MODIFIKASI *HILL CIPHER* DENGAN MENGGUNAKAN MATRIKS KUNCI ORTHOGONAL DAN *TRANSPOSITION SUBSTITUTION LEFT RIGHT SHIFT (TSLRS)*

SKRIPSI

untuk memenuhi persyaratan
dalam menyelesaikan program sarjana Strata-1 Matematika

Oleh
Yuniardi Wahyu Nugraha
NIM. 1811011110011

PROGRAM STUDI MATEMATIKA
FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM
UNIVERSITAS LAMBUNG MANGKURAT
BANJARBARU
2023

SKRIPSI

MODIFIKASI *HILL CIPHER* DENGAN MENGGUNAKAN MATRIKS KUNCI ORTHOGONAL DAN *TRANSPOSITION SUBSTITUTION LEFT RIGHT SHIFT (TSLRS)*

Oleh

Yuniardi Wahyu Nugraha

NIM. 1811011110011

telah dipertahankan di depan Dosen Penguji pada tanggal 6 April 2023

Susunan Dosen Penguji:

Pembimbing I

Thresye, S.Si., M.Si.
NIP. 197205042000122002

Pembimbing II

Oni Soesanto, S.Si., M.Si.
NIP. 197301262005011003

Dosen Penguji:

1. Dr. Na'imah Hijriati, S.Si., M.Si.
2. Akhmad Yusuf, S.Si. M.Kom

Banjarbaru, 28 April 2023

Wakil Dekan Bidang Akademik,

Dr. Gunawan, S.Si., M.Si.
NIP. 197911012005011002

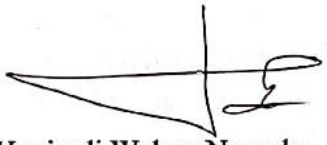
Koordinator Program Studi Matematika FMIPA ULM,

Pardi Affandi, S.Si., M.Sc.
NIP. 197806112005011001

PERNYATAAN

Dengan ini saya menyatakan bahwa dalam skripsi ini tidak terdapat karya yang pernah diajukan untuk memperoleh gelar kesarjanaan di suatu Perguruan Tinggi, dan sepanjang pengetahuan saya juga tidak terdapat karya atau pendapat yang pernah ditulis atau diterbitkan oleh orang lain, kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan dalam Daftar Pustaka.

Banjarbaru, 28 April 2023



Yuniardi Wahyu Nugraha

NIM. 1811011110011

ABSTRAK

MODIFIKASI *HILL CIPHER* DENGAN MENGGUNAKAN MATRIKS KUNCI ORTHOGONAL DAN *TRANSPOSITION SUBSTITUTION LEFT RIGHT SHIFT (TSLRS)* (Oleh : Yuniardi Wahyu Nugraha; Pembimbing : Thresye, Oni Soesanto, 2023, 46 halaman)

