2278-6029-1-SM

by Awaldi Awaldi

Submission date: 17-Oct-2020 02:34PM (UTC+0700)
Submission ID: 1417922932
File name: 2278-6029-1-SM.docx (226.48K)
Word count: 2684
Character count: 16896

IMPLEMENTASI VALIDASI KEY PADA KRIPTOGRAFI ALGORITMA HILL CIPHER

Awaldi[1], Heliawaty Hamrul[2], Adi Heri[3]

Program Studi Teknik Informatika, Fakultas Teknik, Universitas Sulaweis Barat
Jl Prof. Dr. Baharuddin Lopa, S.H, Kabupaten Majene

e-mail: [1]awalditkja@gmail.com, [2] heliawatyhamrul87@gmail.com, [3]adiheripascasarjana@gmail.com

Abstrak

Keamanan informasi merupakan salah saru aspek terpenting di era kemajuan teknologi informasi saat ini. Terutama untuk data yang bersifat sensitif seperti data perusahaan dan informasi yang berkaitan dengan keamanan sebuah data. Pengamanan informasi ini biasanya dilakukan dengan cara berlapis, baik data maupun jalur komunikasinya perlu untuk diamankan. Ada beberapa tehnik atau seni mengamankan data salah satu di antaranya adalah kriptografi dengan algoritma Hill Cipher dimana algoritma ini digunakan untuk mengacak data sehingga tidak dapat dibaca, tentu saja sebelum melakukan proses pengacakan perlu di gunakan *password* atau sandi khusus agar data yang acak dapat di deskripsi kembali ke dalam bentuk semula. Kriptografi *Hill Cipher* (HC) merupakan *poly alphabetic cipher* yang dapat dikategorikan sebagai *blockcipher*, karena teks yang akan diproses dibagi menjadi suatu blok-blok dengan ukuran tertentu. Setiap karakter dalam satu blok dapat mempengaruhi karakter lainnya dalam proses enkripsi maupun deskripsinya, sehingga karakter yang sama tidak dipetakan menjadi karakter yang sama pada blok sesudahnya. Teknik kriptografi ini diciptakan dengan maksud untuk menciptakan *cipher* yang tidak dapat dipecahkan menggunakan teknik analisis frekuensi.

Kata Kunci : Kriptografi, Hill Cipher

KEY VALIDATION IMPLEMENTATION IN HILL CIPHER'S ALGORITHM CRYPTOGRAPHY

Abstract

Information security is one of the most important aspects in the era of advances in information technology today. Especially for sensitive data such as company data and information related to data security. Security of this information is usually carried out in a layered manner, both data and communication channels need to be secured. There are several techniques or art of securing data, one of which is cryptography with the Hill Cipher method where this algorithm is used to scramble data so that it cannot be read, of course before carrying out the randomization process it is necessary to use a special password or password so that random data can be decrypted back into it. original form. Hill Cipher (HC) cryptography is a poly alphabetic cipher that can be categorized as a blockcipher, because the text to be processed is divided into blocks of a certain size. Each character in a block can affect other characters in the encryption process and description, so that the same character is not mapped to the same character in the next block. This cryptographic technique was created with the intention of creating a cipher that could not be cracked using frequency analysis techniques.

Key Words: *Cryptography, Hill Cipher*

I. PENDAHULUAN

Pesatnya perkembangan teknologi sekarang ini membuat proses penyimpanan data menjadi lebih muda. Akan tetapi banyaknya orang yang kini telah meragukan keamanan apabila data disimpan di perangkat komputer. Hal ini tidak terlepas dari terjadinya berbagai tindakan penyadapan dan pemantauan oleh pihak-pihak yang tidak berkepentingan atau tidak bertanggung jawab sehingga kerahasiaannya kurang terjaga dalam mengamankan suatu data [1].

Berbagai teknologi mesin pencari (*search-engine*) semakin berkembang ditambah dengan serangan penyadap, *spam* maupun *hacker/cracker* yang menjamur sehingga dapat mencuri data-data yang bersifat rahasia. *Confidentiality* adalah menjaga informasi dari orang yang tidak berhak mengakses, lebih kearah data-data yang sifatnya pribadi (*private*), seperti e-mail, rekening tabungan, dan lainnya. *Integrity* dalam istilah keamanan informasi berarti aspek yang menjamin bahwa data tidak boleh berubah tanpa ijin pihak yang berwenang (*authorized*). A*uthentication*berarti suatu langkah untuk menentukan atau mengkonfirmasi bahwa seseorang (atau sesuatu) adalah autentik atau asli. Melakukan *autentikasi* terhadap sebuah objek adalah melakukan konfirmasi terhadap kebenarannya. Sedangkan melakukan *autentikasi* terhadap seseorang biasanya

