



Available online at : <http://bit.ly/InfoTekJar>

# InfoTekJar : Jurnal Nasional Informatika dan Teknologi Jaringan

ISSN (Print) 2540-7597 | ISSN (Online) 2540-7600



Click here and write your Article Category

## RANCANG BANGUN APLIKASI KRIPTOGRAFI UNTUK PENGAMANAN DOKUMEN MENGGUNAKAN METODE SHIFT CIPHER SEKALIGUS MENGKOMPRESIKANNYA DENGAN METODE HUFFMAN

Rachmat Aulia, Rahanda Zulfi.S

Prodi Teknik Informatika Fakultas Teknik dan Komputer Universitas Harapan Medan, Jl.H.M Joni No.70C, Medan, Sumatera Utara, Indonesia

### KEYWORDS

Shift Cipher, Kriptografi, File, Modulo

### CORRESPONDENCE

Phone: +62 813 1507 3770

E-mail: jackm4t@gmail.com

zrahanda@gmail.com

### A B S T R A C T

Kriptografi merupakan keahlian dan ilmu yang digunakan terkait cara-cara berkomunikasi dan juga sebagai alat untuk menjamin keamanan dan kerahasiaan informasi. Karena itu proses dalam informasi telah dirasakan oleh banyak pihak dalam keamanan data, khususnya *file*. Informasi sangat rentan jika disalahgunakan dengan yang tidak berkepentingan. Berdasarkan kejadian tersebut, maka dibutuhkan metode untuk mengamankan data. Metode yang dimaksud untuk mengamankan data adalah Kriptografi. Salah satu Algoritma Kriptografi yang diterapkan pada penelitian ini adalah Shift Cipher. Cara kerja Shift Cipher adalah suatu metode yang menggunakan proses penyandian operasi modulo 26 di dalam proses perhitungan. Percobaan yang telah dilakukan pada sejumlah *file* dokumen, membuktikan bahwa Shift Cipher mempunyai kehandalan dalam mengamankan data, dan terkait kompresinya metode Huffman berperan sebagai hasil ekstraksi *file* yang telah berhasil dilakukan tanpa merusak *file* induk dan *file* pesan sekaligus tidak merubah isinya.

### INTRODUCTION

Kemajuan teknologi informasi terutama pengamanan data saat ini berkembang pesat. Berbagai metode yang digunakan manusia untuk pengamanan data atau dokumen. Dalam melindungi keamanan suatu *file* diperlukan teknik enkripsi dan dekripsi. Teknik ini berguna untuk membuat pesan, data, maupun dokumen menjadi aman [1]. Kebutuhan masyarakat akan keamanan informasi dapat terpenuhi dengan adanya teknik kriptografi. Data-data informasi seharusnya hanya boleh diketahui oleh pihak tertentu, karena hal tersebut termasuk kedalam teknologi informasi dalam hal keamanan informasi [2].

Pesatnya sirkulasi teknologi komputer masa ini sering mengakibatkan manipulasi teknologi tercatat bagian dalam sikap kriminal sehingga kemanan dokumen merupakan hal yang sangat penting dalam menjaga kerahasiaan informasi, terutama yang berisi informasi yang sensitif dan tidak boleh diketahui isinya oleh pihak lain. Dokumen-dokumen yang berisi data strategis atau rahasia menjadi sangat beresiko jika tidak diamankan isi dari

data tersebut. Terdapat kemungkinan untuk di salah gunakan oleh pihak lain [3].

Kriptografi merupakan ilmu sistematis yang erkaitan dengan aspek-aspek yang berkaitan dengan kemanan data seperti menyembunyikan isi data, melindungi data dapat dirubah tanpa diketahui, ataupun melindungi isi data digunakan tanpa daya yang cukup [4]. Teknologi kriptografi berkembang dari tahun ke tahun. Perubahan tersebut terdapat pada keamanan data dan pesan, metode tersebut digunakan untuk enkripsi dan dekripsi, dan lain-lain [5]. Enkripsi adalah cara untuk mengubah isi data sehingga tidak dapat dimengerti oleh orang lain kecuali oleh pengguna yang menggunakannya dan orang yang di beri kebebasan untuk mengubah isi data tersebut [1].