Matriks merupakan suatu susunan elemen-elemen yang disusun dalam bentuk baris dan kolom, konsep dari suatu matriks dapat digunakan dalam menyelesaikan suatu permasalahan yang terkait dalam kriptografi. Pada tahun 1929 seorang matematikawan yang bernama Lester Hill menciptakan suatu sistem kriptografi polialfabetik yang disebut *Hill Cipher. Hill cipher* merupakan algoritma yang dalam prosesnya menggunakan matriks berukuran $(m \times m)$ sebagai matriks kuncinya. Dasar dari algoritmanya menggunakan perkalian matriks dalam membuat enkripsi dan kemudian mencari invers tersebut untuk melakukan dekripsinya. *Hill cipher* klasik memiliki kelemahan, yakni operasi yang digunakan terbilang sederhana. Sedangkan pada saat ini, sering dijumpai kasus kejahatan dunia maya (*cybercrime*). Pada penelitian ini *Hill Cipher* klasik akan dimodifikasi dengan menggunakan matriks orthogonal sebagai matriks kuncinya, serta menambahkan beberapa operasi lain seperti transposisi, substitusi, dan pergeseran bit. Tujuan dari penelitian ini adalah untuk menganalisa perbedaan algoritma kriptografi pada data (*text*) dengan menggunakan *Hill Cipher* klasik dan *Hill Cipher* yang telah dimodifikasi. Penelitian ini dilakukan dengan melakukan proses enkripsi dan dekripsi pada *Hill Cipher* klasik dan *Hill Cipher* yang telah dimodifikasi dengan menggunakan data *(text)* yang serupa. Selanjutnya akan dilakukan simulasi menggunakan matlab sehingga dapat menggunakan data *(text)* dengan ukuran yang lebih besar. Pada *Hill Cipher* yang telah dimodifikasi terdapat tiga matriks kunci. Dua matriks kunci tambahan tersebut diperoleh pada proses substitusi dengan menggunakan Caesar Cipher dan saat proses pergeseran kiri-kanan. Adapun hasil yang diperoleh yaitu pada *Hill Cipher* yang telah dimodifikasi menggunakan sistem kriptografi asimetris, yaitu pada proses pergeseran kiri-kanan sehingga matriks kunci yang digunakan untuk enkripsi dan dekripsi berbeda. Karena menggunakan kunci yang berbeda pada proses enkripsi dan dekripsinya sehingga menambah tingkat kesulitan dalam memecahkan pesan tersebut.

Kata kunci : matriks, kriptografi, *Hill Cipher*

ABSTRACT

HILL CIPHER MODIFICATION USING ORTHOGONAL KEY MATRIX AND TRANSPOSITION SUBSTITUTION LEFT RIGHT SHIFT (TSLRS)

(By : Yuniardi Wahyu Nugraha; Advisor : Thresye, Oni Soesanto, 2023, 46 pages)

Matrix is an arrangement of elements arranged in the form of rows and columns, the concept of a matrix can be used in solving a problem related to cryptography. In 1929 a mathematician named Lester Hill created a polyalphabetic cryptographic system called the Hill Cipher. Hill cipher is an algorithm that in its process uses a matrix of size (m × m) as the key matrix. The basis of the algorithm uses matrix multiplication to create the encryption and then uses the inverse of that matrix to decrypt. The classic Hill Cipher has the disadvantage that the operation used is not complicated. In this study, the classic Hill Cipher will be modified by using an orthogonal matrix as the key matrix, as well as adding several other operations such as transposition, substitution, and bit shift. The purpose of this study is to analyze the differences in cryptographic algorithms on data (text) using the classic Hill Cipher and the modified Hill Cipher. This research was conducted by encrypting and decrypting the classic Hill Cipher and modified Hill Cipher using similar data (text). Furthermore, a simulation will be carried out using Matlab so that it can use data (text) with a larger size. In the modified Hill Cipher there are three key matrices. The two additional key matrices were obtained in the substitution process using the Caesar Cipher and during the left-right shift process. The results obtained are Hill Cipher which has been modified using an asymmetric cryptographic system, namely in the left-right shift process so that the matrix keys used for encryption and decryption are different. Because it uses a different key in the encryption and decryption process, thus increasing the level of difficulty in decoding the message.

Keywords : *matrix, cryptography, Hill Cipher*

PRAKATA

Alhamdulillahirobbil alamin, segaja puji syukur penulis panjatkan kehadirat Allah *subhanahu wa ta'ala* atas berkat rahmat, karunia dan hidayah-Nya lah sehingga penulis dapat menyelesaikan pengerjaan serta penulisan skripsi dengan judul "MODIFIKASI *HILL CIPHER* DENGAN MENGGUNAKAN MATRIKS KUNCI ORTHOGONAL DAN *TRANSPOSITION SUBSTITUTION LEFT RIGHT SHIFT (TSLRS)*". Tidak lupa juga shalawat serta salam selalu tercurahkan kepada junjungan besar Nabi Muhammad *sallallahu alaihi wasallam* beserta keluarga, kerabat dan sahabat serta pengikut beliau hingga yaumul qiyamah. Penyusunan skripsi ini bertujuan untuk memenuhi salah satu persyaratan dalam rangka menyelesaikan program sarjana Strata-1 Matematika di Program Studi Matematika Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Lambung Mangkurat.

