BAB I
Pendahuluan

1.1 Latar Belakang

Saat ini, kemajuan teknologi informasi sedang berkembang dengan pesat yang memungkinkan setiap orang dapat berkomunikasi dari suatu tempat ke tempat lain yang berjarak ribuan kilometer dengan berbagai media dan berbagai macam bentuk pengiriman data. Data yang disimpan atau dikirim sebaiknya tidak mudah dibaca oleh semua orang. Sistem keamanan seharusnya dapat meningkatkan keamanan data para penggunanya. Data tersebut biasanya disimpan dalam suatu sistem yang disebut dengan sistem basis data. Basis data merupakan sekumpulan data yang saling terintegrasi satu sama lain dan terorganisasi berdasarkan skema atau struktur tertentu dan tersimpan pada sebuah perangkat keras komputer (Arief 2005).

Dalam perkembangan teknologi, sistem basis data telah menjadi simbol dari salah satu bentuk aset yang paling berharga. Basis data digunakan secara luas untuk berbagai bidang seperti perbankan, pendidikan, kepegawaian dan lain-lain. Dengan semakin luasnya penggunaan sistem basis data pada suatu sistem informasi, perlin-dungan terhadap informasi yang disimpan di dalamnya menjadi sangat diperlukan dari berbagai ancaman diantaranya pembaca data, manipulasi data dan perusakan data oleh pihak yang tidak berkepentingan (Suhendra 2012).

Data yang dikirim menggunakan jalur transmisi telekomunikasi belum tentu terjamin keamanannya. Keamanan dan kerahasiaan data merupakan salah satu aspek yang sangat penting dalam sistem informasi karena pesatnya perkembangan ilmu pengetahuan dan teknologi saat ini memungkinkan munculnya teknik-teknik baru yang disalah gunakan oleh pihak-pihak tertentu yang mengancam keamanan dari sistem informasi tersebut. Jatuhnya informasi ke tangan pihak lain dapat menimbulkan kerugian bagi pemilik informasi.

Secara umum data dikategorikan menjadi dua yaitu data yang bersifat rahasia dan data yang tidak bersifat rahasia. Data yang bersifat rahasia biasanya tidak akan terlalu diperhatikan. Yang sangat perlu diperhatikan data yang bersifat rahasia, dimana setiap informasi yang ada didalamnya akan sangat berharga bagi pihak yang membutuhkan karena data tersebut dengan mudah digandakan. Untuk mendapat

informasi didalamnya biasanya dilakukan berbagai cara yang tidak sesuai aturan (Hasugian 2013). Contoh data yang bersifat rahasia adalah data kepegawaian di suatu instansi tertentu yang dapat disalah gunakan untuk tujuan yang bersifat negatif misalnya untuk tujuan kejahatan, pemalsuan data dan lain-lain.

Berdasarkan pada permasalahan tersebut, muncul suatu gagasan yaitu untuk membuat suatu sistem keamanan yang dapat melindungi data penting dengan penyandian data, sehingga sulit untuk dideteksi oleh pihak yang tidak berke-pentingan. Salah satu cara untuk menjaga kerahasiaan data yang dikirim antara pihak satu dengan yang lainnya adalah dengan konsep penyandian yang disebut dengan kriptografi. Kriptografi merupakan seni dalam menyimpan atau merahasiakan data dari penerima yang tidak berkepentingan. Dalam hal ini data asli dari pengirim disebut dengan plaintext, sedangkan data yang disembunyikan disebut dengan ciphertext. Proses untuk membuat sandi dari data aslinya disebut dengan enkripsi, sedangkan proses untuk membaca kembali data yang telah disandikan disebut dengan deskrpsi.

