PENERAPAN ALGORITMA VIGENERE CIPHER DAN HILL CIPHER MENGGUNAKAN SATUAN MASSA

Victor Saputra Ginting

Program Stud Magister Teknik Informatika, Universitas Amikom Yogyakarta
Jl. Ringroad Utara, Condongcatur, Sleman, Yogyakarta
victor.ginting@students.amikom.ac.id

Abstract – Technological developments in data security systems to ensure the confidentiality of data information has developed rapidly. To maintain the confidentiality of data information, there are sciences in development such as steganography and cryptography. The application is carried out not only for one data security technique but also by combining or modifying algorithms. This study aims to create a data security system by implementing a modified vigenere cipher and hill cipher algorithm. The results of this research are in the form of The encryption process using combined methods such as the Vigenere Cipher Algorithm and the Hill Cipher Algorithm can be carried out and Combining two or more methods can make messages more difficult to understand for others. this can make it easier for the sender of the message to convey messages that are confidential to the recipient.
Keywords - Cryptography, Vigenere Cipher, Hill Cipher, Encryption, Decryption

Abstrak - Perkembangan teknologi dalam sistem pengaman data untuk menjamin kerahasiaan informasi data sudah berkembang dengan pesat. Dalam menjaga kerahasiaan dalam informasi data terdapat ilmu dalam pengembangan seperti steganografi dan kriptopgrafi. Penerapan yang dilakukan tidak hanya pada satu teknik pengamanan data, melainkan bisa juga dengan melakukan kombinasi atau modifikasi algoritma. Penelitian ini bertujuan untuk membuat sistem keamanan data dengan melakukan penerapan modifikasi algoritma vigenere cipher dan hill cipher. Hasil dari penelitian ini sendiri berupa Proses Enkripsi dengan menggunakan metode gabungan seperti Algoritma Vigenere Cipher dan Algoritma Hill Cipher dapat dilakukan dan Menggabungkan dua metode atau lebih dapat membuat pesan semakin sulit dimengerti bagi orang lain. hal ini dapat memudahkan bagi pengirim pesan untuk menyampaikan pesan yang bersifat rahasia ke penerima.
Kata Kunci - Kriptografi, Vigenere Cipher, Hill Cipher, Enkripsi, Dekripsi

I. PENDAHULUAN

Pada Pengirim dapat melakukan pesan rahasia dengan cara mengenkripsikan pesan dan dapat di dekripsi oleh penerima ketika ingin mendapatkan pesan [1]. Pesan dapat diterima yang bermaksud untuk memberikan suatu maksud, pengetahuan, atau sesuatu yang bersifat rahasia, dimana pesan disampaikan agar yang dapat membaca atau mengetahui isi pesan tersebut hanyalah penerima saja tanpa diketahui oleh orang lain. Pesan boleh disampaikan kepada penerimba baik secara tulisan maupun lisan melalui media komunikasi atau sebuah aplikasi yang memang sudah banyak dibuat.

Media komunikasi dijaman sekarang merupakan tindak dari perkembangan teknologi dimana teknologi memang semakin pesat. Namun pada saat bersamaan, keamanan pesan merupakan masalah pokok yang masih banyak jaringan yang tidak dapat dipercaya, yang mampu dibaca oleh semua orang begitupun sebaliknya [2], hal ini tentu membuka bagi orang yang yang ingin mencuri data dan informasi dari pesan yang dimaksu untuk menggunakannya dan tentunya akan merugikan pihak tertentu [3]. Dengan demikian, dibutuhkan teknik dalam mengamankan suatu pesan, khususnya pesan yang ada di dalamnya yang juga terdapat informasi bersifat penting atau rahasia dengan melakukan enkripsi sebelum dikirim ke tujuan, maka tingkat keamanan informasi dari pesan tersebut dapat dijamin.

