BAB I

PENDAHULUAN

1.1. Latar Belakang

Masalah keamanan data merupakan suatu aspek penting dalam pengiriman data maupun informasi melalui jaringan. Hal ini disebabkan karena kemajuan di bidang jaringan computer dengan konsep *open system*-nya, sehingga memudahkan seseorang untuk masuk ke dalam jaringan tersebut. Hal tersebut dapat mengakibatkan proses pengiriman data menjadi tidak aman dan dapat dimanfaatkan oleh orang maupun pihak lain yang tidak bertanggungjawab untuk mengambil data maupun informasi di tengah jalan. Oleh karena itu, dibutuhkan suatu sistem keamanan data yang dapat menjaga kerahasiaan suatu data maupun informasi.

Dalam hal teknik pengamanan data, banyak metoda kriptografi yang dapat digunakan. Metode – metode kriptografi tersebut mempunyai teknik dan cara tersendiri. Langkah – langkah pengerjaan setiap metode pun berbeda – beda, baik dari segi panjang maupun kerumitan. Salah satu metoda kriptografi yang menarik untuk dipelajari adalah metode WAKE (*Word Auto Key Encryption*). Metode WAKE merupakan salah satu algoritma *stream cipher* yang telah digunakan secara komersial. Metode ini ditemukan oleh David J. Wheeler. Metode WAKE memiliki kelebihan dibandingkan metode lain karena dalam proses pembentukan

kunci terdapat beberapa putaran yang bersifat fleksibel dan berbeda-beda dalam setiap putaran. (Ridho, 2008)

Berdasarkan uraian diatas, maka dalam tugas akhir ini membahas bagaimana kinerja dari algoritma WAKE dalam proses enkripsi dan dekripsi data teks serta dibuat suatu program untuk melakukan proses enkripsi dan dekripsi data teks menggunakan bahasa pemrograman Visual Basic 6.0.

1.2. Perumusan Masalah

Berdasarkan latar belakang yang diuraikan di atas, didapat suatu permasalahan yaitu bagaimana membuat suatu perangkat lunak enkripsi-dekripsi dengan metode WAKE menggunakan bahasa pemrograman Visual Basic 6.0.

1.3. Tujuan dan Manfaat

Tujuan penyusunan tugas akhir ini adalah untuk merancang suatu perangkat lunak enkripsi-dekripsi dengan menggunakan kriptografi WAKE yang dapat digunakan dalam hal pengamanan data teks agar tidak diakses oleh pihak yang tidak berhak.

Manfaaat dari aplikasi yang dibuat untuk memudahkan bagi siapa saja yang ingin melindungi datanya agar tidak dapat dibaca oleh pihak-pihak yang tidak berhak mengaksesnya.

1.4. Pembatasan Masalah

Dalam perancangan perangkat lunak dibatasi oleh :

1. Input data berupa file berjenis teks dengan ekstensi .txt.
2. Aplikasi ini mensimulasikan proses enkripsi-dekripsi dengan metode WAKE.
3. Panjang kunci 128 bit
4. Aplikasi dibuat menggunakan bahasa pemrograman Visual Basic 6.0.

1.5. Metodologi Penelitian

Metodologi yang digunakan dalam penulisan tugas akhir ini adalah studi pustaka, yaitu pengumpulan data dengan cara mengumpulkan literature, jurnal dan bacaan-bacaan yang berkaitan dengan metode kriptografi WAKE.

1.6. Sistematika Penulisan

Tugas Akhir ini terdiri dari 4 bab dan beberapa subbab.

Bab I pendahuluan menguraikan tentang latar belakang permasalahan, mencoba merumuskan inti permasalahan yang dihadapi, menentukan tujuan dan kegunaan penelitian, yang kemudian diikuti dengan pembatasan masalah, asumsi, serta sistematika penulisan. Bab II landasan teori membahas berbagai konsep dasar dan teori-teori yang berkaitan dengan topik penelitian yang dilakukan dan hal-hal yang berguna dalam proses analisis permasalahan serta tinjauan terhadap penelitian-penelitian serupa yang telah pernah dilakukan sebelumnya termasuk sintesisnya. Bab III Menganalisis masalah dari model penelitian untuk memperlihatkan keterkaitan antar variabel yang diteliti serta model matematis untuk analisisnya. Bab IV merupakan tahapan yang dilakukan dalam penelitian secara garis besar sejak dari tahap persiapan sampai penarikan kesimpulan,

metode dan kaidah yang diterapkan dalam penelitian. Termasuk menentukan variabel penelitian, identifikasi data yang diperlukan dan cara pengumpulannya, penentuan sampel penelitian dan teknik pengambilannya, serta metode/teknik analisis yang akan dipergunakan dan perangkat lunak yang akan dibangun jika ada. Bab V berisi kesimpulan dan saran yang sudah diperoleh dari hasil penulisan tugas akhir.