PENGAMANAN PESAN RAHASIA MENGGUNAKAN METODE ALGORITMA HILL CIPEHR

Riski Trinanda Tarigan
[1]STMIK Kristen Neumann Indonesia Jl. Letjen Jamin Ginting KM. 10,5 Medan
Riskitarigan45@gmail.com

Program Studi Teknik Informatika

ABSTRAK

Hill Cipher merupakan salah satu algoritma kriptografi yang memanfaatkan matriks sebagai kunci untuk melakukan enkripsi dan dekripsi dari aritmatika modulo. Setiap karakter pada plainteks ataupun cipherteks di konversikan ke dalam bentuk angka. Enkripsi dilakukan dengan mengalikan matriks kunci dengan matriks plainteks, sedangkan dekripsi delakukan dengan megalikan invers matriks kunci dengan matriks cipherteks. Karna itulah, hill cipher hanya bisa menggunakan matriks persegi sebagai matriks kuncinya. Invers semu atau pseudo dapat dimanfaatkan pada algoritma hill cipher, sehingga matriks kunci yang digunakan tidak terbatas pada matriks persegi saja. Penggunaan matriks persegi panjang menjadikan cipherteks lebih panjang dari plainteks. Hal ini tentunya membuat pesan menjadi lebih tersamarkan. Pada tulisan ini, penulis menggunakan modulo 26 artinya inputan data ada 26 simbol. Untuk mempermudah perhitungan pada saat inisialisasi matriks kunci, proses enkripsi dan proses dekripsi menggunakan program Microsoft visual studio 2010.

Kata Kunci: Kriptografi, enkripsi, Dekripsi, Hill Cipher yang diperluas

1. PENDAHULUAN

Keamanan data kini menjadi hal penting yang harus dipertahankan pada era digital. Banyak pihak tidak berwenang yang berusaha mencuri akses terhadap suatu data milik orang lain tanpa izin. Dalam mengirim data, terutama yang bersifat rahasia, data tersebut harus terlebih dahulu diamankan dengan memakai metode kriptografi sebelum dikirimkan. Hal ini dilakukan untuk mencegah orang yang tidak berhak dan tidak berkepentingan untuk mencuri, membuka ataupun mengganti isi dari data yang dikirim.

Kini, metode kriptografi telah berkembang dan memiliki banyak jenisnya. Setiap metode ini memiliki cara yang berbeda dalam mengenkripsi data, serta memiliki kelebihan dan kekurangan tersendiri. Metode dalam kritografi klasik memberikan gambaran awal mengenai proses enkripsi dan dekripsi secara mendasar. Namun, pembelajaran kriptografi pada perkuliahan lebih mengarah kepada teoritis, karena kurangnya aplikasi yang bisa secara langsung mengajarkan kriptografi klasik. Proses belajar mengajar untuk kriptografi klasik hanya melalui penjelasan lisan dan tulisan tanpa ada perangkat lunak yang mendampingi pembelajaran topik tersebut.

Manfaat dari penelitian ini adalah untuk merancang suatu sarana atau aplikasi pembelajaran kriptografi klasik sehingga memudahkan staf pengajar/dosen untuk menjelaskan teknik-teknik kriptografi klasik kepada mahasiswa. Selain itu aplikasi yang dirancang dapat memperkaya materi ajar dalam mata kuliah Kriptografi maupun Keamanan Komputer

Untuk mengamankan file data yang akan di simpan maupun yang akan dikirim. Maka dengan itu data atau file yang sudah disandikan atau dienkripsikan tidak akan mudah atau tidak akan dimengerti pihak lain tanpa melakukan dekripsi data. Kriptografi berbasis pada algoritma pengkodean data informasi yang mendukung kebutuhan dari dua aspek informasi, yaitu *secrecy* (perlindungan terhadap pemalsuan dan pengubahan informasi yang tidak diinginkan).

