INNOVATIVE: Journal Of Social Science Research
Volume 4 Nomor 2 Tahun 2024 Page 5953-5965
E-ISSN 2807-4238 and P-ISSN 2807-4246
Website: https://j-innovative.org/index.php/Innovative

Implemementasi Kriptografi Algoritma Hillcipher Dengan Kunci Tandatangan Pengirim Pesan Terhadap Keamanan Message Handling System Di Bandara Kualanamu

Susi Diriyanti[1✉], Lisda Juliana Pangaribuan[2], Rahmawati Sukra[3], Bella Noer Achaddiah[4]
Politeknik Penerbangan Medan
Email: diriyantisusi@gmail.com[1✉]

Abstrak

Kepadatan lalu lintas udara semakin meningkat, memerlukan sarana komunikasi yang terstandar dan otomatis. AFTN digantikan oleh AMHS, yang menggunakan MHS X.400, untuk keamanan ATS. Metode kriptografi, khususnya Hill Cipher, digunakan untuk enkripsi pesan dan tandatangan pengirim untuk keamanan data penerbangan melalui MHS. Hasil penelitian menunjukkan pesan yang dienkripsi dengan Hill Cipher dan kunci tanda tangan pengirim menjadi aman dan tidak dapat dimengerti oleh pihak yang tidak berhak. Proses enkripsi dan dekripsi mempertahankan ukuran file. Waktu proses tergantung pada ukuran pesan dan kompleksitas kunci enkripsi. Penelitian ini meningkatkan keamanan pertukaran informasi antar bandara.

Keyword: *AFTN, AMHS, kriptografi, Hill Cipher, enkripsi, keamanan data penerbangan.*

Abstrak

The increasing air traffic density necessitates standardized and automated communication means. AFTN is replaced by AMHS, utilizing MHS X.400, for ATS security. Cryptography, particularly Hill Cipher, is employed for message encryption and sender's signature for flight data security via MHS. Research findings reveal messages encrypted with Hill Cipher and sender's signature key are secure and unintelligible to unauthorized parties. The encryption and decryption processes maintain file size. Processing time depends on message size and encryption key complexity. This study enhances security in inter-airport information exchange.

Keywords: *AFTN, AMHS, cryptography, Hill Cipher, encryption, flight data security.*

PENDAHULUAN

Kemajuan dibidang teknologi informasi membuat seseorang dapat melakukan komunikasi dan transaksi melalui internet. Nilai informasi sangat penting karena itu informasi memerlukan pengamanan yang baik saat didistribusikan ataupun saat disimpan.

Jaringan yang sering digunakan dalam sistem telekomunikasi data penerbangan di dunia penerbangan internasional adalah Jaringan Aeronautical Fixed Telecommunication Network (AFTN). Jaringan ini menghubungkan antara bandara satu dengan lainnya dan memuat data penerbangan untuk informasi pesawat terbang yang sedang beroperasi. Sebagai pengganti AFTN sekarang diganti dengan Message Handling System dengan system web base dengan menggunakan jaringan internet. Jika jaringan ini mengalami gangguan non teknis seperti interferensi data, peretasan sistem, penyadapan, dan hacking, akan sangat berbahaya bagi pihak yang terkait. Karena akan menyebabkan pesawat berubah arah atau bandara yang dituju belum siap untuk menyediakan fasilitas yang dibutuhkan pesawat terbang.

Pengiriman informasi melalui MHS, mengirim seluruh informasi terkait berita bandara asal pesawat take off , bandara yang dilalui pesawat tersebut sampai kepada bandara tempat pesawat landing , bukan saja dari bandara asal pesawat take off ke pesawat landing. Hal ini membuat berita/informasi yang di sampaikan perlu disandikan. Salah satu metode pengamanan data adalah dengan proses penyandian terhadap data yang akan dikirim kan yang kenal dengan kriptografi.

Untuk menentukan algoritma kriptografi yang akan di gunakan dalam di gunakan dalam keamanan data selain pertimbangan kekuatan terhadap serangan *CRYPTANALIS* DAN *BRUTEFORSE* yang tidak kalah penting adalah pertimbangan kecepatan. Namun dibidang keamanan informasi sering terjadi *TREADEOFF* antara keamanan dengan kenyamanan. Semakin aman semakin tidak nyaman, demikian juga sebaliknya semakin nyaman semakin tidak aman.

