

BAB I

PENDAHULUAN

1.1. Latar Belakang

Informasi merupakan hal yang sangat penting dalam segala aspek kehidupan manusia di era yang modern ini. Peran informasi akan semakin krusial apabila dapat dipergunakan dan diolah dengan baik, sehingga banyak aspek yang sangat terkait pada peran informasi. Oleh sebab itu, dibutuhkan sebuah metode pertukaran informasi yang efektif dan efisien.

Pada perkembangannya, telah banyak sarana pertukaran informasi yang dikembangkan, salah satunya adalah aplikasi *messenger* yang dapat diterapkan di berbagai *platform* dan perangkat. Namun permasalahan yang timbul kemudian adalah kurangnya jaminan terhadap keamanan dan kerahasiaan pesan yang berisi informasi – informasi tersebut. Sehingga sering terjadi pembajakan pesan oleh pihak – pihak yang tidak bertanggung jawab yang menyebabkan bocornya informasi penting yang menimbulkan kerugian bagi pihak tertentu.

Metode kriptografi merupakan salah satu cara untuk mengamankan informasi yang dikirimkan melalui pesan. Dengan menerapkan algoritma kriptografi dalam proses pengiriman pesan pada aplikasi *messenger*, maka hanya penerima pesan yang mengetahui kata kunci yang dapat menerjemahkan pesan yang berisi informasi tersebut, sehingga informasi yang terdapat dalam pesan tersebut aman dan

mengurangi resiko pembajakan. Dengan metode ini diharapkan kemungkinan bocornya informasi dapat diminimalisir sehingga keamanan informasi tersebut lebih terjamin. Hal ini melatar belakangi penelitian tentang cara penerapan algoritma kriptografi *Slide Cipher* pada aplikasi *messenger*.

1.2. Rumusan Masalah

Rumusan masalah berdasarkan latar belakang yang telah diuraikan adalah :

1. Apakah metode enkripsi dengan memanfaatkan algoritma kriptografi *Slide Cipher* dapat diterapkan dalam proses pengiriman pesan pada aplikasi Chat-Ok Messenger?
2. Apakah proses enkripsi dan dekripsi pesan pada aplikasi Chat-Ok Messenger dapat mudah dilakukan oleh pengguna?
3. Apakah proses enkripsi yang dilakukan pada pesan tidak merubah nilai informasi yang dikirimkan setelah dilakukan proses dekripsi?

1.3. Batasan Masalah

Batasan permasalahan yang dibahas pada penelitian ini meliputi :

1. Perancangan dan pembuatan algoritma kriptografi *Slide Cipher*.
2. Rancang bangun dan gambaran umum aplikasi Chat-Ok Messenger.
3. Penerapan algoritma *Slide Cipher* pada aplikasi Chat-Ok Messenger.
4. Pengujian aplikasi Chat-Ok Messenger untuk pengiriman pesan yang terenkripsi.

5. Algoritma kriptografi pembanding yang digunakan pada penelitian ini adalah algoritma *Caesar Cipher*.
6. Tahap perancangan dan pembuatan aplikasi Chat-Ok Messenger yang dibahas dalam penelitian ini hanya bagian - bagian utama yang berhubungan langsung dengan proses implementasi algoritma kriptografi meliputi representasi algoritma kriptografi kedalam bahasa pemrograman, pembuatan fungsi *encrypt* dan *decrypt*, pembuatan fungsi pengiriman pesan, dan pembuatan fungsi untuk menampilkan pesan. Detail perancangan dan pembuatan yang tidak berhubungan langsung dengan implementasi algoritma kriptografi tidak dibahas pada penelitian ini.
7. Fitur yang dibuat pada *prototype* aplikasi Chat-Ok Messenger meliputi pengiriman pesan, penerimaan pesan, enkripsi pesan, dekripsi pesan, update status, update informasi pengguna dan tambah pengguna.
8. Penelitian ini tidak membahas performa dan kecepatan pengiriman data pada aplikasi Chat-Ok Messenger.
9. Aplikasi Chat-Ok Messenger yang digunakan sebagai obyek implementasi pada penelitian ini masih bersifat *prototype*.

