PEMBANGKITAN ALGORITMA *HILL CIPHER* MENGGUNAKAN *PLAYFAIR CIPHER* DENGAN MATRIKS KUNCI PERSEGI PANJANG

SKRIPSI

untuk memenuhi persyaratan

dalam menyelesaikan program sarjana Strata-1 Matematika

Oleh:

Siti Zulaikah

NIM. 2011011120006

PROGRAM STUDI MATEMATIKA

FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM

UNIVERSITAS LAMBUNG MANGKURAT

BANJARBARU

2024

HALAMAN PENGESAHAN

SKRIPSI

PEMBANGKITAN ALGORITMA HILL CIPHER MENGGUNAKAN PLAYFAIR CIPHER DENGAN MATRIKS KUNCI PERSEGI PANJANG

Oleh:

Siti Zulaikah

NIM. 2011011120006

telah dipertahankan di depan Dosen Penguji pada tanggal 6 Maret 2024

Susunan Dosen Penguji:

Pembimbing I

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

Pembimbing II

Nurul Huda, S.Si., M.Si.
NIP. 19810422 2006041003

Dosen Penguji:

1. Dr. Na'imah Hijriati, S.Si., M.Si. ( )
2. Saman Abdurrahman, S.Si., M.Sc. ( )

Banjarbaru, 22 Maret 2024
Koordinator Program Studi Matematika

Fadly Ahmadi, S.Si., M.Sc.
NIP. 197806112005011001

PERNYATAAN

Dengan ini say amenyatakan 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, 25 Maret 2024

Siti Zulaikah
2011011120006

ABSTRAK

PEMBANGKITAN ALGORITMA *HILL CIPHER* MENGGUNAKAN *PLAYFAIR CIPHER* DENGAN MATRIKS KUNCI PERSEGI PANJANG

(Oleh: Siti Zulaikah; Pembimbing: Thresye, Nurul Huda, 2023; 57 halaman)

Kriptografi merupakan ilmu menyandikan pesan atau data asli (*plaintext*) yang akan diubah ke bentuk tidak mudah dipahami oleh penerima yang tidak diinginkan (*ciphertext*). Algoritma *Hill Cipher* diperkenalkan oleh L.S. Hill pada tahun 1929. Algoritma kriptografi *Hill Cipher* biasanya menggunakan matriks persegi berukuran $m \times m$ sebagai matriks kunci dan memanfaatkan operasi modulo. *Hill Cipher* menggunakan perkalian matriks untuk proses enkripsi dan mencari invers matriks untuk melakukan dekripsi. Pada penelitian ini matriks kunci yang digunakan adalah matriks persegi panjang $(m \times n)$ yang diperoleh berdasarkan algoritma *Playfair Cipher*. *Playfair Cipher* dikembangkan oleh Charles Wheatstone pada tahun 1854 dan dipublikasikan oleh Lord Playfair. Konsep algoritma *Playfair Cipher* adalah menyandikan pasangan huruf dengan menggunakan matriks 5×5 sebagai kunci dari *Playfair Cipher*. Tujuan dari penelitian ini adalah untuk membentuk matriks kunci persegi panjang untuk algoritma *Hill Cipher* dengan menggunakan algoritma *Playfair Cipher* dan melakukan enkripsi serta dekripsi pada algoritma *Hill Cipher*. Metode penelitian ini dengan studi literatur yaitu mengumpulkan bahan terkait dengan penelitian. Kemudian menjalankan algoritma Playfair Cipher untuk membentuk matriks kunci Hill Cipher. Hasil penelitian ini menunjukkan bahwa penggunaan kunci matriks persegi panjang dapat menyamarkan pesan karena ciphertext yang dihasilkan lebih panjang dibandingkan *plaintext* yang diberikan. Matriks kunci yang dibentuk merupakan matriks yang memiliki invers moore-penrose yang digunakan pada proses dekripsi. Jika matriks kunci tidak memiliki invers moore-penrose maka tidak dapat dilakukan proses dekripsi.

Kata kunci: Enkripsi, Dekripsi, *Hill Cipher*, Invers Moore-Penrose, *Playfair Cipher*.

ABSTRACT

GENERATING HILL CHIPER ALGORITHM BY USING PLAYFAIR CIPHER WITH RECTANGULAR KEY MATRIX (By: Siti Zulaikah; Advisors: Thresye, Nurul Huda, 2023; 57 pages)

Cryptography is the science of encoding original messages or data (plaintext) which will be converted into a form which is not easy to understand by the unintended recipient (ciphertext). The Hill Cipher algorithm was introduced by L.S. Hill in 1929. The Hill Cipher cryptography algorithm usually uses a $m \times n$ squares matrix as the key matrix and utilizes the modulo operation. Hill Cipher uses matrix multiplication for the encryption process and looks for the inverse matrix for decryption process. In this research, the key matrix is a rectangular matrix $(m \times n)$ which is based on the Playfair Cipher algorithm. The Playfair Cipher was developed by Charles Wheatstone in 1854 and published by Lord Playfair. The concept of the Playfair Cipher algorithm is to encode pairs of letters using a 5×5 matrix as the key of the Playfair Cipher. The purpose of this research is to form a rectangular key matrix for the Hill Cipher algorithm by using the Playfair Cipher algorithm and do encryption and decryption on the Hill Cipher algorithm. This research method is a literature study, by reading and collecting information about the research. And then, use Playfair Cipher algorithm to form Hill Cipher key matrix. The results of this research is rectangular matrix keys can disguise messages because the result of ciphertext is longer than the plaintext provided. The key matrix formed is a matrix which has the Moore-Penrose inverse which can be used in the decryption process. If the key matrix does not have an inverse Moore-Penrose, then the decryption process cannot be carried out.