adalah untuk memverifikasi identitasnya. Pada suatu sistem komputer, *autentikasi* biasanya terjadi pada saat *login* atau permintaan akses. *Availability* merupakan upaya pencegahan ditahannya informasi atau sumber daya terkait oleh mereka yang tidak berhak. Secara umum maka makna yang dikandung adalah bahwa informasi yang tepat dapat diakses bila dibutuhkan oleh siapapun yang memiliki legitimasi untuk tujuan ini. Berkaitan dengan "*messagingsystem*" maka pesan itu harus dapat dibaca oleh siapapun yang dialamatkan atau yang diarahkan, sewaktu mereka ingin membacanya. *Access Control* dalam istilah keamanan informasi berarti mekanisme untuk mengatur "siapa boleh melakukan apa", "dari mana boleh ke mana', sedangkan untuk penerapannya membutuhkan klasifikasi data (*public*, *private*, *confident*, *secret*) dan berbasiskan *role* (kelompok atau grup hak akses). *Non-repudiation*adalah aspek untuk menjaga agar seseorang tidak dapat menyangkal telah melakukan sebuah transaksi, sebagai contoh, seseorang yang mengirimkan email untuk memesan barang tidak dapat menyangkal bahwa dia telah mengirimkan email tersebut

Ada beberapa seni pengamanan data salah satu di antaranya adalah kriptografi. Dalam kriptografi data/pesan rahasia akan disandikan menjadi karakter acak sehingga walaupun data/pesan diketahui oleh pihak yang tidak berkepentingan, mereka tetap tidak dapat mengetahui informasi yang sebenarnya.

Kriptografi *Hill Cipher* (HC) merupakan *poly alphabetic cipher* yang dapat dikategorikan sebagai *block cipher*, karena teks yang akan diproses dibagi menjadi suatu blok-blok dengan ukuran tertentu. Setiap karakter dalam satu blok dapat mempengaruhi karakter lainnya dalam proses enkripsi maupun deskripsinya, sehingga karakter yang sama tidak dipetakan menjadi karakter yang sama pada blok sesudahnya. Teknik kriptografi ini diciptakan dengan maksud untuk menciptakan *cipher* yang tidak dapat dipecahkan menggunakan teknik analisis frekuensi.

Terdapat beberapa alasan mengapa algoritma kriptografi HC sulit untuk dipecahkan. Alasan tersebut adalah: pertama, HC menggunakan perkalian matriks untuk dasar enkripsi dan deskripsinya, jadi abjad pada *plaintext* tidak digantikan oleh abjad yang sama begitu juga dengan *ciphertext* [2].

II. TINJAUAN PUSTAKA

A Kriptografi

Kriptografi berasal dari bahasa Yunani yaitu *kryptos* yang berarti tersembunyi dan *grapheiny*ang bermakna tulisan. Kriptografi adalah ilmu menulis pesan rahasia yang mana bertujuan untuk menyembunyikan makna sesungguhnya dari pesan tersebut. Tetapi seiring perkembangan zaman hingga saat ini pengertian kriptografi berkembang menjadi ilmu tentang teknik matematis yang digunakan untuk menyelesaikan persoalan keamanan berupa privasi dan *otentikasi*.[3]

Dalam kriptografi sendiri terdapat beberapa istilah, yaitu :

1. *Plaintext* merupakan pesan asli sebelum diubah menjadi pesan rahasia.
2. *Key* merupakan kunci rahasia yang digunakan untuk mengubah atau mengembalikan pesan rahasia.
3. *Ciphertext* merupakan pesan rahasia yang telah diubah bentuknya menjadi kode-kode yang sukar diterjemahkan.
4. Enkripsi merupakan proses pengubahan *plaintext* menjadi *ciphertext*.
5. Deskripsi merupakan proses pengembalian *ciphertext* menjadi *plaintext*.

Berdasarkan kunci yang di gunakan untuk enkripsi dan deskripsi, kriptografi dapat dibedakan menjadi Kriptografi Kunci-simetri (*symmetric-keycryptography*) dan kriptografi kunci-nirsimetri (*symmetric-keycryptography*).