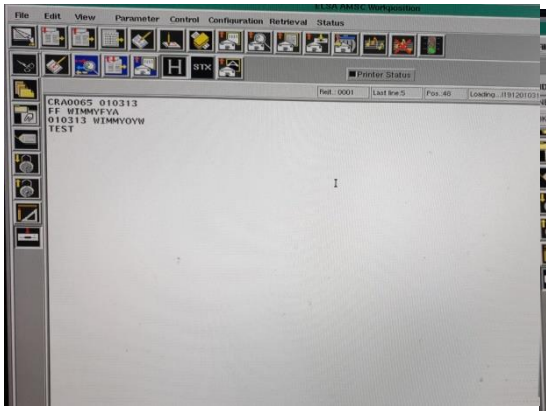
METODE PENELITIAN

Jenis penelitian

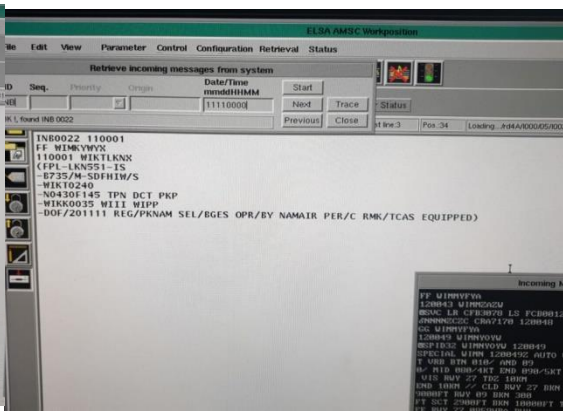
Jenis penelitian ini adalah penelitian eskriptif menggunakan metode Pengolahan data untuk mengetahaui hadil enkripsi dan dekripsi pesan pada Message Handling System (MHS) menggunakan metode Hill Cipher dengan melakukan proses pengolahan citra kedalam matriks ordo 3x3 untuk menjadi kunci Hill. Pada penelitihan ini, pengumpulan data didapatkan dengan penelusuran kepustakaan,penelitian lapangan yang berupa wawancara, pengambilan data dan pengamatan langsung terhadap keadaan yang sebenarnya.

Sample dan Populasi

Sampel dalam penelitian ini adalah informasi yang dikiri pada message Handling System (MHS) Air Nav Kuala Namu yang dapat dililhat pada gambar 1.



Gambar 1. Pesan pada Message Handling System



Gambar 2. sample image kunci

Metode Pengumpulan data

Metode pengumpulan Data dalam penulisan laporan ini penulis menggunakan teknik pengumpulan data sebagai berikut:

Wawancara merupakan teknik pengumpulan data berupa tanya jawab dengan bagian pengolahan data dan keamanan data di air Navigation Medan bagian Flight data officer (FDO) untuk memperoleh data2 yang dibutuhkan diantaranya informasi yang dikirim melalui MHS;

Studi Pustaka Merupakan teknik pengumpulan data dengan cara mempelajari dan membaca berbagai macam buku, laporan, artikel dan jurnal yang ada kaitan dengan penelitihan;

Observasi merupakan metode pengumpulan data melalui pengamatan yang dilakukan Penelitian ini secara langsung menyoroti penggunaan Message Handling System (MHS) sebagai objek penelitian. Pendekatan yang digunakan adalah metode kuantitatif yang bersifat pengembangan, dengan fokus utama pada enkripsi dan dekripsi menggunakan algoritma Hill Cipher. Kunci yang digunakan adalah tandatangan pengirim pesan dengan threshold terendah, yang menjadi aspek kunci dalam keamanan informasi.

Tahapan penelitian dimulai dengan studi literatur yang menyelidiki berbagai sumber kepustakaan, termasuk jurnal, buku, dan hasil penelitian terdahulu mengenai kriptografi, algoritma Hill Cipher, serta proses pengolahan kunci baik asimetrik maupun simetrik. Pengumpulan data dilakukan dari bagian keamanan data Bandara Kuala Namu, yang mencakup informasi tentang data input dan scan tandatangan pengirim pesan untuk

kunci.Selanjutnya, perancangan sistem dilakukan setelah analisis kebutuhan sistem dilakukan secara menyeluruh. Hal ini melahirkan sebuah sistem yang menjadi alat bantu dalam pengujian hasil penelitian. Implementasi sistem dilakukan setelah desain sistem selesai, yang melibatkan pembuatan program atau aplikasi yang sesuai.

Analisis hasil penelitian dan simulasi hasil penelitian menjadi langkah terakhir dalam menanggapi rumusan masalah sesuai dengan tujuan penelitian ini. Hasil penelitian dianalisis untuk memberikan pemahaman yang lebih mendalam, dan simulasi hasil penelitian ditampilkan untuk memperjelas temuan yang diperoleh.