Ada dua macam teknik yang saat ini populer dan banyak digunakan dalam proses keamanan pesan, yakni, steganografi dan kriptografi [4]. Steganografi merupakan sebuah teknik dalam menyembunyikan suatu pesan pada suatu objek untuk menghindari indra penglihatan manusia [5]. Sedangkan kriptografi merupakan sebuah teknik untuk merubah bentuk pesan menjadi bentuk lain yang mempunyai arti berbeda dengan pesan itu sendiri, bahkan membuatnya seperti file yang rusak, sehingga pesan yang dimaksud sulit dibaca atau dimengerti oleh pihak lain [6]. Kriptografi adalah sebuah teknik yang dapat berguna untuk mengenkripsi suatu naskah asli (*plaintext*) yang kemudian diacak menggunakan suatu kunci enkripsi menjadi naskah acak yang Ada begitu banyak metode yang digunakan dalam proses mengamankan pesan, salah satunya adalah algoritma Vigenere Cipher [7]. Algortma Vigenere Cipher merupakan suatu teknik dalam menyandikan teks alfabet dengan deretan sandi Caesar berdasarkan huruf dalam kata kunci. Algoritma Vigenere Cipher merupakan penyederahaan daru polialfabetik. Salah satu kelebihan dalam Algoritma Vigene Cipher sendiri adalah teknik ini tidak mudah rentan dalam metode pemecahan sandi.

A. Kriptografi

Kriptografi merupakan suatu ilmu yang bertujuan menjaga kerahasiaan suatu pesan dengan cara menyandikan ke dalam bentuk yang tidak dapat dipahami oleh semua orang. Tujuan utama kriptografi adalah memberikan suatu pesan yang ditujukan kepada penerima yang dituju(1). Didalam ilmu kriptografi terdapat dua proses yakni enkripsi dan dekripsi. Pesan yang akan dienkripsi dinamakan sebagai *plain text.* Algoritma yang nantinya digunakan untuk mengenkripsi suatu pesam dengan melibatkan suatu kunci. Pesan yang dienkripsi (yang sudah disandikan) dikenal sebagai *cipher text* (teks sandi).

Dalam kriptografi akan banyak istilah yang dipakai. Beberapa istilah antara lain :

a. Plain Text dan Cipherteks
   Data atau informasi dapat dibaca dan dimengerti maknanya oleh orang yang akan dituju. Nama lain pesan adalah (plain text).
b. Enkripsi dan Dekripsi
   Proses persandian plain teks menjadi cipher teks disebut sebagai enkripsi, sedangkan proses kebalikan nya disebut dekripsi.

B. Vigenere Cipher

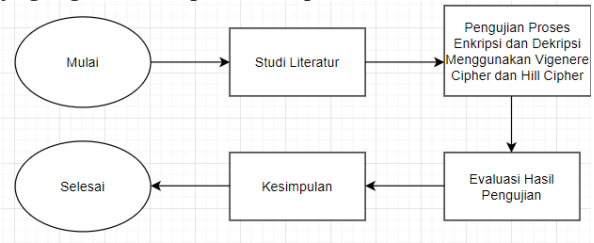
Metode Vigenere Cipher adalah suatu metode penyandian teks alfabet menggunakan deretan sandi Caesar berdasarkan huruf pada kunci. Sandi Vigenere merupakan bentuk sederhana dari substitusi [8]. Kelebihan sandi dibanding sandi Caesar dan sandi monoalfabetik lain adalah sandi yang tidak rentan terhadap metode pemecahan sandi.

C. Algoritma Hill Cipher

Algoritma Hill Cipher merupakan algoritma kriptografi kunci simetris yang mempunyai berbagai kelebihan dalam mengenkripsi data) [9]. Hill Cipher ialah penerapan aritmatika modulo pada kriptografi. Teknik kriprografi ini menggunakan matrik persegi sebagai kunci yang nantinya digunakan untuk melakukan enkripsi dan dekripsi [10]

II. METODE PENELITIAN

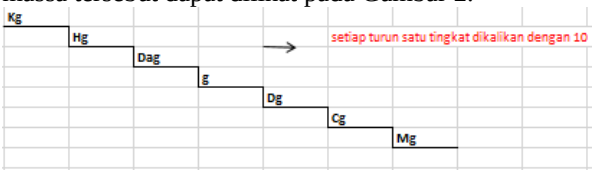
Penelitian yang dilakukan merupakan penelitian yang bersifat studi literatur. Adapun alur penelitian yng digunakan dapat dilihat pada Gambar 1.



