BAB I

PENDAHULUAN

I.1. Latar Belakang

Penggunaan utama ruang obrolan adalah untuk berbagi informasi melalui *teks* dengan sekelompok pengguna lain. Secara umum, kemampuan komunikasi dengan banyak orang dalam percakapan yang sama membedakan ruang obrolan dengan program pengiriman pesan instan , yang biasanya dirancang untuk komunikasi satu-ke-satu. Para pengguna di ruang obrolan tertentu umumnya terhubung melalui *internet* bersama atau koneksi serupa lainnya, dan ruang obrolan tersedia untuk berbagai subjek. Teknologi baru telah memungkinkan penggunaan berbagi file dan kamera web untuk dimasukkan dalam beberapa program. Ini akan dianggap sebagai ruang obrolan..

Dengan semakin banyaknya penggunaan *chat text* maka perlu adanya keamanan pesan yang dikirimkan karena pesan tersebut rawan terhadap penyadapan. Salah satu cara untuk menjaga keamanan pesan tersebut adalah dengan memanfaatkan kriptografi untuk mengenkripsi pesan sehingga pesan tidak mudah untuk dibaca.

Permasalahan pada sistem yang sedang berjalan sebelumnya adalah kurang berkembang sebuah *chat text* dengan memanfaatkan sistem keamanan data yang dapat menjaga kerahasiaan dan keamanan pengiriman data pada *chat text* dan kurang berkembang sebuah *chat text* dengan menggunakan Algoritma *Beafort Chiper*. Berdasarkan permasalahan tersebut maka dibangun sebuah Aplikasi

Keamanan Transmisi Data *Chat Text* Menggunakan Algoritma *Beafort Chiper* agar memberikan dasar dan pembangunan aplikasi *chat* dengan memanfaatkan sistem keamanan data dapat menjaga kerahasiaan dan keamanan pengiriman data pada aplikasi *chat* sehingga pengirim pesan dapat merasa nyaman dan aman dalam melakukan transfer data atau pesan dan Implementasi *Beafort Chiper* terhadap aplikasi *chat* dapat memberikan referensi baru terhadap peneliti selanjutnya mengenai metode keamanan data.

Program skripsi ini khusus merancang suatu sistem keamanan *chat text*. Berdasarkan penjelasan tersebut, maka penulis mengambil judul penelitian "**Perancangan Aplikasi Keamanan Transmisi Data *Chat Text* Menggunakan Algoritma Beafort Chiper**".

I.2. Ruang Lingkup Permasalahan

I.2.1. Identifikasi Masalah

Permasalahan yang ada pada penelitian ini adalah :

1. Pada *chat text* dengan sistem keamanan data masih rentan terhadap pencurian data.
2. Belum berkembang sebuah *chat text* dengan menggunakan Algoritma *Beafort Chiper.*

I.2.2. Perumusan Masalah

Berdasarkan uraian latar belakang masalah di atas, maka dapat dirumuskan beberapa masalahnya adalah sebagai berikut :

1. Bagaimana merancang sebuah *chat text* dengan memanfaatkan sistem keamanan data yang dapat menjaga kerahasiaan dan keamanan pengiriman data pada *chat text* ?
2. Bagaimana merancang dan membangun sebuah *chat text* dengan menggunakan Algoritma *Beafort Chiper* ?

I.2.3. Batasan Masalah

Batasan masalah pada penelitian ini yaitu:

1. Data yang dibutuhkan dalam melakukan perancangan sistem adalah *data user, profil user, data kontak, data pesan, key kriptografi.*
2. Bahasa pemrograman yang digunakan untuk membuat aplikasi yaitu *java.*
3. Pemodelan sistem dilakukan dengan *UML 2.0.*
4. Metode yang digunakan yaitu Algoritma *Beafort Chiper*

I.3. Tujuan dan Manfaat

I.3.1. Tujuan

Adapun tujuan dari merancang Aplikasi Keamanan Transmisi Data *Chat Text* Menggunakan Algoritma *Beafort Chiper* adalah :

