

BAB I

PENDAHULUAN

I.1 Latar Belakang

Perkembangan sistem keamanan sangat cepat dan pesat, hal ini yang menyebabkan munculnya kemajuan teknologi informasi. Secara langsung atau tidak, teknologi informasi telah menjadi bagian penting dari berbagai bidang kehidupan. Teknologi juga memberikan kemudahan untuk bertukar informasi sehingga keamanan data tidak dapat lepas dari berbagai aspek kegiatan manusia yang memungkinkan dapat menjaga kerahasiaan informasi tersebut, namun dalam implementasinya masih terdapat kecurangan dan ancaman terhadap data khususnya pada ekspor kayu. Akibat dari maraknya pencurian data, maka diperlukan aplikasi keamanan data ekspor kayu yang memberikan kerahasiaan data lebih terjaga dan kurangnya keamanan kerahasiaan data ekspor kayu maka diperlukan sebuah aplikasi kriptografi untuk melakukan enkripsi pada data ekspor kayu yang menyembunyikannya dapat diperkuat dengan sistem penguncian.

Terdapat banyak metode pengamanan data yang bisa dimanfaatkan untuk mencegah adanya kecurangan ataupun manipulasi data salah satunya menggunakan kriptografi ataupun teknik penyamaran lainnya. Kriptografi adalah ilmu yang berdasarkan pada teknik matematika untuk berurusan dengan keamanan informasi seperti kerahasiaan, keutuhan data dan otentikasi entitas. Jadi pengertian kriptografi modern adalah tidak saja berurusan hanya dengan menyembunyian pesan namun lebih pada sekumpulan teknik yang menyediakan keamanan informasi.

RSA (*Rivest Shamir Adleman*) merupakan salah satu algoritma *public key* yang populer dipakai dan bahkan hingga saat ini Algoritma RSA masih dianggap aman dan *Affine cipher* adalah perluasan dari *caesar cipher*, yang menggalikan plainteks dengan sebuah nilai dan menambahkannya dengan sebuah pergeseran.

Kecurangan pada Keamanan Data Ekspor tersebut dapat diatasi dengan memanfaatkan metode *RSA dan Afiine Chiper* secara enkrip dan deskrip.

Oleh karena itu dibutuhkan suatu sistem keamanan yang mampu menjaga keamanan data ekspor dari ancaman lain yang dilakukan oleh pihak yang tidak bertanggung jawab. Dengan memanfaatkan algoritma RSA dan *Affine chiper* ini *system* akan mengenkripsi data asli yang diinputkan pengguna menjadi *chipertkes* dengan menggunakan *key*, kemudian mengirimkan kepada orang lain ataupun rekannya. Untuk penerimaan data asli dideskripsi menjadi *plainteks* menggunakan *key* juga oleh penerima sehingga pengiriman informasi atau pemanfaatan informasi melalui keamanan algoritma *RSA dan Affine chiper* menjadi lebih mudah dipahami oleh perusahaan dalam mengatasi keamanan data ekspor tersebut.

Berdasarkan pembahasan latar belakang diatas maka penulis melakukan penelitian dengan judul **“Rancang Bangun Aplikasi Keamanan Data Ekspor Kayu Pada PT. Mujur Timber Menggunakan Metode Affine Cipher Dan Rsa Berbasis Web”**.

I.2. Ruang Lingkup Permasalahan

Ruang lingkup permasalahan yang dapat diberikan untuk penelitian ini berdasarkan latar belakang adalah sebagai berikut :

I.2.1. Identifikasi Masalah

Masalah Identifikasi masalah berdasarkan latar belakang yang telah dijelaskan di atas adalah sebagai berikut :

1. Belum adanya aplikasi keamanan data ekspor kayu pada PT. Mujur Timber
2. Belum ada penerapan metode RSA dan *Affine Chiper* pada keamanan data ekspor kayu pada PT. Mujur Timber
3. Belum ada aplikasi pada PT. Mujur Timber untuk keamanan data ekspor kayu pada PT. Mujur Timber

