JUSIKOM PRIMA (Junal Sistem Informasi Ilmu Komputer Prima)
Vol. 2 No. 1, Juli 2018 e-ISSN : 2580-2879

FUNGSI ALGORITMA HILL CIPHER UNTUK PENGAMANAN FILE GAMBAR DARI SERANGAN BRUTE FORCE

[1]Indra Gunawan, [2]Sumarno, [3]Heru Satria Tambunan, [4]Eka Irawan

STIKOM Tunas Bangsa Pematangsiantar
[1,2]Program Studi Teknik Informatika, [3,4]Program Studi Sistem Informasi
indra@amiktunasbangsa.ac.id[1], sumarno@amiktunasbangsa.ac.id[2],
heru@amiktunasbangsa.ac.id[3], eka.irawan@amiktunasbangsa.ac.id[4]

ABSTRAK

Disetiap saat, perkembangan dari Teknologi Informasi Ilmu Komputer sangatlah cepat, hal ini didasari dengan munculnya berbagai teknologi terbaru yang mana teknologi tersebut dapat berimbas kepada *user*/pengguna. Sebagai bentuk dari penggunaan teknologi terbaru yang digunakan manusia adalah penggunaan dari file/data, salah satunya seperti file gambar yang dapat disimpan didalam media penyimpanan perangkat keras. Terkadang dalam proses penyimpanan data, manusia tidak menyadari jika file data tersebut akan dibajak oleh yang tidak memiliki hak. Salah satu media/algoritma pembajakan yang digunakan adalah menggunakan serangan *Brute Force*. Dalam penggunaan serangan *Brute Force* dapat membobol sistem keamanan yang terletak didalam media perangkat keras. Dalam hal ini dibutuhkan fungsi dari metode/algoritma untuk pengamanan file gambar, salah satunya adalah algoritma Hill Cipher.

Kata Kunci : Hill Cipher, Pengaman Data, *Brute Force*, Ilmu Komputer

1. PENDAHULUAN

Brute Force adalah algoritma yang memecahkan masalah dengan sangat sederhana, langsung dan dengan cara yang jelas/lempang. Penyelesaian masalah kode cracking dengan menggunakan algoritma brute force akan menempatkan dan mencari semua kemungkinan kode dengan memasukkan karakter dan panjang kode tertentu dan tentunya dengan banyaknya kombinasi kode yang digunakan [1]. Algoritma Brute Force merupakan algoritma yang lempang atau apa adanya, dimana pengguna hanya tinggal mendefinisikan karakter set yang diinginkan dan beberapa dari ukuran kodenya, tiap kemungkinan kode akan digenerate oleh algoritma ini [2]. Maka dengan menggunakan algoritma brute force ini, pengguna dapat lebih efisien dalam melakukan pemecahan keamanan file, terutama file gambar.

Keamanan merupakan masalah besar dan untuk mengamankan data penting merupakan suatu hal yang sangat penting, sehingga data yang digunakan tidak dapat disalah gunakan oleh pihak lain [3]. Masalah dalam pengamanan data masih merupakan suatu aspek penting didalam bidang penjagaan penyimpanan data, terutama data yang tersimpan dalam bentuk digital. Hal ini disebabkan kemajuan teknologi 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 data yang tersimpan dalam bentuk digital tanpa harus diketahui oleh pihak penyimpan data [4].

Dengan begitu pesatnya perkembangan era moderenisasi, pemecahan masalah dalam penemuan kode/pembajakan data dapat dilakukan dengan berbagai cara dan bisa juga menggunakan beberaoa model algoritma [5]. Beberapa jenis algoritma yang sering digunakan untuk proses pembajakan data diantaranya seperti *Brute Force*, karena algoritma jenis ini dapat digunakan untuk pemecahan masalah dengan menggunakan model yang sangat sederhana untuk proses pembajakan dan pencarian kode-kode dengan cara yang sangat sederhana.

Dengan meningkatkan sistem keamanan dari dokumen, dapat membantu mengamankan data-data yang terdapat didalam media penyimpanan

[6], sehingga berkas dokumen terutama file gambar dapat terjaga kemanannya disaat data tersebut tersimpan didalam media penyimpanan (*Harddisk*).

Kriptografi sendiri merupakan sebuah seni yang meliputi prinsip-prinsip dan metode-metode pengubahan data yang dimengerti (*plaintext*) menjadi pesan yang tidak dimengerti (*ciphertext*) dan kemudian retransforming, pesan yang akan kembali kebentuk aslinya [7]. 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 [8].

Banyak teknik kriptografi yang telah dipergunakan untuk menjaga keamanan data saat ini, contohnya seperti LOKI, GOST, 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 [9].

2. IMPLEMENTASI

Data yang digunakan adalah file gambar yang akan dijadikan sampel data dan data yang akan diproses untuk diamanan keaslian datanya dari serangan *brute force* dengan menggunakan metode algoritma hill cipher. Berikut sampel data gambar yang dijadikan dan dilakukan uji peningkatan keamanan datanya.

