

SUPER ENKRIPSI TEKS KRIPTOGRAFI MENGGUNAKAN ALGORITMA HILL CIPHER DAN TRANSPOSISI KOLOM

Rama Aria Megantara¹, Fauzi Adi Rafrastara²

^{1,2}Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Dian Nuswantoro
Jl. Imam Bonjol 207 Semarang 50131
e-mail: rama.aria.megantara@dsn.dinus.ac.id, fauzi.adi.rafrastara@dsn.dinus.ac.id

ABSTRAK

Dalam kemajuan teknologi keamanan data adalah salah satu faktor yang sangat penting. Perancangan kriptografi baru menjadi alternatif apabila metode pengamanan informasi lain sudah ada kriptanalisisnya. Hill Cipher merupakan salah satu algoritma kriptografi yang memanfaatkan matriks sebagai kunci untuk melakukan enkripsi dan Dekripsi dan aritmatika modulo. Setiap karakter pada plaintext ataupun ciphertext dikonversikan kedalam bentuk angka. Enkripsi dilakukan dengan mengalikan matriks kunci dengan matriks plaintext, sedangkan Dekripsi dilakukan dengan mengalikan invers matriks kunci dengan matriks ciphertext. Transposisi kolom yaitu teknik membagi plainteks menjadi blok-blok dengan panjang kunci (k) tertentu yang kemudian blok-blok tersebut disusun dalam bentuk baris dan kolom. Metode SuperEnkripsi dengan metode Hill Cipher dan Transposisi Kolom agar di dapatkan Cipher text yang bersifat aman. Untuk mempermudah penghitungannya, proses Super Enkripsi menggunakan PHP Native serta Javascript.

Kata kunci: kriptografi, Hill Cipher, Transposisi Kolom, Super Enkripsi

1. PENDAHULUAN

Pertukaran informasi menjadi hal yang sangat penting di era kehidupan saat ini. Begitu pentingnya pertukaran informasi tentunya harus disertai dengan keamanan informasi [1]. Keamanan informasi yang berkaitan dengan penggunaan komputer, tidak dapat dipisahkan dengan kriptografi., aman bisa berarti bahwa selama pengiriman informasi tentu diharapkan informasi tersebut tidak dapat dibaca oleh orang yang tidak berhak. Kriptografi berasal dari bahasa Yunani yang terdiri dari kata kryptos yang berarti "hidden, secret" dan graphin yang berarti "writing, study". Jadi kriptografi adalah sebuah ilmu yang mempelajari tentang bagaimana menyembunyikan informasi. Kriptografi modern menggabungkan berbagai ilmu [2].

Algoritma Hill Cipher merupakan salah satu algoritma kriptografi yang memanfaatkan aritmatika modulo [3] dan matriks. Setiap karakter pada plaintext dan ciphertext dikonversikan kedalam angka. Proses enkripsi dilakukan dengan mengalikan matriks kunci dengan matriks plaintext, sedangkan proses Dekripsi mengalikan invers matriks kunci dengan ciphertextnya. Karena itulah, Hill Cipher hanya dapat menggunakan matriks persegi. Dalam paper ini, plaintext yang berupa huruf, angka dan simbol dikonversikan sebanyak 26 karakter dan simbol [4]. Semua operasi bilangan, menggunakan modulo 26 artinya ada 26 simbol, Sedangkan data yang diolah merupakan data yang disimpan pada file text. Untuk mempermudah penghitungan saat inisialisasi matriks kunci.

Transposition Cipher yaitu merubah posisi huruf-huruf pada plainteks untuk mendapatkan ciphertexts, salah satunya Transposisi kolom. Dengan memasukan plaintext ke dalam grid atau matriks sepanjang (n) dari kunci yang telah ditentukan karena kata kunci menentukan urutan kolom [5]. Indeks kunci di konversikan menjadi angka yang nantinya akan menghasilkan cipher text sesuai urutan kunci tadi. Super Enkripsi [6] salah satu teknik penggabungan 2 algoritma dalam kriptografi agar keamanan yang digunakan semakin bersifat rahasia, maka untuk membuat program aplikasi menggunakan PHP Native dan Javascript sebagai tools agar dapat mempermudah dalam perhitungannya.

