Enkripsi & Dekripsi Teks Menggunakan Hill Cipher Dengan Matriks Ordo 3 x 3

Fajar Sudana Putra[*1], Dony Ariyus[2]
[1,2] MTI Universitas Amikom, Yogyakarta
e-mail : **[1]fajar.0106@students.amikom.ac.id**, [2]dony.a@amikom.ac.id

Abstrak

Kriptografi banyak digunakan sebagai cara agar pesan rahasia dapat tersampaikan ke seseorang. Pesan tersebut di enkripsi agar orang yang tidak berhak untuk membaca pesan tersebut tidak akan dapat membacanya. Namun, penggunaan kriptografi sering kali dapat dipecahkan/diselesaikan oleh orang lain karena terkadang kunci dari pesan tersebut tidak sulit untuk dipecahkan. Dalam tulisan ini, penulis memodifikasi metode Hill Cipher yang menghasilkan chipertext berupa kode plat suatu wilayah provinsi dan luas wilayah provinsi tersebut.

***Kata Kunci** – Hill Cipher, Kriptografi,Matrix ordo 3x3*

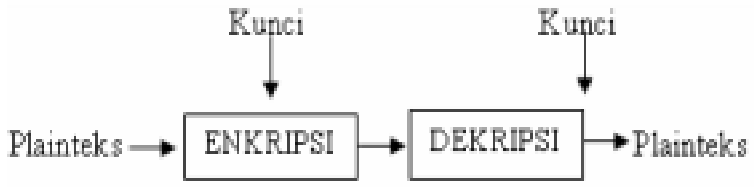
1. PENDAHULUAN

Kriptografi (cryptography) berasal dari Bahasa Yunani: ”cryptos” artinya ”secret” (rahasia), sedangkan ”graphein” artinya ”writing” (tulisan), Jadi, kriptografi berarti ”secret writing” (tulisan rahasia). Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data, serta otentikasi [1].

Definisi yang digunakan di dalam buku menyatakan bahwa kriptografi adalah ilmu dan seni untuk menjaga kerahasiaan pesan dengan cara menyandikannya ke dalam bentuk yang tidak dapat dimengerti lagi maknanya. Definisi ini mungkin cocok pada masa lalu di mana kriptografi digunakan untuk keamanan komunikasi penting seperti komunikasi di kalangan militer, diplomat, dan mata-mata. Namun saat ini kriptografi lebih dari sekadar privacy, tetapi juga untuk tujuan data integrity, authentication, dan non-repudation [2].

Enkripsi merupakan bagian dari kriptografi, dan merupakan hal yang sangat penting supaya keamanan data yang dikirimkan bisa terjaga kerahasiaannya. Enkripsi bisa diartikan dengan chiper atau kode, di mana pesan asli (plaintext) diubah menjadi kode-kode tersendiri sesuai metode yang disepakati oleh kedua belah pihak, baik pihak pengirim pesan maupun penerima pesan [3].

Dekripsi merupakan proses sebaliknya dari enkripsi yaitu mengembalikan sandi-sandi atau informasi yang telah dilacak kebentuk file aslinya dengan menggunakan kunci atau kode [4].



Gambar 1 Proses Enkripsi & Dekripsi (sumber : Andy Pramono, 2009)

Algoritma kriptografi atau cipher, dan juga sering disebut dengan istilah sandi adalah suatu fungsi matematis yang digunakan untuk melakukan enkripsi dan dekripsi Ada dua macam algoritma kriptografi, yaitu algoritma simetris (symmetric algorithms) dan algoritma asimetris

(asymmetric algorithms). Hill cipher yang merupakan polyalphabetic cipher dapat dikategorikan sebagai block cipher, karena teks yang akan diproses akan dibagi menjadi blok-blok dengan ukuran tertentu. Setiap karakter dalam satu blok akan saling mempengaruhi karakter lainnya dalam proses enkripsi dan dekripsinya, sehingga karakter yang sama tidak dipetakan menjadi karakter yang sama pula [5].

Teknik kriptografi ini menggunakan sebuah matriks persegi sebagai kunci yang digunakan untuk melakukan enkripsi dan dekripsi [6]. Hill Cipher diciptakan oleh Lester S. Hill pada tahun 1929. Hill Cipher tidak mengganti setiap abjad yang sama pada plaintext dengan abjad lainnya yang sama pada ciphertext karena menggunakan perkalian matriks pada dasar enkripsi dan dekripsinya [7]. Hill Cipher termasuk kepada algoritma kriptografi klasik yang sangat sulit dipecahkan oleh kriptanalis apabila dilakukan hanya dengan mengetahui berkas ciphertext saja [8]. Namun, teknik ini dapat dipecahkan dengan cukup mudah apabila kriptanalis memiliki berkas ciphertext dan potongan berkas plaintext [9]. Teknik kriptanalisis ini disebut known-plaintext attack [10].