Dengan demikian, melalui tahapan-tahapan tersebut, penelitian ini bertujuan untuk memberikan kontribusi dalam pemahaman tentang keamanan informasi, khususnya dalam konteks penggunaan MHS dengan memanfaatkan metode kuantitatif dan algoritma kriptografi.

Tahapan Metode Hill Cipher

Algoritma yang digunakan untuk enkipsi dan dekripsi pesan dalam penelitian ini adalah algoritma hill cipher. Untuk meningkan keamanan pesan dilakukan modifikasi terhadap kunci.

Langkah-langkah penyelesaian masalah

Penyelesaian masalah menggunakan Metode Hill Cipher mengikuti serangkaian langkah-langkah yang terstruktur. Pertama, plaintext ditentukan, kemudian diubah menjadi kode ASCII. Selanjutnya, plaintext yang sudah diubah dikonversi menjadi matriks.Langkah berikutnya adalah memasukkan kunci, yang dalam kasus ini adalah hasil pemindaian tandatangan pengirim pesan. Tandatangan tersebut diubah menjadi matriks 3 x 3 setelah diubah menjadi format file bmp dengan ukuran standar 180 x 120 piksel.

Selanjutnya, matriks kunci Hill yang terbentuk harus memiliki determinan yang tidak nol dan memiliki inversi multiplikatif (K-1). Jika determinan matriks sama dengan 0 atau bilangan genap, maka nilai threshold dari citra akan diubah. Sebagai contoh, jika determinan matriks adalah 0, maka threshold akan diubah menjadi 200, dengan rentang nilai threshold antara 0 hingga 255.

Setelah kunci ditetapkan, plaintext dienkripsi menggunakan matriks kunci yang telah dibuat. Kemudian, ciphertext yang dihasilkan dapat didekripsi kembali menggunakan algoritma Hill Cipher untuk mendapatkan pesan aslinya.

Selama proses enkripsi dan dekripsi dilakukan, waktu yang diperlukan untuk masing-masing proses dihitung. Selain itu, besar plaintext yang telah dienkripsi dan ciphertext yang

telah didekripsi juga dihitung untuk evaluasi keamanan dan keberhasilan proses enkripsi dan dekripsi.

Dengan demikian, melalui langkah-langkah ini, Metode Hill Cipher memberikan solusi yang terstruktur dan aman untuk mengamankan komunikasi dengan menggunakan kunci kriptografi berbasis matriks.

Proses Pembuatan Kunci Hill

Proses pembuatan kunci Hill dimulai dengan langkah-langkah tertentu untuk mengubah sebuah gambar tandatangan digital menjadi kunci kriptografi. Pertama, gambar tandatangan dimuat. Kemudian, gambar tersebut diubah ukurannya menjadi 180 x 120 piksel untuk standarisasi. Selanjutnya, nilai threshold ditentukan untuk mengidentifikasi intensitas gambar, yang berkisar dari 0 hingga 255.

Langkah berikutnya adalah membagi gambar menjadi sembilan bagian, membentuk matriks 3 x 3. Setiap bagian gambar dievaluasi untuk menentukan nilai bitnya. Jika bagian tersebut kosong (berwarna putih), bitnya ditetapkan sebagai 0; sedangkan jika berisi (berwarna), bitnya adalah 1.

Bit-bit dari setiap bagian kemudian dijumlahkan untuk membentuk elemen-elemen matriks. Total elemen matriks yang dihasilkan adalah 9, membentuk matriks berordo 3 x 3. Selanjutnya, determinan dari matriks ini dihitung. Jika determinan tidak sama dengan 0 dan gcd (greatest common divisor) dari determinan dan 256 adalah 1, maka matriks ini dapat digunakan sebagai kunci Hill.

Jika determinan tidak memenuhi syarat tersebut, nilai threshold diubah, dan proses dimulai kembali. Dengan demikian, langkah-langkah ini membentuk prosedur untuk mengonversi gambar tandatangan digital menjadi kunci kriptografi menggunakan metode Hill.