Beberapa penelitian terdahulu yang relevan dengan penelitian yang akan dilakukan oleh penulis antara lain seperti algoritma Zig-zag Cipher dapat diterapkan lebih dari sekali untuk menghasilkan ciphertext dengan keamanan yang lebih tinggi. Transposisi juga dapat dikombinasikan dengan teknik lain seperti substitusi untuk menghasilkan ciphertext yang lebih sulit dipecahkan [7]. Pada penelitian yang dilakukan oleh Sinaga menggunakan metode transposisi [8] menyimpulkan bahwa metode transposisi sebagian besar dikombinasikan dengan metode lain. Metode substitusi dan transposisi mudah dilakukan, teknik-teknik klasik kombinasi memberikan cipher lebih aman dan kuat. Cipher akhir yang dihasilkan akan sangat kuat dan sangat sulit untuk dipecahkan. Sedangkan Nandal (Nandal et al., 2012) mengimplementasikan Caesar Cipher dengan Rail Fence Cipher Untuk Meningkatkan Keamanan Data. Penelitian tersebut membuktikan bahwa kombinasi teknik transposisi dan substitusi akan memberikan keamanan yang lebih pada teks. Akhirnya, algoritma yang digunakan dapat ditingkatkan untuk mendapatkan hasil yang lebih baik.

Pada penelitian lain disebutkan bahwa Algoritma Affine Cipher sudah dapat di kriptanalisis, maka algoritma yang lebih mudah dari algoritma Affine Cipher seperti algoritma linear pasti juga dapat di kriptanalisis [3]. Implementasi Algoritma RSA (Rivest-Shamir-Adleman) Untuk Pengamanan Kunci Algoritma

Hill Cipher Pada Citra Digital telah dilakukan oleh Rahman dkk [9], menyatakan bahwa kedua algoritma digabungkan untuk meningkatkan keamanan suatu citra digital melalui proses enkripsi dan dekripsi.

2. METODOLOGI

Metode penelitian pada penyusunan ini terdiri dari atas Studi pustaka yaitu Mengumpulkan bahan-bahan referensi baik buku, artikel, makalah maupun situs internet mengenai algoritma kriptografi Hill Cipher, aritmatika modulo, teori dasar matriks, pseudo invers serta pemrograman untuk pembuatan aplikasinya. Selanjutnya analisis masalah pada tahap ini dilakukan analisis terhadap algoritma Hill Cipher dan pseudo invers, kemudian menerapkan pseudo invers pada algoritma Hill Cipher.

Desain Dalam tahap ini hasil analisis dibuat pemodelan sistem, menggunakan konsep algoritma dan struktur program, rancangan antar muka dibuat untuk mempermudah sistem alur yang terjadi dalam pembuatan program dan analisa program sehingga system secara keseluruhan lebih terperinci dan terakhir adalah Coding adalah mengaplikasikan pemodelan sistem ke dalam bahasa pemrograman dengan source code/syntax yang sesuai dan bahasa yang digunakan oleh penulis merupakan bahasa pemrograman yang menggunakan PHP Native Serta Javascript yaitu suatu bahasa pemrograman yang lebih mudah menentukan model-model matriks.

2.1 Kriptografi

Kriptografi berasal dari bahasa Yunani yaitu dari dua suku kata Crypto dan Graphia. Crypt artinya menyembunyikan, sedangkan graphia artinya ilmu. Kriptografi, secara umum adalah ilmu dan seni untuk menjaga kerahasiaan berita yang mempelajari teknik-teknik matematika [10] yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan data, keabsahan data, integritas data, serta autentikasi data, yang dilakukan oleh seorang Kriptographer". Ada empat tujuan mendasar dari ilmu kriptografi ini yang juga merupakan aspek keamanan informasi yaitu [2] :

1. Kerahasiaan (Confidentiality)
2. Integritas Data (Data Integrity)
3. Otentikasi (Authentication)
4. Ketidadaan Peyangkalan (Nonrepudiation) Kriptografi sebagai bidang ilmu tentu saja memiliki

Beberapa istilah tersendiri yang harus diketahui, beberapa istilah yang sering digunakan dalam kriptografi [11] adalah:

- Plaintext Plaintext merupakan pesan asli yang ingin dikirimkan dan dijaga keamanannya. Pesan ini tidak lain dari informasi tersebut.
- Ciphertext Ciphertext merupakan pesan yang telah dikodekan (disandikan).
- Cipher Cipher merupakan algoritma matematis yang digunakan untuk proses peyandian plaintext menjadi ciphertext.
- Enkripsi Enkripsi (encryption) merupakan proses yang dilakukan untuk meyandikan plaintext sehingga menjadi ciphertext.
- Dekripsi Dekripsi (decryption) merupakan proses yang dilakukan untuk memperoleh kembali plaintext dari ciphertext.
- Kriptanalisis Ilmu dan seni untuk membuka suatu ciphertext secara ilegal.
- Kriptografi Ilmu matematika yang mendasari ilmu kriptografi dan kriptanalisis.

