serta saran yang dapat digunakan untuk meningkatkan penelitian selanjutnya.

DAFTAR PUSTAKA

RIWAYAT HIDUP

LAMPIRAN