HASIL DAN PEMBAHASAN

Deskripi Objek Penelitian

Penelitian ini dilaksanakan di dua lokasi, yaitu Bandara KualaNamu di Pasar Enam KualaNamu, Kecamatan Beringin, Kabupaten Deli Serdang, Sumatera Utara 20553, serta Laboratorium AFTN Poltekbang Medan di Jalan Penerbangan No. 85. Objek utama penelitian ini terdiri dari dua jenis data:

Data primer, yang diperoleh dari Message Handling System (MHS) yang diambil dari bagian Flight Data Officer (FDO) di AirNav Kualanamu. Data ini mencakup informasi penting terkait dengan penerbangan dan operasi bandara.

Scan tandatangan, yang merupakan data tandatangan pengirim pesan. Tandatangan ini digunakan sebagai kunci dalam proses enkripsi dan dekripsi menggunakan algoritma Hill Cipher.

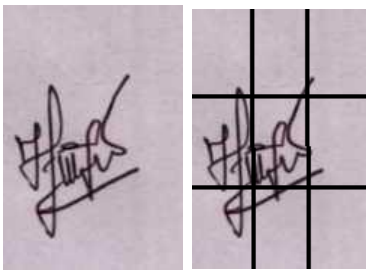
Dengan menggabungkan data primer dari MHS dengan scan tandatangan, penelitian ini bertujuan untuk mengembangkan sistem keamanan informasi yang efektif untuk melindungi komunikasi dalam konteks penggunaan Message Handling System.

Analisis Proses Pembutan Kunci Hill

Algoritma kunci Hill Cipher digunakan untuk mengamanan pesan (*Plaintext*), yang diproses dengan mengubah citra tandatangan pengirim pesan kedalam matriks berordo 3x3.

Pembuatan kunci hill mengikuti langkah – langkah :

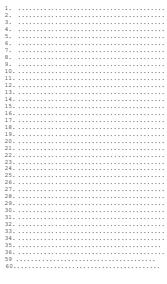
1.Load tandatangan digital



2.Tanpa membuat *threshold* maka cara mengkonversi *image* ke matriks 3x3

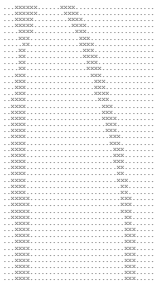
Potongan image tandatangan diubah menjadi bit 0 dan 1 ke dalam ukuran pixel 120 x 180, kemudian pixel yang berisi di jumlahkan untuk mengisi matriks kunci M.

Langkah – langkah :



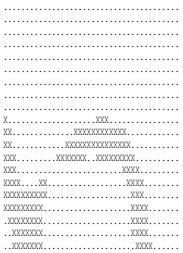
(a) Pixel (1,0) s/d (60,40)

$M_{11} = 0 + 0 + \ldots + 0 = 0$



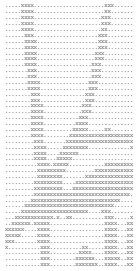
(b) Pixel (41,0) s/d (60,80)

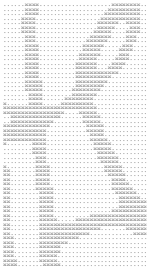
$M_{12} = 10 + 10 + \ldots + 7 + 7 + 7 + 77 + 7 + 7 = 166$



(c) Pixel (61,0) x (60,120)

$M_{13} = 0 + 0 + 0 + 0 + 0 \ldots + 4 + + 2 + 12 = 89$





(d) Pixel (61,0) s/d (61,40)

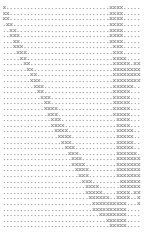
M_{21} = 5 + 6 + 3+ 2+ 2 + 2 +2 + 1 = 110

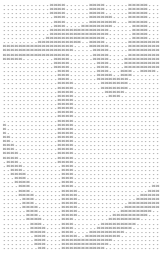
(e) Pixel (61,41) x (61,80)

M_{22} = 7 + 6 + 7 +...+ 16 + 16 = 79

(f) Pixel (61,81) s/d (61,120)

M_{23}=0+0+0+2+4+...+55 = 71





(g) Pixel (121,0) s/d (180,40)

M_{31}= 5+6+6+...+ 0+ 0 = 73

(h) Pixel (121,40) s/d (180,80)

M_{32}= 13+13+ ... +12+12 = 217

(i) Pixel (121,81) s/d (180,120)

M_{33}=9+10+1+...+4+3+1 = 207

Maka diperoleh matriks kunci hill $= \begin{bmatrix} 0 & 166 & 89 \\ 110 & 79 & 71 \\ 73 & 217 & 207 \end{bmatrix}$

Det = ((24*60*0)+(18*36*229)+(13*237*147)) - ((229*60*13)+(147*36*24)+(0*237*18))

