FUNGSI ALGORITMA KRIPTOGRAFI HILL CIPHER UNTUK PENGAMANAN FILE GAMBAR DAN PESAN TEKS

Indra Gunawan[1], Sumarno[2], Heru Satria Tambunan[3],Eka Irawan[4],Ika Okta Kirana[5]
[1,2,3,4,5]STIKOM Tunas Banga Pematangsiantar
[1,2,3,4,5]Jl. Jend. Sudirman Blok A, No. 1, 2 dan 3, Kota Pematangsiantar, Sumatera Utara
[1]indra@amiktunasbangsa.ac.id, [2]sumarno@amiktunasbangsa.ac.id, [3]heru@amiktunasbangsa.ac.id,[4]eka.irawan@amiktunasbangsa.ac.id,[5]ikaoktakirana@stikomtb.ac.id

Abstrak

Dari banyaknya bidang ilmu komputer yang harus dibahas, diantaranya adalah pengamanan dari sebuah data. Diantara banyaknya data yang harus diamankan, bisa menggunakan algoritma kriptografi yang salah satunya adalah algoritma kriptografi Hill Cipher. Pengamanan data file gambar dan pesan teks dipadukan dengan fungsi algoritma kriptografi Hill Cipher yang dapat membantu meningkatkan keaslian pesan teks dan file gambar pada saat proses pengiriman pesan berlangsung. Sehingga pada saat pesan sampai kepada sipenerima, pesan tersebut masih bisa dijamin keaslian dari isi pesannya. Analisa ini bertujuan untuk meningkatkan keamanan pesan teks yang dari pesan asli sebelumnya dilakukan penyandian, sehingga menghasilkan pesan teracak yang selanjutnya pesan teks tersebut dipadukan kedalam file gambar.

Kata kunci : Data, Ilmu Komputer, Kriptografi, Hill Cipher

Abstract

Of the many areas of computer science that must be discussed, among them is the security of a data. Among the many data that must be secured, can use a cryptographic algorithm, one of which is Hill Cipher cryptography algorithm. The data security of image files and text messages is combined with Hill Cipher's cryptographic algorithm functionality which can help to enhance the authenticity of text messages

DOI: https://doi.org/10.29103/techsi.v10i1.605

and image files during the sending process. So when the message gets to the recipient, the message can still be guaranteed the authenticity of the contents of the message. This analysis aims to improve the security of text messages from previously encoded original messages, thereby generating random messages which are then integrated into the image file.

Keywords: Data, Computer Science, Cryptography, Hill Cipher

1. PENDAHULUAN

Dalam menjaga kerahasiaan dan keamanan data merupakan sesuatu yang sangat penting didalam sebuah proses pengiriman data, baik itu data gambar maupun data teks melalui sebuah jaringan yang sudah banyak digunakan oleh masyarakat luas yang saling terkoneksi satu dengan lainnya, yaitu internet [Gunawan, I. Maret 2018].

Dengan begitu pesatnya perkembangan era modrenisasi, pemecahan masalah dalam penemuan kode/pembajakan data dapat dilakukan dengan berbagai cara dan bisa juga menggunakan beberapa model algoritma. Diantara jenis algoritma untuk pembajakan data bisa menggunakan algoritma brute force, dimana algoritma ini dapat memecahkan masalah dengan sangat sederhana dalam pembajakan dan pencarian kode dengan cara yang jelas dan lempang (Gunawan, 2016).

Keamanan merupakan masalah besar dan mengamankan data yang penting merupakan hal yang sangat penting, sehingga data tersebut tidak dapat disadap atau disalah gunakan untuk tujuan ilegal sehingga dapat merugikan pihak lain. Untuk itu pemerintah dan lembaga lainnya berusaha mengamankan data mereka sekuat tenaga agar tidak terjadi pembobolan data. Faktor keamanan dalam proses pengiriman data melalui saluran internet menjadi factor yang penting. Apabila hal ini diabaikan, maka orang yang tidak berhak akan dengan mudah memanfaatkan data

DOI: https://doi.org/10.29103/techsi.v10i1.605

tersebut untuk tujuan tertentu. Jika hal ini terjadi ada dua pihak yang dirugikan yaitu pengirim data dan penerima data. Salah satu metode untuk mengamankan data tersebut adalah dengan menyamarkan menjadi tidak bermakna.