2. METODE PENELITIAN

2.1. Dasar Teknik Hill Cipher

Dasar dari teknik Hill Cipher adalah aritmatika modulo terhadap matriks. Dalam penerapannya, Hill Cipher menggunakan teknik perkalian matriks dan teknik invers terhadap matriks. Kunci pada Hill Cipher adalah matriks n x n dengan n merupakan ukuran blok [11]. Jika kunci disebut dengan K, maka K adalah sebagai berikut :

$$K = \begin{bmatrix} k_{11} & k_{12} & \dots & k_{1n} \\ k_{21} & k_{22} & \dots & k_{2n} \\ \dots & \dots & \dots & \dots \\ k_{m1} & k_{m2} & \dots & k_{mn} \end{bmatrix}$$

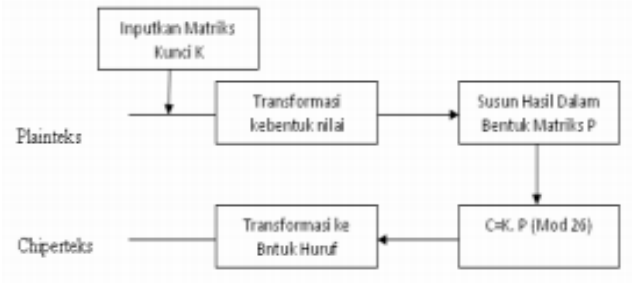
Gambar 2. Matriks K

Matriks K yang menjadi kunci harus merupakan matriks yang invertible, yaitu memiliki multiplicative inverse K^1sehingga : K . K = 1 Kunci harus memiliki invers karena matriks K^1tersebut adalah kunci yang digunakan untuk melakukan dekripsi.

2.2. Teknik Enkripsi Pada Hill Cipher

Proses enkripsi pada Hill Cipher dilakukan per blok plaintext. Ukuran blok tersebut sama dengan ukuran matriks kunci [12]. Sebelum membagi teks menjadi deretan blok-blok, plaintext terlebih dahulu dikonversi menjadi angka, masing-masing sehingga A=0, B=1, hingga Z=25. Secara matematis, proses enkripsi pada Hill Cipher adalah:

C = K . P
C = Ciphertext
K = Kunci
P = Plaintext



Gambar 3. Ilustrasi Proses Enkripsi Hill Cipher

2.3. Teknik Dekripsi Pada Hill Cipher

Proses dekripsi pada Hill Cipher pada dasarnya sama dengan proses enkripsinya. Namun matriks kunci harus dibalik (invers) terlebih dahulu. Secara matematis, proses dekripsi pada Hill Cipher dapat diturunkan dari persamaan [13].

$C = K \cdot P$

$K\text{-}1 \cdot C = |K^1| \cdot K \cdot P$

$|K^1| \cdot C = I \cdot P$

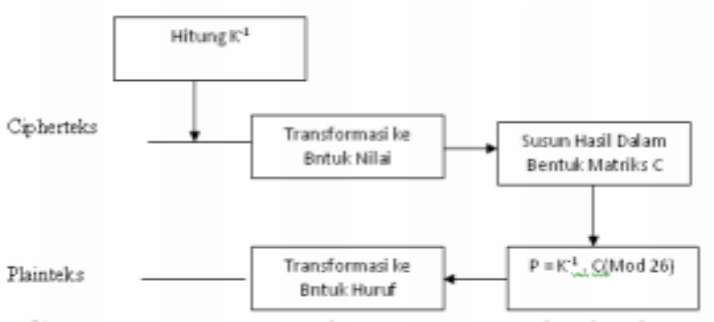
$P = |K^1| \cdot C$

Menjadi persamaan proses deskripsi :

$P = |K^1| \cdot C$

Di mana untuk menentukan $|K^1|$dengan menggunakan rumus:

$\frac{1}{\det K} \bmod 26 = x$ atau (det K * x mod 26 = 1)



