BAB I

PENDAHULUAN

I.1. Latar Belakang

Kemajuan teknologi komputer membantu semua aspek kehidupan manusia, dari hal yang terkecil sampai ke berbagai hal yang sangat rumit sekalipun bisa dikerjakan oleh teknologi komputer. Semua lapisan masyarakat memerlukan komputer sebagai alat bantu dalam kehidupan sehari - hari. Hal ini mendorong setiap instansi untuk tetap mengikuti perkembangan teknologi dan terus meningkatkan kemampuannya dalam pengolahan data-data dan informasi yang disimpan menggunakan *database* agar data tersebut lebih aman, akurat, dan efisien. Salah satu hal terpenting dalam penyimpanan menggunakan *database* adalah untuk menjamin keamanan pesan, data ataupun informasi dalam proses pengiriman atau penyimanan data, sehingga salah satu munculnya teknologi kriptografi. Teknologi kriptografi digunakan untuk keamanan *database* dari ancaman, baik dari kesengajaan atau pun bukan.

Seiring banyaknya aplikasi, pengguna internet, dan data digital, maka semakin banyak juga celah-celah yang terbuka bagi orang-orang yang ingin melakukan kejahatan. Oleh karena itu, faktor keamanan menjadi suatu hal yang serius dalam semua aplikasi yang di internet dan aplikasi berbasis web. Kejahatan yang paling sering terjadi adalah kejahatan terhadap pencurian data atau informasi dari data *server* atau *database* melalui aplikasi berbasis web.

Contoh kasus dalam penelitian yang dilakukan oleh Deanne Destriani Firmansyah Putri dan Muhammad Helmi Fahrozi (2020), yaitu saat ini sedang maraknya terjadi kasus kebocoran data, peningkatan pengguna internet dan *e-commerce* yang kian meningkat semenjak terjadinya pandemi COVID-19 membuat sistem keamanan internet menjadi rentan. Banyak website yang diretas oleh oknum tidak bertanggung jawab, termasuk *website e-commerce* Bhinneka.com yang merupakan situs *e-commerce* Indonesia. Sebelumnya Bhinneka.com *website* yang didirikan oleh Hendrik Tio, Nicholas, Johannes, Darsono dan Tommy pada tahun 1999. Bhinneka.com mengalami kasus kebocoran data sebanyak 1,2 juta data pengguna Bhinneka.com dijual bebas oleh sekelompok *hacker* bernama *ShinyHunter*. Data pengguna Bhinneka.com dan 10 perusahaan lainnya yang serupa juga dijual bebas di sebuah pasar gelap web, sehingga tercatat setidaknya terdapat 73,2 juta data diri pengguna e-commerce dan data perusahaan lainnya terjual bebas dengan harga mencapai USD 18 ribu per-datanya. Melihat hal ini tentu harus menjadi perhatian besar bahwa sudah saatnya pengesahan RUU Perlindungan Data Pribadi harus dilakukan.

Melihat permasalahan yang ada menjadikan pertimbangan bagi penulis untuk memilih sebuah algoritma yang akan digunakan dalam penyusunan tugas akhir ini, penulis memilih *Algoritma stream cipher* dan *playfair cipher* karena dapat di implementasikan untuk pengamanan *database. Algoritma stream cipher* memiliki kunci yang unik, dimana kunci tersebut menggunakan karakter sebelumnya sebagai kunci dan *playfair cipher* klasik memiliki kelebihan yang sulit untuk dikriptanalisis secara manual. Komponen yang penting pada *algoritma*

playfair adalah tabel *cipher* yang digunakan untuk melakukan enkripsi dan dekripsi tabel bawaan yang diperkenalkan oleh playfair adalah tabel yang memiliki bentuk matriks berukuran (5x5) yang berisi huruf kapital dari A-Z dengan menghilangkan huruf J. Dari kedua *algoritma* ini cukup mudah untuk dijelaskan dan sudah digunakan secara luas pada beberapa aplikasi dan algoritmanya sudah dinyatakan cukup aman untuk diterapkan.