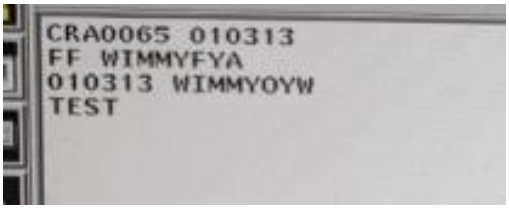
= 601299 - 305628

= 295671) ≠ 0

GCD (295671, 256) = 1 maka matriks dapat di jadikan kunci Hill

Analisis Proses Enkripsi Pesan Dengan Algoritma Hill Cipher

1. Pesan asli



Arti pesan : Flaigh Plain Dari Medan

Maka Plaintext : CRA0065 010313

FF WIMMYFYA (Medan

010313 WIMMYOYM (Medan

TEST

Jumlah karakter plainteks : 48 karakter = 48 byte

2. Enkripsi Pesan

a. Konversi ke angka desimal pada kode ASCII menjadi : 67 82 65 48 48 54 53 32 49 48 51 49 51 10 70 70 32 87 73 77 77 89 65 10 48 49 48 51 49 51 32 87 73 77 77 89 79 89 77 10 84 69 83 84 null.

b. Ubah plaintext ke dalam matriks dengan jumlah kolom 3 menjadi :

$$\begin{bmatrix} 67 & 48 & 53 & 48 & 10 & 32 & 77 & 65 & 49 & 49 & 87 & 77 & 89 & 84 & 84 \\ 82 & 48 & 32 & 51 & 70 & 87 & 77 & 10 & 48 & 51 & 73 & 89 & 77 & 69 & 0 \\ 65 & 54 & 49 & 49 & 70 & 73 & 89 & 48 & 51 & 32 & 77 & 79 & 10 & 83 & 0 \end{bmatrix}$$

Angka 0 ditambah dibelakang untuk mengisi kekosongan karakter.

c. Kunci Hill adalah : dengan nilai threshold =0

Diubah menjadi matriks 3x3 $\begin{bmatrix} 0 & 166 & 89 \\ 110 & 79 & 71 \\ 73 & 217 & 207 \end{bmatrix}$ (Proses pembentukan matrik kunci dapat dilihat pada langkah 4.3.)

Ciphertext = $\begin{bmatrix} 0 & 166 & 89 \\ 110 & 106 & 71 \\ 73 & 217 & 207 \end{bmatrix} *$

$$\begin{bmatrix} 67 & 48 & 53 & 48 & 10 & 32 & 77 & 65 & 49 & 49 & 87 & 77 & 89 & 84 & 84 \\ 82 & 48 & 32 & 51 & 70 & 87 & 77 & 10 & 48 & 51 & 73 & 89 & 77 & 69 & 0 \\ 65 & 54 & 49 & 49 & 70 & 73 & 89 & 48 & 51 & 32 & 77 & 79 & 10 & 83 & 0 \end{bmatrix} \text{ mod } 256$$

C11 = ((0*67) + (166*) 82) + (89*65)) mod 256

= 197

C12 dst sehingga diperoleh hasil :

$$= \begin{bmatrix} 197 & 230 & 112 & 219 & 140 & 132 & 27 & 12 & 160 & 118 & 129 & 203 & 223 & 123 & 117 & 16 \\ 31 & 106 & 246 & 3 & 145 & 142 & 68 & 247 & 19 & 15 & 46 & 216 & 136 & 196 & 91 & 254 \\ 44 & 10 & 13 & 230 & 74 & 44 & 243 & 0 & 144 & 9 & 81 & 230 & 49 & 59 & 217 & 7 \end{bmatrix}$$

Diubah menjadi ASCII menjadi Å_,æj

pö

Û_æŒ'J„☒,_Dó

÷

Maka pesan yang dikrim pada Message Handling Service = Å_,æj

pö

Û_æŒ'J„☒,_Dó

÷

Untuk beberapa karakter kode ASCII tidak kelihatan karena symbol tombol. Ciphertext ini yang akan dikirim kepada penerima.