Gambar 1. Alur Penelitian

1. Proses Enkripsi

Proses Enkripsi dalam penelitian ini dilakukan dengan memasukkan plainteks atau pesan yang digunakan berupa huruf. Pertama pesan akan disembunyikan dalam Tabel Tebula Recta dengan menggunakan plain text dan kata kunci yang sudah didapatkan. Setelah mendapatkan cipherteks dari Tabel tersebut, selanjutnya menggunakan Algoritma Hill Cipher yang sudah dimodifikasi oleh peneliti. Untuk modifikasi Hill Cipher, Peneliti menggunakan persamaan Matriks Plainteks Mod 26, dimana kunci matriks yang digunakan adalah 2 x 2 dari nama-nama Negara, dan yang diambil adalah 3 digit huruf diawal saja. kemudian selanjutnya merubah plain tekx menjadi matriks 2 x 1, dengan merubah alphabet menjadi numerik. Setelah menggunakan persamaan Matriks Mod 26, hasil dari plainteks kemudian akan dibagi dengan 10. Hasil cipherteks dari pembagian 10 tersebut selanjutnya akan dikonversi kedalam satuan massa, dimana disini setiap penuruan 1 tingkat kebawah, akan dikali dengan 10. Konversi satuan massa tersebut dapat dilihat pada Gambar 2.



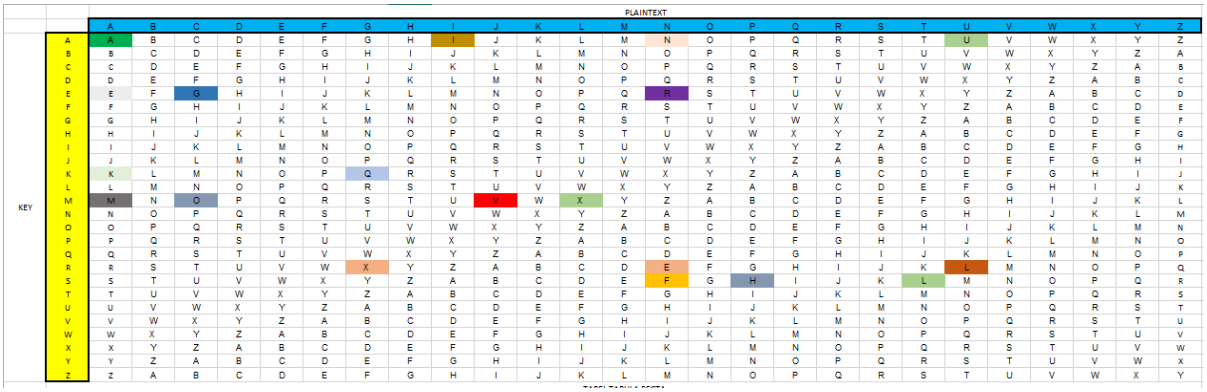
Gambar 2. Konversi Satuan Massa

2. Proses Dekripsi

Proses Dekripsi dilakukan dengan melakukan kebalikan (*Reverse*) dari proses enkripsi. Langkah Pertama memasukkan Plainteks yang didapatkan dari proses enkripsi, Plainteks selanjutnya akan dibagi dengan 10 apabila naik 1 tingkat dari satuan massa Kilogram. Setelah mendapatkan cipherteks dari konversi ke satuan massa Kilogram, Langkah kedua Cipherteks dikali dengan 10. Lalu selanjutnya Langkah ketiga, melakukan persamaan menggunakan matriks Cipherteks Mod 26. Setelah didapatkan cipherteks dari Mod 26, langkah keempat yakni mengubah plainteks menjadi 2 x 1 dengan mengubah numerik menjadi alphabet. Kemudian setelah didapatkan alphabet, langkah kelima yakni menggunakan Tabel Tebula Recta untuk mendapatkan pesan rahasia yang dimaksud, dengan menggunakan kunci awal pertama.

