BAB I

PENDAHULUAN

I.1. Latar Belakang

Keamanan data adalah usaha untuk melindungi dan menjamin tiga aspek terpenting dalam dunia siber yaitu : Kerahasiaan data, Keutuhan data, Ketersediaan data. data menjamin pengguna siber terlindungi privasinya baik itu privasi yang berada pada komputer pribadi, piranti genggam maupun terlindungi data privasinya ketika melakukan berbagai aktifitas jelajah internet. Keutuhan data menjamin pengguna siber mendapatkan data yang utuh dan benar tanpa dimodifikasi dan dirubah pihak lain ditengah-tengah jalan. Ketersediaan data menjamin pengguna siber mendapatkan data pada saat yang diinginkannya tanpa ditutupi dan tanpa dicegah oleh pihak lain. *Cryptography* adalah ilmu yang membahas tentang ilmu penyandian, encryption adalah metode dalam *cryptography* dimana data yang bermacam-macam panjangnya/ukurannya diubah/diacak menjadi data yang panjangnya tetap. Enkripsi merupakan metode paling utama, efektif dan efisien dalam teknik keamanan data. Enkripsi memastikan proses komunikasi data dimana satu pihak mengirim data kepada pihak lain dapat dilakukan secara aman, akurat dan efisien. (Gunawan et al., n.d.)

Pada penelitian sebelumnya juga dilakukan Keamaanan data sensitif Menggunakan RSA dan ElGamal, algoritma Kriptografi dengan Fungsi Hash. Tujuan dari penelitian ini adalah untuk dapat melakukan autentikasi data bersama dengan penerapan fungsi SHA-256 pada algoritma kriptografi. Hasil percobaan

menunjukkan bahwa algoritma RSA memiliki kinerja lebih baik dibandingkan ElGamal pada proses enkripsi dan verifikasi tanda tangan, sedangkan ElGamal memiliki kinerja lebih baik dibandingkan RSA pada proses dekripsi dan pembuatan tanda tangan (Adeniyi et al., 2022) .

Penelitian yang dilakukan oleh (Irawan & Rachmawanto, n.d.)dengan judul "Keamanan Data Menggunakan Gabungan Kriptografi AES Dan RSA" peneliti ini menggunakan metode Algoritma AES, algoritma RSA Tujuan gabungan ini adalah meningkatkan nilai Avalanche Effect pada hasil implementasi serta untuk menganalisa waktu kebutuhan untuk proses enkripsi dan dekripsi. Pada penelitian ini, digunakan sejumlah data teks, audio dan video dengan jumlah byte antara 100 smapai 4000 bytes. Telah dilakukan perbandingan hasil perhitungan Avalanche effect (AE) pada AES, modified AES dan AES-RSA melalui 15 kali percobaan. Hasil perbandingan menunjukkan bahwa AES-RSA menghasilkan AE paling tinggi yaitu 44,74%. Adapun saran untuk pengembangan selanjutnya adalah menggunakan hardware yang lebih baru untuk mempercepat proses enkripsi dan dekripsi. File yang dapat dienkripsi dan dekripsi tidak hanya file pdf, word, ppt, excel, mp3, gambar dan video tetapi dapat dikembang untuk file yang lain.

Penelitian yang dilakukan oleh (Pendahuluan et al., n.d.)dengan judul " Manajemen Kunci Menggunakan Kombinasi dari Pertukaran Kunci Diffie–Hellman dengan Enkripsi AES" dilakukan aplikasi kriptografi untuk keamanan data oleh menggunakan pertukaran kunci Diffie-Hellman dan algoritma AES adalah untuk mengamankan data saat mengirim, pengirim pertama penerima

menukar kunci atau menghasilkan kunci untuk file yang dienkripsi oleh menggunakan pertukaran kunci Diffie-Hellman, setelah mendapatkan kunci file akan dienkripsi dengan menggunakan algoritma AES untuk enkripsi dan file dekripsi, pengirim akan mengirim file ke pihak penerima melalui server terlebih dahulu untuk menyimpan data, kemudian penerima untuk mendekripsi file membaca file agar dapat dibaca kembali oleh penerima. Di dalam tugas, aplikasi yang menggabungkan Diffie-Hellman. Pertukaran Kunci dengan algoritma enkripsi AES. Aplikasi ini yang pertama kali menggunakan Pertukaran Kunci Diffie-Hellman untuk mencapai tujuan bertukar kunci rahasia bersama. Hasil menunjukkan bahwa dengan menggunakan Diffie-Hellman dengan kunci 1024 bit keamanannya setara dengan algoritma kunci 3DES, kemudian jika Diffie-Hellman dengan 2048 kunci bit maka keamanannya sama dengan kunci 3DES, dan jika Diffie-Hellman dengan kunci 3072 bit maka keamanan yang sama dengan AES-128 bit, maka Diffie-Hellman dengan kunci 7680 bit maka keamanannya setaraAES-182 bit, dan jika Diffie-Hellman dengan kunci 15360 bit maka keamanan setara dengan AES-256 bit.