Keywords: Encryption, Decryption, *Hill Cipher*, Invers Moore-Penrose, *Playfair Cipher*.

PRAKATA

Alhamdulillahirabbil'alamin, puji syukur ke hadirat Allah *subhanahu wa ta'ala* yang telah memberikan kemudahan bagi penulis, puji syukur penulis panjatkan kehadirat Allah *subhanahu wa ta'ala* atas segala berkat, rahmat, hidayah, karunia, dan izin-Nya, serta shalawat dan salam tercurahkan kepada junjungan besar Nabi Muhammad shalallahu 'alaihi wasallam beserta para keluarga, sahabat serta pengikut hingga akhir zaman sehingga penulis dapat menyelesaikan skripsi yang berjudul "Pembangkitan Algoritma *Hill Cipher* menggunakan *Playfair Cipher* dengan Matriks Kunci Persegi Panjang" dengan baik. Penyusunan skripsi ini bertujuan untuk memenuhi salah satu persyaratan dalam menyelesaikan program Strata-1 Matematika di Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Lambung Mangkurat.

Proses penyusunan skripsi ini tidak terlepas dari dukungan, doa, kerja sama, bimbingan, dan bantuan dari berbagai pihak. Selesainya penulisan skripsi ini penulis persembahkan kepada orang tua, keluarga tercinta, dan teman-teman yang penulis banggakan. Pada kesempatan ini juga, penulis mengucapkan terima kasih yang sebesar-besarnya kepada:

1. Bapak Drs. Abdul Gafur, M.Si., M.Sc., Ph.D selaku Dekan Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Lambung Mangkurat Banjarbaru.
2. Bapak Pardi Affandi, S.Si., M.Sc., selaku koordinator program studi Matematika Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Lambung Mangkurat Banjarbaru.
3. Ibu Thresye S.Si., M.Si., dan Bapak Nurul Huda S.Si., M.Si. selaku dosen pembimbing yang telah mendampingi dan membimbing dalam penyusunan skripsi ini dari awal sampai akhir.
4. Ibu Dr. Na'imah Hijriati, S.Si., M.Si dan Bapak Saman Abdurrahman, S.Si., M.Sc. selaku dosen penguji yang telah memberikan masukan untuk perbaikan dalam penyusunan skripsi ini.

5. Ibu Dr. Na'imah Hijriati, S.Si., M.Si selaku dosen penasehat akademik yang telah memberikan arahan dan bimbingan selama perkuliahan.
6. Bapak dan Ibu Dosen dan Staf Program Studi Matematika yang sudah memberikan ilmunya, memberikan arahan dan bantuan dalam hal kelengkapan administrasi dalam rangka penyusunan skripsi ini.
7. Ayah, Ibu, dan nenek serta keluarga di rumah, karena tanpa dukungan dan motivasi dari mereka saya mungkin tidak dapat menyelesaikan penelitian ini.
8. Kak Yusti, Kak Iffa, dan Kak Qia yang telah banyak membantu dalam memahami, memberi motivasi, dukungan dan bantuan lainnya yang dibutuhkan dalam penelitian ini.
9. Seluruh sahabat saya (Uyong, Randra, Siti, Alip, Qibti, Aini, Rosyadi, Yani, Eta dan Cipa), teman kos (Nisa), teman kuliah kriptografi (Jihandika) dan rekan mahasiswa yang telah banyak memberikan bantuan, semangat, bimbingan, dan kerja sama dalam menyelesaikan penyusunan skripsi ini.
10. Dan banyak pihak yang tidak dapat penulis sebut 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 membangun akan senantiasa penulis harapkan demi kesempurnaan dimasa yang akan datang. Semoga skripsi ini dapat memberikan sumbangan yang bermanfaat bagi semua pihak.

Banjarbaru, 25 Maret 2024

Siti Zulaikah

2011011120006

DAFTAR ISI

Halaman

DAFTAR TABEL

Tabel **Halaman**

ARTI LAMBANG DAN SINGKATAN

a_{ij}	: elemen matriks A yang terletak pada baris ke-i dan kolom ke-j
A^T	: transpose dari matriks A
A^{-1}	: invers dari matriks A
$A^{\dagger}$	: invers moore penrose dari matriks A
$\bar{A}$	: matriks konjugat
A^*	: matriks transpose konjugat
$a \bmod m$	: sisa dari a dibagi oleh m
$a \equiv b (mod\ m)$	: a kongruen b modulo m
$a \mid b$	: a membagi m
$a \nmid b$	: a tidak membagi m
$rank(A)$	: rank dari matriks A
C	: matriks enkripsi dari *plaintext* P
P	: matriks dekripsi dari *ciphertext* C
■	: terbukti
I	: matriks identitas
$S^{\perp}$	: himpunan ortogonal dari S
R^n	: vektor berdimensi n