Ada beberapa algoritma kriptografi yang bisa mengamankan dokumen salah satunya adalah metode Shift Cipher. Shift Cipher adalah suatu metode yang menggunakan proses penyandian operasi modulo 26 di dalam proses perhitungan. Untuk proses enkripsi dan proses dekripsi menggunakan kunci yang sama dalam penggunaannya [6].

Hasil dari algoritma Shift Cipher tersebut akan di kompresikan ke metode Huffman. Sementara definisi dari metode Huffman adalah metode yang dikembangkan David A. Huffman pada 1952. Metode Huffman menganjurkan prinsip pengkodean yang sangat mirip dengan aturan morse, yaitu tiap tanda dan simbol dianjurkan menggunakan rangkaian beberapa *bit*, dimana karakter yang sering muncul dikodekan dengan rangkaian *bit* yang tidak panjang dan simbol yang tidak muncul dikodekan dengan deretan *bit* yang lebih panjang, karena caranya yang menggunakan kode ini [7].

Pada penelitian sebelumnya dinyatakan, informasi hanya bisa digunakan oleh pihak yang berwenang melalui teknik kriptografi dengan menerapkan algoritma kriptografi cipher dari hasil penelitian dengan memakai file .docx, file hasil proses enkripsi tidak mengalami perubahan baik isi ataupun ukuran data. Proses ekstrak berjalan sempurna dan membuat file *output* dekripsi sama halnya dengan file dekripsi [3].

Pada penelitian sebelumnya dinyatakan, keamanan data pribadi pada pengarsipan surat sudah terbilang aman karena algoritma *vignere* hasil dari pengenkripsannya tidak persis dengan plainteksnya jadi sehingga bagi orang awam itu sudah sangat rumit jika karakter algoritmanya panjang [8].

Pada penelitian sebelumnya dinyatakan, metode huffman yang digunakan menghasilkan nilai *output* yang sama dengan hasil perhitungan biasa serta dari hasil pengujian black box diperoleh luaran bahwa sistem telah bisa melakukan proses enkripsi dan dekripsi file txt, serta kompresi file tanpa merusak isi dari file seperti yang diharapkan [9].

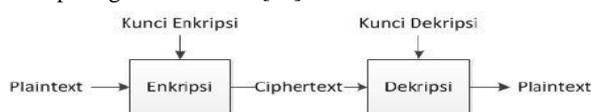
Tujuan dilakukannya penelitian ini untuk merancang dan membangun aplikasi kriptografi keamanan data berupa file menggunakan algoritma Shift Cipher sekaligus mengkompresikannya dengan metode Huffman.

## METHOD

Observasi yang diterapkan menggunakan beberapa tahap untuk mengamankan dokumen dengan metode Shift Cipher dan Metode Huffman. Adapun tahapan metode penelitian yang diterapkan adalah sebagai berikut:

### Kriptografi

Untuk mengubah pesan asli ke dalam susunan yang tidak beraturan diperlukan suatu tahapan. Dalam ilmu kriptografi, ada cara untuk mendapatkan pesan yang terenkripsi dapat diterapkan sesuai pada gambar berikut [10]:



Gambar 1. Dasar Kriptografi

Teknik enkripsi dapat diterapkan dengan menggunakan pesan asli dan kunci, selanjutnya menghasilkan *output* ciphertext (pesan terenkripsi). Ciphertext dapat dikembalikan dalam bentuk aslinya (plaintext) dengan memasukkan kembali kunci beserta

ciphertext-nya.

### Metode Shift Cipher

Algoritma Shift Cipher adalah salah satu bentuk *mono alphabet* cipher selain Caesar Cipher. Untuk Menerapkan cara dari algoritma *Shift Cipher* persis seperti *Caesar Cipher* yaitu menggeser isi pesan sejauh *key* yang ditentukan. Pada *Shift Cipher*, *key* yang berfungsi umumnya 13 sehingga *Shift Cipher* dinamakan sebagai rot 13. Maksimal perpindahan kunci pada *Shift Cipher* adalah 26 pergeseran. *Shift Cipher* persis dengan *Caesar Cipher* yang menggunakan pergeseran modulo 26 [6].