Algoritma kriptografi adalah fungsi matematika yang digunakan untuk enkripsi dan depeneliti. Algoritma kriptografi semakin kuat jika waktu untuk proses pemecahan sandi semakin lama. Dengan begitu algoritma tersebut semakin aman untuk digunakan. Untuk mengenkripsi dan mendekripsi data kriptografi menggunakan suatu algoritma (cipher) adan kunci (key). Algoritma kriptografi modern tidak lagi mengandalkan keamanannya pada kerahasiaan algoritma tetapi kerahasiaan kunci. Plaintext yang sama bila disandikan dengan kunci yang berbeda akan menghasilkan ciphertext yang sama bila disandikan dengan kunci yang berbeda akan menghasilkan ciphertext yang berbed pula [12]. Dengan demikian algoritma kriptografi dapat bersifat umum dna boleh diketahui siapa saja, akan tetapi tanpa pengetahuan tentang kunci, data tersandi tetap saja tidak dapat dipecahkan. Sistem kriptografi adalah sebuah kunci algoritma kriptografi ditambah semua kemungkinan plaintext, ciphertext dan kunci.

2.2 Transposisi Kolom

Pada kali ini teknik enkripsi yang digunakan adalah permutasi atau lebih sering disebut transposisi Teknik ini memindahkan atau merotasikan karakter dengan aturan tertentu. Prinsipnya adalah berlawanan dengan teknik substitusi [8]. Dalam teknik substitusi, karakter berada pada posisi yang tetap tapi identitasnya yang diacak. Pada teknik permutasi, identitas karakternya tetap, namun posisinya yang diacak. Sebelum dilakukan permutasi, umumnya plaintext terlebih dahulu dibagi menjadi blok-blok dengan panjang yang sama. Enkripsi dengan menggunakan cipher transposisi yang paling sederhana dapat dilakukan dengan cara membagi karakter pada plainteks ke dalam beberapa blok berisi karakter dengan kunci enkripsi dan dekripsinya adalah jumlah karakter pada tiap-tiap blok [13]. Untuk melakukan dekripsi, karakter pada ciphertexts juga dibagi

Ke dalam beberapa blok namun pembagiannya belum tentu adalah kunci mula-mula, dan jumlah karakter pada tiap-tiap blok yang baru belum tentu sama dengan jumlah karakter pada blok awal.

2.3 Hill Cipher

Algoritma kriptografi atau cipher, dan juga sering disebut dengan istilah sandi adalah suatu fungsi matematis yang digunakan untuk melakukan enkripsi dan dekripsi. Ada dua macam algoritma kriptografi, yaitu algoritma simetris (symmetric algorithms) dan algoritma asimetris (asymmetric algorithms). Hill cipher yang merupakan polyalphabetic cipher dapat dikategorikan sebagai block cipher, karena teks yang akan diproses akan dibagi menjadi blok-blok dengan ukuran tertentu [3]. Setiap karakter dalam satu blok akan saling mempengaruhi karakter lainnya dalam proses enkripsi dan dekripsinya, sehingga karakter yang sama tidak dipetakan menjadi karakter yang sama pula. Teknik kriptografi ini menggunakan sebuah matriks persegi sebagai kunci yang digunakan untuk melakukan enkripsi dan dekripsi. Hill Cipher diciptakan oleh Lester S. Hill pada tahun 1929. 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. Hill Cipher termasuk kepada algoritma kriptografi klasik yang sangat sulit dipecahkan oleh kriptanalis apabila dilakukan hanya dengan mengetahui berkas ciphertext saja. Namun, teknik ini dapat dipecahkan dengan cukup mudah apabila kriptanalis memiliki berkas ciphertext dan potongan berkas plaintext [4]. Teknik kriptanalis ini disebut known-plaintext attack.