Kriptografi adalah seni atau ilmu meliputi prinsip-prinsip dan metode mengubah pesan yang dimengerti (*plaintext*) menjadi pesan yang tidak dapat dimengerti (*ciphertext*) dan kemudian retransforming pesan yang akan kembali ke bentuk aslinya (Ariyus, D. 2008). Ada empat tujuan mendasar yang juga aspek keamanan informasi, yaitu:

1. Kerahasiaan, adalah layanan yang digunakan untuk menjaga isi dari informasi.
2. Integritas data, adalah hubungan dari perubahan data secara tidak sah.
3. Autentikasi, adalah berhubungan dengan identifikasi/pengenalan secara kesatuan sistem.
4. Non repudiasi, adalah usaha untuk mencegah terjadinya penyangkalan terhadap terciptanya suatu informasi.

Substitution cipher adalah salah satu komponen dasar dari cipher klasik. Dua macam Substitution cipher pada kriptografi klasik yaitu *Polyalphabetic Substitution Cipher* dan *Monoalphabetic Substitution Cipher*. Pada *Polyalphabetic Substitution Cipher*, enkripsi terhadap satu huruf yang sama bisa menghasilkan huruf yang berbeda sehingga lebih sulit untuk menemukan pola enkripsinya. Pada *monoalphabetic substitution cipher*, satu huruf tertentu pasti akan berubah menjadi huruf tertentu yang lain, sehingga pola enkripsinya lebih mudah diketahui, karena satu huruf pada ciphertext pasti merepresentasikan satu huruf pada plaintext [Supiyanto, 2015].

Banyak teknik kriptografi yang telah dipergunakan untuk menjaga keamanan data saat ini, contohnya seperti LOKI, GOST,

DOI: https://doi.org/10.29103/techsi.v10i1.605

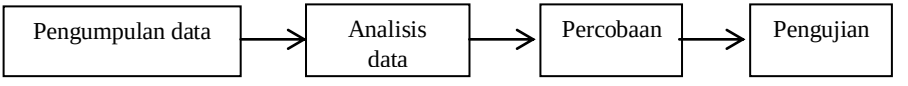
Blowfish, Vigenere, MD2, MD4, RSA dan lain sebagainya. Masing-masing teknik kriptografi tersebut memiliki kelemahan dan kelebihan. Selain teknik kriptografi yang telah disebutkan di atas masih ada teknik kriptografi lainnya maka disini penulis mencoba membahas mengenai teknik kriptogarafi *Hill Cipher*. *Hill Cipher* termasuk kepada algoritma kriptografi klasik yang sangat sulit dipecahkan oleh kriptanalis apabila dilakukan hanya dengan mengetahui berkas *ciphertext* saja. Karena *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 (Hasugian, 2013)

Masalah dalam pengamanan data masih merupanan suatu aspek penting didalam penjagaan penyimpanan data, terutama contoh data yang dipakai atau disisipkan kedalam bentuk digital. Hal ini disebabkan karena kemajuan yang sangat pesat didalam bidang ilmu komputer dengan konsep *open-system* yang sudah banyak digunakan, sehingga hal ini dapat memudahkan seseorang untuk melakukan perusakan data terutama contoh data yang dipakai atau disisipkan kedalam bentuk digital tanpa harus diketahui oleh pihak penyimpan data (Gunawan,2018).

2. METODOLOGI PENELITIAN

Tujuan dari penulisan tesis ini adalah untuk menganalisis keamanan File Gambar dan Pesan Teks dengan menggunakan algoritma Hill Cipher. Pengamanan data yang dihasilkan dari algoritma hill cipher akan mengacak ulang nilai bit data menggunakan algoritma Hill Cipher menjadi lebih kompleks.