Berdasarkan uraian diatas, maka penulis mengambil judul Skripsi mengenai "**Rancang Bangun Aplikasi Keamanan *Database* Dengan Menggunakan Metode *Stream Cipher* dan *Playfair Cipher* Berbasis *Hybrid*".**

I.2. Ruang Lingkup Permasalahan

Adapun ruang lingkup permasalahan dalam penelitian ini adalah sebagai berikut:

I.2.1. Identifikasi Masalah

Adapun identifikasi masalah yang penulis temukan dalam penelitian ini adalah sebagai berikut:

1. Jumlah penggunaan internet yang semakin banyak membuat sistem keamanan yang rentan sering terjadi kebocoran data dikarenakan.
2. Banyak sebuah *website* yang diretas dikarenakan belum adanya keamanan pada *database* yang mengakibatkan data dan informasi dicuri oleh oknum yang tidak bertanggung jawab.
3. Belum menerapkan metode *Stream Cipher* dan *Playfair Cipher* ke dalam sebuah aplikasi untuk mengamankan *database.*

I.2.2. Rumusan Masalah

Berdasarkan latar belakang masalah yang telah diuraikan, maka dapat dirumuskan masalah yang dibahas dalam penulisan penelitian ini adalah:

1. Bagaimana melakukan proses keamanan *database* agar data yang terdapat didalam sebuah aplikasi tidak diketahui isinya dengan mudah oleh pihak yang tidak diinginkan ?
2. Bagaimana merancang aplikasi keamanan untuk menghindari *website* direta oleh oknum yang tidak bertanggung jawab?
3. Bagaimana menerapkan metode *Stream Cipher* dan *Playfair Chipher* dalam keamanan *database* berbasis *Hybrid* ?

I.2.3. Batasan Masalah

Adapun batasan masalah agar pembuat sistem ini tidak terlalu luas cakupannya adalah sebagai berikut:

1. Aplikasi ini berbasis *hybrid* dalam proses keamanan *database.*
2. Metode yang digunakan keamanan *database* adalah metode *Stream Cipher* dan *Playfair Cipher*.
3. Dengan aplikasi ini pengguna dapat melakukan Dekripsi terhadap *database* yang telah di Enkripsi.
4. Data yang dienkripsi adalah *file* atau isi *database*.
5. Sistem yang dibangun dalam penelitian ini menggunakan bahasa pemrograman PHP dan MySQL sebagai *database*.

6. Perancangan aplikasi dibuat menggunakan *Unified Modelling Language* (UML).

I.3. Tujuan dan Manfaat

I.3.1. Tujuan

Adapun beberapa tujuan pada penelitian ini adalah sebagai berikut:

1. Menerapkan metode *Stream Cipher* dan *Playfair Chipher* dalam keamanan *database* berbasis *Hybrid*.
2. Membuat aplikasi keamanan *database* agar data lebih aman, akurat dan efisien .
3. Untuk menjaga keutuhan dan keamanan *database* dari pihak yang tidak berwenang.

I.3.2. Manfaat

Adapun manfaat yang diperoleh dari penulisan skripsi ini adalah sebagai berikut:

1. Aplikasi yang dibangun dapat digunakan sebagai alternatif untuk pengamanan *database.*
2. Dengan adanya aplikasi keamanan ini, data yang tersimpan di *database* menjadi lebih aman, sehingga pengguna tidak perlu khawatir akan terjadinya kebocoran data dan kehilangan data.
3. Keamanan pada *database* lebih terjamin menggunakan algoritma *Stream Cipher* dan *Playfair Chipher*.

I.4. Metodologi Penelitian

I.4.1. Metode Pengumpulan Data

Sistem yang dirancang tentunya memerlukan pengumpulan data, dalam proses pengumpulan data terdapat beberapa cara, berikut diantaranya:

1. Studi Literatur

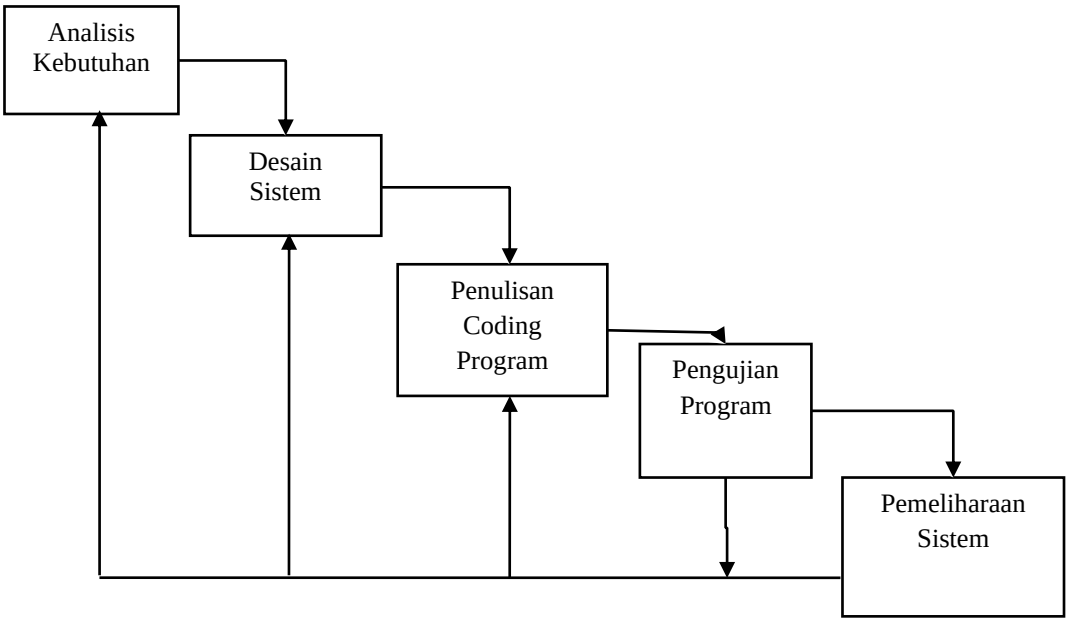
   Yaitu dengan cara mempelajari acuan dan literatur yang berhubungan dengan materi dalam penulisan skripsi. Acuan yang digunakan umumnya adalah tentang cara penyusunan skripsi pada Universitas Potensi Utama dan juga jurnal-jurnal tentang studi pustaka yang digunakan dalam penulisan skripsi.

2. Pengamatan,

   yaitu pengumpulan data dan informasi yang dilakukan dengan cara pengamatan langsung beberapa contoh aplikasih kamus. Pengamatan yang dilakukan adalah dengan mengumpulkan informasi dan mempelajari tentang metode *Stream Cipher* dan *Playfair Cipher* serta mempelajari contoh teknik-teknik pengenkripsian yang berhubungan dengan penulisan skripsi.

1.4.2. Metode Perancangan Sistem

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 III.1 berikut ini:



Gambar I.1. RANCANG BANGUN APLIKASI KEAMANAN DATABASE DENGAN MENGGUNAKAN METODE STREAM CIPHER DAN PALYFAIR CIPHER BERBASIS HYBRID.

1. Analisis Kebutuhan

   Berisi tentang hal-hal yang harus ada pada hasil perancangan agar mampu menyelesaikan masalah yang ada sesuai tujuan. Dalam proses perancangan aplikasi hal-hal yang dibutuhkan adalah sebuah perangkat keras komputer atau laptop, serta perangkat lunak *android studio* dan *sublime text* untuk merancang sebuah aplikasi berbasis *hybrid*.

2. Desain Sistem

   Pada tahapan desain yang dilakukan dalam pembuatan sistem dan aplikasi yang akan dirancang penulis adalah:

   a. Mendesain sistem dengan menggunakan UML (*Unified Modeling Language*).
   b. Menggunakan bahasa pemrograman PHP dan MySQL sebagai *database.*
   c. Menggunakan aplikasi *Visio* untuk menggambarkan *Flowchart* sistem.

3. Penulisan *Coding* Program

Coding merupakan penerjemahan design dalam bahasa yang bisa dikenali oleh komputer. Dilakukan oleh *programmer* yang akan meterjemahkan transaksi yang diminta oleh *user*. Tahapan inilah yang merupakan tahapan secara nyata dalam mengerjakan suatu sistem. Dalam artian penggunaan komputer akan dimaksimalkan dalam tahapan ini. Sedangkan implementasi merupakan tahap pengkodean yang merupakan suatu proses translasi. Rancangan detil ditranslasikan ke dalam suatu bahasa pemrograman. Dalam hal ini implementasi menggunakan bahasa pemrograman PHP dan *database* MySQL. Setelah pengkodean selesai maka akan dilakukan testing terhadap sistem yang telah dibuat tadi. Tujuan testing adalah menemukan kesalahan - kesalahan terhadap s*ystem* tersebut dan kemudian bisa diperbaiki.