1. Merancang sebuah aplikasi *chat* dengan memanfaatkan sistem keamanan data yang dapat menjaga kerahasiaan dan keamanan pengiriman data pada aplikasi *chat*.
2. Merancang dan membangun sebulah aplikasi *chat* dengan menggunakan Algoritma *Beafort Chiper*

I.3.2. Manfaat

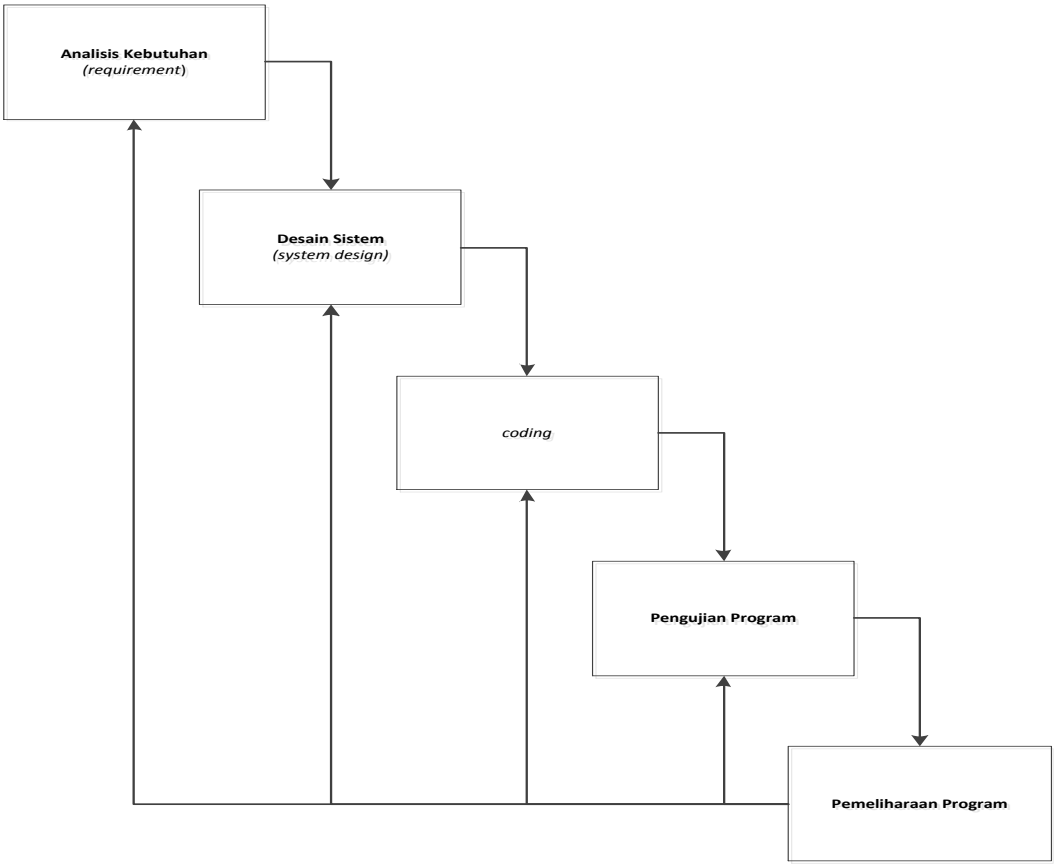
Manfaat penelitian dari penelitian ini yaitu :

1. Aplikasi *chat* yang dibangun dapat menjaga kerahasiaan dan keamanan pengiriman data pada aplikasi *chat* sehingga pengirim pesan dapat merasa nyaman dan aman dalam melakukan transfer data atau pesan.
2. Implementasi *Beafort Chiper* terhadap aplikasi *chat* dapat memberikan referensi baru terhadap peneliti selanjutnya mengenai metode keamanan data

I.4. Metodologi Penelitian

Metode penelitian yang dipakai oleh penulisan adalah metode penelitian deskriptif atau disebut juga metode penelitian analitis. Dalam metode penelitian deskriptif ini digunakan teknik-teknik analisis, klasifikasi masalah, survei, studi kepustakaan terhadap masalah-masalah yang berhubungan dengan skripsi yang penulis susun, wawancara (*interview*) dengan narasumber, observasi, dan teknik *Test* terhadap objek penelitian yang telah ada.