Kriptografi dan enkripsi sangat dibutuhkan dalam pengamanan file. Dengan adanya kriptografi, data atau informasi yang dikirim dapat terhindar dari pembajakan, penghapusan, dan penyubtitusian yang dilakukan oleh user yang tidak berhak. Dalam hal ini, digunakan suatu metode yaitu autentikasi yang berkaitan dengan identifikasi/pengenalan kesatuan sistem maupun informasi itu sendiri. Namun terkadang keamanan terhadap data nilai masih terlihat lemah bahkan terkadang tidak diperhatikan.

Berikut ini beberapa penelitian tentang kriptografi yang berkaitan dengan Algoritma *Hill Cipher* :

1. Adam Rotal Yuliandaru. (2016) dengan judul penelitian Teknik Kriptografi Hill Cipher Menggunakan Matriks. Algoritma *Hill Cipher* merupakan algoritma pengenkripsian data dan informasi yang relatif sederhana dan mudah digunakan namun cukup aman dalam menjamin kerahasiaan informasi atau data yang ingin dikirimkan oleh pengirim pesan kepada penerima pesan tanpa dapat diketahui oleh pihak lain.
2. Alz Danny Wowor (2013) dengan judul Modifikasi Kriptografi Hill Cipher Menggunakan *Convert Between Base*. Algoritma Hill Cipher merupakan sebuah teknik kriptografi klasik, yang menggunakan matriks sebagai kunci. Pada sisi lain, Hill cipher telah dipecahkan dengan kriptanalisis *Known Plaintext Attack* menggunakan perkalian matriks dan persamaan linier. Pada penelitian ini dilakukan modifikasi algoritma *Hill Cipher* dengan menggunakan *Convert Between Base* dan perkalian n-matriks kunci untuk setiap iterasi. Cipherteks dihasilkan dalam elemen bit sehingga dapat mempersulit kriptanalisis dengan perkalian matriks dan fungsi linier untuk dapat memecahkan kunci dan menemukan plainteks. Modifikasi ini berhasil menyelesaikan berbagai permasalahan pada Hill cipher.
3. Nisak, K (2015) dengan judul Penyandian Kriptografi Metode Hill Cipher Dan Caesar Cipher Dengan Menggunakan Appinventor. Metode yang digunakan dalam penelitian ini adalah deskriptif kualitatif dengan menggunakan metode kepustakaan. Penelitian ini bertujuan untuk mengetahui perbandingan perbedaan pada metode Hill Cipher yang membahas perbedaan kunci matriks 2x2, 3x3, dan 4x4. Sedangkan pada metode Caesar Cipher membahas perbedaan banyak blok, banyak karakter tiap bloknya dan pengacakan kunci yang digunakan. Berdasarkan penelitian ini dengan perbedaan-perbedaan yang ada pada proses pada metode Hill Cipher dan Caesar Cipher diperoleh hasil yang sama. Untuk penelitian selanjutnya, disarankan menggunakan program komputer yang lebih baik atau dengan menggunakan metode kriptografi modern yang lebih kompleks.

Berdasarkan latar belakang diatas, maka peneliti melakukan penelitian dengan judul Pengamanan Pesan Rahasia Menggunakan Metode Algoritma Hill Cipher**.** Pada penelitian ini penulis akan menjelaskan bagaimana mengamankan file. Maka dengan itu data atau file yang sudah disandikan atau dienkripsikan tidak akan mudah atau tidak akan dimengerti pihak lain tanpa melakukan dekripsi data.

1. Bagaimana menerapkan algoritma Hill Cipher pada proses enkripsi dan dekripsi.
2. Bagaimana mengetahui proses enkripsi dan dekripsi dengan algoritma *Hill Cipher*.
3. Bagaimana merancang aplikasi kriptografi dengan algoritma *Hill Cipher*.
4. Bagaimana menjelaskan proses file yang sudah dienkripsikan dan dikembalikan menjadi file yang sesungguhnya dengan melakukan dekripsi file.

