

# BAB I

## PENDAHULUAN

### 1.1 Latar Belakang

Teknologi komunikasi modern merupakan suatu teknologi yang memudahkan proses komunikasi dengan memanfaatkan alat digital. Misalnya seperti *Short Message Service* (SMS), *Multimedia Message Service* (MMS), *instant messaging* dan *email*. *Email* merupakan sarana komunikasi surat elektronik via internet yang mudah dan cepat dibandingkan dengan surat menyurat secara tradisional. Tetapi perkembangan teknologi informasi dan komunikasi semakin pesat, mobilitas penggunanya semakin tinggi, sehingga penggunaan *email* atau surat elektronik masih dianggap kurang efisien dan kurang praktis. Sebagai contoh, pengirim *email* tidak tahu apakah penerima *email* tersebut *online* atau tidak, sehingga si pengirim tidak tahu kapan *email* tersebut akan dibaca oleh si penerima *email*. Itu yang menyebabkan *email* belum sepenuhnya efisien dan cepat untuk digunakan pada zaman teknologi *mobile* yang terus berkembang ini.

Oleh karena itu, layanan *instant messaging* atau pesan instan menjadi lebih banyak digunakan karena dianggap memiliki banyak keunggulan dibandingkan dengan *email*. Beberapa keunggulan *instant messaging* adalah memungkinkan pengguna untuk mengirimkan pesan singkat secara langsung atau *real-time*, kemudahan akses yang diberikan dimana pengguna dengan perangkat *mobile* langsung bisa menggunakannya, dan aplikasinya bisa dipasang pada berbagai *platform* (*multi-platform*). Karena kelebihan-kelebihan itu juga *instant messaging* mampu meningkatkan produktifitas penggunanya.

Pesan yang dikirimkan dari pengguna satu ke pengguna lainnya rentan terhadap berbagai serangan jaringan. Pihak yang tidak bertanggung jawab bisa saja menyisipkan *url phishing*, *malicious code* atau memata-matai percakapan pengguna. Maka dari itu, keamanan menjadi faktor penting yang harus dipertimbangkan. Perangkat keamanan data yang melintas di jaringan publik harus disediakan untuk melindungi data dari akses, pengubahan, dan penghalangan yang dilakukan oleh orang tidak berwenang. Teknik kriptografi merupakan salah satu solusi yang dibutuhkan untuk

mengamankan data dengan mengenkripsi data atau dokumen tersebut sehingga menjadi tidak terbaca.

Vigenere merupakan salah satu teknik kriptografi yang populer di zamannya. Data awal (*plain*) yang melewati proses enkripsi vigenere akan menjadi data samar (*cipher*) yang tidak akan bisa dibaca kecuali dibongkar atau didekripsi menggunakan kata sandi atau kunci yang sudah ditentukan. Kunci yang digunakan oleh vigenere adalah kunci simetrik.

Berdasarkan pemaparan diatas, fokus tugas akhir ini adalah melakukan penelitian mengenai implementasi kriptografi pada aplikasi *instant messaging* pada *platform* Android menggunakan algoritma kriptografi Vigenere *cipher* yang telah dimodifikasi. Berbasis Android karena sistem operasi ini memiliki banyak pengguna dan bersifat *open source*. Aplikasi ini tidak hanya bisa melakukan personal chat saja tetapi juga grup chat. Aplikasi messaging tersebut akan diperkuat menggunakan algoritma Vigenere cipher yang dimodifikasi untuk mendapatkan layanan dan keamanan yang lebih baik. [5]

## **1.2 Perumusan Masalah**

Berdasarkan latar belakang masalah yang telah dipaparkan diatas, maka penulis merumuskan permasalahan pada penelitian ini adalah bagaimana menerapkan sistem kriptografi modifikasi pada aplikasi *instant messaging* di sistem operasi Android untuk mengamankan komunikasi antar pengguna.

## **1.3 Tujuan dan Manfaat**

### **1.3.1 Tujuan**

Adapun tujuan dari penelitian skripsi ini yaitu mengamankan pesan menggunakan kriptografi modifikasi Vigenere pada aplikasi *instant messaging* di sistem operasi Android.