1. Kriptografi Kunci-simetri

   Pada sistem kriptografi kunci-simetri, kunci untuk enkripsi sama dengan kunci untuk deskripsi, oleh karna itulah dinamakan kriptografi simetri. Istilah lain untuk kriptografi kunci-simetri adalah kriptografi kunci privat (*private-keycryptography*), kriptografi kunci rahasia (*sectret-keycryptography*), atau kriptografi konvensional (*conventionalcryptography*). Sistem kriptografi kunci-simetri mengasumsikan pengiriman dan penerima pesan sudah berbagi kunci yang sama sebelum bertukar pesan. Keamanan sistem kriptografi simetri terletak pada kerahasiaan kuncinya. Kriptografi simetri satu-satunya jenis kriptografi yang dikenal dalam catatan sejarah hingga tahun 1976. Semua algoritma kriptografi klasik termasuk ke dalam kriptografi simetri. Kelemahan dari sistem ini adalah baik pengirim maupun penerima pesan harus memiliki kunci yang sama, sehingga pengirim pesan harus mencari cara aman untuk memberitahukan kunci kepada penerima pesan.
2. kriptografi kunci-nirsimetri

   Jika kunci enkripsi tidak sama dengan kunci untuk deskripsi, maka kriptografinya dinamakan kriptografi nirsimetri. Nama lain adalah kriptografi kunci-*public* (*public-keycryptography*), sebab kunci tidak rahasia dan dapat diketahui oleh siapa pun, sementara kunci untuk deskripsinya hanya di ketahui oleh si penerima pesan. Pada kriptografi jenis ini, setiap orang yang berkomunikasi mempunyai sepasang kunci, yaitu kunci privat dan kunci publik. Pengirim mengenkripsi pesan dengan menggunakan kunci publik si penerima pesan (*receiver*) hanya menerima pesan yang dapat mendeskripsi pesan karena hanya ia yang mengetahui kunci *perivatnya* sendiri.

B Hill Cipher

Algoritma Hill Cipher adalah suatu fungsi matematis yang digunakan untuk melakukan enkripsi dan deskripsi. HC merupakan *polyalphabeticcipher* dapat dikategorikan sebagai *blockcipher*, karena teks yang akan diproses dibagi menjadi blok-blok dengan ukuran tertentu. Setiap karakter dalam satu blok akan saling mempengaruhi karakter lainya dalam proses enkripsi dan deskripsinya, 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 deskripsi. HC diciptakan oleh Lester S. Hill pada tahun 1929. HC tidak mengganti setiap abjad yang sama pada *plaintext* dengan abjad lainnya yang sama pada *ciphertext* karena menggunakan perkalian matriks pada dasar enkripsi dan deskripsinya. HC 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*. Teknik *kriptanalisis* ini disebut *known-plaintextattack*

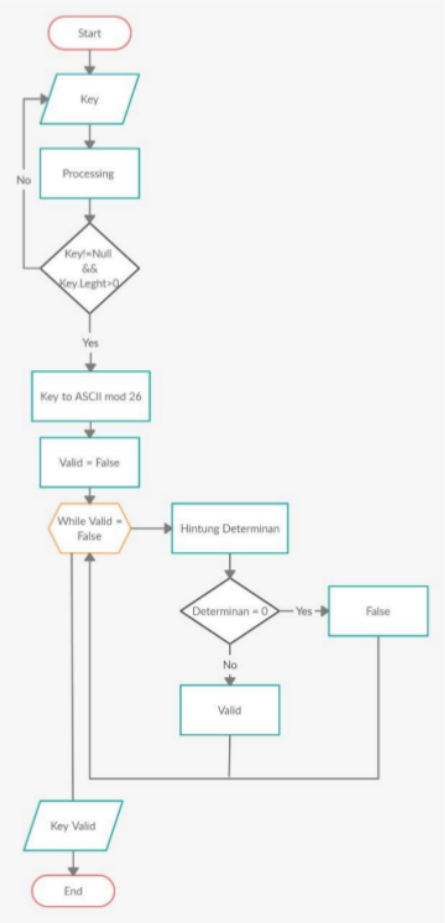
III. METODE PENELITIAN

Pada penelitian ini menjelaskan proses dan cara kerja algoritma *Hill Cipher* sebagai salah satu seni pengaman data pada komputer.