Pesan ini tidak dapat dimengerti oleh pembajak *(cryptanalyst*)

3. Dekripsi Pesan

Untuk mengetahui pesan asli dekripsi dengan rumus = Pi = K^{-1} * Ci mod 256

Kunci = $\begin{bmatrix} 0 & 166 & 89 \\ 110 & 79 & 71 \\ 73 & 217 & 207 \end{bmatrix}$

Maka di cari K^{-1} = $\begin{bmatrix} -0{,}001 & 0{,}012 & -0{,}004 \\ 0{,}013 & 0{,}005 & -0.007 \\ -0{,}014 & -0{,}009 & 0{,}014 \end{bmatrix}$ mod 256

Sehingga kunci invers = $\begin{bmatrix} 250 & 211 & 159 \\ 193 & 219 & 182 \\ 83 & 46 & 92 \end{bmatrix}$

Pi = $\begin{bmatrix} 250 & 211 & 159 \\ 193 & 219 & 182 \\ 83 & 46 & 92 \end{bmatrix}$ *

$\begin{bmatrix} 197 & 230 & 112 & 219 & 140 & 132 & 27 & 12 & 160 & 118 & 129 & 203 & 223 & 123 & 117 & 16 \\ 31 & 106 & 246 & 3 & 145 & 142 & 68 & 247 & 19 & 15 & 46 & 216 & 136 & 196 & 91 & 254 \\ 44 & 10 & 13 & 230 & 74 & 44 & 243 & 0 & 144 & 9 & 81 & 230 & 49 & 59 & 217 & 7 \end{bmatrix}$ mod 256

= $\begin{bmatrix} 67 & 48 & 53 & 48 & 10 & 32 & 77 & 65 & 49 & 49 & 87 & 77 & 89 & 84 & 84 \\ 82 & 48 & 32 & 51 & 70 & 87 & 77 & 10 & 48 & 51 & 73 & 89 & 77 & 69 & 0 \\ 65 & 54 & 49 & 49 & 70 & 73 & 89 & 48 & 51 & 32 & 77 & 79 & 10 & 83 & 0 \end{bmatrix}$; dimana 0 adalah *Dummy*

Angka pada matriks dikonversikan pada kode ASCII, maka Plaintext =

CRA0065 010313

FF WIMMYFYA

010313 WIMMYOYM

TEST terbukti.

Implementasi System Informasi Metode Hill Cipher Terhadap Keamanan Message Handling System (MHS)

Data yang dimasukkan kedalam system adalah pesan pada MHS dengan jumlah karakter = 48 byte.

Pesan CRA0065 010313

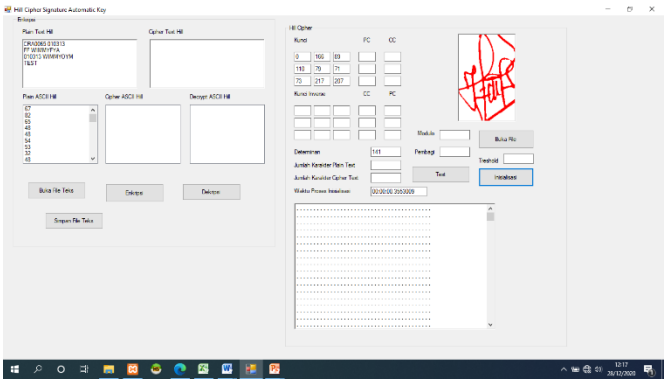
FF WIMMYFYA (Medan

010313 WIMMYOYM (Medan

TEST

Image tandatangan = 

Hasil input pesan dan proses pembuatan kunci dapat dilihat pada gambar 2



Gambar 3. Inisialisasi imange kunci dengan Threshold 0

Dari gambar 3 dapat dilihat bahwa image tanda tangan yang diberikan dengan nilai threshold 0 menghasilkan nilai determinan 141 sehingga menghasilkan matriks kunci $\begin{bmatrix} 0 & 166 & 89 \\ 110 & 79 & 71 \\ 73 & 217 & 207 \end{bmatrix}$

Pada system yang dibangun hasil enkripsi dan konversi enkripsi terhadap kode ASCII serta waktu enkripsi dapat dilihat pada gambar 4. Dari gambar 4 dapat dilihat hasil enkripsi adalah = Å_‚æj

