# Modifikasi Keamanan File dengan Algoritma Hill Cipher Untuk Mengantisipasi Dari Serangan Brute Force

**Indra Gunawan** [1]
STIKOM Tunas Bangsa Pematangsiantar
Program Studi Teknik Informatika
indra@amiktunasbangsa.ac.id[1]

**Abstrak**

*Abstrak*— Pada saat ini, perkembangan dan perubahan Teknologi Informasi Ilmu Komputer sangatlah cepat, hal ini didasari dengan mulai beredarnya berbagai teknologi yang terbaru dimana teknologi tersebut dapat terkena kepada *user*/pengguna. Sebagai bentuk dari pemakaian teknologi terbaru yang dipakai oleh manusia adalah penggunaan dari data/file yang dapat disimpan didalam media penyimpanan perangkat keras (*hardware*). Ada kalanya dalam proses penyimpanan data, *user* tidak menyadari jika file data tersebut akan dibajak dan disalahgunakan oleh orang-orang yang tidak memiliki hak. Dengan melakukan penyerangan data menggunakan beberapa metode, seperti *Brute Force*, keamanan data langsung dapat dibobol. Dalam hal ini dibutuhkan fungsi dari metode/algoritma kriptografi untuk pengamanan file/data, salah satunya adalah algoritma Hill Cipher.

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

## 1. Pendahuluan

Brute Force merupakan suatu algoritma yang dapat memecahkan suatu masalah dengan sangat sederhana, langsung dan dengan cara yang jelas. Dalam penyelesaian suatu masalah kode cracking dengan menggunakan algoritma *brute force* akan memposisikan dan melakukan pencarian ke semua kemungkinan kode dengan memasukkan karakter dan panjang kode tertentu dan tentunya dengan banyaknya kombinasi kode yang

DOI: https://doi.org/10.29103/techsi.v11i2.1272

digunakan[1]. Jadi dengan kata lain, penggunaan algoritma *brute force* bagi orang yang tidak memikirkan masalah kedepannya, dapat melakukan pembobolan data dari mana dan kapan saja jika mereka menginginkan untuk melakukan pencurian data.

Algoritma *Brute Force* adalah beberapa dari jenis 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 suatu masalah yang sangat besar dan untuk melakukan pengamanan data yang penting merupakan suatu hal yang sangat penting dan tidak boleh untuk diabaikan, sehingga data yang digunakan tidak dapat disalah gunakan oleh pihak lain[3]. Karena keamanan data merupakan suatu faktor yang sangat penting, maka untuk mengamankan data sangat dibutuhkan penambahan metode-metode yang dapat berfungsi untuk meningkatkan sistem keamanan dari sebuah data.

Masalah didalam proses pengamanan data masih merupakan suatu aspek yang sangat penting didalam proses bidang penjagaan penyimpanan data, terutama data yang tersimpan didalam bentuk digital. Hal ini dapat disebabkan oleh kemajuan teknologi yang sangat cepat dan pesat didalam bidang ilmu komputer dengan konsep *open system* dan *open source* 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]. Jadi dengan meningkatkan sistem keamanan data dengan menggunakan beberapa metode dari ilmu kriptografi, dapat menambah kekuatan proteksi dari keamanan data.

Dengan begitu kencang dan pesatnya perkembangan era moderenisasi, penyelesaian dan pemecahan masalah dalam penemuan kode/pembajakan data dapat dilakukan dengan berbagai cara dan bisa juga menggunakan beberapa model dari metode algoritma[5]. Dari beberapa jenis metode algoritma yang

DOI: https://doi.org/10.29103/techsi.v11i2.1272

paling sering dipakai untuk proses pembobolan data adalah seperti metode *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 data, dapat membantu mengamankan data-data yang terdapat didalam media penyimpanan[6], sehingga berkas dokumen data terutama file-file data yang penting dapat terjaga kemanannya disaat data tersebut tersimpan didalam media penyimpanan (*Harddisk*).

Kriptografi sendiri adalah 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:

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

Kriptografi (*Cryptography*) adalah suatu cabang ilmu dari matematika yang membahas tentang penyandian data agar keamanan data dapat terjaga[8].

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

DOI: https://doi.org/10.29103/techsi.v11i2.1272

enkripsinya lebih mudah diketahui, karena satu huruf pada ciphertext pasti merepresentasikan satu huruf pada plaintext[9]. 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 [10].

## 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 File

| No | Nama Gambar | Ukuran |
|---|---|---|
| 1. | Kopi.Jpg | 5,93 KB |
| 2. | Piala_dunia.xlsx | 130,1 KB |
| 3. | Apstaren.docx | 411 KB |
| 4. | pesan.pdf | 309 KB |
| 5. | IPTV.Jpg | 838 KB |
| 6. | Intel.pdf | 157 KB |
| 7. | Transfer.docx | 673 KB |
| 8. | Ultah.Jpg | 42,0 KB |
| 9. | Earnmoney.xlsx | 457 KB |
| 10. | Assp.pdf | 341,8 KB |
| 11. | Koala.Jpg | 155 KB |

DOI: https://doi.org/10.29103/techsi.v11i2.1272

| | | |
|---|---|---|
| 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 data, sehingga file data akan sedikit terjadi perubahan mengenai ukuran file dan posisi bit-bit dari file gambar dikarenakan proses enkripsi dari file data.