I.2.2 Rumusan Masalah

Rumusan masalah dalam pembahasan dan permasalahan yang akan dihadapi dalam perancangan aplikasi ini :

1. Bagaimana merancang aplikasi keamanan data ekspor kayu dengan menerapkan *Algoritma RSA dan Affine Chiper* ?
2. Bagaimana cara melakukan enkripsi dan deskripsi terhadap data ekspor kayu dengan menerapkan *Algoritma RSA dan Affine Chiper*?
3. Bagaimana mengimplementasikan aplikasi *keamanan* ekspor kayu dengan menerapkan *Algoritma RSA dan Affine Chiper* untuk pengamanan ekspor kayu berbasis *Web*?

I.2.3. Batasan Masalah

Batasan masalah pada penelitian ini berdasarkan latar belakang adalah sebagai berikut :

1. Aplikasi hanya untuk keamanan data ekspor kayu pada PT. Mujur Timber
2. Input data berupa data ekspor kayu
3. Output aplikasi ini berupa hasil keamanan data ekspor kayu
4. Pembuatan Aplikasi ini menggunakan bahasa pemrograman PHP dan juga menggunakan Xampp
5. Perancangan Aplikasi ini menggunakan pemodelan UML.
6. Metode yang digunakan adalah metode RSA dan *Affine Chiper*.

1.3. 1 Tujuan Penelitian

Adapun tujuan penelitian ini adalah Sebagai berikut:

1. Untuk membangun aplikasi keamanan data dengan penerapan *Algoritma RSA* dan *Affine Chiper* dalam mengamankan data ekspor kayu berbasis *Web*.
2. Memberikan hasil enkripsi dan dekripsi data ekspor kayu dengan penerapan *Algoritma RSA* dan *Affine Chiper* berbasis *Web*.
3. Menerapkan *Algoritma RSA* dan *Affine Chiper* kedalam pengamanan ekspor kayu karyawan berbasis *Web*.

1.3.2. Manfaat Penelitian

Adapun manfaat dari penelitian ini adalah :

1. Membantu pihak perusahaan atau hrd menjaga kerahasiaan informasi dari data ekspor kayu.
2. Dengan adanya penerapan algoritma *RSA* dan *Affine Chiper* pada keamanan data *absensi* karyawan pengguna terhindar dari pencurian data ekspor kayu.

3. Penerapan algoritma *RSA* dan *Affine Cipher* ini membantu pihak perusahaan memberikan hasil keamanan data ekspor kayu yang lebih tepat dan akurat hingga pemanfaatan informasi selanjutnya dapat berjalan dengan baik.

I.4. Metodologi Penelitian

I.4.1. Metode Pengumpulan Data

Berikut ini adalah beberapa teknik pengumpulan data yang peneliti lakukan untuk melengkapi bahan penelitian :

- a. Pengamatan Langsung (*Observation*)

Melakukan pengamatan secara langsung ke tempat objek pembahasan yang ingin diperoleh yaitu bagian-bagian penting dalam pengambilan data seperti data ekspor kayu.

- b. Wawancara (*Interview*)

Teknik ini digunakan secara langsung bertatap muka dengan pihak bersangkutan yaitu Zulkipli S.H. Selaku HRD untuk mendapatkan informasi serta ekspor kayu

Pertanyaan:

- c. Sampel (*Sampling*)