4. Pengujian Program

Pada tahap ini dilakukan pengujian aplikasi secara menyeluruh, meliputi pengujian fungsional dan pengujian ketahanan sistem. Pengujian secara *black box (interface)* yaitu pengujian perangkat lunak yang tes fungsionalitas dari aplikasi yang bertentangan dengan struktur internal atau kerja. Pengetahuan khusus dari kode aplikasi / struktur internal dan pengetahuan pemrograman pada umumnya tidak diperlukan, pengujian tersebut untuk masing-masing blok peralatan yang dirancang.

5. Pemeliharaan Sistem

Perangkat lunak yang susah disampaikan kepada pelanggan pasti akan mengalami perubahan. Perubahan tersebut bisa karena mengalami kesalahan

karena perangkat lunak harus menyesuaikan dengan lingkungan (periperal atau system operasi baru) baru, atau karena pelanggan membutuhkan perkembangan fungsional.

I.5. Kontribusi Penelitian

Pada penelitian yang dilakukan oleh Galih Agustian Perdana, dkk (2021) dengan judul "Implementasi Algoritma Kriptografi *Playfair Cipher* untuk mengamankan data aset (Studi kasus: PT. Adywinsa Stamping Industries)". Penelitian ini menghasilkan pengamanan data aset degan algoritma kriptografi *Playfair Cipher* dilakukan untuk mengamankan *field* data aset yaitu nama *user* dan nama aset yang bertujuan aplikasi mampu melakukan enkripsi data dengan menggunakan algoritma kriptografi *Playfair Cipher* kemudian memasukkan data yang telah di enskripsi ke dalam *database* dan mampu melakukan dekripsi dari data di dalam *database* telah di enskripsi.

Sedangkan penelitian yang dilakukan oleh penulis dengan judul "Rancang Bangun Aplikasi Keamanan *Database* Dengan Menggunakan Metode *Stream Cipher* dan *Playfair Cipher* Berbasis *Hybrid*". Penelitian ini menghasilkan sebuah aplikasi untuk mengamankan *database* yang berisikan data-data rahasia sebelum ke orang lain sehingga dapat mencegah pencurian data atau informasi. Dengan menerapkan *algoritma Stream Cipher* dan *Playfair Cipher* untuk mengamankan *database* dan pengembalian *database* yang telah di amankan kedalam bentuk aslinya.

I.6. Sistematika Penulisan

Langkah-langkah yang ditempuh dalam menyelesaikan penulisan ini adalah:

BAB I : PENDAHULUAN

Dalam bab ini berisikan mengenai latar belakang, ruang lingkup permasalahan (identifikasi masalah, rumusan masalah, batasan masalah), tujuan dan manfaat, metodologi penelitian, kontribusi penelitian, dan Sistematika Penulisan.

BAB II : TINJAUAN PUSTAKA

Dalam bab ini mencakup uraian penyelesaian secara teoritis serta konsep baru dalam penyelesaian masalah berkenaan dengan sistem dan fokus kajian. Adapun landasan teori yang diuraikan oleh penulis adalah: penjelasan mengenai sistem, informasi, metode *Stream Cipher* dan *Playfair Cipher*, materi tentang keamanan *database*, serta 11 metode konseptual yang menggambarkan cara kerja dari sistem yang akan dirancang.

BAB III : ANALISA DAN PERANCANGAN

Pada bab ini berisi analisa sistem yang sedang berjalan, perancangan proses dalam bentuk diagram UML yang mencakup analisa dan perancangan sistem pengolahan data yang mencakup seluruh aktivitas yang terjadi pada sistem yang akan dibangun.

BAB IV : HASIL DAN UJI COBA

Dalam bab ini penulis menguraikan tentang tampilan hasil sistem yang dirancang beserta pembahasannya untuk mengetahui kelebihan dan kekurangan system yang dirancang.

BAB V : KESIMPULAN DAN SARAN

Dalam bab ini penulis menguraikan tentang kesimpulan untuk meningkatkan kualitas dari aplikasi yang sudah dirancang.