Banyak teknik kriptografi yang telah dipergunakan untuk menjaga keamanan data saat ini, contohnya seperti LOKI, GOST, Blowfish, Vigenere, MD2, MD3, MD4, MD5, RSA dan lain sebagainya. Masing-masing teknik kriptografi tersebut memiliki kelebihan dan kelemahan. Selain teknik kriptografi yang telah disebut di atas masih terdapat teknik kriptografi lainnya yaitu teknik kriptografi Hill cipher. Metode Algoritma Hill Cipher termasuk algoritma kriptografi klasik yang sulit dipecahkan oleh kriptanalis apabila dilakukan dengan mengetahui berkas ciphertext saja. Hill Cipher tidak mengganti setiap abjad yang sama pada plaintext dengan abjad lainnya yang sama pada ciphertext karena menggunakan perkalian matriks dasar enkripsi dan deskripsinya (Setyaningsih 2015). Untuk semakin meningkatkan keamanan penyandian data maka penulis menggabungkan metode enkripsi algoritma Hill Cipher dengan menggunakan kode ASCII (American Standart Code for Information Interchange) dengan memanfaatkan digit desimal bilangan Euler sebagai kunci dasar untuk proses enkripsi dan deskripsinya.

Berdasarkan uraian di atas, penulis tertarik untuk melakukan penelitian dengan judul Implementasi Algoritma Hill Cipher dalam Penyandian Data Menggunakan Kode ASCII Memanfaatkan Digit Desimal Bilangan Euler.

1.2 Rumusan Masalah

Berdasarkan latar belakang masalah yang telah dikemukakan di atas dan judul yang dipilih maka yang menjadi rumusan masalah yaitu:

1. Bagaimana cara mengimplementasikan algoritma Hill Cipher pada database dosen Jurusan Matematika dengan menggunakan kode ASCII?
2. Bagaimana manfaat penggunaan kode ASCII dalam proses penyandian data?
3. Bagaimana manfaat digit desimal bilangan Euler pada algoritma Hill Cipher pada penyandian data?
4. Bagaimana pengaruh pemilihan matriks kunci terhadap proses enkripsi dan deskripsi data?
5. Bagaimana metode algoritma kriptografi Hill Cipher bisa diimplemen-tasikan terhadap studi kasus yang lain?

1.3 Batasan Masalah

Agar permasalahan tidak menyimpang dari maksud dan tujuan yang diharapkan, maka dibuat beberapa pembatasan masalah antara lain:

1. Data yang diproses adalah data personil dosen Jurusan Matematika Unimed golongan IV/e diperoleh dari bagian Kepegawaian Biro Admin-istrasi Umum dan Keuangan Universitas Negeri Medan.
2. Metode yang digunakan pada algoritma Hill Cipher menggunakan kunci matriks 2 x 2.
3. Pemilihan elemen matriks kunci yang digunakan, yaitu matriks yang menghasilkan Identitas jika matriks kunci dikuadratkan kemudian dimodulo 97.
4. Menggunakan tabel kode ASCII manipulasi teks modulo 97.
5. Entri-entri matriks kunci sebagai dasar enkripsi dan deskripsi yang digunakan berdasarkan digit desimal bilangan Euler yang dihitung oleh Sebastian Wedeniwski.

1.4 Tujuan Penelitian

Adapun tujuan yang hendak dicapai dalam penelitian ini adalah sebagai berikut:

1. Untuk mengimplementasikan algoritma Hill Cipher pada data personil dosen Jurusan Matematika golongan IV/e dengan menggunakan kode ASCII.
2. Untuk mengetahui manfaat kode ASCII pada proses penyandian data.
3. Untuk mengetahui pemanfaatan digit desimal bilangan Euler dalam matriks kunci pada algoritma Hill Cipher pada penyandian data.
4. Mengetahui pengaruh pemilihan matriks kunci terhadap proses enkripsi dan deskripsi data.
5. Agar metode kriptografi Hill Cipher bisa diimplementasikan terhadap studi kasus yang lain.

1.5 Manfaat Penelitian

Adapun manfaat yang diharapkan dari penelitian ini sebagai berikut:

1. Memiliki wawasan terhadap pengaplikasian matematika yaitu operasi matriks pada penyandian data dengan metode kriptografi Hill Cipher.
2. Mengetahui cara mengimplementasikan metode Hill Cipher dengan kode ASCII terhadap studi kasus yang lain.
3. Dapat menyembunyikan data yang bersifat rahasia sehingga tidak bisa digunakan terhadap pengguna yang tidak berkepentingan.