1.4. Maksud dan Tujuan Penelitian

Maksud dan tujuan dari penelitian ini antara lain :

1. Untuk mengembangkan algoritma kriptografi baru yang dikembangkan dari algoritma yang sudah ada sebelumnya.

2. Untuk menguji apakah algoritma kriptografi yang dibuat dapat diterapkan dalam proses pengiriman pesan pada aplikasi *messenger*.
3. Sebagai syarat kelulusan program studi strata 1 jurusan Teknik Informatika di STMIK AMIKOM YOGYAKARTA untuk memperoleh gelar Sarjana (S.Kom) :

1.5. Metode Penelitian

1.5.1. Metode Pengumpulan Data

Metode yang digunakan dalam pengumpulan data – data terkait dengan penelitian. Metode yang digunakan dalam penelitian ini adalah :

1.5.1.1. Metode Studi Pustaka

Metode ini dilakukan untuk mendapatkan informasi dari pustaka berupa referensi, jurnal, atau penelitian sebelumnya yang berkaitan dengan kriptografi.

1.5.2. Metode Analisis

Metode analisis yang digunakan dalam penelitian ini adalah :

1. Analisis SWOT

Analisis ini meliputi 4 aspek analisis, yaitu *Strenght, Weakness, Opportunity, Threat*.

Analisis ini yang akan digunakan dalam penelitian ini.

1.5.3. Metode Perancangan

Metode perancangan yang digunakan dalam proses penelitian adalah ERD, Relasi Antar Tabel, dan DFD.

1.5.4. Metode Pengembangan

Metode pengembangan yang dilakukan meliputi beberapa *step*, yaitu :

1. Perancangan dan pembuatan algoritma kriptografi *Slide Cipher*.
2. Perancangan dan pembuatan *prototype* aplikasi Chat-Ok Messenger.
3. Penerjemahan algoritma kriptografi *Slide Cipher* kedalam bahasa pemrograman untuk membuat fungsi enkripsi dan dekripsi.
4. Implementasi fungsi enkripsi dan dekripsi pada aplikasi Chat-Ok Messenger.
5. Pengujian aplikasi dan proses pengiriman pesan.

1.5.5. Metode Testing

Metode testing yang digunakan pada penelitian ini adalah :

1. Whitebox Testing

Pengujian dengan melihat kedalam modul untuk meneliti kode – kode program yang ada, lalu menganalisis apakah ada kesalahan atau tidak. Jika terdapat modul yang menghasilkan output yang tidak sesuai, maka baris – baris program, parameter, dan variabel yang terlibat akan dianalisa dan dicek satu persatu, diperbaiki, lalu dicompile ulang.

2. Blackbox Testing

Pengujian yang menitik beratkan pada keperluan fungsionalitas dari software yang dibuat. Pengujian ini digunakan untuk melengkapi pengujian yang telah dilakukan pada whitebox testing untuk menemukan kesalahan lainnya yang belum ditemukan pada whitebox testing.

1.5.6. Sistematika Penulisan

Bab I – Pendahuluan, bab ini berisi tentang latar belakang masalah, rumusan masalah, batasan masalah, maksud dan tujuan penelitian, metode penelitian, dan sistematika penulisan.

Bab II – Landasan Teori, menguraikan teori - teori yang mendasari pembahasan beserta tinjauan pustaka.

Bab III – Analisis dan Perancangan, berisi tentang analisis data yang telah dikumpulkan, perancangan algoritma kriptografi, dan perancangan aplikasi *messeger* yang digunakan. Selain itu juga berisi cara pengimplementasian algoritma kriptografi pada aplikasi *messenger* yang dibuat.

Bab IV – Implementasi dan Pembahasan, bab ini berisi tentang pengujian aplikasi yang dibuat, serta pembahasan dari fungsi - fungsi serta fitur yang terkait.

Bab V – Penutup, berisi kesimpulan dan saran yang dapat diambil dari hasil penelitian yang telah dilakukan.

DAFTAR PUSTAKA