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 data absensi. Akibat dari maraknya pencurian data, maka diperlukan aplikasi keamanan data absensi karyawan yang memberikan kerahasiaan data lebih terjaga dan kurangnya keamanan kerahasian data absensi karyawan maka diperlukan sebuah aplikasi kriptografi untuk melakukan enkripsi pada data absensi karyawan yang penyembunyiannya 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

penyembunyian pesan namun lebih pada sekumpulan teknik yang menyediakan keamanan informasi.

Affine cipher merupakan kriptografi klasik yaitu algoritma substitusi. Algoritma ini mengandalkan kunci berupa dua nilai bilangan bulat (integer). Dan RSA merupakan algoritma yang banyak digunakan saat ini untuk mengamankan data. RSA menggunakan algoritma pemfaktoran bilangan yang sangat besar, sehingga RSA dianggap paling aman dari serangan kriptaanalisis. (Muhamad Wais Al Qorny, 2018).

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

Berdasarkan pembahasan latar belakang diatas maka penulis melakukan penelitian dengan judul **"*Rancang Bangun Aplikasi Keamanan Data Absensi Karyawan Pada PT. Duta Jelita Dengan 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 absensi pegawai pada PT. Duta Jelita.
2. Belum ada penerapan metode *Affine Cipher* dan *RSA* pada keamanan data absensi pada PT. Duta Jelita.
3. Belum ada aplikasi pada PT. Duta Jelita untuk keamanan data absensi pada PT. Duta Jelita.

I.2.2. Rumusan Masalah

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

1. Bagaimana merancang aplikasi keamanan data absensi karyawan dengan menerapkan algoritma *Affine Cipher* dan *RSA*?
2. Bagaimana cara melakukan enkripsi dan deskripsi terhadap data absensi karyawan dengan menerapkan algoritma *Affine Cipher* dan *RSA*?
3. Bagaimana mengimplementasikan aplikasi keamanan data absensi dengan menerapkan algoritma *Affine Cipher* dan *RSA* untuk pengamanan absensi karyawan berbasis *web*?

I.2.3. Batasan Masalah

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

1. Aplikasi hanya untuk keamanan data absensi pada PT. Duta Jelita
2. Input data berupa data absensi
3. Output aplikasi ini berupa hasil keamanan data absensi.
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 *Affine Cipher* dan *RSA*.

1.3. Tujuan Penelitian

Adapun tujuan penelitian ini adalah sebagai berikut:

1. Untuk membangun aplikasi keamanan data dengan penerapan algoritma *Affine Cipher* dan *RSA* dalam mengamankan data absensi karyawan berbasis *web*.
2. Memberikan hasil enkripsi dan dekripsi data absensi karyawan dengan penerapan algoritma *Affine Cipher* dan *RSA* berbasis *web*.
3. Menerapkan algoritma *Affine Cipher* dan *RSA* kedalam pengamanan data absensi karyawan berbasis *web.*

1.4 Manfaat Penelitian

Adapun maanfaat dari penelitian ini adalah :

1. Meminimalisasikan kesalahan dalam hal keamanan data absensi karyawan dengan penerapan algoritma *Affine Cipher* dan *RSA.*

2. Dengan adanya penerapan algoritma *Affine Cipher* dan *RSA* pada keamanan data absensi karyawan sehingga menghasilkan data enkripsi dan deskripsi yang aman dari pencurian data absensi.
3. Diterapkannya algoritma *Affine Cipher* dan *RSA* kedalam pengamanan data absensi karyawan berbasis *web* membantu pihak perusahaan memberikan hasil keamanan data absensi karyawan yang lebih tepat dan akurat hingga pemanfaatan informasi selanjutnya dapat berjalan dengan baik

I.5. Metodologi Penelitian

Metode merupakan suatu cara yang sistematik untuk mengerjakan suatu permasalahan. Penelitian ini akan melalui beberapa tahapan. Adapun beberapa tahapan yang digunakan dalam penelitian ini adalah sebagai berikut :

I.5.1. 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 absensi karyawan.

b. Wawancara (*Interview*)

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

serta data absensi.

Pertanyaan:

1. Bagaimana absensi yang dilakukan oleh PT. Duta Jelita?

   Jawab: Pada saat ini absensi yang dilakukan menggunakan *fingerprint*.

2. Apakah ada kendala saat melakukan keamanan absensi pegawai

   Jawab: Pada saat ini belum ada aplikasi yang mengatasi keamanan data absensi pegawai.

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.

11	7	Rio Bojo Saja	X	X	X	A		X	X	X	X	A	X		X	X	X	A	X	X		X	X	X	X	X	X		X	X	X	X	X	24	0	3
12	8	Bondang Bahrudin	X	X	X	X		X	X	X	A	X	X		X	X	X	X	X	X		X	A	X	X	X	X		A	X	X	X	X	24	0	3
13	9	Maghfidah Lestari	X	X	X	X		X	X	A	X	X	X		X	X	X	X	A	X		X	X	X	[illegible]	[illegible]	[illegible]		X	X	X	X	X	22	3	2
14	10	Kusmiran Edi Purnomo	X	X	X	X		X	A	X	X	X	X		X	X	X	X	X	X		A	X	X	X	X	X		X	X	X	X	X	25	0	2
15	11	Johan Sitompul	X	X	X	X		A	X	X	X	X	X		X	X	X	X	X	A		X	X	X	X	X	X		X	X	X	X	X	25	0	2
16	12	Idul Fitryani	X	X	X	X		X	X	X	X	X	X		X	X	X	X	X	X		X	X	X	X	X	X		X	X	X	X	X	27	0	0
17																													Total =					291	6	26
18						Keterangan		X = Hadir																												
19								S = Sakit																												
20								A = Tidak Hadir																												