Gambar 4. Ilustrasi Proses Dekripsi Hill Cipher

3. HASIL & PEMBAHASAN

3.1. Proses Enkripsi

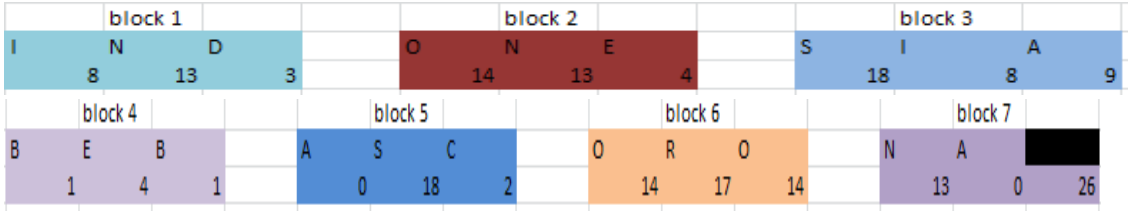
Penulis mencoba membuat susunan kunci sebagai berikut: Diketahui Matriks 3x3

	15	10	30	
	9	8	6	
KUNCI	14	22	40	
PLAINTEXT : INDONESIA BEBAS CORONA				

Gambar 4. Kunci Matriks 3x3

Adapun Tabel Konversi huruf ke angka yaitu 0-25 dan A-Z.

Selanjutnya penulis mencoba dengan plaintext “Indonesia Bebas Corona”. Langkah pertama didapatkan sebagai berikut:



Gambar 5. Hasil Langkah 1

Pada gambar tersebut dapat kita lihat hasil setelah melakukan proses langkah 1, Karena penulis menggunakan Metode Hill Cipher dengan ordo matriks 3x3 jadi hasil langkah pertama telah terbagi 7 block dimana dalam satu block terdapat 3 huruf yang berisi hasil perubahan plaintext yang bernilai angka di bawahnya.

						Hasil Perkalian Matrix		Mod 14	Hasil
	15	10	30		8	340		4	KHD8830
Kunci	9	8	6	block 1	13	194		12	KHJ8997
	14	22	40		3	518		0	KHA239950
	15	10	30		14	460		12	KHJ8997
Kunci	9	8	6	block 2	13	254		2	KHF1679600
	14	22	40		4	642		12	KHJ8997
	15	10	30		18	620		4	KHD8830
Kunci	9	8	6	block 3	8	280		0	KHA239950
	14	22	40		9	788		4	KHD8830
	15	10	30		1	85		1	KHG1075900
Kunci	9	8	6	block 4	4	47		5	KHB1499900
	14	22	40		1	142		2	KHF1679600
	15	10	30		0	240		2	KHF1679600
Kunci	9	8	6	block 5	18	156		2	KHF1679600
	14	22	40		2	476		0	KHA239950
	15	10	30		14	800		2	KHF1679600
Kunci	9	8	6	block 6	17	346		10	KHM23700
	14	22	40		14	1130		10	KHM23700
	15	10	30		13	975		9	KHN17500
Kunci	9	8	6	block 7	0	273		7	KHR6414
	14	22	40		26	1222		4	KHD8830

Gambar 6. Hasil Perkalian matriks ordo 3x3 dan perhitungan MOD 14

Pada gambar 6 penulis melakukan perhitungan matriks ordo 3x3 dari hasil sebuah langkah sebelumnya, kemudian dilakukan lah perhitungan sisa pembagian yaitu MOD, sehingga menghasilkan kode plat provinsi dan luas wilayah.

NAMA WILAYAH		KODE PLAT DEPAN BLAKANG DAN LUAS WILAYAH
KOTA PALANGKARAYA	0	KHA239950
KABUPATEN KOTAWARINGIN BARA	1	KHG1075900
KABUPATEN KOTAWARINGIN TIMU	2	KHF1679600
KABUPATEN BARITO UTARA	3	KHE8300
KABUPATEN BARITO SELATAN	4	KHD8830
KABUPATEN KAPUAS	5	KHB1499900
KABUPATEN SUKAMARA	6	KHS3827
KABUPATEN LAMANDAU	7	KHR6414
KABUPATEN SERUYAN	8	KHP16404
KABUPATEN KATINGAN	9	KHN17500
KABUPATEN MURUNG RAYA	10	KHM23700
KABUPATEN BARITO TIMUR	11	KHK3834
KABUPATEN PULANG PISAU	12	KHJ8997
KABUPATEN GUNUNG MAS	13	KHH10805

Gambar 7. Kode Plat dan Luas Wilayah Provinsi Kalimantan tengah

Pada gambar 7 penulis meggunakan object kode plat dan luas wilayah provinsi Kalimantan tengah. Jadi hasil dari enkripsi yang telah penulis lakukan agar menghasilkan kode tersebut.