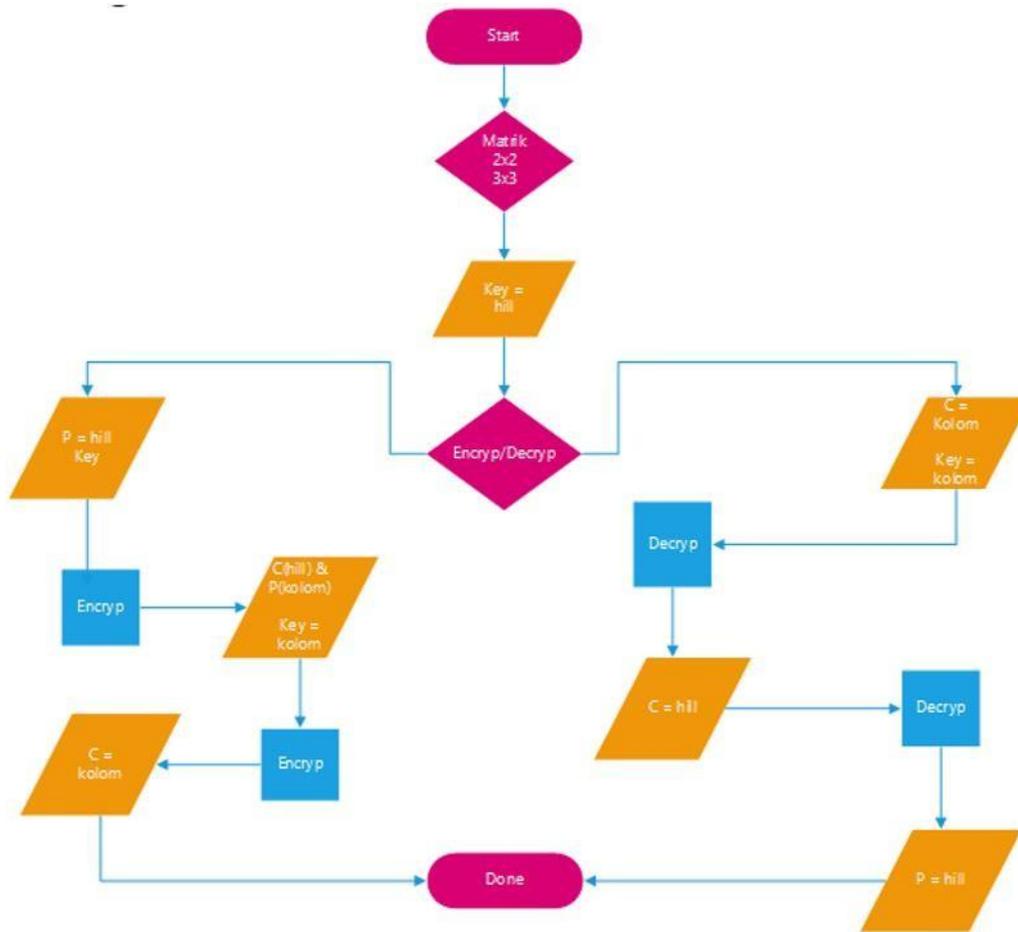
3. HASIL DAN PEMBAHASAN

Pembahasan terhadap hasil penelitian dan pengujian yang diperoleh disajikan dalam bentuk uraian teoritik, baik secara kualitatif maupun kuantitatif. Hasil percobaan bila dimungkinkan ditampilkan dalam bentuk gambar/tabel seperti contoh pada Gambar 2 berikut.

Enkripsi merupakan proses perubahan data asli (plaintext) menjadi ciphertext (data yang tidak dapat dimengerti) sedangkan Dekripsi kebalikan dari enkripsi yaitu proses pengembalian bentuk ciphertext menjadi plaintext kembali sehingga bisa dipahami. Enkripsi dan Dekripsi dilakukan menggunakan kunci yang sudah ditentukan. Hill Cipher merupakan salah satu algoritma kriptografi kunci simetris yang menggunakan aritmatika modulo terhadap matriks.

Algoritma Hill Cipher menggunakan matriks berukuran $m \times m$ (matriks persegi) yang invertible dalam modulus p , sebagai kunci untuk melakukan enkripsi dan dekripsi. Dasar teori matriks yang digunakan dalam Hill Cipher antara lain adalah perkalian antar matriks dan melakukan invers pada matriks. Proses enkripsi pada algoritma Hill Cipher dimulai dengan mengkonversikan plaintext kedalam angka sesuai dengan table korespondensi. Selanjutnya angka-angka tersebut dikelompokkan menjadi beberapa blok, dimana masing-masing blok terdiri dari m anggota sesuai dengan ordo matriks kunci $K(m \times m)$. selanjutnya dicari ciphertext dengan $C = K * P$. Proses Dekripsi diawali dengan mengkonversikan ciphertext kedalam angka sesuai dengan table korespondensi. Seperti halnya pada proses enkripsi, angka-angka tersebut dikelompokkan menjadi beberapa blok dengan anggota masing-masing blok sebanyak m , lalu dicari plaintextnya dengan $P = K^{-1} * C$.