A Proses Validasi Key

Dasar dari teknik *Hill Cipher* adalah *aritmatika modulo* terhadap matriks. Dalam penerapannya, *Hill Cipher* menggunakan teknik perkalian matriks dan teknik invers terhadap matriks. Kunci pada *Hill Cipher* adalah matriks n x n dengan n merupakan ukuran blok. Matriks K yang menjadi kunci ini harus merupakan matriks yang invertible, yaitu memiliki inverse K^{-1} sehingga : Kunci harus memiliki invers karena matriks K^{-1} tersebut adalah kunci yang digunakan untuk melakukan dekripsi. Sehingga untuk memudahkan pengguna dalam pembuatan kunci algoritma ini perlu di buat sebuah sistem validasi kunci dengan tujuan memberikan informasi kepada pengguna bahwa kunci yang di buat memiliki invers atau tidak. Jika pengguna memasukkan kunci yang tidak memiliki invers maka secara otomatis akan memberikan saran kunci berdasarkan panjang kunci yang di buat.

Berikut gambaran proses validasi kunci dalam bentuk flowchart



Gambar 1. Proses Validasi Kunci

B Proses Enkripsi

Pada rancangan sistem proses enkripsi dan deskripsi menggunakan algoritma Hill Cipher, input data *plaintext* yang digunakan berupa teks setelah di ubah untuk menjadi karakter acak.

Tahapan-tahapan algoritma enkripsi *Hill Cipher*sebagai berikut :

1 Korespondenkan abjad dengan numerik

2 Buat matriks kunci berukuran m x m

$$K_{mxm} = \begin{bmatrix} k_{11} & k_{12} & \cdots & k_{1m} \\ k_{21} & k_{22} & \cdots & k_{2m} \\ \cdots & \cdots & \cdots & \cdots \\ k_{m1} & k_{m2} & \cdots & k_{mm} \end{bmatrix}$$

3 Matrik K merupakan matriks *yang invertible* yaitu memiliki *multiplicative inverse* $K-1$ sehingga $K.K-1 = 1$

4 Plainteks $P = p1\ p2\ \ldots\ pn$, diblok dengan ukuran sama dengan baris atau kolom matriks K, sehingga

$$K_{mxm} = \begin{bmatrix} k_{11} & k_{12} & \ldots & k_{1m} \\ k_{21} & k_{22} & \ldots & k_{2m} \\ \ldots & \ldots & \ldots & \ldots \\ k_{m1} & k_{m2} & \ldots & k_{mm} \end{bmatrix}$$

5 Matriks P di transpos menjadi

$$P^{t}_{mxq} = \begin{bmatrix} p_{11} & p_{21} & \ldots & p_{1q} \\ p_{12} & p_{22} & \ldots & p_{2q} \\ \ldots & \ldots & \ldots & \ldots \\ p_{1m} & p_{2m} & \ldots & p_{qm} \end{bmatrix}$$

6 Mengalikan matriks K dengan matriks P transpose dalam modulo 26

$$C^{t} = K_{mxm} P^{t}_{mxq}$$

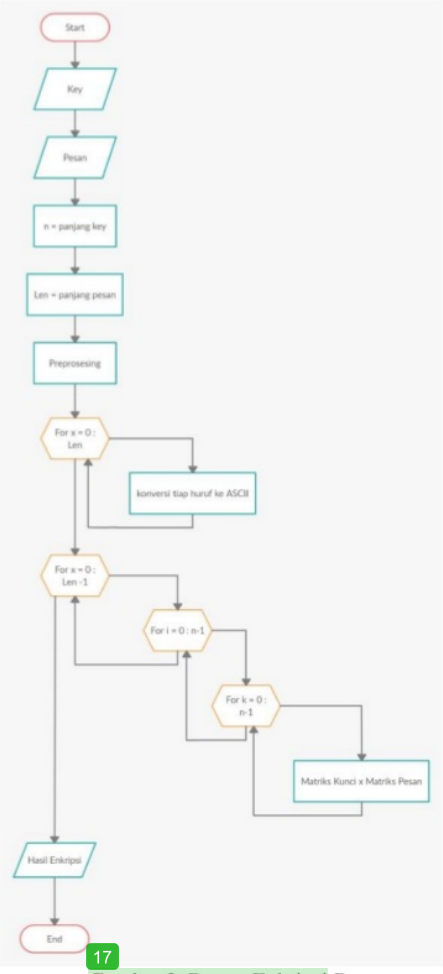
$$C^{t} = \begin{bmatrix} k_{11} & k_{12} & \ldots & k_{1m} \\ k_{21} & k_{22} & \ldots & k_{2m} \\ \ldots & \ldots & \ldots & \ldots \\ k_{m1} & k_{m2} & \ldots & k_{mm} \end{bmatrix} \begin{bmatrix} p_{11} & p_{21} & \ldots & p_{1q} \\ p_{12} & p_{22} & \ldots & p_{2q} \\ \ldots & \ldots & \ldots & \ldots \\ p_{1m} & p_{2m} & \ldots & p_{qm} \end{bmatrix} = \begin{bmatrix} c_{11} & c_{21} & \ldots & c_{m1} \\ c_{12} & c_{22} & \ldots & c_{m2} \\ \ldots & \ldots & \ldots & \ldots \\ c_{1q} & c_{2q} & \ldots & c_{mq} \end{bmatrix}$$