Gambar I.1 Data Absensi

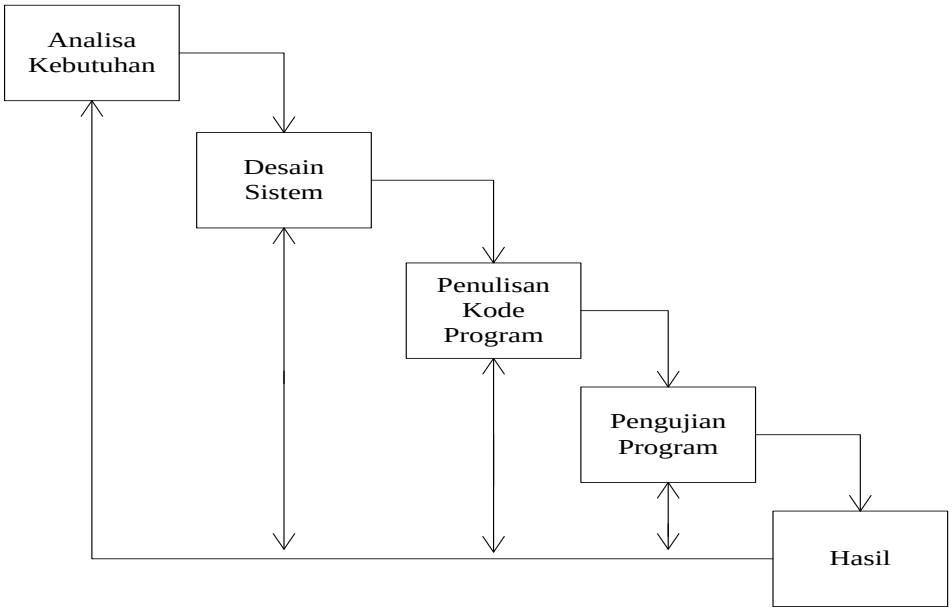
(Sumber: *PT. Duta Jelita*)

d. Penelitian Perpustakaan (*Library Research*)

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.2.:



Gambar I.2. Diagram *Waterfall*

Keterangan :

Penjelasan Gambar I.2. Perancangan pengamanan data absensi karyawan menggunakan Algoritma *Affine Cipher* dan *RSA* berbasis *web* pada model *waterfall.*

1. Analisis Kebutuhan

Pada tahap ini menganalisis sistem yang sedang berjalan khususnya keamanan mengenai data absensi karyawan. Pada tahap ini dilakukan pengumpulan data-data teori yang terkait dengan data absensi karyawan dan metode *Affine Cipher* dan *RSA.*

1. Dalam memproses data pada perancangan sistem keamanan data absensi karyawan menggunakan metode *Affine Cipher* dan *RSA* adalah dengan

menggunakan pemrograman PHP.

2. *Database* yang digunakan sebagai media penyimpanan data dalam pembuatan keamanan data absensi karyawan.

2. Desain Sistem

Pada tahap desain sistem peneliti melakukan pembuatan sistem keamana data absensi pada PT. Duta Jelita dengan menggunakan model perancangan *Unified Modelling Language (*UML*)* yaitu *use case diagram, activity diagram, sequence diagram* dan *class diagram.*

3. Penulisan Kode Program

Pada tahap ini desain sistem akan diimplementasikan ke dalam kode program. Penulisan kode program merupakan desain dalam bahasa yang bisa dikenali oleh komputer. Pemrograman dimulai dengan menggunakan pemrograman PHP dan menggunakan database MySQL.

4. Pengujian Program

Pengujian program merupakan langkah yang dilakukan setelah penulisan kode program. Pengujian dilakukan dengan menggunakan *blackbox testing*. *Blackbox testing* adalah metode pengujian perangkat lunak yang menguji fungsionalitas sistem yang bertentangan dengan struktur internal atau kerja. Pengetahuan khusus dari kode sistem/struktur internal dan pengetahuan pemrograman pada umumnya tidak diperlukan. Uji kasus dibangun di sekitar spesifikasi dan persyaratan, yakni, sistem apa yang seharusnya dilakukan. Menggunakan deskripsi eksternal perangkat lunak, termasuk spesifikasi, persyaratan, dan desain untuk menurunkan uji kasus.

5. Hasil

Pada tahap ini program akan diterapkan untuk keamanan data absensi. Kemudian program akan secara otomatis menampilkan hasil berupa data keamanan absensi.

I.6. Kontribusi Penelitian

Adapun yang menjadi Kontribusi Penelitian dalam penelitian ini adalah:

1. Memberikan kontribusi bagi Perusahaan dalam mengaplikasikan serta menjalankan program keamanan data absensi karyawan
2. Meningkatkan pengetahuan tentang metode *Affine Chiper* dan *RSA* sehingga dapat menerapkan metode ini kedalam penelitian yang ingin dilakukan.
3. Bahan referensi penyusunan, mata kuliah, khususnya dengan penerapan metode *Affine Chiper* dan *RSA* dalam keamanan data absensi karyawan berbasis *web*.

I.7. Lokasi Penelitian

Lokasi penelitian yang peneliti lakukan yaitu pada MM8G+R8P, Jl. Pulau Sumatera, M A B A R, Kec. Medan Deli, Kota Medan, Sumatera Utara 20242.

I.8. 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 Absensi Karyawan Pada PT. Duta Jelita Dengan Menggunakan Metode *Affine Chiper* Dan *RSA***.**

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.