Pada makalah ini, telah diimplementasikan teori pseudo invers, sehingga penggunaan matriks kunci tidak hanya matriks persegi saja, tapi juga dapat menggunakan matriks persegi panjang. Dalam tulisan ini, penulis menggunakan matriks persegi panjang $m \times n$ dengan $m > n$ dan $n > 1$ yang merupakan matriks full column rank. Dengan penggunaan pseudo invers diharapkan semakin banyak jenis matriks yang dapat dijadikan matriks kunci seperti pada Gambar 1 di bawah ini.



Gambar 1. Alur enkripsi dan dekripsi

Simulasi enkripsi akan dilakukan menggunakan matriks A sebagai kunci enkripsi dan Dekripsi. Plaintext pertama yaitu: “FINODIWA”. Panjang plaintext adalah 6 dan jumlah kolom matriks A adalah 2x2. Selanjutnya dicari korespondensi sehingga mendapat angka. P = [5,8,13,14,3,8]. P dipartisi menjadi beberapa matriks yang masing-masing memiliki 2 elemen (sesuai dengan jumlah kolom matriks kunci A). jadi P dipartisi menjadi 3 matriks yaitu P1 sampai P3. P1 : [5,8], P2 : [13,14], P3 : [3,8]. Lakukan perkalian kunci(A) dengan plaintext dengan modulo 26.

PLAINTEKS = FINODIWA

Enkripsi FI

$$F \begin{bmatrix} 5 \\ 8 \end{bmatrix} X \begin{bmatrix} 5 & 8 \\ 17 & 3 \end{bmatrix} = \begin{pmatrix} 25 + 64 \\ 85 + 24 \end{pmatrix} = \begin{pmatrix} 89 \\ 109 \end{pmatrix} \text{mod}26 = \begin{pmatrix} 11 \\ 5 \end{pmatrix} / \begin{pmatrix} L \\ F \end{pmatrix}$$

Enkripsi NO

$$N \begin{bmatrix} 13 \\ 14 \end{bmatrix} X \begin{bmatrix} 5 & 8 \\ 17 & 3 \end{bmatrix} = \begin{pmatrix} 65 + 112 \\ 221 + 42 \end{pmatrix} = \begin{pmatrix} 277 \\ 263 \end{pmatrix} \text{mod}26 = \begin{pmatrix} 21 \\ 3 \end{pmatrix} / \begin{pmatrix} V \\ D \end{pmatrix}$$

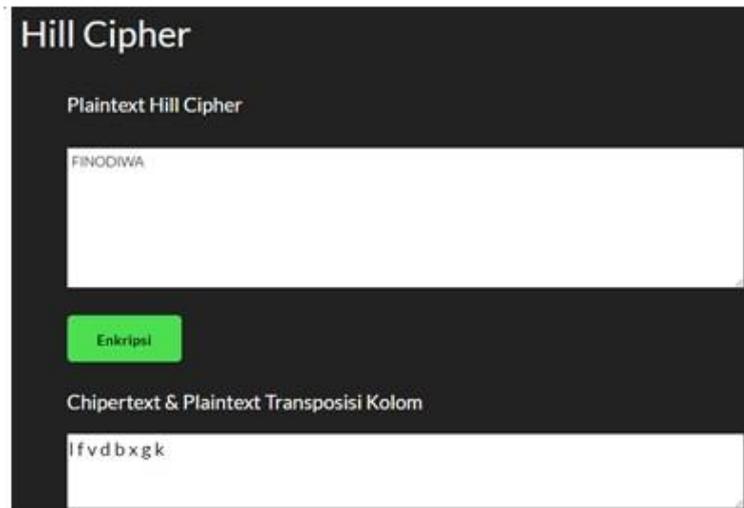
Enkripsi DI

$$D \begin{bmatrix} 5 \\ 8 \end{bmatrix} X \begin{bmatrix} 5 & 8 \\ 17 & 3 \end{bmatrix} = \begin{pmatrix} 15 + 64 \\ 51 + 24 \end{pmatrix} = \begin{pmatrix} 79 \\ 75 \end{pmatrix} \text{mod}26 = \begin{pmatrix} 1 \\ 23 \end{pmatrix} / \begin{pmatrix} B \\ X \end{pmatrix}$$