Tabel 1. Sampel Data Gambar

No	Nama Gambar	Ukuran
1.	Kopi.Jpg	5,93 KB
2.	Piala_dunia.Jpg	67,1 KB
3.	Apstaren.Jpg	411 KB
4.	Aqua.Jpg	209 KB
5.	IPTV.Jpg	838 KB
6.	Intel.Jpg	107 KB
7.	Transfer.jpg	173 KB
8.	Ultah.Jpg	42,0 KB
9.	Earnmoney.Jpg	257 KB
10.	Assp.Jpg	41,8 KB
11.	Koala.Jpg	155 KB
12.	Desert.Jpg	250 KB
13.	Penguins.Jpg	313 KB
14.	Tulips.Jpg	213 KB
15.	Jellyfish.Jpg	155 KB
16.	Hydrangeas.Jpg	213 KB
17.	Chrysanthenum.Jpg	431 KB
18.	Lighthouse.Jpg	324 KB

Dari sampel data yang terdapat pada tabel diatas selanjutnya akan dianalisis dan dilakukan proses pengujian pengenkripsian file gambar, sehingga file gambar akan sedikit terjadi perubahan mengenai ukuran file dan posisi bit-bit dari file gambar dikarenakan proses enkripsi dari file gambar.

Selanjutnya melakukan pengujian dan analisis dari sampel data yang sudah ditetapkan dengan menggunakan algoritma Hill Cipher. Proses enkripsi menggunakan algoritma Hill Cipher dilakukan secara blok per blok dari plaintext. Dengan kata lain sebelum melakukan proses enkripsi, maka file gambar akan terlebih dahulu di ekstrak kedalam bentuk bilangan biner, selanjutnya dilakukan proses enkripsi. Selanjutnya melakukan konversi plainteks kebilangan desimal / angka, A=0, B=1, . ., Z=25.

Tabel 2. Konversi Plainteks 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 hitungan matematis, proses dari perhitungan enkripsi algoritma Hill Cipher adalah sebagai berikut :

C = K . P (2)

Dimana :

C = Cipherteks ; P = Plainteks

K = Kunci

Contoh Plainteks yang akan disandikan adalah Indra Gunawan, sebagai berikut :

Tabel 3. Proses Plainteks ke Desimal

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

Dimana kunci yang digunakan merupakan himpunan dari sebuah matriks yang memikiki ordo 2x2. Untuk proses perhitungannya dilakukan secara blok per blok.

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

Untuk proses Blok I :

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

Sedangkan untuk proses penyandiannya adalah sebagai berikut :

$$C_{1,2} = \begin{bmatrix} 5 & 6 \\ 2 & 3 \end{bmatrix} \begin{bmatrix} 8 \\ 13 \end{bmatrix} = \begin{bmatrix} (5x8) & + & (6x8) \\ (2x13) & + & (3x13) \end{bmatrix}$$

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

= 10 13 - > kn

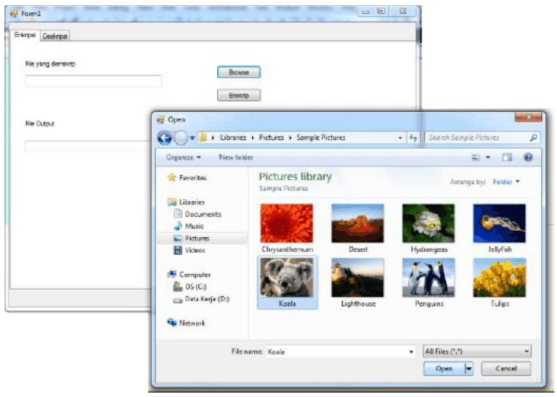
Dan begitu seterusnya, sehingga hasil dari proses enkripsi untuk keseluruhan plainteks adalah :

Plainteks : indragunawan

Cipherteks : knhhaemnagan

3. HASIL

Hasil dari pembahasan dituangkan kedalam sebuah rancangan aplikasi, agar dapat mempercepat proses perhitungan proses enkripsi.

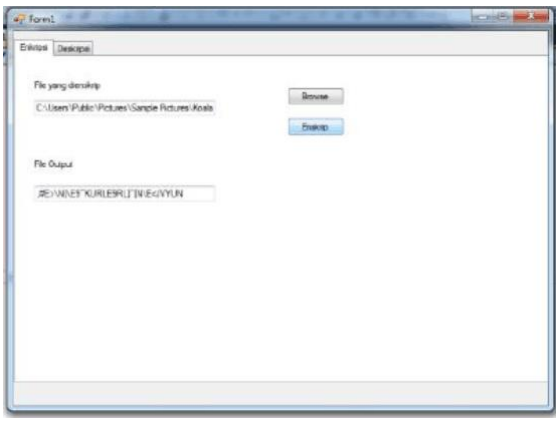


Gambar 1. Pemilihan File Gambar

Pada gambar 1, proses pencarian file gambar yang akan di enkripsi. Jenis gambar yang digunakan adalah jenis gambar yang melikiki ekstensi Jpg.

