. .


UNIVERSITAS ANDALAS
UNTUK
KEDJAJAAN
BANGSA

BAB I

KESIMPULAN

Pada tugas akhir ini telah dibahas bagaimana menterjemahkan suatu pesan menjadi suatu kode dengan menggunakan *Chiper Hill* atas matriks bilangan modulo 26, dan mengubah kode-kode menjadi pesan sebenarnya menggunakan metode *Dechiper* atas matriks bilangan modulo 26.

Adapun langkah-langkah pengkodean menggunakan metode *Chiper Hill* (*Chiper* $n - Hill$) terhadap bilangan bulat modulo m adalah sebagai berikut:

1. Pilih sebuah matriks A berukuran $n \times n$ dengan entri bilangan bulat pada modulo m untuk melakukan pengkodean.

2. Kelompokkan setiap n buah huruf *plaintext* yang berurutan, misalkan setiap kelompok terdiri dari $p_1, p_2, \cdots, p_n$ huruf. Jika *plaintext* tidak dapat dibagi menjadi n kelompok, maka harus ditambahkan huruf khayalan (*dummy*) untuk menggenapi kelompok huruf terakhir, dan gantilah tiap huruf *plaintext* dengan huruf numeriknya.

3. Berdasarkan urutan huruf *plaintext* yang telah dikelompokkan, ubahlah tiap pasangan *plaintext* $p_1 \cdots p_n$ menjadi sebuah vektor kolom $p = \begin{bmatrix} p_1 \\ \vdots \\ p_n \end{bmatrix}$.

4. Bentuklah suatu perkalian dari matriks yang telah ditentukan sebelumnya dengan vektor kolom p menggunakan prinsip perkalian modulo m, yang disebut dengan vektor *chipertext* yang berhubungan.

5. Ubah tiap verktor menjadi abjad yang ekivalennya sehingga membentuk sebuah *chipertext*.

Sedangkan langkah-langkah pengkodean menggunakan metode *Dechiper* hampir sama dengan langkah-langkah pada metode *Chiper Hill*, yang membedakan hanya langkah pertama yaitu menginverskan matriksnya terlebih dahulu.

1. Pilih sebuah matriks $n \times n$ dengan entri bilangan bulat, A = $[a_{ij}]$, i= 1,2, $\cdots, n$ dan $j = 1, 2, \cdots, n$, lalu carilah inversnya.

2. Kelompokkan setiap n buah huruf *chipertext* yang berurutan, misalkan setiap kelompok terdiri dari $c_1, c_2, \cdots, c_n$ huruf. Jika *chipertext* berjumlah ganjil maka harus ditambahkan huruf khayalan (*dummy*) untuk menggenapi pasangan huruf terakhir, dan gantilah tiap huruf *chipertext* dengan huruf numeriknya.

3. Secara berurutan, ubahlah tiap pasangan *chipertext* $c_1 \cdots c_n$ menjadi sebuah vektor kolom $c = \begin{bmatrix} c_1 \\ \vdots \\ c_n \end{bmatrix}$.

4. Bentuklah suatu perkalian $A^{-1}c$ dengan menggunakan prinsip perkalian modulo m, yang disebut dengan vektor *plaintext* yang berhubungan.

5. Ubah tiap verktor menjadi abjad yang ekivalennya sehingga membentuk sebuah *plaintext*.

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.