Secara detail, metodologi penelitian ini dirancang seperti diagram blok yang terlihat dalam gambar 1.



Gambar 1. Diagram Blok Penelitian

DOI: https://doi.org/10.29103/techsi.v10i1.605

a. Pengumpulan Data

Pengumpulan data dilakukan dengan cara melakukan pemilihan beberapa jenis gambar dan sampel pesan untuk dijadikan sampel data.

b. Analisis Data

Pada tahapan analisis data ini meliputi pengecekan sampel data gambar dan pesan untuk dilakukan uji coba pencocokan pengamanan data menggunakan algoritma kriptografi hill cipher.

c. Percobaan

Percobaan dilakukan dengan melihat hasil dari uji coba pengamanan data gambar dan pesan terhadap algoritma kriptografi hill cipher.

d. Pengujian

Data yang didapat dalam proses pengujian data, akan di enkripsi menggunakan algoritma kriptografi hill cipher.

3. HASIL DAN PEMBAHASAN

3.1. Analisis Pemilihan Sampel Data

Data yang akan digunakan adalah file gambar dan sampel pesan teks untuk dijadikan sebagai sampel uji coba meningkatkan keamanan data menggunakan algoritma kriptografi hill cipher. Berikut sampel data gambar dan pesan teks yang akan dilakukan uji peningkatan keamanan data.

Tabel 1. Sampel data gambar dan pesan teks

No	Nama Gambar	Size	Pesan Teks
1	Apstar_7	411KB	STIKOM Tunas Bangsa
2	Psms_medan	142KB	Tehnik Informatika

DOI: https://doi.org/10.29103/techsi.v10i1.605

3	Ten_HD	55,3KB	Sistem Informasi
4	Kopi	5,93KB	AMIK Tunas Bangsa
5	Dolar	102KB	Manajemen Informatika
6	Assp	41,8KB	Komputerisasi Akuntansi
7	A013	67,7KB	Keamanan Data Algoritma Kriptografi Klasik
8	Assp2	58,5KB	Keamanan Data Algoritma Kriptografi Modern
9	Assp3	52,2KB	Algoritma Kriptografi Hill cipher
10	Assp4	64,6KB	Algoritma Kriptografi Caesar Cipher

3.2. Analisis Penggunaan Algoritma Kriptografi Hill Cipher

Pada tahapan ini dilakukan pengujian untuk proses pengenkripsian pesan terhadap gambar, sehingga pesan yang terisip didalam gambar akan menjadi acak dan berubah dari aslinya (enkripsi). Proses enkripsi algoritma *hill cipher* dilakukan per blok dari plainteks, dengan terlabih dahulu melakuka konversi plainteks menjadi bilangan desimal/angka, A=0, B-1, . ., Z=25.

DOI: https://doi.org/10.29103/techsi.v10i1.605

Tabel 2. Konversi Karakter Ke Desimal

A	B	C	D	E	F	G	H	I	J
0	1	2	3	4	5	6	7	8	9
K	L	M	N	O	P	Q	R	S	T
10	11	12	13	14	15	16	17	18	19
U	V	W	X	Y	Z				
20	21	22	23	24	25				

Secara matematis, proses enkripsi dari hill cipher :

C = K . P (2)

Dimana :

C = Cipherteks

K = Kunci

P = Plainteks

Contoh plainteks yang akan di sandikan adalah Indra Gunawan sebagai berikut :

Tabel 3. Plainteks dikonversi ke Desimal

1	**2**	**3**	**4**	**5**	**6**
8 13	3 17	0 6	20 13	0 22	0 13

Dimana kunci yang digunakan adalah matriks 2x2. Untuk proses perhitungan dilakukan secara blok per blok.