Penulis menyadari dalam penulisan skripsi ini masih jauh dari kata sempurna, banyak kekurangan baik dalam penulisan maupun dalam pembahasan materi. Proses penyusunan skripsi ini tidak terlepas dari bantuan, dukungan maupun bimbingan dari berbagai pihak. Oleh karena itu penulis ingin mengucapkan terima kasih sebesar-besarnya kepada:

1. Kedua orang tua penulis, Sumardi dan Muji Rahayu berserta keluarga yang selalu memberikan dukungan, doa, nasehat, motivasi, kasih sayang dan pengertian serta kesabaran yang sangat luar biasa dalam menemani penulis di setiap langkah hidupnya.
2. Bapak Drs. Abdul Gafur, M.Si, M.Sc, Ph.D. selaku Dekan Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Lambung Mangkurat Banjarbaru.
3. Bapak Pardi Affandi, S.Si, M.Sc selaku Koordinator Program Studi Matematika Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Lambung Mangkurat Banjarbaru.
4. Ibu Thresye, S.Si, M.Si dan Bapak Oni Soesanto, S.Si, M.Si selaku Dosen

Pembimbing yang telah sabar membimbing, memberikan masukan dalam penulisan dan penyusunan skripsi ini dari awal sampai akhir.

5. Ibu Dr. Na'imah Hijriati, S.Si, M.Si dan Bapak Akhmad Yusuf, S.Si, M.Kom selaku Dosen Penguji yang telah memberikan masukan dalam penulisan dan penyusunan skripsi ini.
6. Bapak Saman Abdurrahman, S.Si, M.Sc selaku dosen penasehat Akademik atas arahan dan bimbingannya selama perkuliahan.
7. Bapak dan Ibu Dosen dan Staf Program Studi Matematika yang sudah memberikan Ilmunya, memberikan arahan dan bantuan dalam hal kelengkapan administrasi dalam rangka medukung penulisan dan penyusuan skripsi ini.
8. Teman-teman kontrakan, yaitu Husni, Andika, Ufik, Anshar dan Raisan yang telah memberikan bantuan dalam penulisan dan penyusunan skripsi baik berupa saran, masukan serta motivasi untuk penulis dalam menyelesaikan skripsi ini.
9. Seluruh teman-teman Mahasiswa Matematika Angkatan 2018 keluarga Integrasi yang sudah membersamai selama ini.
10. Dan semua pihak yang telah membantu hingga terselesainya penulisan dan penyusunan skripsi ini tidak dapat penulis sebutkan satu persatu.

Penulis menyadari dalam penulisan dan penyusunan skripsi ini masih jauh dari kata sempurna, masih terdapat kekurangan baik dalam penulisan maupun dalam pembahasan materi. Oleh karena itu kritik dan saran yang membagnun akan senantiasa penulis harapkan demi kesempurnaan di masa mendatang. Semoga skripsi ini dapat memberikan sumbangan yang bermanfaat bagi semua pihak.

Banjarbaru, 28 April 2023

Yuniardi Wahyu Nugraha
NIM. 1811011110011

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

Gambar Halaman

DAFTAR LAMBANG

$\forall\, x$	: untuk setiap x
$x \in X$	: x anggota dari X
$a \mid b$	: a habis membagi b
$a \nmid b$	: a tidak habis membagi b
a mod b	: a modulo b
$a \equiv b$	: a kongruen b
A^{-1}	: Invers A
A^{T}	: Transpose A
$W^{\perp}$	: Komplemen orthogonal dari W
$\text{proj}_{\text{W}}\, \boldsymbol{u}$	: Proyeksi orthogonal $\boldsymbol{u}$ pada W