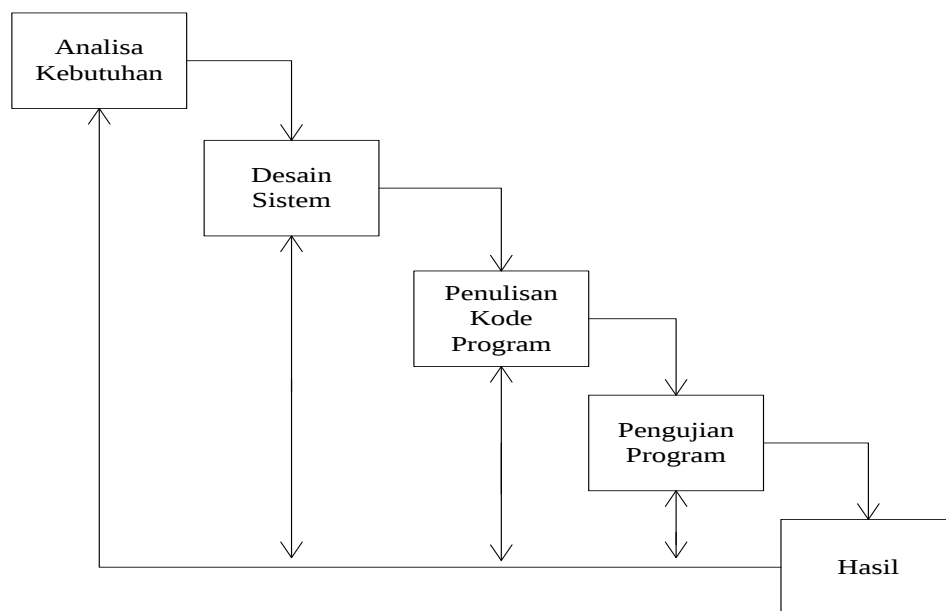
Dalam sampel ini penulis meneliti dokumen apa yang dibutuhkan dalam pengambilan data yang sesuai dengan judul penulis yaitu menggunakan metode untuk merancang sistem keamanan data.

- d. Penelitian Perpustakaan (*LibraryResearch*)

Pada teknik ini penulis mengutip dari beberapa bacaan yang berkaitan dengan

pelaksanaan skripsi. Bacaan yang dikutip dapat berupa teori atau pendapat dari beberapa bacaan. Hal ini dimaksudkan untuk memberikan landasan teori yang kuat melalui buku-buku, jurnal yang berhubungan dengan penulisan skripsi ini.

Dalam metode penelitian ini digunakan teknik-teknik analisis, klasifikasi masalah, terhadap masalah-masalah yang berhubungan dengan skripsi yang penulis buat. Langkah-langkah yang dilakukan penulis untuk mencapai tujuan perancangan ditunjukkan pada Gambar I.1 berikut ini:



Gambar I.1. Diagram Waterfall

Keterangan :

Penjelasan gambar I.1 Perancangan pengamanan data ekspor kayu menggunakan Algoritma RSA dan *Affine Chiper* berbasis desktop pada model *waterfall*:

a. Analisa Kebutuhan

Analisa Kebutuhan merupakan metode yang dilakukan penulis dengan mengambil, mengumpulkan dan menyiapkan data yang berisi tentang Perancangan pengamanan data ekspor kayu menggunakan Algoritma RSA dan *Affine Chiper*

berbasis *web*. Pada penelitian ini penulis memilih referensi dari jurnal, *web*, buku, perpustakaan dan skripsi yang berkaitan dengan penelitian ini.

b. *Design Sistem*

Pada tahapan ini, design sistem membantu dalam menentukan perangkat keras (*hardware*) dan mendefinisikan arsitektur sistem secara keseluruhan dengan menggunakan *use case* pada sistem yang akan dibangun.

c. Penulisan kode program

Pada tahap ini, sistem pertama kali dikembangkan di program kecil yang disebut unit, yang terintegrasi dalam tahap selanjutnya. Setiap unit dikembangkan dan diuji untuk fungsionalitas yang disebut sebagai unit testing.

d. Pengujian Program

Dalam tahapan ini, sistem yang dirancang diuji kemampuan dan keefektifan nya dalam suatu *BlackBox Testing*. Sehingga didapatkan kekurangan dan kelemahan sistem yang kemudian dilakukan pengkajian ulang dan perbaikan terhadap aplikasi.

e. Hasil

Tahap akhir dalam model *waterfall* ini perangkat lunak yang sudah jadi, dijalankan serta dilakukan pemeliharaan. Pemeliharaan termasuk dalam memperbaiki kesalahan yang tidak ditemukan pada langkah sebelumnya. Perbaikan implementasi unit sistem dan peningkatan jasa sistem sebagai kebutuhan baru.

