BAB I

PENDAHULUAN

1.1. Latar Belakang Masalah

Perkembangan dunia digital sangatlah pesat sehingga tidak ada lagi batasan-batasan dalam berkomunikasi. Hal tersebut berujuan untuk dapat menyikapi persoalan-persoalan yang semakin kompetitif dalam telekominikasi. Mudahnya mendapatkan akses internet membuat seolah olah tidak ada batasan lagi dalam berkomunikasi. Dua orang dapat berkomunikasi secara *real time* walaupun mereka berbeda negara. Seseorang dapat dengan mudah membagikan apa yang sedang mereka lihat atau lakukan ke dalam media sosial. Segala bentuk gambar, suara atau video tersebut dapat dikirimkan melalui media transmisi dalam bentuk sebuah data.

Data merupakan subjek yang terdiri dari satu atau lebih karakter yang berisikan suatu informasi yang memiliki nilai kuantitatif atau kualitatif agar dapat dipindahkan atau di proses lebih lanjut. Dalam era digital seperti sekarang memungkinkan pertukaran data jarak jauh yang relatif cepat dan murah. Data dapat dikirimkan melalui media internet, gelombang radio maupun media yang lain. Data tersebut dapat berisikan informasi penting yang bersifat rahasia. Di sisi lain, perkembangan telekomunikasi data juga terdapat beberapa kekurangan. Ketika sebuah data dikirimkan data tersebut tidak bisa kita awasi ataupun kita olah kembali oleh karena itu seseorang yang dengan sengaja bisa menembus jalur pengiriman data tersebut kemudian mencuri atau melihat isi data tersebut[1].

Dibalik perkembangan internet saat ini ada bahaya yang mengancam dan kurang disadari oleh pengguna internet terutama untuk pemula. Yaitu kurangnya pemahaman mengenai keamanan data. Banyak pengguna yang lalai terhadap keamanan data terutama di internet. Banyaknya bahaya yang mengancam seperti malware,virus ataupun physing yang dapat dengan mudah mencuri data yang kita miliki. Oleh karena itu sebuah sistem kemanan data harus dibentuk. Sistem ini mencakup sistem deteksi, proteksi dan pengamanan. Oleh karena itu hal pertama yang perlu diperhatikan dalam pengiriman data adalah keamanan data tersebut.

Keamanan data perlu diperhatikan guna melindungi informasi digital dari akses tidak sah, korupsi, atau pencurian di seluruh siklus. Sistem Keamanan data mencakup setiap aspek keamanan informasi dari keamanan fisik perangkat keras dan perangkat penyimpanan hingga kontrol administratif dan akses, serta keamanan logis dari aplikasi perangkat lunak. Ini juga mencakup kebijakan dan prosedur organisasi. Salah satu bentuk data yang sering dikirimkan serta tidak jarang berisikan informasi pribadi adalah pesan. Pesan sangatlah rentan untuk dicuri ketika dalam proses

pengiriman. Untuk meminimalisir bocornya informasi pada data yang tercurierlu dilakukannya tindak pengamanan salah satunya adalah enkripsi[2].

Enkripsi merupakan cabang ilmu dari kriptografi. Algoritma kriptografi sendri mengalami banyak perubahan dari masa ke masa. Berawal dari kriptografi *paper and pencils* hingga kriptografi moderen seperti sekarang. Kriptografi pada awal mulanya didefinisikan sebagai ilmu tentang seni menulis atau menyelesaikan kode. Hal ini dikarenakan bahwa kriptografi di masa lampau lebih banyak digunakan untuk pertukaran pesan rahasia terutama di bidang militer. Kriptografi juga dianggap sebagai sebuah seni karena teknikpembuatannya sangat bergantung dari kreativitas pembuat dan bukan berdasarkan model perhitunganatau algoritma yang sudah diteliti secara formal. Pada kriptografi modern algoritma mulai melibatkan mesin dan komputer dalam membentuk sebuah algoritma serta bertujuan untuk mengamankan informasi sehingga dapat dikirim melaui jaringan komputer[3].