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 | | | | |

DOI: https://doi.org/10.29103/techsi.v11i2.1272

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 :

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

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

$$= 10 \quad 13 \text{ -> kn}$$

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

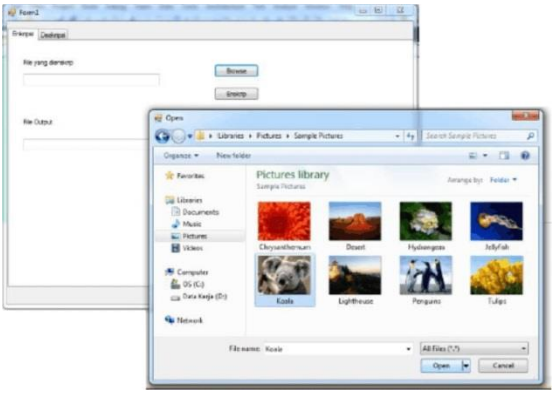
Plainteks : indragunawan

Cipherteks : knhhaemnagan

DOI: https://doi.org/10.29103/techsi.v11i2.1272

## 3. Hasil dan Pembahasan

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



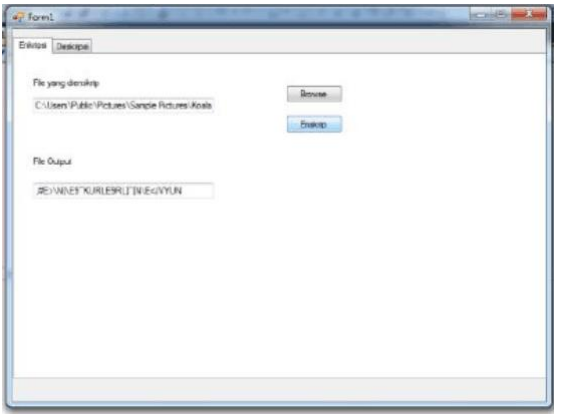

**Gambar 1.** Pemilihan File data

Pada gambar 1, proses pencarian file data yang akan di enkripsi. Jenis file data yang digunakan adalah jenis file data yang terdapat didalam komputer (docx, xlsx. Pdf, jpg).


**Gambar 2.** Proses Validasi Sandi

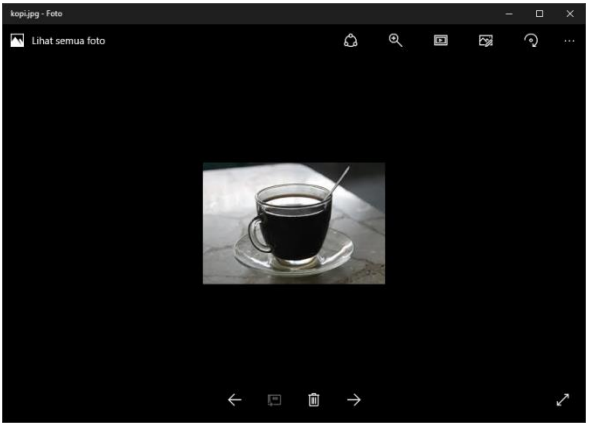
Pada gambar 2 menerangkan proses untuk memvalidasi file data dengan memberikan password, agar keaslian file data bisa semakin terjaga.

DOI: https://doi.org/10.29103/techsi.v11i2.1272




**Gambar 3.** Proses Penyadian /Enkripsi

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




Gambar 4. Hasil file data sesudah di enkripsi

Pada gambar 4, hasil file data sesudah dienkripsi tidak akan terjadi perubahan yang sangat signifikan terhadap file data, dikarenakan proses enkripsi / penyandian yang dilakukan terhadap file data hanya memberikan sandi-sandi serta sedikit merubah bilangan bit yang terdapat pada file data. Perubahan

DOI: https://doi.org/10.29103/techsi.v11i2.1272

yang terjadi pada file data adalah hanya sebatas penambahan ukuran/besar kapasitas dari file data saja.

**Tabel 3.** Perubahan Ukuran File Data

| No | Nama Gambar | Ukuran |
|---|---|---|
| 1. | Kopi.Jpg | 6,93 KB |
| 2. | Piala_dunia.xlsx | 140,1 KB |
| 3. | Apstaren.docx | 461 KB |
| 4. | pesan.pdf | 369 KB |
| 5. | IPTV.Jpg | 888 KB |
| 6. | Intel.pdf | 257 KB |
| 7. | Transfer.docx | 773 KB |
| 8. | Ultah.Jpg | 52,0 KB |
| 9. | Earnmoney.xlsx | 497 KB |
| 10. | Assp.pdf | 391,8 KB |
| 11. | Koala.Jpg | 255 KB |
| 12. | Desert.Jpg | 350 KB |
| 13. | Penguins.Jpg | 393 KB |
| 14. | Tulips.Jpg | 283 KB |
| 15. | Jellyfish.Jpg | 255 KB |
| 16. | Hydrangeas.Jpg | 283 KB |
| 17. | Chrysanthenum.Jpg | 531 KB |
| 18. | Lighthouse.Jpg | 394 KB |

## 4. Kesimpulan

Kesimpulan yang dapat diambil dari pembahasan diatas adalah sebagai berikut :

a. Didapat sebuah model baru yang dapat digunakan untuk meningkatkan proses pengamanan data file data.
b. Metode algoritma hill cipher dapat bekerja dan berproses secara optimal dalam pengamanan file data.

DOI: https://doi.org/10.29103/techsi.v11i2.1272

## 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]. Gunawan, I., Sumarno., Tambunan, H. S., "*Fungsi Algoritma RSA Untuk Memodifikasi dan Meningkatkan Pengamanan Acakan BISS*". CESS (Journal of Computer Engineering System and Science). Vol. 3, No. 2, pp. 62-68. Juli 2018.

[9]. Supiyanto. "*Implementasi Hill Cipher Pada CITRA Menggunakan Koefisien Binominal Sebagai Matriks Kunci*". Seminar Nasional Informatika 2015 (SemNas IF 2015). pp. 284-291.

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

DOI: https://doi.org/10.29103/techsi.v11i2.1272