Penelitian yang dilakukan (Nisa et al., 2020)“ Aplikasi Enkripsi Citra Dan Teks Menggunakan Algoritma Diffie-Hellman Dan ElGamal” Pada Januari 2020, Keamanan data menjadi hal terpenting dalam penyimpanan informasi. Salah satunya adalah keamanan dalam bertukar pesan. Oleh karena itu, diperlukan metode enkripsi. Dalam enkripsi, ada enkripsi simetris dan asimetris. Enkripsi asimetris dianggap lebih aman karena menggunakan dua jenis kunci yang berbeda dibandingkan dengan enkripsi simetris yang hanya menggunakan satu jenis kunci.

ElGamal merupakan salah satu algoritma enkripsi asimetris yang keunggulannya terletak pada perhitungan logaritma diskrit yang sulit dipecahkan Sedangkan Diffie-Hellman merupakan salah satu algoritma proses pertukaran kunci yang menghasilkan kunci rahasia selama proses komunikasi untuk menjaga kerahasiaan kunci tersebut. Pada penelitian ini, kombinasi algoritma Diffie-Hellman dan ElGamal digunakan untuk mengamankan pesan teks dan gambar. gabungan dari kedua algoritma ini terdiri dari 4 proses yaitu proses pertukaran kunci, pembangkitan kunci, enkripsi, dan dekripsi. Dari hasil pengujian diperoleh rata-rata waktu enkripsi file teks sebesar 119,9 ms, dekripsi 248,3 ms, dan throughput 600,96 Kbps. Ratarata waktu enkripsi file citra sebesar 2623,4 ms dan waktu dekripsi 4349,5 ms. Dari hasil pengujian pada beberapa dimensi citra yang berbeda, rata-rata MSE pada citra sebesar 213,9 dan PSNR sebesar 173,27 dB. Nilai ini menunjukkan kualitas citra cukup baik (diatas 40 dB). Semakin besar dimensi citra, maka nilai MSE tiap intensitas piksel akan semakin kecil, dengan rata-rata penurunan sebesar 27.67%. Semakin besar dimensi citra, maka nilai PSNR akan semakin besar, dengan kenaikan rata-rata sebesar 1,94%. Kombinasi algoritma Diffie Hellman dan ElGamal menghasilkan nilai avalanche effect sebesar 85,18% untuk file teks dan 84,46% untuk file citra. Nilai ini menunjukkan kombinasi algoritma cukup baik dengan hasil penyelesaian bit di atas 60%.

Pada penelitian sebelumnya yang dilakukan (Pendahuluan et al., n.d.)yang hanya membahas aplikasi kriptografi untuk keamanan data dengan menggunakan pertukaran kunci Diffie-Hellman dengan satu algoritma saja yaitu algoritma AES, berdasarkan penjelasan diatas maka tujuan dari penelitian ini adalah untuk

melakukan keamananan data file, sebab keamanan data file sangat penting dalam penyimpanan informasi. Salah satunya adalah keamanan saat pertukaran pesan. Apalagi pesan tersebut berisi informasi yang sangat penting dan bersifat rahasia yang menyangkut sebuah orgPenerimasasi atau perusahaan. Kebutuhan akan keamanan data inilah yang disebut dengan kriptografi, yang terdiri dari berbagai metode untuk mengamankan data, salah satunya yaitu enkripsi, yaitu mengubah informasi yang asli (Plaintext) menjadi sandi-sandi atau kode-kode yang tidak di mengerti (Chipertext) dan tidak dapat di dekripsi oleh pihak manapun atau pihak yang tidak berwewenang atas informasi tersebut. Salah satu metode yang di gunakan untuk menjaga kerahasiaan kunci dengan menggunakan Diffie Hellman yang merupakan salah satu algoritma dalam pertukaran kunci terhadap beberapa algoritma enkripsi dan dekripsi diantaranya Algoritma Elgamal dan RSA dalam meningkatkan keamananan data file agar lebih terjamin dan akurat dan tidak dapat disalahgunakan oleh pihak yang tidak bertanggung jawab, dan dapat menghasilkan akurasi yang lebih baik lagi, dengan Pertukaran kunci Diffie–Hellman pada algoritma Elgamal dan RSA maka akan membuat kunci rahasia bersama antara dua pihak yang dapat dipakai untuk komunikasi rahasia atau pertukaran data melalui jaringan publik. Dengan melihat masalah pada latar belakang diatas, maka penulis tertarik untuk melakukan penelitian dengan judul **“Keamanan Data File Dengan Algoritma RSA-Elgamal dan Algoritma Diffie Hellman”.**