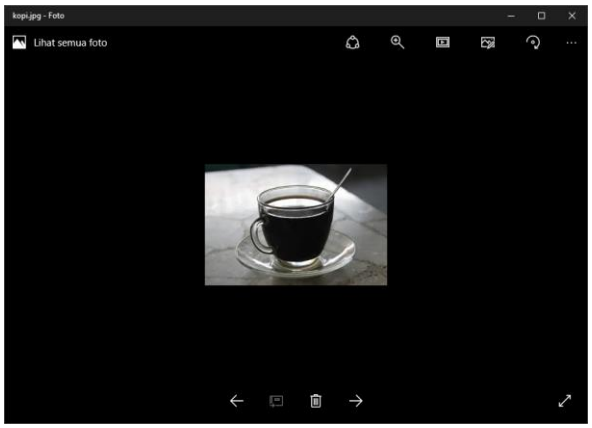
Gambar 2. Proses Validasi Sandi

Pada gambar 2 menerangkan proses untuk memvalidasi file gambar dengan memberikan password, agar keaslian file gambar bisa semakin terjaga.



Gambar 3. Proses Penyadian /Enkripsi

Pada gambar 3, proses penyandian file gambar dilakukan serta menentukan kembali posisi/lokasi penyampinan file gambar yang sudah di sandikan / enkripsi.



Gambar 4. Hasil Gambar sesudah di enkripsi

Pada gambar 4, hasil gambar sesudah dienkripsi tidak akan terjuda perubahan yang sangat signifikan terhadap file gambar, dikarenakan proses enkripsi / penyandian yang dilakukan terhadap file gambar hanya memberikan sandi-sandi serta sedikit memodifikasi bilangan bit yang terdapat pada file gambar. Perubahan yang terjadi pada file gambar adalah hanya sebatas penambahan ukuran/besar kapasitas dari file gambar saja.

Tabel 3. Perubahan Ukuran File Gambar

No	Nama Gambar	Ukuran
1.	Kopi.Jpg	6,80 KB
2.	Piala_dunia.Jpg	77,0 KB
3.	Apstaren.Jpg	451 KB
4.	Aqua.Jpg	299 KB
5.	IPTV.Jpg	878 KB
6.	Intel.Jpg	127 KB
7.	Transfer.jpg	193 KB
8.	Ultah.Jpg	52,1 KB
9.	Earnmoney.Jpg	287 KB
10.	Assp.Jpg	48,8 KB
11.	Koala.Jpg	185 KB
12.	Desert.Jpg	290 KB
13.	Penguins.Jpg	363 KB
14.	Tulips.Jpg	253 KB
15.	Jellyfish.Jpg	195 KB
16.	Hydrangeas.Jpg	253 KB
17.	Chrysanthenum.Jpg	471 KB
18.	Lighthouse.Jpg	374 KB

4. KESIMPULAN

Kesimpulan yang dapat diambil dari pembahasan diatas adalah sebagai berikut :

a. Diperoleh suatu model baru yang dapat digunakan untuk meningkatkan proses pengamanan data file gambar.
b. Fungsi algoritma hill cipher dapat bekerja secara optimal dalam proses pengamanan file gambar.

DAFTAR PUSTAKA

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

[2]. Sianipar, K.D.R., Purba, L.C., Siahaan, S.W., Gunawan, I., Sumarno. "*Pengamanan File Gambar Menggunakan Fungsi Algoritma Steganografi LSB Dari Serangan Brute Force*". Jurnal Techsi. Vol. 10, No. 1, pp 155-162. April 2018.

[3]. Gunawan, I. "*Pengamanan Acakan BISS Menggunakan Algoritma RSA*". Jurnal Riset Sistem Informasi DanTeknik Informatika (JURASIK). Vol. 2, No. 1, pp. 58-63. Juli 2017.

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

[5]. Gunawan, I. "*Fungsi Algoritma Kriptografi Hill Cipher Untuk Pengamanan File Gambar dan Pesan Teks*". Jurnal Techsi. Vol. 10, No. 1. April 2018.

[6]. Gunawan, I. "*Pengamanan Berkas Dokumen Menggunakan Fungsi Algoritma Steganografi LSB*". ALGORITMA : Jurnal Ilmu Komputer dan Informatika. Vol. 2, No. 1, pp. 61-65. April 2018.

[7]. Ariyus, D. "*PENGANTAR ILMU KRIPTOGRAFI, Teori Analisis dan Implementasi*". Yogyakarta : Andi.

[8]. Supiyanto. "*Implementasi Hill Cipher Pada CITRA Menggunakan Koefisien Binominal Sebagai Matriks Kunci*". Seminar Nasional

Informatika 2015 (SemNas IF 2015). pp. 284-291.

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