Enkripsi WA

$$W \begin{bmatrix} 22 \\ 0 \end{bmatrix} X \begin{bmatrix} 5 & 8 \\ 17 & 3 \end{bmatrix} = \begin{pmatrix} 110 + 8 \\ 374 + 3 \end{pmatrix} = \begin{pmatrix} 118 \\ 377 \end{pmatrix} \text{mod}26 = \begin{pmatrix} 6 \\ 13 \end{pmatrix} / \begin{pmatrix} G \\ N \end{pmatrix}$$

Chiperteks yang dihasilkan = LFVDBXGK



Gambar 1. Tampilan Enrkripsi Hil Cipher Melalui aplikasi

Untuk proses matrik 3x3 tetap sama dengan matrik 2x2.

Plaintext : LFVDBXGK

Kunci : OKEY

Panjang Plaintext dibagi dengan kunci $8:4 = 2$ baris sebagai berikut

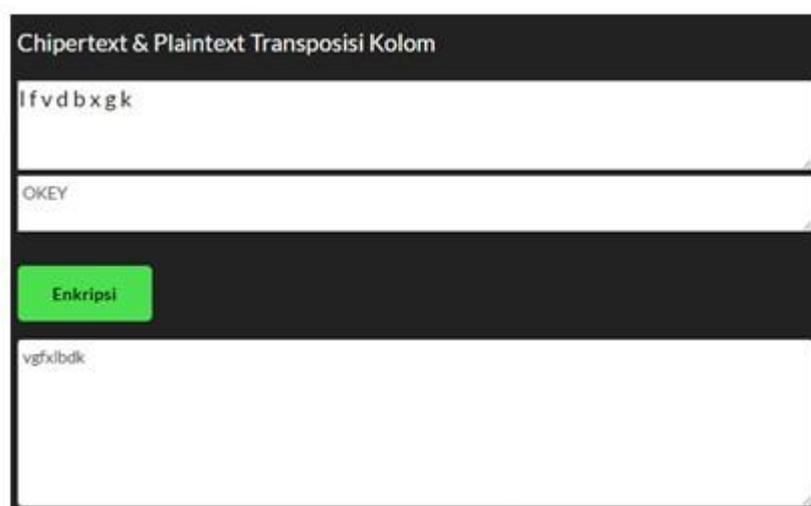
L	F	V	D
B	X	G	K

Urutkan Kunci sesuai abjad

O	K	E	Y
3	2	1	4

3	2	1	4
L	F	V	D
B	X	G	K

Di dapat chiper text : VGFXLBDK



Gambar 2. Tampilan Enrkripsi Hill Cipher setelah melalui Transposisi Kolom

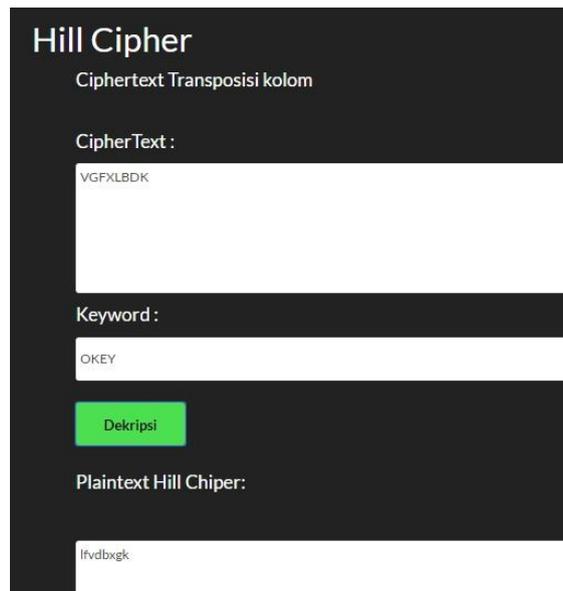
Dalam Proses Dekripsi akan Mengambil contoh diatas dimana menggunakan Chiperteks “LFVDBXGK”. Kemudian di ubah kembali ke plainteks menggunakan hill cipher

Langkah 1 : Cari Invers Dari Plainteks

$$\begin{aligned}
 K^{-1} &= \frac{1}{\det(K)} \text{mod}_{26} \begin{bmatrix} 3 & -8 \\ -17 & 5 \end{bmatrix} = 9^{-1} \text{mod}_{26} \begin{bmatrix} 3 & -8 \\ -17 & 5 \end{bmatrix} \\
 &= 3 \begin{bmatrix} 3 & -8 \\ -17 & 5 \end{bmatrix} \\
 &= \begin{bmatrix} 9 & -24 \\ -51 & 15 \end{bmatrix} \\
 &= \begin{bmatrix} 9 & 2 \\ 1 & 15 \end{bmatrix} \text{mod}_{26}
 \end{aligned}$$