7 Hasil perkalian matriks K dengan Matriks P di tranpose ke dalam modulo 26

$$C = (C^{t})^{t} = \begin{bmatrix} c_{11} & c_{12} & \ldots & c_{1q} \\ c_{21} & c_{22} & \ldots & c_{2q} \\ \ldots & \ldots & \ldots & \ldots \\ c_{m1} & c_{m2} & \ldots & c_{mq} \end{bmatrix}$$

8 Hasil modulo kemudian di transpose kedalam bentuk abjad sehingga diperoleh *Ciphertext*.

Berikut gambaran proses enkripsi pesan dalam bentuk flowchart



Gambar 2. Proses Enkripsi Pesan

C Proses Dekripsi

Proses dekripsi atau proses pengembalian *Ciphertext* ke bentuk *Plaintext* tentunya tidak jauh berbeda dengan proses enkripsi. proses dekripsi juga tentu melakukan proses perkalian matriks namun matriks yang dikalikan adalah matriks invers dari kunci dengan *Ciphertext*.

Tahapan-tahapan algoritma dekripsi *Hill Cipher*sebagai berikut

1 Korespondenkan abjad dengan numerik $A \rightarrow 1, B \rightarrow 2, \ldots, Z \rightarrow 26$
2 Ubah cipherteks kedalam numerik
3 Kunci yang digunakan untuk mendekrip ciphertext ke plaintext adalah invers dari matrik kunci $K\ mxm$
4 Menghitung $K-1$
5 Mengalikan invers matriks kunci dengan cip herteks transpose dalam modulo 26, diperoleh plainteks transpose $P\,t = K-1C\,t$

6 Dari langkah ke-5 diperoleh $P = (P\ t\ )\ t$

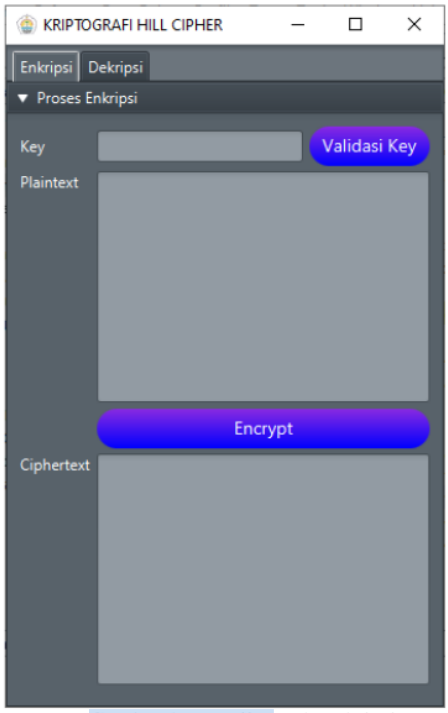
7 Korespondensikan abjad dengan numerik hasil langkah 6 diperoleh plainteks

Berikut gambaran proses dekripsi pesan dalam bentuk flowchart

Gambar 3. Proses Dekripsi Pesan

IV. HASIL DAN PEMBAHASAN

Gambaran umum aplikasi atau sistem yang telah di buat di sajikan dalam dua tab yakni Tab untuk Enkripsi dan Tab dekripsi. Adapun tampilan pada tab Enkripsi dapat dilihat pada gambar berikut:

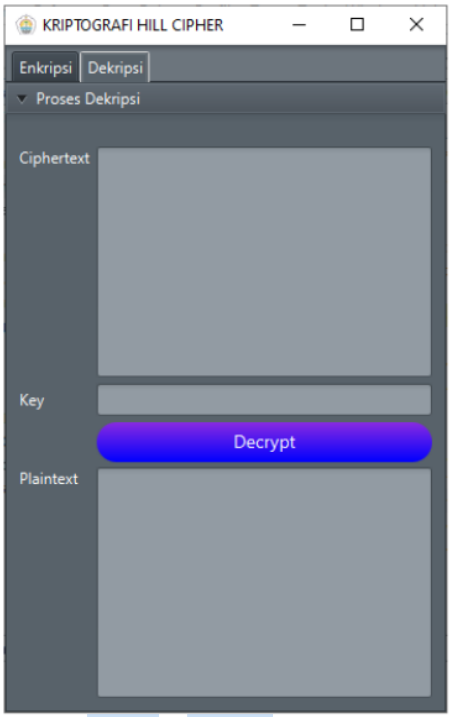


Gambar 4. Tampilan Tab Enkripsi

Pada tab enkripsi terdapat 3 *form* yakni, *form key*, *form Plaintext* (pesan), dan *form output* hasil enkrispi (*form Ciphertext*). *Form key* dan *form Plaintext* berfungsi untuk memasukkan kunci dan pesan yang akan di enkripsi, sedangkan *form Ciphertext* bertujuan untuk menampilkan hasil dari enkripsi.

Pada tab enkripsi juga terdapat 2 tombol yakni, tombol validasi *key* dan tombol *Encrypt*. Tombol validasi *Key* berfungsi untuk memeriksa kunci yang di masukkan telah memiliki invers atau belum, jika kunci tidak memiliki invers maka secara otomatis akan memberikan rekomendasi kunci yang kemudian tampilkan pada *form key* menggantikan kunci yang telah di masukkan. Tombol *Encrypt* berfungsi untuk melakukan proses enkripsi pesan.

Adapun tampilan pada tab Dekripsi dapat dilihat pada gambar berikut



Gambar 5. Tampilan Tab Dekripsi

Pada tab Dekripsi terdapat 3 *form* yakni, *form Ciphertext, form key,* dan *form Plaintext*. *Form key* dan *form Ciphertext* berfungsi untuk memasukkan kunci dan *Ciphertext* yang akan di dekripsi, sedangkan *form Plaintext* bertujuan untuk menampilkan hasil dari dekripsi. Pada Tab Dekripsi hanya memiliki satu tombol yakni tombol *Decrypt* yang berfungsi untuk melakukan proses dekripsi pesan rahasia.

Adapun pembahasan dari hasil penelitian ini yakni:

A Validasi Kunci

Berikut tabel hasil validasi kunci matriks 2 x 2 , 3 x 3, dan 4 x 4:

Tabel 1. Validasi kunci matriks 2 x 2

No.	Input Key	Key Valid
1.	PERS	PNRS
2.	HILL	HILL
3.	CHIP	NHWV
4.	PHER	PHER
5.	ASDB	AVDB

Tabel 2. Validasi kunci matriks 3 x 3

No.	Input Key	Key Valid
1.	SORSRIXZA	SORSRIXZA
2.	JKLOIPUYT	FWUANFKMR
3.	CNICERTJX	CNICERTJX
4.	LKVAMDNFJ	LKVAMDNFJ
5.	TIKAWALDI	TIKAETLDI

Tabel 3. Validasi kunci matriks 4 x 4

No.	Input Key	Key Valid
1.	ASLKJPOIKNMJKKLL	ASLKJPOIKNMJKKLL
2.	LKJHGFDSAQWEROIU	LKJHGFDSAQWFROUU
3.	POIUYTGHJNBVCFGYT	POIUYTGHJNBVCFGY
4.	MKOILKJHMNBVCJHY	MPOITQOHTBBCCRHM
5.	YHNJMKIJBHUJVGYH	YHNJMKIJBHUJVGYH

B Proses Enkripsi Hill Cipher

Setelah *key* atau *password* tervalidasi selanjutnya mengimput pesan yang ingin di enkripsi. *plaintext* atau pesan yang ingin di enkripsi akan di konversi menjadi matriks untuk di kalikan dengan matriks *key*.

Tabel 4. Hasil Enkripsi

Plaintext	Key	Ciphertext
INFORMATIKA	QLVR	LZAFOPBLEATB
INFORMATIKA	FLSOJRKEL	NCFFHCPVIWLP
INFORMATIKA	POIUYTGHJNBVCFGY	YVUFXPGESXJU

C Proses Dekripsi Hill Cipher

Proses deskripsi dilakukan sama seperti enkripsi namun sedikit berbeda karna pada proses ini tidak perlu melakukan validasi *key*. *User* hanya perlu memasukkan *key* atau *password* yang sama pada saat melakukan enkripsi pesan.