Di indonesia sendiri tindak kejahatan siber masih sangat tinggi. Jika dilihat dari sumber data pusat pengaduan kejahatan siber di situs patroli siber. Jumlah kejahatan siber dilaporkan sebanyak 6.388 kasus yang terdiri dari :

Jenis kejahatan siber	Jumlah kasus
Penyebaran konten provokatif	2584
Penipuan online	2147
Pornografi	536
Akes	352
Pencurian data/identitas	179
Manupilasi data	168
Peretasan sistem elektronik	165
Pemerasan	148
Perjudian	56
Intersepsi ilegal	27
Ganggguan sistem	13
Pengubahan tampilan situs	13

Tabel 1.1 informasi jumlah kejahatan siber di indonesia dari tahun 2019-2020

Dari data tersebut dapat dilihat jumlah kejahatan siber di indoneisa masih terbilang sangat banyak. Diperlukannya kesadaran pemerintah dan masyarakat akan betapa pentingnya keamanan data.

Dalam beberapa penelitian yang meneliti penggunaan algoritma RSA seperti pada penelitian yang dilakukan (Ginting, Isnanto dan Windasari, 2015) dengan penelitian implementasi algoritma kriptografi RSA pada e-mail pada penelitian ini menjelaskan tentang penggunaan algoritma RSA untuk melakukan enkripsi dan pengamanan pesan pada e-mail. Pada penelitian ini algoritma yang dipakai sudah baik

dalam melakukan enkripsi akan tetapi kunci yang dipakai terlalu kecil hingga membuat keamanannya berkurang.[16]

Dalam penelitian (Wulansari, Setyawan, & Susanto, 2016) berikutnya ada juga yang meneliti mengukur kecepatan enkripsi dan dekripsi algoritma RSA pada pengembangan sistem informasi text security , pada penelitian ini membandingkan kecepatan logika algoritma dalam melakukan enkripsi data teks. Pada penelitian ini hanya melihat kecepatan enkripsi akan tetapi tidak melihat kualitas data yang diperoleh dari enkripsi tersebut.

Dalam penelitian (Asmoro, 2015) juga meneliti pengamanan file citra atau gambar, meneliti dengan menggunakan algoritma RSA dan otp dalam penggabungannya. Dalam penelitian ini gambar di enkripsi dengan RSA lalu di enkripsi kembali dengan otp. Pada penelitian ini keamanan file sudah kuat, akan tetapi waktu yang dipakai cukup lama.

Dalam penelitian yang dilakukan (Jepriyanto, 2019) meneliti mengenai penggunaan enkripsi RSA dengan tambahan kompresi shanon fano dengan perbandingan rentang nilai p dan q dari 1 hingga 100000 memberikan hasil perbedaan ukuran kunci dapat memepengaruhi kecepatan dalam pembangkitan kunci.

Dan pada penelitian yang dilakukan oleh (Christine Lamorahan, Benny Pinontoan, 2013) meneliti tentang perbandingan kompresi Shannon – Fano dan kompresi Huffman, mendapatkan hasil kompresi Shannon – Fano lebih unggul dibandingkan kompresi Huffman ketika data yang berukuran besar. [19]

Berdasarkan dari itu dibuatlah penelitian tentang enkripsi dan dekripsi data teks dengan menggunakan algoritma RSA dan kompresi Shannon - Fano. Ingin menguji keamanan dan juga melihat ukuran data teks yang sudah di enkripsi dan juga dikompress dengan menggunakan algoritma RSA dan kompresi Shannon - Fano.

1.2. Rumusan Masalah

Rumusan masalah yang akan dibahas pada penelitian kali ini :

1. Bagimana Simulasi enkripsi pesan dengan kriptografi RSA.
2. Bagaimana enkripsi RSA dapat memberikan keamananbagi data yang dismpan.

1.3. Batasan Masalah

Pada penelitian proyek akhir ini hanya akan membahas enkripsi asimetri menggunakan metode rivest shamir aldeman dengan batasan rentang nilai p dan q dari 1 hingga 100000

1.4. Tujuan Penelitian

Tujuan penelitian proyek akhir kali ini :

1. mensimulasikan kriptografi RSA pada pesan dengan kunci seacak mungkin sehingga lebih susah untuk dipecahkan dengan menggunakan pasangan bilangan prima untuk masukan nilai p dan q dalam proses enkripsi.
2. Merancang sistem keamanan teks dengan menggunakan Algoritma RSA untuk melakukan proses enkripsi dan dekripsi.

1.5. Manfaat Penelitian

Manfaat yang diharapkan dari penelitian ini yaitu :

1) Adanya rasa aman yang dirasakan oleh pengirim pesan dan data yang berisi informasi tanpa takut informasi tersebut akan diketahui oleh orang lain.
2) Sebagai sarana pengembangan aplikasi pada bidang kemanan (security).