Langkah selanjutnya masukan invers tadi kemudian hitung menggunakan chiperteks maka akan bertemu dengan plaintext kembali.

$$\begin{aligned}
 \begin{pmatrix} 89 \\ 109 \end{pmatrix} \times \begin{bmatrix} 9 & 2 \\ 1 & 15 \end{bmatrix} &= \begin{pmatrix} 801 + 218 \\ 89 + 1635 \end{pmatrix} = \begin{pmatrix} 1019 \\ 1724 \end{pmatrix} \text{mod } 26 = \begin{pmatrix} 5 \\ 8 \end{pmatrix} \begin{matrix} F \\ I \end{matrix} \\
 \begin{pmatrix} 177 \\ 263 \end{pmatrix} \times \begin{bmatrix} 9 & 2 \\ 1 & 15 \end{bmatrix} &= \begin{pmatrix} 1593 + 526 \\ 177 + 3945 \end{pmatrix} = \begin{pmatrix} 2119 \\ 4122 \end{pmatrix} \text{mod}_{26} = \begin{pmatrix} 13 \\ 14 \end{pmatrix} \begin{matrix} N \\ O \end{matrix} \\
 \begin{pmatrix} 89 \\ 109 \end{pmatrix} \times \begin{bmatrix} 9 & 2 \\ 1 & 15 \end{bmatrix} &= \begin{pmatrix} 711 + 150 \\ 79 + 11225 \end{pmatrix} = \begin{pmatrix} 861 \\ 1204 \end{pmatrix} \text{mod}_{26} = \begin{pmatrix} 3 \\ 8 \end{pmatrix} \begin{matrix} D \\ I \end{matrix} \\
 \begin{pmatrix} 118 \\ 377 \end{pmatrix} \times \begin{bmatrix} 9 & 2 \\ 1 & 15 \end{bmatrix} &= \begin{pmatrix} 1062 + 454 \\ 118 + 5655 \end{pmatrix} = \begin{pmatrix} 1816 \\ 5773 \end{pmatrix} \text{mod}_{26} = \begin{pmatrix} 22 \\ 0 \end{pmatrix} \begin{matrix} W \\ A \end{matrix}
 \end{aligned}$$



Gambar 3. Tampilan Form Dikripsi dari Hill Chiper

Kemudian diuji dengan avalanche effect, yaitu menghitung perbedaan antara suatu plaintext yang diuji pertama yang kemudian plaintext kedua diubah 1 suku katanya. Plainteks 1 = finodiwa. Plainteks 2 = finodewa. Plainteks Pertama 'LFVDBXGK' Dikonvert dengan kotak sebanyak 8bit.

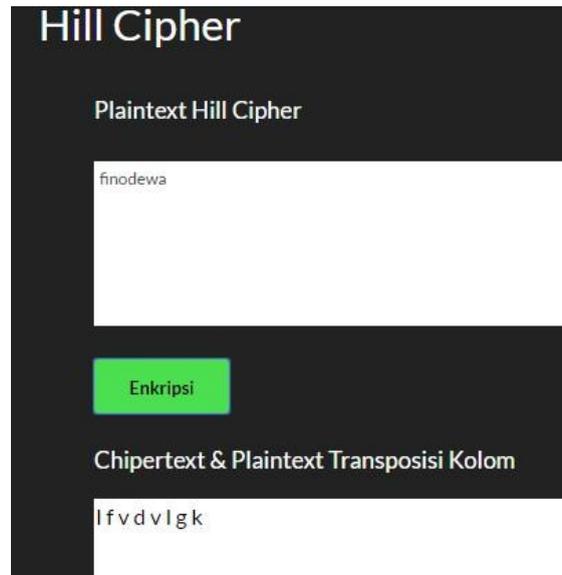
00001011	00000101	00010101	00000011	00000001	00010111	00000110	00001010
L / 11	F/5	V / 21	D/3	B/1	X/23	G/6	K/10

Kemudian Plainteks Kedua 'LFVDVLGK'

00001011	00000101	00010101	00000011	00010101	00001011	00000110	00001010
L/11	F/5	V/21	D/3	V/21	L/11	G/6	K/10

Dengan perhitungan berdaan avalanche effect yaitu

$$\frac{\text{plainteks 1}}{\text{plainteks 2}} \times 100\% = \frac{5}{64} \times 100\% = 7,8125 \%$$