Penulis menggunakan metode penelitian deskriptif dikarenakan pemecahan masalah yang actual yaitu masalah yang berkembang pada bidang *artifisial intelligence* yang sekarang sedang berkembang pesat. Dengan metode deskriptif, aplikasi yang telah penulis kumpulkan mula-mula disusun, dijelaskan, dianalisis, dan kemudian diimplementasikan dalam sebuah perangkat lunak. Metodologi pengembangan sistem *waterfall* dapatdilihat pada gambar I.1 berikut :



Gambar I.1. Prosedur Perancangan Sistem

Dalam pengembangannya metode *waterfall* memiliki beberapa tahapan yaitu : *requirement* (analisis kebutuhan), design sistem (*system design*), *coding*, pengujian program, pemeliharaan sistem

1. Analisis Kebutuhan

   Berisi tentang hal-hal yang harus ada pada hasil perancangan agar mampu menyelesaikan masalah yang ada sesuai tujuan. Bahasa pemrograman yang digunakan untuk membuat aplikasi adalah *netbeans* dengan pengembangan IDE *java.*

2. Desain Sistem

Secara umum ***Perancangan Aplikasi Keamanan Transmisi Data Chat Text Menggunakan Algoritma Beafort Chiper*** menggunakan model perancangan *Unified Modelling Language*.

3. Penulisan Sinkode Program

Coding merupakan penerjemahan desain dalam bahasa yang bisa dikenali oleh komputer. Dilakukan oleh *programmer* yang akan menterjemahkan 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. Setelah pengkodean selesai maka akan dilakukan *testing* terhadap sistem yang telah dibuat tadi. Tujuan *testing* adalah menemukan kesalahan-kesalahan terhadap *system* 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 (peripheral atau system operasi baru), atau karena pelanggan membutuhkan perkembangan fungsional.

I.5. Konstribusi Penelitian

Penelitian yang dilakukan oleh Naniek Widyastuti (2014) dengan Judul Pengembangan Metode Beaufort Cipher Menggunakan Pembangkit Kunci Chaos. Penelitian ini secara khusus membahas tentang bagaimana teori chaos diterapkan pada penyandian menggunakan metode Beaufort Cipher untuk meningkatkan keamanan pada kunci yang digunakan. Berdasarkan hasil pengujian yang dilakukan terhadadap citra yang diujikan menunjukkan bahwa algoritma Beaufort Cipher yang menggunakan kunci yang dibangkitkan menggunakan fungsi chaos terbukti efektif dan aman. Hal ini dibuktikan dengan rata-rata waktu proses yang dibutuhkan untuk melakukan proses enkripsi maupun dekripsi cukup cepat yaitu sekitar 0,7 detik. Dan berdasarkan pengujian secara visual dan uji statistik algoritma enkripsi yang digunakan tidak dapat memberikan petunjuk apa-apa untuk dilakukan statistical attack oleh kriptanalis.

Penelitian yang dilakukan oleh Mia Diana (2018) dengan judul Optimalisasi *Beaufort Cipher* Menggunakan Pembangkit Kunci RC4 Dalam Penyandian SMS. Kunci pada algoritma kriptografi sangat penting

peranannya dalam proses enkripsi dan dekripsi. Semakin acak bilangan kunci yang digunakan, maka semakin acak pula cipher yang dihasilkan. Algoritma RC4 dan beaufort cipher merupakan algoritma dari teknik kriptografi. Algoritma RC4 memiliki kelebihan dalam membangkitkan kunci yang acak, sedangkan beaufort cipher memiliki kelemahan dalam hal jumlah kunci yang digunakan terlalu banyak. Penelitian ini menguraikan bagaimana mengoptimalkan pembentukan kunci pada algoritma beaufort dengan memanfaatkan proses pembangkitan kunci pada algoritma RC4 yang diimplementasikan pada menyandikan SMS yang sampai saat ini belum bersifat point-to-point (tidak langsung dikirim kepada tujuan). Hasil penelitian ini memberikan kemudahan bagi pengguna dalam proses pembangkitan kunci enkripsi maupun dekripsi serta menghasilkan cipher SMS yang lebih acak dan sulit dipahami oleh pihak lain.