$$K = \begin{bmatrix} 5 & 6 \\ 2 & 3 \end{bmatrix}$$

Blok I

$$P_{1,2} = \begin{bmatrix} 8 \\ 13 \end{bmatrix}$$

Sedangkan proses enkripsinya adalah :

$$C_{1,2} = \begin{bmatrix} 5 & 6 \\ 2 & 3 \end{bmatrix} \begin{bmatrix} 8 \\ 13 \end{bmatrix} = \begin{bmatrix} (5 \times 8) + (6 \times 8) \\ (2 \times 13) + (3 \times 13) \end{bmatrix}$$

DOI: https://doi.org/10.29103/techsi.v10i1.605

$= \begin{bmatrix} 88 \\ 65 \end{bmatrix} \bmod 26$

= 10 13 -> k n

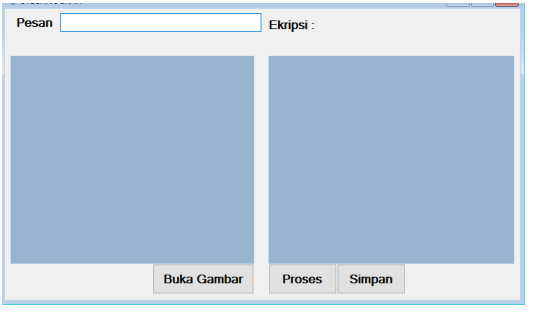
Dan begitu seterusnya, sehingga hasil enkripsinya :

Plainteks : indragunawan

Ciperteks : knhhaemnagan

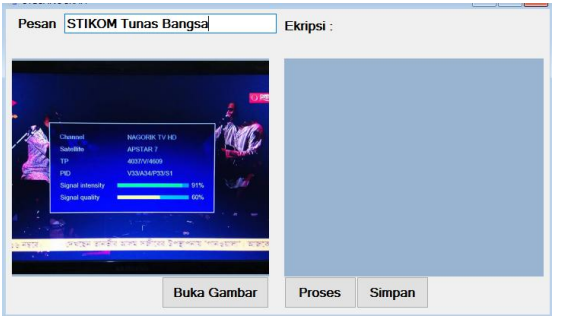
3.3. Pembahasan

Tampilan rancangan antarm uka yang akan muncul adalah sebagai berikut.



Gambar 1. Tampilan antarmuka aplikasi

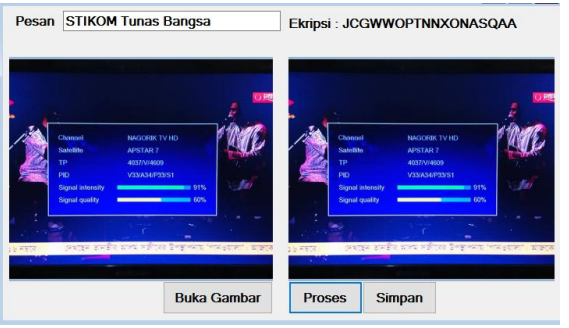
Pada gambar 1 merupakan tampilan aplikasi yang digunakan untuk proses pemilihan gambar dan pesan teks yang akan di sandikan.



Gambar 2. Proses pemilihan gambar dan Pesan Teks yang digunakan

DOI: https://doi.org/10.29103/techsi.v10i1.605

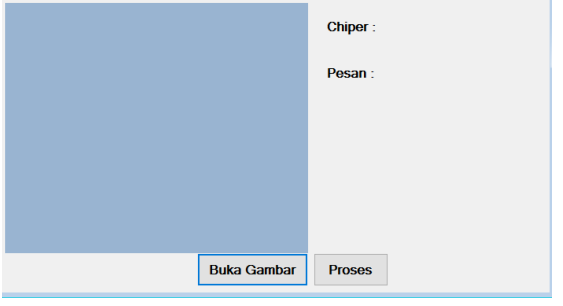
Pada gambar 2 merupakan proses pemilihan gambar dan pesan teks sebelum dikirim.



Gambar 3. Proses penyandian pesan teks dan gambar

Pada gambar 3 merupakan proses penyandian pesan teks yang sudah di enkripsi, selanjutnya dilakukan proses penyisipan kedalam gambar dan di simpan. Setelah dilakukan penyimpan file, pesan dan gambar tersebut sudah terenskripsi/tersandi dan bisa dilakukan proses pengiriman.