### **1.3.2 Manfaat**

Dan manfaat yang diharapkan dari penelitian ini adalah sebagai berikut:

1. Meningkatkan keamanan aliran data pesan yang dikirim.
2. Melindungi privasi percakapan antar pengguna.
3. Memahami teknik keamanan data pada jaringan komunikasi yang sedang berkembang.

## **1.4 Batasan Masalah**

Dalam penelitian ini, untuk membatasi permasalahan agar tetap terarah dan tidak menyimpang dari apa yang sudah direncanakan sebelumnya maka penulis membuat batasan-batasan masalah sebagai berikut:

1. Algoritma enkripsi dan dekripsi menggunakan Vigenere *cipher* yang dimodifikasi.
2. Ruang lingkup pengujian dilakukan pada jaringan lokal dengan 1 *server* dan beberapa klien (Android).
3. Aplikasi ini hanya mengirim dan menerima pesan berbasis teks.

## **1.5 Metodologi Penelitian**

Penelitian ini menerapkan jenis metode penelitian bersifat eksperimen. Metode eksperimen yang diterapkan oleh penulis berdasarkan pada langkah-langkah berikut:

1. Tahap Observasi  
Peneliti melakukan pengamatan dan mengidentifikasi masalah-masalah yang telah terjadi kemudian menjadikannya sebagai

acuan rumusan masalah. Selain itu peneliti juga mengumpulkan data-data yang diperlukan dan referensi-referensi yang relevan untuk diolah menjadi dasar teori.

2. Tahap Rancangan sistem  
Pada tahap ini peneliti menganalisis permasalahan yang berkaitan dengan judul kemudian membuat rancangan sistem. Rancangan tersebut merupakan gambaran umum dari sistem yang akan dibangun.
3. Tahap Implementasi sistem  
Peneliti menerapkan implementasi dari rancangan sistem yang telah dibuat. Proses implementasi membutuhkan beberapa perangkat pendukung yang telah ditentukan untuk mendapatkan hasil yang sesuai.
4. Tahap Uji coba dan evaluasi  
Setelah itu, peneliti melakukan pengujian dan evaluasi dari hasil yang didapat dari implementasi kriptografi pada aplikasi *instant messaging* Android menggunakan modifikasi algoritma vigenere *cipher*.
5. Tahap Penyusunan Laporan  
Terakhir, peneliti melakukan penulisan atau dokumentasi tahap demi tahap dari proses hingga hasil yang didapat dari observasi sampai pengujian dari kriptografi pada aplikasi *messaging* Android menggunakan modifikasi vigenere *cipher*.

## **1.6 Sistematika Penulisan**

Sistematika penulisan tugas akhir ini adalah sebagai berikut:

### **BAB I : PENDAHULUAN**

Pada bab ini terdiri dari: latar belakang, penegasan dan alasan pemilihan judul, perumusan masalah, tujuan dan manfaat, batasan masalah, metodologi penelitian serta sistematika penulisan.

### **BAB II : STUDI PUSTAKA**

Pada bab ini dipaparkan penelitian terdahulu dan teori-teori pendukung yang berhubungan dengan kriptografi, *instant messaging*, dan Android.

### **BAB III : PERANCANGAN SISTEM**

Pada bab ini dijelaskan analisis kebutuhan sistem, desain dan perancangan sistem dalam implementasi kriptografi modifikasi Vigenere *cipher* pada *instant messaging* sistem operasi Android

### **BAB IV : IMPLEMENTASI SISTEM**

Pada bab ini menjelaskan tentang implementasi sistem berdasarkan rancangan yang telah dibuat pada BAB III, yang kemudian dilakukan tahap uji coba pada sistem.

### **BAB V : PENUTUP**

Pada bab ini peneliti memberikan kesimpulan dari hasil uji coba dan saran yang sekiranya bisa dimanfaatkan pada pengembangan selanjutnya.

*(Halaman ini sengaja dikosongkan)*