Penelitian yang dilakukan oleh De Rosal Ignatius Moses Setiadi (2018) dengan judul Kombinasi Cipher Subtitusi (Beaufort Dan Vigenere) Pada Citra Digital. Riset tentang kriptografi pada citra terus berkembang. Banyak metode yang telah diterapkan pada kriptografi citra. Algoritma Vigenere merupakan algoritma yang cukup populer dan masih dikembangkan sampai saat ini. Vigenere memiliki kelebihan dalam komputasi yang cepat, dan kuat terhadap serangan. Beaufort cipher murupakan salah satu turunan dari algoritma Vigenere yang menggunakan operator pengurangan pada kunci. Penelitian ini mengusulkan kombinasi algoritma Beaufort dan Vigenere cipher dengan menggunakan dua kunci untuk meningkatkan

keamanan. Metode diusulkan dalam penelitian ini diimplementasikan untuk enkripsi pada citra digital dan diukur dengan nilai MSE, PSNR dan analisis histogram. Hasil pengukuran dari kombinasi kedua metode ini didapatkan kualitas enkripsi yang lebih baik dibandingkan dengan metode Beaufort atau Vigenere saja.

Penelitian yang dilakukan oleh Arios, Jesfer Robin (2018) dengan judul Implementasi Algoritma Kriptografi Beaufort Cipher dan Algoritma Kompresi Reverse Unary Code Pada File Citra. Adapun jenis data yang digunakan adalah file citra dengan format Bitmap (*. bmp) dan hasil akhir kompresi jika didekompresi hasilnya adalah sebuah file asli dengan ekstensi (*.bmp). Dalam percobaan yang dirancang belum mampu memampatkan ukuran citra dengan Algoritma Reverse Unary Code sehingga pembesaran file ketika melakukan proses enkripsi dengan Algoritma Beaufort Cipher, dimana metode ini menghasilkan Ratio of compression (Rc)rata-rata sebesar 7,48%, Compression ratio (CR) 557,72% dan Space Saving (SS) -452,78%

Penelitian yang dilakukan oleh Angga Aditya Permana (2018) dengan judul Penerapan Kriptografi Pada Teks Pesan dengan Menggunakan Metode Vigenere Cipher Berbasis Android. Perkembangan teknologi khususnya dalam bidang komunikasi antar manusia sudah sangat mudah dilakukan dengan telepon genggam dan fiturnya sangat bervariasi. Pertukaran informasi jarak jauh ini menuntut keamanan terhadap kerahasiaan informasi yang dipertukarkan. Oleh karena itu, metode kriptografi dilakukan untuk mengamankan informasi tersebut. Salah satu metode kriptografi untuk

penyandian teks adalah metode Vigenere Cipher. Penelitian ini bertujuan untuk membangun aplikasi kriptografi teks pesan pada smartphone berbasis android dengan metode Vigenere Cipher. Metode ini mengenkripsi teks pesan menjadi pesan rahasia yang kemudian hasilnya diteruskan sebagai teks pesan ke aplikasi pengiriman pesan seperti aplikasi SMS (Short Message Service), Whatsapp, Line, dan sejenisnya untuk selanjutnya didekripsi. Penelitian ini menghasilkan aplikasi berbasis android yang dapat mengirimkan teks pesan terenkripsi menggunakan metode Vigenere Cipher untuk memberikan keamanan lebih pada proses pertukaran informasi

I.6. Sistematika Penulisan

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

BAB I : PENDAHULUAN

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

BAB II : TINJAUAN PUSTAKA

Pada bab ini menerangkan tentang teori-teori dan metode yang berhubungan dengan topik yang dibahas atau permasalahan yang

sedang dihadapi yaitu berupa pembahasan mengenai sistem wireless.

BAB III : ANALISIS DAN PERANCANGAN

Pada bab ini mengemukakan tentang analisa sistem yang sedang berjalan, evaluasi sistem yang berjalan dan desain sistem secara detail.

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

Pada bab ini berisi kesimpulan penulisan dan saran dari penulis sebagai perbaikan di masa yang akan datang untuk sistem.