. .


UNIVERSITAS ANDALAS
UNTUK
KEDJAJAAN
BANGSA

BAB I

PENDAHULUAN

1.1 Latar Belakang

Matriks adalah susunan jajaran empat persegi panjang dengan entri-entri tertentu dalam suatu himpunan bilangan. Terdapat beberapa operasi dalam matriks, seperti penjumlahan (pengurangan) matriks, perkalian matriks dan perkalian skalar dengan matriks. Pada matriks juga dapat dilakukan operasi baris yang dikenal dengan operasi baris elementer.

Salah satu aplikasi matriks yang dapat digunakan untuk menterjemahkan suatu pesan yaitu Kriptografi. Kriptografi berasal dari bahasa Yunani *cryptos* yaing artinya *secret* (rahasia) dan *graphein* yang artinya *writing* (tulisan). Jadi kriptografi berarti *secret writing* (tulisan rahasia). Ada beberapa definisi kriptografi yang telah dikemukakan diberbagai literatur antara lain; Kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan [9]. Kata seni di dalam definisi di atas berasal dari fakta sejarah bahwa pada masa-masa awal sejarah kriptografi, setiap orang mungkin mempunyai cara yang unik untuk merahasiakan pesan. Cara-cara unik tersebut berbeda-beda pada setiap pelaku kriptografi sehingga setiap cara menulis pesan rahasia, pesan mempunyai nilai estetika tersendiri sehingga kriptografi berkembang menjadi sebuah seni merahasiakan pesan.

Pada skripsi ini akan dijelaskan bagaimana penggunaan matriks dalam menterjemahkan suatu pesan. Pesan-pesan diterjemahkan dengan huruf-huruf lain dengan menggunakan matriks dan operasi pada matriks.

Matriks yang digunakan adalah matriks nonsingular dengan entri-entri pada himpunan bilangan bulat modulo 26. Hal ini dilakukan karena adanya pengkodean huruf alphabet yang berjumlah 26 buah dengan urutan 0 sampai 25. Pada skripsi ini juga akan diberikan proses operasi baris elementer yang dilakukan pada matriks dengan entri-entri di himpunan bilangan bulat modulo 26. Operasi baris elementer ini digunakan pada penentuan invers matriks tersebut.

1.2 Perumusan Masalah

Berdasarkan matriks nonsingular yang diberikan, maka perumusan masalah dalam skripsi ini adalah bagaimana menerjemahkan suatu pesan menjadi suatu kode dengan menggunakan metode *ChiperHill* atas matriks bilangan modulo 26, dan mengubah kode-kode menjadi pesan yang sebenarnya menggunakan metode *Dechiper* atas matriks bilangan modulo 26.

1.3 Tujuan Penelitian

Adapun tujuan dari tulisan ini adalah :

1. Menjelaskan metode *ChiperHill* atas bilangan bulat modulo 26 untuk mengubah suatu pesan menjadi kode-kode tertentu.

2. Menjelaskan metode *Dechiper* atas bilangan bulat modulo 26 untuk mengubah kode-kode menjadi pesan yang sebenarnya.

1.4 Sistematika Penulisan

Sistematika penulisan tugas akhir ini terdiri dari empat bab, yaitu : BAB I Pendahuluan, memberikan gambaran singkat tentang latar belakang, rumusan masalah, batasan masalah, tujuan penelitian, dan sistematika penulisan. BAB II Landasan Teori, membahas tentang teori-teori sebagai dasar acuan dalam pembahasan. BAB III Menjelaskan cara penerjemahkan suatu pesan atas matriks dengan entri-entri bilangan modulo 26 dengan menggunakan metode *ChiperHill* dan *Dechiper*. BAB IV Kesimpulan dari hasil pembahasan.

DAFTAR PUSTAKA

[1] Anton, H. dan Rorres, C. 2004. *Aljabar Linear Elementer; edisi ke-8*. Erlangga, Jakarta.

[2] Burton, David M. 2007. *Elementary Number Theory, Sixth Edition*. The Tim McGraw-Hill Companies, Inc. New York.

[3] Eisenberg, Murray. 1998. *Hill Ciphers and Modular Linear Algebra*. University of Massachusetts Amherst, United States.

[4] Grillet, Pierre Antoine. 2007. *Abstract Algebra*. Springer, New York.

[5] Menezes, Oorcshot and Vanstone. 1996. *Handbook of Applied Chryptography*. CRC Press, Inc. USA.

[6] Mishra, A. 2013. *Security of Caesar Cipher Using Different Methods*. IJRET. India. 2, 327-332.

[7] Muhsetyo, Gatot. 1997. *Dasar Dasar Teori Bilangan*. Debdikbud, Jakarta.

[8] Munir, Rinaldi. 2006. *Kriptografi*. Informatika Bandung. Bandung.

[9] Scheneier, Bruce. 1996. *Applied Cryptography Second Edition: Protocol, Algorithm, and Source Code in C*. John Wiley and Son, Inc.