Adapun tujuan dari penulisan proposal ini adalah sebagai berikut:

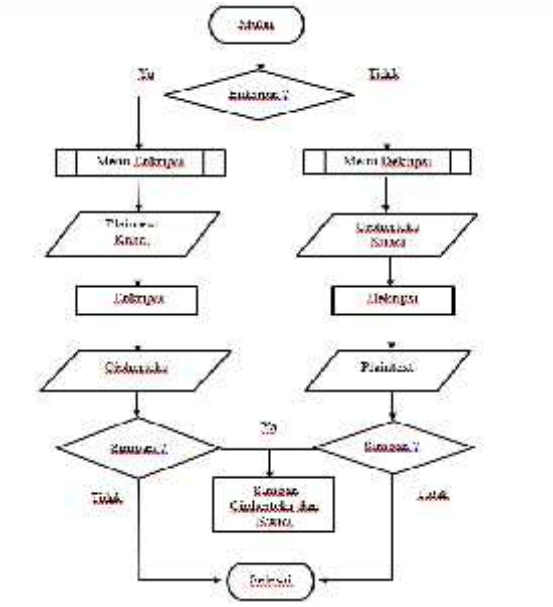
1. Membangun suatu aplikasi yang dapat mengamankan file teks menggunakan algoritma *Hill Cipher*.
2. Menghasilkan sebuah kode yang tidak bisa dimengerti oleh pengguna informasi yang tidak berhak.
3. Menganalisis bagaimana cara kerja algoritma *Hill Cipher* dalam memberi layanan kerahasiaan data.

2. LANDASAN TEORI

PENGERTIAN HILL CIPHER

Hill Cipher salah satu algoritma kriptografi kunci simetris untuk mengenkripsi data. Untuk menghindari matrik kunci yang tidak *invertible*, matrik kunci dibangkitkan menggunakan koefisien binomial newton. Proses enkripsi dan deskripsi menggunakan kunci yang sama, plaintext dapat menggunakan text.

3. METODE PENELITIAN



Gambar 1 Flowchart

4. HASIL DAN PEMBAHASAN

Implemetasi

Setelah melakukan perancangan perangkat lunak kriptografi modifikasi Algoritma *Hill Cipher* untuk pengamanan pesan rahasia, maka tahap selanjutnya adalah penulisan kode program (*coding*). Perangkat lunak yang akan di-*coding* adalah berupa menu utama serta program Kriptografi algoritma *Hill Cipher*, program Bantuan serta Keterangan.

Tampilan Menu Utama

Tampilan Menu Utama adalah berfungsi untuk menampilkan menu-menu aplikasi. Pada rancangan ini terdapat judul aplikasi, gambar latar serta sub menu antara lain Hill Cipher, *About* serta *Exit*. Tampilan Menu Utama terlihat seperti pada Gambar

Gambar 2 Menu Utama

Keterangan :
Pada halaman menu utama yang terdapat gambar latar dan terdapat tampilan sub menu pilihan aplikasi yang dapat diakses terdiri dari Hill Cipher *About* serta tombol *Exit*, yang berfungsi sebagai berikut:

1. Sub Menu Hill Cipher berfungsi untuk menampilkan program untuk melakukan proses enkripsi dan dekripsi dengan algoritma *Hill Cipher*.
2. Menu *About* berfungsi untuk menampilkan halaman keterangan.
3. Menu *Close* berfungsi untuk keluar dari halaman menu utama.

Tampilan Hill Cipher

Tampilan Hill Cipher berfungsi untuk melakukan enkripsi dan dekripsi dengan algoritma *Hill Cipher*. Tampilan Hill Cipher dapat dilihat seperti pada Gambar 4.2.
Pada Gambar 4.2 diatas terdiri dari bagian Input Plainteks yaitu proses enkripsi dan dekripsi dengan cara pemasukan plainteks melalui *keyboad* atau Load Plainteks yaitu proses enkripsi dan dekripsi dengan cara pemasukan plainteks melalui file plainteks yang sudah tersedia.