I.2. Rumusan Masalah

Adapun yang menjadi rumusan masalah dalam penelitian ini adalah sebagai berikut :

1. Bagaimana menggunakan pembangkit kunci Diffie Hellman terhadap Algoritma RSA dan ElGamal untuk meningkatkan keamanan data file?
2. Bagaimana menghubungkan algoritma kriptografi RSA dan Elgamal dengan kunci dari algoritma kriptografi Diffie Hellman?

I.3. Batasan Masalah

Batasan masalah penelitian selanjutnya di uraikan berupa pertanyaan berikut:

1. Algoritma yang digunakan pada penelitian ini adalah Algoritma RSA, ElGamal dan Diffie Hellman.
2. *Data* yang dienkripsi adalah data teks dan berekstensi .pdf.
3. Proses keamanan data file meliputi proses enkripsi dan dekripsi data.
4. Kombinasi Algoritma RSA, Elgamal dan Diffie Hellman sebagai keamanan data file.

I.4. Tujuan Penelitian

Berdasarkan pada rumusan dan batasan masalah diatas maka penulis

mempunyai tujuan. Adapun tujuan dari penelitian ini adalah:

1. Menggunakan pembangkit kunci Diffie Hellman terhadap Algoritma RSA dan Elgamal untuk meningkatkan keamanan data file
2. Menghasilkan koneksi yang solid antara algoritma kriptografi RSA dan Elgamal dengan menggunakan kunci dari algoritma kriptografi Diffie Hellman.

I.5. Manfaat Penelitian

Adapun manfaat dari penelitian ini adalah :

1. Dapat mengamankan data agar terjamin kerahasiannya.
2. Mencegah agar orang yang tidak bertanggungjawab tidak dapat mengubah, menyisipkan atau menghapus data tersebut.
3. Meningkatkan Efektifitas Peningkatan dari kedua algoritma RSA dan Elgamal dengan kunci Diffie Hellman dalam keamanan data file.

I.6. Sistematika Pembahasan

Adapun sistematika penulisan propsal ini untuk memudahkan para pembaca dalam mengikuti pembahasan dalam penelitian ini, maka penulisan akan membagi penulisan tersebut dalam 5 (lima) bab, adapun bab-bab tersebut adalah sebagai berikut yaitu :

BAB I PENDAHULUAN

Dalam bab ini memuat hal – hal yang bersifat umum, yang meliputi latar belakang masalah, pernyataan masalah yang terdiri dari

identifikasi masalah dan batasan masalah tujuan penelitian, manfaat penelitian, sistematika penulisan dan rancangan kegiatan.

BAB II TINJAUAN PUSTAKA

Tinjauan pustaka menjelaskan tentang teori-teori yang akan penjelasan tentang Teori, Konsep dan Prinsip Dasar yang diperlukan untuk menyelesaikan masalah dalam pengkajian yang dilakukan.

BAB III METODOLOGI PENELITIAN

Pada Bab ini menjelaskan tentang metode-metode yang digunakan dalam penelitian ini meliputi metode pengumpulan data, dan metode simulasi serta alur penelitian.

BAB IV HASIL

Dalam Bab ini menjelaskan penjabaran dari teknik yang digunakan untuk pelaksanaan metode yang diterapkan berdasarkan tingkat dari prioritasnya.

BAB V PEMBAHASAN

Pada Bab ini berisikan berbagai kesimpulan yang dapat dibuat berdasarkan uraian yang telah disampaikan, serta saran kepada perusahaan atau peneliti selanjutnya.

BAB VI KESIMPULAN DAN SARAN

Pada Bab ini berisikan berbagai kesimpulan yang dapat dibuat

berdasarkan uraian yang telah disimpulkan, serta saran kepada perusahaan atau untuk peneliti selanjutnya.