Gambar 4. Tampilan Pengujian avalanche effect

4. KESIMPULAN

Kesimpulan dari pembahasan yang telah dilakukan tersebut adalah:

- Teknik Super Enkripsi sangatlah baik digunakan dalam keamanan berganda tepatnya pada menanggulangi kebocoran data karena menggunakan super enkripsi dapat menambah keamanan yang lebih.
- Penggabungan algoritma Hill Cipher dan transposisi kolom Super enkripsi lebih sulit dipecahkan dengan dari pada hanya menggunakan cipher substitusi atau cipher transposisi saja karena jumlah kunci yang harus dicoba lebih banyak.

DAFTAR PUSTAKA

- [1] K. Negrat, R. Smko, and A. Almarimi, "Variable length encoding in multiple frequency domain steganography," in *2010 2nd International Conference on Software Technology and Engineering (ICSTE)*, 2010, pp. 305–309.
- [2] Y. Anggraini and D. V. S. Y. Sakti, "Penerapan Steganografi Metode End of File (Eof) Dan Enkripsi Metode Data Encryption Standard (Des) Pada Aplikasi Pengamanan Data Gambar Berbasis Java," in *Konferensi Nasional Sistem Informasi, STMIK Dipanegara Makassar*, 2014, no. September 2016, pp. 1743–1753.
- [3] M. Mohan, M. K. K. Devi, and V. J. Prakash, "Security Analysis and Modification of Classical Encryption Scheme," *Indian J. Sci. Technol.*, vol. 8, no. 8, pp. 542–548, 2015.
- [4] E. Suryani and T. S. Martini, "Kombinasi kriptografi dengan hillcipher dan steganografi dengan lsb untuk keamanan data teks," in *Prosiding Seminar Nasional Teknoin*, 2008, pp. 47–51.
- [5] R. Setiawan, "ENKRIPSI PESAN DALAM MEDIA GAMBAR MENGGUNAKAN METODE HIBRID TRANSPOSISI KOLOM DAN ADAPTIVE MINIMUM ERROR LEAST SIGNIFICANT BIT REPLACEMENT (AMELSBR)," 2016.
- [6] E. Setyaningsih, C. Iswahyudi, and N. Widyastuti, "Image Encryption on Mobile Phone using Super Encryption Algorithm," *Telkomnika*, vol. 10, no. 4, pp. 837–845, 2012.
- [7] G. A. Pradipta, "Penerapan Kombinasi Metode Enkripsi Vigenere Cipher Dan Transposisi Pada Aplikasi Client Server Chatting," *STMIK STIKOM Bali*, vol. 10, no. 2, pp. 119–127, 2016.
- [8] D. Sinaga, C. Umam, D. R. I. M. Setiadi, and E. H. Rachmawanto, "TEKNIK SUPER ENKRIPSI MENGGUNAKAN TRANSPOSISI KOLOM," *Din. Rekayasa*, vol. 14, no. 1, pp. 57–64, 2018.
- [9] M. M. Rahman, T. K. Saha, and M. A.-A. Bhuiyan, "Implementation of RSA Algorithm for Speech Data Encryption and Decryption," *74 IJCSNS Int. J. Comput. Sci. Netw. Secur.*, vol. 12, no. 3, pp. 74–82, 2012.
- [10] P. A. Nani, "PENERAPAN ENKRIPSI ALGORITMA BLOWFISH PADA PROSES STEGANOGRAFI METODE EOF," *Penerapan Enkripsi Algoritma Blowfish Pada Proses Steganografi Metod. Eof*, pp. 1–6,

- [11] Y. P. Astuti, E. H. Rachmawanto, and C. A. Sari, "Optimasi Enkripsi Password Menggunakan Algoritma Blowfish," *Techno.COM*, vol. 15, no. 1, pp. 15–21, 2016.
- [12] W. S. Sari, E. H. Rachmawanto, D. R. I. M. Setiadi, and C. A. Sari, "A Good Performance OTP Encryption Image based on DCT-DWT Steganography," *TELKOMNIKA*, vol. 15, no. 4, pp. 1987–1995, 2017.
- [13] A. M. H. Pardede and Y. Maulita, "PERANCANGAN PERANGKAT LUNAK ENKRIPSI DAN DESKRIPSI FILE DENGAN METODE TRANSPOSISI KOLOM," *KAPUTAMA*, vol. 8, no. 1, pp. 28–35, 2014.