I.5. Kontribusi Penelitian

Adapun yang menjadi Kontribusi Penelitian dalam penelitian ini adalah:

Penelitian terkait yang dilakukan oleh Raja Nasrul Fuad, Haikal Nando Winata, dkk yang berjudul Aplikasi Keamanan File Audio Wav (Waveform) Dengan Terapan Algoritma Rsa. Perangkat lunak (software) dapat melakukan penyandian data audio dengan menerapkan algoritma RSA dan struktur data audio WAV. Ukuran berkas audio WAV menjadi bertambah besar setelah dilakukan enkripsi menggunakan algoritma RSA berdasarkan besar kunci yang digunakan.

Penelitian terkait lain yang dilakukan oleh Prasetyo Perancangan Aplikasi Pengamanan File Teks dengan Skema Hybrid Menggunakan Algoritma *Enigma* dan Algoritma RSA” Perkembangan teknologi informasi yang semakin pesat memberi pengaruh yang besar, Salah satunya adalah kriptografi dimana pesan disamarkan menjadi pesan tersandi. Dalam proses penyandian, penyandian yang digunakan adalah Enigma dan RSA (*Rivest Shamir Adleman*). Dimana Enigma sebagai proses penyandian simetris pada pesan dan RSA (*Rivest Shamir Adleman*) sebagai proses penyandian asimetris pada kunci sehingga terjadinya *Kriptografi Hybrid*. *Kriptografi Hybrid* sebenarnya metode yang sangat aman dikarenakan memakai dua jenis algoritma yaitu algoritma simetris dan asimetris, untuk algoritma simetris Ciphertext yang dihasilkan akan sama panjang dengan Plaintext yang di enkripsi, lain halnya dengan algoritma asimetris yang berfungsi hanya untuk proses enkripsi kunci pada penelitian ini, karena jika algoritma asimetris dipakai untuk enkripsi maka *Ciphertext* yang dihasilkan akan lebih besar jumlah datanya.

Sedangkan penelitian yang dilakukan oleh penulis dengan judul “Rancang Bangun Aplikasi Keamanan Data Ekspor Kayu Pada Pt. Mujur Timber Menggunakan

Metode Affine Cipher Dan Rsa Berbasis Web” bertujuan untuk membuat aplikasi keamanan yang digunakan untuk mengamankan data ekspor kayu yang ada di perusahaan.

I.6. Lokasi Penelitian

Lokasi penelitian yang peneliti lakukan yaitu pada Jl. Kol. Sugiono No No.10def, A U R, Kec. Medan Maimun, Kota Medan, Sumatera Utara 20151

I.7. Sistematika Penulisan

Adapun sistematika penulisan yang diajukan dalam skripsi ini adalah sebagai berikut :

BAB I PENDAHULUAN

Pada bab ini menerangkan tentang latar belakang, ruang lingkup permasalahan, tujuan dan manfaat, metode penelitian, lokasi penelitian dan sistematika penulisan.

BAB II TINJAUAN PUSTAKA

Bab ini berisi teori-teori yang berkaitan dengan Rancang Bangun Aplikasi Keamanan Data Ekspor Kayu Pada Pt. Muju Timber Menggunakan Metode Affine Cipher Dan Rsa Berbasis Web

BAB III ANALISIS DAN PERANCANGAN

Pada bab ini mengemukakan tentang pembahasan analisis dan perancangan sistem aplikasi.

BAB IV HASIL DAN UJI COBA

Pada bab ini menerangkan hasil dan pembahasan program yang dirancang serta kelebihan dan kekurangan sistem yang dirancang.

BAB V KESIMPULAN DAN SARAN

Bab ini berisi kesimpulan dari seluruh bab sebelumnya serta saran yang diharapkan dapat bermanfaat dalam proses pengembangan penelitian selanjutnya.