Tabel 5. Hasil Dekripsi

Ciphertext	Key	Plaintext
LZAFOPBLEATB	QLVR	INFORMATIKAX
NCFFHCPVIWLP	FLSOJRKEL	INFORMATIKAX
YVUFXPGESXJU	POIUYTGHJNBVCFGY	INFORMATIKAX

D Pengujian

Pada algoritma Hill Cipher akan dilakukan pengujian secara manual, untuk menguji apakah algoritma yang di gunakan bekerja sesuai dengan yang di harapkan. Pada pengujian ini sistem akan melakukan enkripsi menggunakan *key* 2x2, 3x3, dan 4x4 dan peneliti juga melakukan enkripsi secara manual untuk mencocokkan hasil enkripsi.

Tabel 6. Hasil Enkripsi Sistem

Plaintext	Key	Ciphertext
INFORMATIKA	QLVR	LZAFOPBLEATB

INFORMATIKA	FLSOJRKEL	NCFFHCPVIWLP
INFORMATIKA	POIUYTGHJNBVCFGY	YVUFXPGESXJU

Berikut enkripsi yang dilakukan secara manual.

1) K = QLVR = $\begin{bmatrix}16 & 11\\ 21 & 17\end{bmatrix}$

P = INFORMATIKA =
$\begin{bmatrix}8 & 5 & 17 & 0 & 8 & 0\\ 13 & 14 & 12 & 19 & 10 & 23\end{bmatrix}$

C = K x P

Penyelesaian

$= \begin{bmatrix}16 & 11\\ 21 & 17\end{bmatrix} \text{x} \begin{bmatrix}8 & 5 & 17 & 0 & 8 & 0\\ 13 & 14 & 12 & 19 & 10 & 23\end{bmatrix}$

$= \begin{bmatrix}271 & 234 & 404 & 209 & 238 & 253\\ 389 & 343 & 561 & 323 & 338 & 391\end{bmatrix} \text{mod } 26$

$= \begin{bmatrix}11 & 014 & 1 & 4 & 19\\ 25 & 15 & 110 & 1\end{bmatrix}$

$= \begin{bmatrix}L & A & O & B & E & T\\ Z & F & P & L & A & B\end{bmatrix}$

= Maka hasil enkripsi manual adalah LZAFOPBLEATB

2) K = FLSOJRKEL = $\begin{bmatrix}5 & 11 & 18\\ 14 & 9 & 17\\ 10 & 4 & 11\end{bmatrix}$

P = INFORMATIKA = $\begin{bmatrix}8 & 14 & 0 & 10\\ 13 & 17 & 19 & 0\\ 5 & 12 & 8 & 23\end{bmatrix}$

C = K x P

Penyelesaian

$= \begin{bmatrix}5 & 11 & 18\\ 14 & 9 & 17\\ 10 & 4 & 11\end{bmatrix} \text{x} \begin{bmatrix}8 & 14 & 0 & 10\\ 13 & 17 & 19 & 0\\ 5 & 12 & 8 & 23\end{bmatrix}$

$= \begin{bmatrix}273 & 473 & 353 & 464\\ 314 & 553 & 307 & 531\\ 187 & 340 & 164 & 353\end{bmatrix} \text{mod } 26$

$= \begin{bmatrix}13 & 15 & 15 & 22\\ 2 & 7 & 21 & 11\\ 5 & 2 & 8 & 15\end{bmatrix}$

$= \begin{bmatrix}N & F & PW\\ C & H & V\ L\\ F & C & I\ P\end{bmatrix}$

= Maka hasil enkripsi manual adalah NCFFHCPVIWLP

3) K = POIUYTGHJNBVCFGY

$= \begin{bmatrix}15 & 14 & 8 & 20\\ 24 & 19 & 6 & 7\\ 9 & 13 & 1 & 21\\ 2 & 5 & 6 & 24\end{bmatrix}$

P = INFORMATIKA = $\begin{bmatrix}8 & 17 & 8\\ 13 & 12 & 10\\ 5 & 0 & 0\\ 14 & 19 & 23\end{bmatrix}$

C = K x P

Penyelesaian

$= \begin{bmatrix}15 & 14 & 8 & 20\\ 24 & 19 & 6 & 7\\ 9 & 13 & 1 & 21\\ 2 & 5 & 6 & 24\end{bmatrix} \text{x} \begin{bmatrix}8 & 17 & 8\\ 13 & 12 & 10\\ 5 & 0 & 0\\ 14 & 19 & 23\end{bmatrix}$

$= \begin{bmatrix}622 & 803 & 720\\ 567 & 769 & 543\\ 540 & 708 & 685\\ 447 & 550 & 618\end{bmatrix} \text{mod } 26$