Berikut ini rumus yang diterapkan untuk mencari nilai enkripsi dan dekripsi [8]:

### Enkripsi

$$E_K(x) = (x+k) \bmod 26$$

Keterangan:

E = Enkripsi

k = *Key*

x = *Plaintext*

### Dekripsi

$$D_K(y) = (y-k) \bmod 26$$

Keterangan:

D = Dekripsi

k = *Key*

y = *Plaintext*

### Metode Huffman

Metode Huffman dicetuskan pertama kali oleh D.A Huffman pada tahun 1952. Metode ini merupakan terusan dari metode yang berfungsi sebagai metode mengecilkan data yang ditulis oleh R.M. Fano dan *Claude Shannon*. Metode ini memanfaatkan graf dan pohon biner. Graf yang bisa dibuat seperti pohon memusat dan bisa menyesuaikan pohon biner. Sedangkan pohon biner ditujukan kepada awal penyusunan kode. Pohon biner yang digunakan haruslah merupakan kumpulan dari kode awalan. Kode awal yang digunakan untuk menjauhi keambiguan, karena akan sangat bermanfaat pada kompresi data yang memperuntukkan ukuran bit yang berbeda-beda. Ide pokok berasal dari metode Huffman yang memuat kode dengan gambaran bit yang lebih kecil pada kode ASCII yang sering terlihat di bagian dalam file dan menciptakan intruksi dengan bentuk bit yang lebih panjang untuk kode ASCII yang sedikit terlihat di dalam file [9].

Cara kerja kompresi pada metode Huffman [11]:

- 1) Membentuk karakter yang ada pada pesan dan menghitung probabilitas (kemunculannya).
- 2) Setelah membentuk urutan karakter beserta probabilitas (kemunculannya), kemudian mengurutkan dari yang terbesar sampai terkecil.

- 3) Setelah menyusun kemunculannya, lalu membuat dua tanda (karakter) dengan kemunculan sedikit lalu menyatukannya jadi satu bagian. Dua karakter yang menyimpan kemunculan sedikit maka dapat dipisahkan dari karakter yang kemunculannya banyak.
- 4) Dua karkater yang kemunculannya terendah kemudian diubah dengan karakter baru yang menggambarkan kedua karakter tersebut, yang dimana nilai kemunculannya adalah hasil kemunculan dari dua karakter tersebut.

**RESULTS AND DISCUSSION**

**Proses enkripsi dengan Metode Shift Cipher**

Cara yang dilakukan untuk mengamankan dokumen adalah dengan memasukan pesan “RAHANDA” dengan kunci pergeseran sebanyak lima pergeseran ke kanan. Adapun rincian substitusi :

Tabel 1. Tabel Konversi Shift Cipher

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				

Tabel 2. Proses Pengubahan Karakter Pesan Ke Angka

P Karakter	R	A	H	A	N	D	A
P Tabel	17	0	7	0	13	3	0

Perhitungan:

$E(x)=(x+k)\text{mod } 26$

- a)  $E(R)=(17+5) \text{ mod } 26$   
 $E(R)=(22) \text{ mod } 26$   
 $E(R)=22 (W)$
- b)  $E(A)=(0+5) \text{ mod } 26$   
 $E(A)=(5) \text{ mod } 26$   
 $E(A)=5 (F)$
- c)  $E(H)=(7+5) \text{ mod } 26$   
 $E(H)=(12) \text{ mod } 26$   
 $E(H)=12 (M)$
- d)  $E(A)=(0+5) \text{ mod } 26$   
 $E(A)=(5) \text{ mod } 26$   
 $E(A)=5 (F)$
- e)  $E(N)=(13+5) \text{ mod } 26$   
 $E(N)=(18) \text{ mod } 26$   
 $E(N)=18(S)$
- f)  $E(D)=(3+5) \text{ mod } 26$   
 $E(D)=(8) \text{ mod } 26$   
 $E(D)=8(I)$