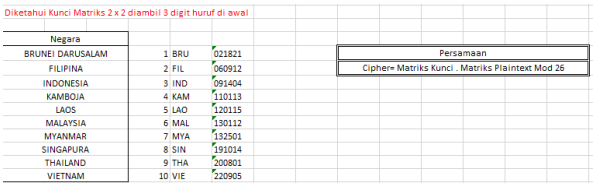
III. HASIL DAN PEMBAHASAN

Tabel Tabula Recta digunakan dalam Algoritma Vigenere Cipher, dimana Plaintext yang digunakan adalah “Jangan Lupa Cuci Tangan” dengan Kunci adalah “Masker”. Gambar Tabel Tabula Recta dapat dilihat pada Gambar 2.



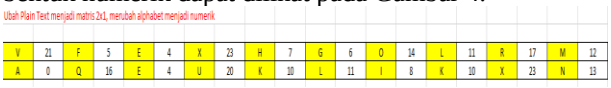
Gambar 2. Tabel Tabula Recta

Hasil yang didapatkan dari Tabula Recta dengan plaintext "VAFQEEXUHKGLOILKRXMN". Dari plaintext yang sudah didapatkan dari Algoritma Vigenere Cipher, kemudian selanjutnya menggunakan modifikasi dengan Algoritma Hill Cipher dari plaintext yang sudah didapatkan. Modifikasi Hill Cipher sendiri menggunakan Nama Negara dimana kunci matriks 2x2 akan diambil 3 digit huruf diawal dan matriks plaintext mod 26. Modifikasi dari Algoritma Hill Cipher menggunakan Nama Negara dapat dilihat pada Gambar 3.



Gambar 3. Modifikasi Hill Cipher

Plaintext yang didapat dari modifikasi Hill Cipher kemudian diubah kedalam bentuk numerik. Plaintext yang didapatkan dan sudah dibentuk kedalam bentuk numerik dapat dilihat pada Gambar 4.



Gambar 4. Proses alphabet dirubah kedalam bentuk numerik

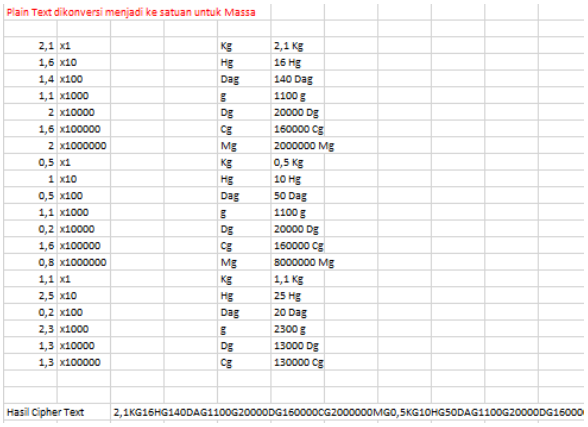
Setelah merubah plaintext kedalam bentuk numerik, selanjutnya melakukan perhitungan dengan menggunakan persamaan 2logaritma dibagi dengan 10. Hasil dari Cipherteks yang didapatkan selanjutnya dibagi dengan 10 dapat dilihat pada Gambar 5.

Cipherteks yang didapatkan kemudian dibagi dengan 10

Plaintext	dibagi 10	Hasil
21		2.1
16		1,60
14		1,40
11		1,10
20		2,00
16		1,60
20		2,00
5	=	0,50
10		1,00
5		0,50
11		1,10
2		0,20
16		1,60
8		0,80
11		1,10
25		2,50
2		0,20
23		2,30
13		1,30
13		1,30

Gambar 5. Cipherteks dibagi dengan 10

Plaintext yang didapatkan dari pembagian dengan 10, selanjutnya dikonversi kedalam Satuan Massa. disini Satuan Massa akan dimulai dari Kilogram (Kg) hingga nantinya berakhir di Miligram (Mg). Setelah sampai di Miligram (Mg) lakukan pengulangan lagi dari awal,yakni Kilogram (Kg). Setiap penurunan maka akan dikali dengan 10. Proses konversi ke Satuan Massa dapat dilihat pada Gambar 6.