pö

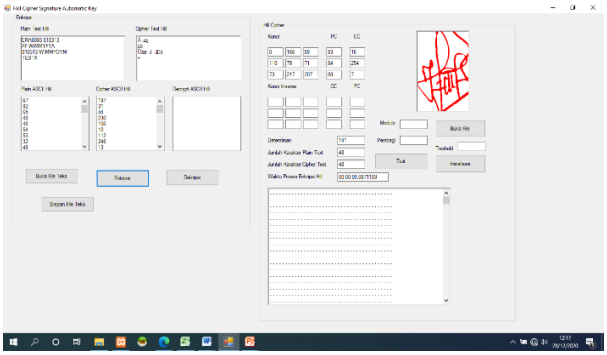
Û_æŒ'J„☒‚_Dó

÷

Konversi ke dalam ASCII menjadi

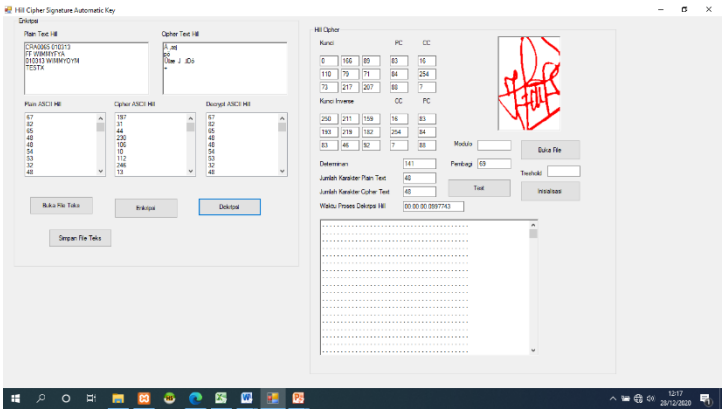
$$\begin{bmatrix} 197 & 230 & 112 & 219 & 140 & 132 & 27 & 12 & 160 & 118 & 129 & 203 & 223 & 123 & 117 & 16 \\ 31 & 106 & 246 & 3 & 145 & 142 & 68 & 247 & 19 & 15 & 46 & 216 & 136 & 196 & 91 & 254 \\ 44 & 10 & 13 & 230 & 74 & 44 & 243 & 0 & 144 & 9 & 81 & 230 & 49 & 59 & 217 & 7 \end{bmatrix}$$

Waktu proses enkripsi 00:00:00.3892486 detik.



Gambar 4. Enkripsi file dan waktu proses enkripsi

Sedangkan proses dekripsi, kunci inverse, waktu proses dekripsi dan jumlah karakter dekripsi dapat dilihat pada gambar 5.



Gambar 5. Dekripsi file

Dari gambar 5 dapat dilihat bahwa kunci invers :

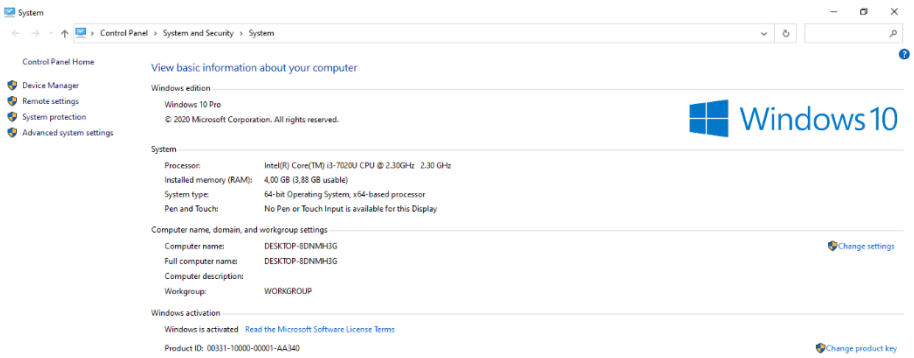
Hasil dekripsi dapat mengembalikan ke pesan semula dengan kunci invers matriks = $\begin{bmatrix} 250 & 211 & 159 \\ 193 & 219 & 182 \\ 83 & 46 & 92 \end{bmatrix}$

Waktu proses dekripsi 00:00:00.0992495 detik.

Jumlah karakter = 48 byte

Dengan menggunakan *CPU time* pada spec komputer Processor Intel Core i3 7020 U CPU 2,3 GHz , Memory 4 GB, OS 64 bit dilakukan ujicoba sebanyak 256 kali terhadap data 48 byte dengan image kunci :

Hasil uji coba sistem enkripsi pesan pada Message Handling System selengkapnya dapat dilihat pada tabel 3 sedangkan Hasil uji coba sistem dekripsi pesan pada Message Handli System dengan pesan dengan panjang yang berbeda selengkapnya dapat dilihat pada tabel 4 .



Gambar 6. Perangkat Komputer Uji Coba System.

SIMPULAN

Berdasarkan analisis dan pembahasan yang telah dilakukan, beberapa kesimpulan dapat ditarik. Pertama, kunci Hill dapat diperoleh dengan mengonversi scan tandatangan pengirim pesan menggunakan threshold tertentu, yang terkecil sehingga menghasilkan inversi matriks. Proses ini memastikan keamanan pesan yang dikirim melalui Message Handling System (MHS).