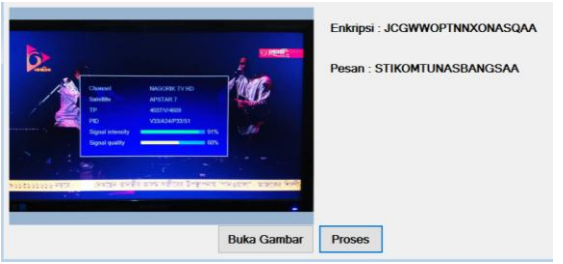
Selanjutnya untuk melakukan pengambilan pesan dari gambar yang sudah dienkripsi/disandikan adalah seperti tampilan form berikut



Gambar 4. Tampilan dasar Dekripsi Pesan

Pada gambar 4 merupakan tampilan dasar dari form untuk memproses pengambilan pesan yang sudah tersandi.

DOI: https://doi.org/10.29103/techsi.v10i1.605



Gambar 5. Proses Pengambilan Pesan tersandi

Pada gambar 5 merupakan proses pengambilan pesan dari sebuah gambar yang tersandi. Pada gambar ini menyajikan isi pesan yang tersandi dan pesan yang sudah terdeskripsi.

4. KESIMPULAN

Kesimpulan dari pembahasan diatas yang dapat diambil adalah :

a. Telah diperoleh suatu model yang baru untuk meningkatkan keamanan data gambar dan pesan teks menggunakan algoritma kriptografi hill cipher. Berdasarkan hasil pengujian aplikasi dengan menggunakan algoritma kriptografi hill cipher, dapat memberikan masukan data secara tersandi untuk memberikan tingkat keamanan pesan.
b. Dengan menambahkan algoritma kriptografi hill cipher didalam data gambar dan pesan teks, dapat meningkatkan sistem keamanan dan keabsahan originalitas dari pesan gambar dan teks.

Daftar Pustaka

Ariyus, D. 2008. *PENGANTAR ILMU KRIPTOGRAFITeori Analisis dan Implementasi*. Yogyakarta: Andi.

DOI: https://doi.org/10.29103/techsi.v10i1.605

Gunawan, I. 2018.*Penggunaan Algoritma Kriptografi Steganografi Least Significant Bit Untuk Pengamanan Pesan Teks dan Data Video*. Jurnal Sains Komputer & Informatika (J-SAKTI), Vol. 2. No. 1, Maret, pp. 57-65.

Gunawan, I. 2016.*Penggunaan Brute Force Attack Dalam Penerapannya Pada Crypt8 Dan CSA-Rainbow Tool Untuk Mencari BISS*. Jurnal Nasional Informatika dan Teknologi Jaringan (InfoTekJar), Vol. 1. No. 1, September, pp. 52-55.

Gunawan, I. 2016.*Penggunaan Acakan BISS Menggunakan Algoritma RSA*. Jurnal Riset Sistem Informasi Dan Teknik Informatika (JURASIK), Vol. 2, No. 1, Juli, pp. 58-63.

Gunawan, I. 2018. "*Kombinasi Algoritma Caesar Cipher dan Algoritma RSA Untuk Pengamanan File Dokumen Dan Pesan Teks*". Jurnal Nasional Informatika dan Teknologi Jaringan (InfoTekjar), Vol. 2. No. 2. Maret.

Hasugian, A. H. 2013. *Implemetasi Algoritma Hill Cipher Dalam Penyandian Data*. Pelita Informatika Budi Darma, Vol. IV, No. 2, Agustus 2013. pp. 115-122.

Supiyanto. 2015.*Implementasi Hill Cipher Pada Citra Menggunakan Koefisien Binominal Sebagai Matriks Kunci*. Seminar Nasional Informatika 2015 (semnasIF 2015), pp. 284-291.

DOI: https://doi.org/10.29103/techsi.v10i1.605