

SUPER ENKRIPSI DENGAN MODIFIKASI VIGENERE CHIPER DENGAN TRANSPOSISI KOLOM KEDALAM SANDI MORSE UNTUK KEAMANAN PESAN

ADITYO RAZZAQI¹⁾, IMMANUEL SURBAKTI²⁾, RIZKY JONATAN SURBAKTI³⁾,
ACHMAD FAUZI⁴⁾

^{1,2,3,4)} STMIK KAPUTAMA

Jl. Veteran No. 4A-9A, Binjai 20714, Sumatra Utara, Telp: (061)8828840, Fax: (061)8828845
Email: Yogahes87@gmail.com.

ABSTRACT

Text message security is a major concern in the digital era due to the risk of interception and unauthorized access. This study proposes a super encryption method by combining modified Vigenere Cipher, columnar transposition, and Morse encryption to enhance text message security. The encryption process begins with the Vigenere algorithm to generate the initial ciphertext, followed by columnar transposition, and concludes with conversion to Morse code. The results demonstrate that this method provides layered security that is difficult to penetrate, making it an effective solution for protecting digital communications from cyber threats. The strength of this method lies in its ability to synergize cryptographic algorithms, offering a higher level of confidentiality compared to conventional methods.

Keywords: Columnar_Transposition, Super_encryption, Message_Security, Morse_Code.

1. PENDAHULUAN

Di era yang semakin digital, kebutuhan akan keamanan informasi menjadi salah satu prioritas utama. Pesan teks, salah satu media komunikasi yang paling banyak digunakan, rentan terhadap intersepsi dan akses oleh pihak yang tidak berkepentingan. Oleh karena itu, pengembangan teknik enkripsi yang lebih kompleks dan aman sangatlah penting.

Berdasarkan keamanan datanya, akan mungkin untuk mengembangkan sistem pengumpulan data yang lebih efektif yang dapat mengumpulkan data dari beberapa potensi ancaman yang timbul. Ini adalah komponen utama dari sistem keamanan data yang berfungsi untuk melindungi data yang dikirim atau diterima melalui jaringan komunikasi[1].

Kriptografi merupakan salah satu teknik yang dapat digunakan untuk menghasilkan informasi. Dua langkah yang sering

dilakukan dalam kriptografi adalah enkripsi dan deskripsi. Salah satu yang digunakan untuk mengubah teks menjadi Ciphertext adalah enkripsi, sedangkan proses lainnya adalah dekripsi, yang digunakan untuk mengubah teks ke dalam format yang dapat dibaca dan dipahami [2]. Caesar cipher merupakan salah satu metode yang dapat digunakan dalam kriptografi. Julius Caesar menggunakan Caesar cipher lebih cekatan untuk pertama kalinya pada tahun 50 SM untuk menyampaikan pesan kepada Marcus Cicero. Mengikuti informasi asli dalam alfabet, Caesar merestrukturisasi informasi dengan membuat setiap huruf dalam informasi menjadi tiga huruf alfabet. Algoritma yang digunakan dalam cipher caesar cukup sederhana dan mudah dipahami. Oleh karena itu, mereka hampir tidak pernah gagal dalam menangkap kerahasiaan informasi[3].

2. METODOLOGI PENELITIAN

2.1. Vigenere Chiper

Perkembangan teknologi dalam sistem keamanan yang bertujuan untuk menjamin kerahasiaan data dan informasi berkembang pesat . Untuk menjaga kerahasiaan data dikembangkan suatu ilmu pengetahuan seperti kriptografi Vigenère . Implementasinya tidak dilakukan dengan satu teknik keamanan data saja , tetapi bisa juga dengan menggabungkan atau memodifikasi algoritma . Keamanan data dan informasi sangat penting di era reformasi saat ini . Umumnya, setiap lembaga memiliki dokumen penting dan rahasia yang hanya dapat diakses oleh orang-orang tertentu . Sistem informasi yang dikembangkan harus menjamin keamanan dan kerahasiaan dokumen - dokumen tersebut . Masalahnya , media yang digunakan sering kali dapat dieksploitasi oleh pihak lain . Masalah keamanan dan privasi data merupakan aspek penting dari sistem distribusi informasi .[4]. Berikut ini kami sajikan contoh penggunaan Vigenere Cipher dengan berpedoman pada susunan alfabet seperti gambar dibawah ini.

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Gambar 1. Indeks Susunan Huruf Alfabet

2.2. Algoritma Transposisi Kolom

Kali ini teknik enkripsi yang digunakan adalah permutasi atau lebih sering disebut transposisi. Teknik ini memindahkan atau memutar karakter menurut aturan tertentu . Prinsipnya adalah kebalikan dari teknik substitusi. Dalam Teknik substitusi ,

karakter berada pada posisi tetap , tetapi identitasnya acak. Dalam teknik konversi identitas karakter tetap sama tetapi posisinya acak. Sebelum konversi dilakukan teks biasa biasanya terlebih dahulu dibagi menjadi blok - blok dengan panjang yang sama. Enkripsi menggunakan sandi transposisi yang paling sederhana dapat dilakukan dengan membagi karakter-karakter plaintext menjadi beberapa blok yang berisi karakter-karakter dengan kunci enkripsi dan kunci enkripsi adalah jumlah karakter pada setiap blok [5].