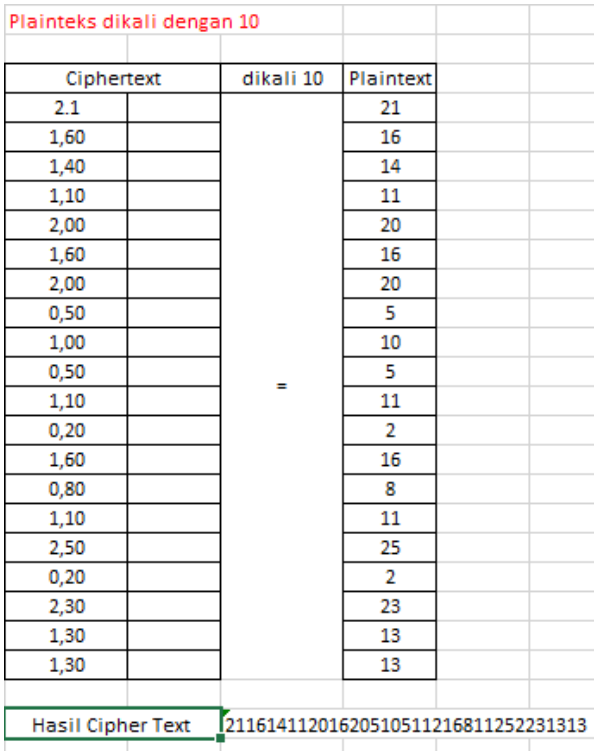
Gambar 6. Proses konversi ke Satuan Massa

Dari modifikasi 2 algoritma, yakni Algoritma Vigenere Cipher dan Algoritma Hill Cipher, maka didapatkanlah Plaintext akhirnya adalah "2,1KG16HG140DAG1100G20000DG160000CG2000000MG0,5KG10HG50DAG1100G20000DG160000CG8000000MG1,1KG25HG20DAG2300G13000DG130000CG".

Untuk proses dekripsi, kita melakukan kebalikan (*Reverse*) dari penjabaran diatas. Plaintext awal yakni "2,1KG16HG140DAG1100G20000DG160000CG2000000MG0,5KG10HG50DAG1100G20000DG160000CG8000000MG1,1KG25HG20DAG2300G13000DG130000CG". Kemudian selanjutnya dikonversi kedalam satuan massa Kilogram (Kg). Proses konversi ke satuan massa Kilogram dapat dilihat pada Gambar 7.

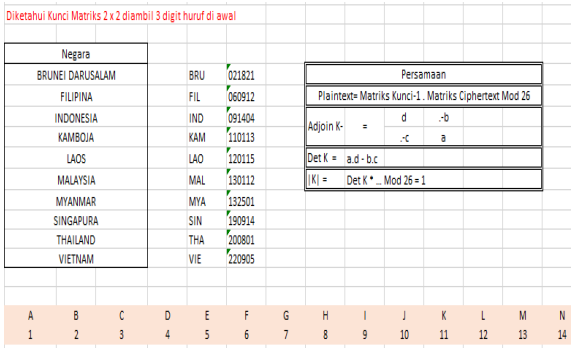
Gambar 7. Proses konversi ke satuan massa Kilogram

Kemudian langkah berikutnya, hasil yang didapatkan setelah dikonversi kedalam Kg, maka plaintext dikali dengan 10. Proses perkalian 10 pada Plaintext dapat dilihat pada Gambar 8.



Gambar 8. Plaintext dikali dengan 10

Setelah dikali dengan 10, maka proses selanjutnya menggunakan kunci matriks 2 x 2 dari Nama Negara, yang nantinya akan diambil 3 digit huruf diawal. proses matriks 2 x 2 dapat dilihat pada Gambar 9.



Gambar 9. Proses Matriks 2 x 2 Menggunakan Nama Negara

Setelah mendapatkan hasilnya dari proses matriks 2 x 2, kemudian langkah selanjutnya menggunakan Matriks 2 x 1 dengan merubah alphabet menjadi numerik. Proses matriks 2 x 1 dengan merubah alphabet menjadi numberik dapat dilihat pada Gambar 10.