- g)  $E(A)=(0+5) \text{ mod } 26$   
 $E(A)=(5) \text{ mod } 26$   
 $E(A)=5 (F)$

Hasil enkripsinya adalah : “WFMFSIF”

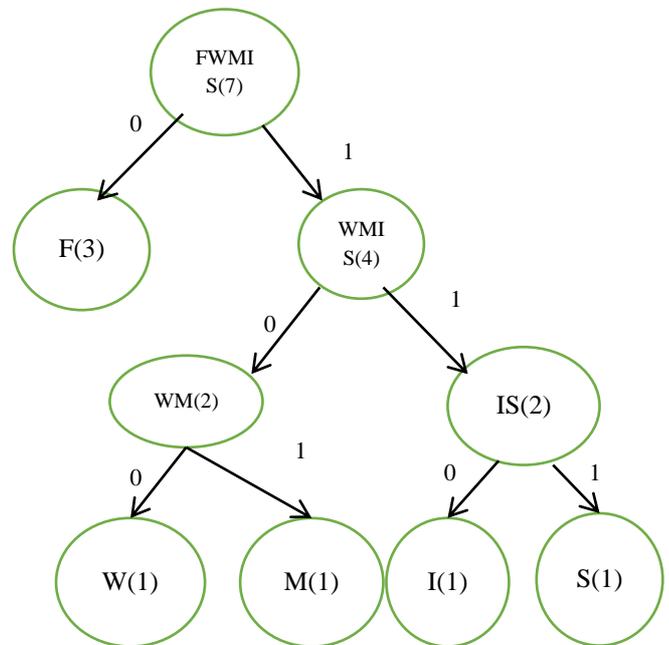
**Proses Kompresi Metode Huffman**

Proses kompresi file dengan metode Huffman yang berisikan string “WFMFSIF”. Penjelasan string tersebut sebelum dikompresi:

Table 3. String Sebelum Kompresi

No	Karakter	Frekuensi	Decimal
1	W	1	87
2	F	3	70
3	M	1	77
4	S	1	83
5	I	1	73

Berdasarkan frekuensi tersebut maka pohon Huffmannya adalah sebagai berikut



Gambar 1. Pohon Huffman

Table 4. Substitusi Frekuensi

No	Karakter	Frekuensi	Bit Substitusi
1	F	3	0
2	W	1	100
3	M	1	101
4	S	1	110
5	I	1	111

**Proses Dekompresi Metode Huffman**





- [8] Refnaldi kurniawan saputra, G. Rahmi Fajri, S. Ahmad, E. Haris Sembiring, and M. A. Hasan, "Keamanan Data Pada Pengarsipan Surat Menggunakan Metode Kriptografi Klasik Vigenere Cipher Dan Shift Cipher," *Zo. J. Sist. Inf.*, vol. 2, no. 1, pp. 61–72, 2021, doi: 10.31849/zn.v2i1.6220.
- [9] G. A. Pradnyana and I. B. P. Suarma Putra, "Pengamanan Berkas Data Digital Dengan Algoritma Kombinasi Triple Transposition Vigenere Cipher Dan Metode Huffman," *J. Pendidik. Teknol. dan Kejur.*, vol. 15, no. 1, pp. 81–91, 2018, doi: 10.23887/jptk-undiksha.v15i1.13045.
- [10] R. Aulia, A. Zakir, and M. Zulhafiz, "Penerapan Algoritma One Time Pad & Linear Congruential Generator Untuk Keamanan Pesan Teks," *InfoTekJar (Jurnal Nas. Inform. dan Teknol. Jaringan)*, vol. 1, pp. 37-41, 2019, doi: <http://dx.doi.org/10.30743/infotekjar.v4i1.1375>.
- [11] K. Mahesa, "Rancang Bangun Aplikasi Kompresi Dan Dekompresi Pada Citra Digital Menggunakan Metode Huffman," *J. Process.*, vol. 12, no. 1, pp. 948–963, 2017.