2.3. Kriptografi

Kriptografi adalah ilmu dan seni mengamankan pesan .(Kriptografi adalah seni dan ilmu mengamankan pesan) Kripto berarti rahasia dan graphia berarti tulisan. Praktisi kriptografi disebut kriptografer. Algoritma kriptografi , yang disebut cipher, adalah persamaan matematika yang digunakan untuk proses enkripsi dan dekripsi. Biasanya dua persamaan matematika (untuk enkripsi dan dekripsi) memiliki hubungan matematika yang cukup dekat. Proses enkapsulasi pesan (disebut plaintext) menjadi pesan tersembunyi (disebut ciphertext) adalah enkripsi. Ciphertext adalah pesan yang tidak dapat dibaca dengan mudah. Terminologi yang lebih tepat untuk digunakan adalah "enkripsi". Algoritma kriptografi adalah langkah logis untuk menyembunyikan data dari orang yang tidak berwenang.

Fungsi algoritma kriptografi adalah sebagai berikut :

1. Enkripsi Enkripsi merupakan hal yang sangat penting dalam kriptografi yang mengamankan data yang dikirim agar tetap rahasia .Data asli disebut plaintext dan diubah menjadi kode yang tidak dapat dipahami. Enkripsi dapat diartikan sebagai sandi atau kode .

2. Deskripsi Dekripsi adalah kebalikan dari enkripsi, pesan yang dikodekan dikembalikan ke bentuk aslinya (teks biasa) , yang disebut dekripsi data . Algoritma yang digunakan untuk enkripsi tentu saja berbeda dengan yang digunakan untuk enkripsi.
3. Kunci Kunci yang dimaksud adalah kunci yang digunakan untuk melakukan enkripsi dan dekripsi[6].

2.4. Pesan Teks

Pesan teks adalah data atau informasi yang dapat dibaca dan dipahami. Nama lain untuk Pesan teks adalah data atau informasi yang dapat dibaca dan dipahami. Nama lain untuk pesan adalah plaintext. Agar pesan tidak dapat dipahami oleh pihak lain, pesan tersebut harus dikodekan ke dalam bentuk lain yang tidak dapat dipahami. Bentuk pesan yang dikodekan disebut ciphertext. Teks terenkripsi harus dapat diubah kembali ke teks asli sehingga pesan yang diterima dapat dibaca.[7]

3. METODE PENELITIAN

Alur dari proses enkripsi suatu pesan teks dapat dilihat pada flowcart di bawa ini.



Gambar 1. Flowchat Alur Plainteks pada proses enkripsi.

Keterangan :

1. Plaintext
Proses dimulai dengan pesan asli (plaintext) yang akan dienkripsi. Plaintext adalah informasi yang masih bisa dibaca tanpa perlindungan kriptografi.
2. Kunci (Key)
Untuk mengamankan plaintext, digunakan sebuah kunci yang akan dipadukan dengan algoritma Vigenere. Kunci ini berfungsi sebagai faktor pengacak agar hasil enkripsi berbeda-beda meskipun plaintext sama.
3. Algoritma Vigenere Cipher
Algoritma Vigenere digunakan sebagai tahap awal enkripsi. Plaintext diproses dengan kunci melalui pergeseran huruf

Chipertext yang di hasilkan dari proses enkripsi pertama dengan menggunakan algoritma vigenere chiper ini adalah :

“ZVOVEPTNULID”

Setelah mendapatkan chipertext pertama maka kita melanjutkan proses enkripsi kedua menggunakan Trasposisi Kolom. Pada tahap ini kita menggunakan chipertext I untuk mejadi plaintext pada tahap enkripsi dua ini.

2. Proses Enkripsi Trasposisi Kolom

Dibawah ini merupakan gambar proses transposisi kolom yang telah dikerjakan pada dokumen excel, dapat dilihat pada gambar 3:

ENKRIPSI II						
PLAINTEKS II	Z	V	O	V	E	P
KEY	A	M	A	N		
	KEY	A	M	A	N	
		1	3	2	4	
CHIPERTEKS II	Z	E	U	O	T	I
	T	N	U	L	I	D
	1	3	2	4		
	Z	V	O	V		
	E	P	T	N		
	U	L	I	D		
	V	P	L	V	N	D

Gambar 3. Algoritma Trasposisi Kolom (Enkripsi II)

Setelah dilakukan perhitungan/pemrosesan seperti gambar di atas maka diperoleh chiperteks II adalah :

“ ZEUOTIVLVND “

3. Mencari bilangan biner dari masing-masing huruf chipertext II

CHIPERTEKS II	Z	E	U	O	T	I
KONVERSI HURUF KE ANGKA	90	69	85	79	84	73
KONVERSI BIL. DESIMAL KE B (RUMUS = DEC2BIN)	1011010	1000101	1010101	1001111	1010100	1001001
	V	P	L	V	N	D
	86	80	76	86	78	68
	1010110	1010000	1001100	1010110	1001110	1000100

Gambar 4. Konversi Huruf Ke Biner

Pada gambar 4. di atas dapat dilihat hasil konversi masing-masing huruf dari chipertext II menjadi bilangan biner dengan menggunakan rumus excel =DEC2BIN agar hurufnya menjadi biner.

4. Mengubah bilangan biner dari masing-masing huruf kedalam bilangan hexadecimal, seperti pada gambar dibawah ini:

KONVERSI BIL. DESIMAL KE B (RUMUS = DEC2BIN)	1011010	1000101	1010101	1001111	1010100		
KONVERSI BINER KE HEXA	5A	45	55	4F	54		
	1001001	1010110	1010000	1001100	1010110	1001110	1000100
	25	56	50	4C	56	4E	44

Gambar 5. Konversi Biner ke Hexa

Pada gambar 5. di atas memperlihatkan hasil konversi bilangan biner tiap huruf menjadi Hexadesimal, dalam contoh