MOD 26	HASIL CIPHER
18	V
17	A
6	F
5	Q
8	E
8	E
15	X
3	U
21	H
24	K
4	G
21	L
8	O
0	I
18	L
15	K
13	R
2	X
0	M
13	N

Gambar 10. Proses Matriks 2 x 1 Merubah Numerik Menjadi Alphabet

Hasil Ciphertext yang didapat dari proses matriks 2 x 1 adalah “vafqeexuhkgloilkrxmn”, kemudian langkah selanjutnya menggunakan Algoritma Vigenere Cipher dengan menggunakan Tabel Tebula Recta untuk mendapatkan hasil Cipherteks akhir. Proses Algoritma Vigenere Cipher dengan menggunakan Tabel Tebula Recta dapat dilihat pada Gambar 11.

Kunci	M	A	S	K	E	R	M	A	S	K	E	R	M	A	S	K	E	R	M	A
	V	A	F	Q	E	E	X	U	H	K	G	L	O	I	L	K	R	X	M	N
	J	A	N	G	A	N	L	U	P	A	C	U	C	I	T	A	N	G	A	N

Gambar 11. Hasil Algoritma Vigenere Cipher

Kemudian didapatkan hasil cipherteks akhirnya adalah “Jangan Lupa Cuci Tangan” dengan menggunakan kunci “Masker”.

IV. KESIMPULAN

Berdasarkan penelitian dan pengujian yang didapat dari studi literatur, maka dapat diambil kesimpulan sebagai berikut :

1. Proses Enkripsi dengan menggunakan metode gabungan seperti Algoritma Vigenere Cipher dan Algoritma Hill Cipher dapat dilakukan.
2. Menggabungkan 2 metode atau lebih dapat membuat pesan semakin sulit dimengerti bagi orang lain. hal ini dapat memudahkan bagi pengirim pesan untuk menyampaikan pesan yang bersifat rahasia ke penerima.

DAFTAR PUSTAKA

[1] D. Nurnaningsih and A. A. Permana, "RANCANGAN APLIKASI PENGAMANAN DATA DENGAN ALGORITMA ADVANCED ENCYPTION STANDARD (AES)," *J. Tek. Inform.*, 2018, doi: 10.15408/jti.v11i2.7811.

[2] O. K. Sulaiman, M. Ihwani, and S. F. Rizki, "MODEL KEAMANAN INFORMASI BERBASIS TANDA TANGAN DIGITAL DENGAN DATA ENCRYPTION STANDARD (DES) ALGORITHM," *InfoTekJar (Jurnal Nas. Inform. dan Teknol. Jaringan)*, 2016, doi: 10.30743/infotekjar.v1i1.82.

[3] R. Munir, "Kriptografi," in *2*, 2019.

[4] C. Program, S. Magister, K. Kunci, : Kriptografi, and K. Publik, "KEAMANAN DATA DENGAN METODE KRIPTOGRAFI KUNCI PUBLIK," *J. TIMES*, 2016.

[5] Sumandri, "Studi Model Algoritma Kriptografi Klasik dan Modern," *Semin. Mat. dan Pendidik. Mat. UNY*, 2017.

[6] A. Rohmanu, "Implementasi Kriptografi dan Steganografi Dengan Metode Algoritma Des dan Metode End Of File," *J. Inform. SIMANTIK*, 2017.

[7] M. K. Harahap, "ANALISIS PERBANDINGAN ALGORITMA KRIPTOGRAFI KLASIK VIGENERE CIPHER DAN ONE TIME PAD," *InfoTekJar (Jurnal Nas. Inform. dan Teknol. Jaringan)*, 2016, doi: 10.30743/infotekjar.v1i1.43.

[8] M. D. Irawan, "IMPLEMENTASI KRIPTOGRAFI VIGENERE CIPHER DENGAN PHP," *J. Teknol. Inf.*, 2017, doi: 10.36294/jurti.v1i1.21.

[9] D. Rodriguez-Clark, "Hill Cipher - Crypto Corner," *Interactive-Maths.Com*, 2017.

[10] A. M. H. Pardede, "ALGORITMA VIGENERE CIPHER DAN HILL CIPHER DALAM APLIKASI KEAMANAN DATA PADA FILE DOKUMEN," *J. Tek. Inform. Kaputama*, 2017.