$= \begin{bmatrix}24 & 23 & 18\\ 21 & 15 & 23\\ 20 & 6 & 9\\ 5 & 4 & 20\end{bmatrix}$

$= \begin{bmatrix}Y & X & S\\ V & P & X\\ U & G & J\\ F & E & U\end{bmatrix}$

= Maka hasil enkripsi manual adalah YVUFXPGESXJU

Dari hasil enkripsi dari sistem dan hasil enkripsi secara manual terlihat sama baik itu menggunakan *key* ordo 2x2, 3x3, dan 4x4 maka dapat di simpulkan bahwa algoritma pada sistem berjalan sesuai yang di harapkan.

V. KESIMPULAN

Berdasarkan hasil pembahasan maka dapat diambil kesimpulan sebagai berikut

1. Penerapan validasi key untuk pembuatan sandi bekerja sesuai yang di harapkan dan waktu proses validasi key sangat cepat.
2. Hasil enkripsi *plaintext* yang sama dengan menggunakan matriks kunci yang berbeda akan menghasilkan *ciphertext* yang berbeda.

VI. DAFTAR PUSTAKA

[1] Syahril, Jaya, "Aplikasi Steganografi Pengamanan Data Nasabah di Standard Chartered Bank Menggunakan Metode Least Significant Bit Dan Rc4," Vol. Juli 2019

[2] Mardianti, Sutardi, Aksara, "Keamanan Dan Penyisipan Pesan Teks Pada Gambar Dengan Kriptografi Metode *Hill Cipher*Dan Steganografi Metode End Of," Vol. 5, 2019.

[3] Ziaurrahman, A., Utami, E., & Wahyu Wibwo, F. *Modifikasi Kriptografi Klasik Vigenere Cipher Menggunakanone Time Pad Dengan Enkripsi Berlanjut* 2019.

[4] Kumar, "Securing Data At Rest Using *Hill Cipher*And Xor Based Operations," 2019.

[5] Yulius Nahak, Friden Elefri, Ariyus, "Combination Of Xor Binary Algorithm And

Steganography Using Least Significant Bit (Lsb) Method For Data Security," 2019

[6] Rismawati, Femy Mulya, "Analisis Dan Perancangan Simulasi Enkripsi Dan Dekripsi Pada Algoritma Steganografi Untuk Penyisipan Pesan Text Pada Image Menggunakan Metode Least Significant Bit (Lsb) Berbasis Cryptool2," vol. 12, 2019.

[7] Ziaurrahman, Utami, Wahyu Wibwo, "Modifikasi Kriptografi Klasik Vigenere Cipher Menggunakanone Time Pad Dengan Enkripsi Berlanjut," vol. 4, 2019.

[8] Simbolon, "Analisis Kinerja Kombinasi Steganografi Multi-Bit Lsb Dengan Algoritma Kriptografi Modified Vernam," 2019.

[9] Hafiz, "Steganografi Berbasisis Citra Digital Untuk Menyembunyikan Data Menggunakan Metode Least Significant Bit (Lsb)," Vol. XVII, 2019.

2278-6029-1-SM

ORIGINALITY REPORT

42%	42%	6%	22%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	journal.lppmunindra.ac.id Internet Source	8%
2	rahmaglawri.blogspot.com Internet Source	8%
3	elearning.potensi-utama.ac.id Internet Source	5%
4	e-journal.janabadra.ac.id Internet Source	4%
5	core.ac.uk Internet Source	4%
6	es.scribd.com Internet Source	3%
7	repository.usu.ac.id Internet Source	2%
8	repositori.usu.ac.id Internet Source	1%
9	id.123dok.com Internet Source	1%

10	journal.stmikglobal.ac.id Internet Source	1%
11	repository.uinsu.ac.id Internet Source	1%
12	edoc.pub Internet Source	1%
13	teknik-arie.blogspot.com Internet Source	<1%
14	eprints.unsri.ac.id Internet Source	1%
15	media.neliti.com Internet Source	<1%
16	id.scribd.com Internet Source	<1%
17	pt.scribd.com Internet Source	<1%
18	muamalkhoerudin.wordpress.com Internet Source	<1%
19	sciencebooth.com Internet Source	<1%
20	ojs.unsulbar.ac.id Internet Source	<1%
21	www.m4rt3n.com Internet Source	<1%

Exclude quotes	On	Exclude matches	Off
Exclude bibliography	Off		