Tampilan About

Tampilan *About* berfungsi untuk menampilkan informasi tentang profil penulis. Profil penulis meliputi biodata singkat penulis serta data-data akademik berupa nama mahasiswa, Nomor Pokok Mahasiswa, Nama Perguruan Tinggi tempat mahasiswa, serta gambar latar belakang seperti yang dapat dilihat pada Gambar 3

Gambar 3 Tampilan *About*

Tampilan Keterangan pada Gambar 4.3 diatas adalah judul tugas akhir mahasiswa, tampilan logo kampus serta nama dan NPM mahasiswa.

Pengujian

Pada pengujian perangkat lunak kriptografi Algoritma *Hill Cipher* dilakukan dengan pemasukan plainteks serta kunci serta *Load Plainteks* yang menghasilkan cipherteks.

Enkripsi Dengan Input Plainteks

Pengujian enkripsi dengan input plainteks dilakukan cara pemasukan plainteks melalui keybord dengan jumlah huruf 10, 20, 25, 40, serta 50 dengan kunci1= [2 1; 3 4]. Hasil enkripsi Algoritma *Hill Cipher* dengan input teks dapat dilihat pada Tabel 4.1.

Tabel 4.1 Hasil Pengujian Enkripsi Algoritma *Hill Cipher* Input Plainteks

5.KESIMPULAN

Setelah melakukan implementasi perangkat lunak kriptografi modifikasi Algoritma *Hill Cipher* untuk pengamanan pesan rahasia, maka dapat disimpulkan:

a. Perangkat lunak Kriptografi Modifikasi Algoritma *Hill Cipher* untuk Pengamanan Pesan Rahasia dapat melakukan enkripsi dan dekripsi teks serta file teks.

b. Perangkat lunak Kriptografi Modifikasi Algoritma *Hill Cipher* untuk Pengamanan Pesan Rahasia dapat menggunakan kunci matriks 2x2 untuk melakukan enkripsi dan dekripsi teks serta file teks.

c. Tingkat keberhasilan dekripsi untuk memperoleh plainteks adalah 100 %.

DAFTAR PUSTAKA

[1] Daniel A. Mazmanian & Sabatier Paul, (1979), “Pengertian Implementasi”.

[2] Doni. Ariyus, (2006), “Pengertian Kriptografi Modern” Penerbit Informatika, Bandung.

[3] Samosir, R. A. P. (2015), “Pengamanan Data Teks dengan kombinasi Algoritma

Data *Encryption Standard* (DES) dan *First Of File* (FOF)".

[4] Nisak. K. (2015). "Penyandian Kriptografi Metode Hill Cipher Dan Caesar Cipher Dengan Menggunakan Appinventor". Skripsi Jurusan Matematika Fakultas Sains Dan Teknologi Universitas Islam Negeri Maulana Malik Ibrahim Malang.

[5] Wowor, A. D. (2013). **"**Modifikasi Kriptografi Hill Cipher Menggunakan Convert Between Base". Seminar Nasional Sistem Informasi Indonesia, 2 - 4 Desember 2013. Fakultas Teknologi Informasi, Universitas Kristen Satya Wacana, Salatiga.

[6] Yuliandaru, A. R. (2016). "Teknik Kriptografi Hill Cipher Menggunakan Matriks". Program Studi Informatika Sekolah Teknik Elektro dan Informatika Institut Teknologi Bandung, Jl. Ganesha 10 Bandung.

[7] Hidayat, A & Alawiyah, T. (2013). "Enkripsi dan Dekripsi Teks menggunakan Algoritma *Hill Cipher* dengan Kunci Matriks Persegi Panjang". Jurnal Matematika Integratif ISSN 1412-6184 Volume 9 No 1, April 2013.

[8] Pasaribu, J. S. (2016). "Penerapan Algoritma Hill Chiper Dalam Pengamanan Data Dengan Teknik Enkripsi Dan Dekripsi". Seminar Nasional Telekomunikasi dan Informatika (SELISIK 2016) Bandung, 28 Mei 2016. Teknik Informatika Politeknik Piksi Ganesha Bandung