4. KESIMPULAN

Dapat dilihat bahwa hasil yang didapatkan adalah berupa kode plat dan luas wilayah provinsi Kalimantan tengah yang sudah acak melalui beberapa proses, sehingga cara untuk mendeskripsikannya tidak simple. Disini juga terdapat beberapa huruf pelengkap yang membuat enkripsi ini semakin membingungkan pembaca. Jadi kesimpulan pada penulisan ini algoritma Hill Cipher yang dikombinasikan menjadi dengan kode plat nomor kendaraan wilayah Kalimantan Tengan dan luas wilayah daerah Kalimantan Tengah.

5. SARAN

Penelitian selanjutnya dapat ditambahkan kombinasi metode lainnya.

DAFTAR PUSTAKA

[1] A. K. W. F. D. N. M. Kusnawi, "Aplikasi Quiz Psikologis Berbasis Website Dengan Pengaplikasian Algoritma Des," *Semin. Nas. Teknol. Inf. dan Multimed. 2017*, pp. 43–48, 2017.

[2] R. A. Megantara and F. A. Rafrastara, "Super Enkripsi Teks Kriptografi menggunakan Algoritma Hill Cipher dan Transposisi Kolom," *Pros. SENDI_U 2019*, pp. 85–92, 2019.

[3] S. K. Sharma, "An Application of Hill Cipher by Using Modular Matrices," *Eng. Technol. J. Res. Innov.*, vol. II, no. Ii, pp. 32–34, 2020.

[4] A. P. U. Siahaan, "Application of Hill Cipher Algorithm in Securing Text Messages," pp. 55–59, 2018, doi: 10.31227/osf.io/n2kdb.

[5] Nasrudin, A. Pratama, E. Pratama, and E. T. Wulandari, "Implementasi Algoritma Elgamal dan kode HILL Untuk Keamanan Database," *Pap. Tek. Inform.*, 2020, doi:

10.31219/osf.io/vq5yc.

[6] I. Irmayani, “Application of Matrix in Hill Cipher Algorithm,” *Int. Conf. Nat. Soc. Sci. Proceeding Ser.*, no. September, pp. 141–147, 2019.

[7] D. Rachmawati, A. Sharif, and Ericko, “Hybrid Cryptosystem Combination Algorithm of Hill Cipher 3x3 and Elgamal to Secure Instant Messaging for Android,” *J. Phys. Conf. Ser.*, vol. 1235, no. 1, 2019, doi: 10.1088/1742-6596/1235/1/012074.

[8] F. Achmad, Novriyenni, M. Yani, and M. H. P. Akim, “Analisis Hybrid Cryptosystem Algoritma Algoritma,” *J. Tek. Inform. Kaputama*, vol. 1, no. 2, 2017.

[9] L. J. Pangaribuan, “Kriptografi Hybrida Agloritma Hill Cipher Dan Rivest Shamir Adleman (RSA) Sebagai Pengembangan Kriptografi Kunci Simetris (Studi Kasus : Nilai Mahasiswa Amik Mbp),” *J. Teknol. Inf. Dan Komun.*, vol. 7, no. 1, pp. 11–26, 2018.

[10] E. Pawan, K. Kaharuddin, and D. Arius, “Kombinasi Arnold Cat Map dan Modifikasi Hill Cipher Menggunakan Kode Bunyi Beep BIOS PHOENIX,” *Sisfotenika*, vol. 9, no. 2, p. 159, 2019, doi: 10.30700/jst.v9i2.485.

[11] R. Makhomah, K. A. Santoso, and A. Kamsyakawuni, “Pengkodean Teks Menggunakan Kombinasi Hill Cipher dan Operasi XOR,” *Prism. Pros. Semin. Nas. Mat.*, vol. 4, pp. 548–552, 2021.

[12] G. Krisnawanti, K. Agung, and A. Kamsyakawuni, “Modifikasi Huffman dengan Hill Cipher pada Pengkodean Data Teks,” *Prism. Pros. Semin. Nas. Mat.*, vol. 4, pp. 534–539, 2021.

[13] A. Rauf, D. Indra, and F. Fattah, “Kriptanalisis pada Metode Hill Cipher,” *Bul. Sist. Inf. dan Teknol. Islam*, vol. 1, no. 1, pp. 1–5, 2020.