Kedua, dengan menggunakan metode Hill Cipher untuk enkripsi pesan dengan kunci berupa gambar tandatangan pengirim, pesan menjadi lebih aman karena hanya penerima yang memiliki pengetahuan tentang kunci yang dapat membaca pesan tersebut.

Ketiga, proses dekripsi pesan membutuhkan pengetahuan tentang matriks kunci. Meskipun seorang cryptanalyst mengetahui metode untuk mengembalikan pesan asli, proses untuk mencoba semua kemungkinan angka kunci secara brute force sangatlah besar, menghasilkan jumlah percobaan yang tidak mungkin dilakukan dalam waktu yang wajar.

Keempat, hasil pengujian menunjukkan bahwa ukuran file setelah enkripsi dan dekripsi tetap sama, yang mengindikasikan keberhasilan proses enkripsi dan dekripsi serta efisiensi sistem.

Kelima, waktu proses enkripsi dan dekripsi dipengaruhi oleh ukuran file yang dienkripsi dan didekripsi. Semakin besar file tersebut, semakin lama waktu prosesnya.

Keenam, pembentukan matriks kunci dari citra membutuhkan waktu yang tergantung pada besarnya angka yang dihasilkan. Semakin besar angka tersebut, semakin lama prosesnya.

Ketujuh, waktu proses dekripsi pesan cenderung lebih lama daripada waktu proses enkripsinya karena melibatkan perhitungan inversi matriks kunci.

Kesimpulannya, metode Hill Cipher dapat menjadi pilihan yang efektif untuk mengamankan komunikasi melalui MHS, namun perlu memperhatikan waktu proses dan keamanan kunci yang digunakan.

DAFTAR PUSTAKA

Bhakti, A., Suprapto, Y., & Setyo. (2018). Rancangan Sistem Keamanan Aeronautical Telecommunication Network Message Handling System Menggunakan Algoritma Kriptografi Berbasis Raspberry Pi. *Seminar Nasional Inovasi Teknologi Penerbangan (SNITP).* Surabaya: Politeknik Penerbangan Surabaya.

Bishop, M. 2010. Introduction to Computer Security, Pearson Education. *Department of Computer Science National*. Chia Tung University, Cryptanalysis Lab., pp.29-38.

Chmielowiec, A.2010. Fixed Points Of The RSA Encryption Algorithm. *ElsevierTheoretical Computer Science*411: 288-292

Dooley, J.F. 2013.A Brief History of Cryptology and Cryptographic Algorithms. *Springer Brief*

in Computer Science.ISBN 978-3-319-01628-3 99.

Gupta,R.K. and Singh,P. 2013. A New Way to Design and Implementation of Hybrid Crypto System for Security of the Information in Public Network. *International Journal of Emerging Technology and Advanced Engineering* ISSN 2250-2459. (online) http://www.ijetae.com

Hoffstein,J., Pipher,J. and Silverman.J.H. (Editors) .2008.An Introduction Of Mathematical Cryptography. *Springer Science + Business Media* .e-ISBN: 978-0-387-77994-2.

Iyer, S.C., Sedamkar, R.R., Gupta, S., 2016. A Novel Idea on Multimedia Encryption using Hybrid CryptoApproach. *7th International Conference on Communication, Computing and Virtualization* 2016 : pp. 293-298. *Elsevier.*(online) http://www.sciencedirect.com

Kim, S. And Leeb, G. 2013. Secure Verifiable Non-interactive Oblivious Transfer Protocol Using RSA and Bit Commitment on Distributed Environment. *Elsevier.*

Li Chengqing, Zhang, D. & Chen, G. 2008. Cryptanalysis Of An Image Encryption Scheme Based On The Hill Cipher. *Zhejiang University SCIENCE* CS CR.arXiv:0712.0693v1.

Menezes, A. J., Paul C. V. O., & Scott A. V. 1996.*Handbook of Applied Cryptography*, CRC Press.

McAndrew, A. 2007. Using The Hill Cipher To Teach Cryptographic Principles.*International Journal of Mathematical Education in Science and Technology*. DOI: 10.1080/00207390802054508.

Meng, X.& Zheng, X. 2015. Cryptanalysis Of RSA With A Small Parameter Revisited. Information Processing Letters 115: 858–862. (online) http://www.elsevier.com/locate/ipl.

Mollin, R. A. 2007. *An Introduction to Cryptography - 2nd edition*. Chapman and Hall / CRC