MENGEMBANGKAN *HIBRID CAESAR CIPHER* DAN *VIGENERE CIPHER* YANG DIMODIFIKASI UNTUK KOMUNIKASI DATA YANG AMAN

SKRIPSI

untuk memenuhi persyaratan
dalam menyelesaikan program sarjana Strata-1 Matematika

Oleh:
Muhammad Fikri Ilhami
NIM. 1611011210012

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

SKRIPSI

MENGEMBANGKAN *HIBRID CAESAR CIPHER* DAN *VIGENERE CIPHER* YANG DIMODIFIKASI UNTUK KOMUNIKASI DATA YANG AMAN

Oleh:

MUHAMMAD FIKRI ILHAMI

NIM 1611011210012

telah dipertahankan di depan Dosen Penguji pada tanggal 5 Januari 2024.

Susunan Dosen Penguji:

Pembimbing I

Thresye, S.Si., M.Si.

NIP. 197205042000122002

Dosen Penguji:

1. Oni Soesanto, S.Si., M.Si.
2. Pardi Affandi, S.Si., M.Sc.

Pembimbing II

Akhmad Yusuf, S.Si., M.Kom.

NIP. 198004022005011001

Banjarbaru, 5 Januari 2024

Wakil Dekan Bidang Akademik,

Dr. Gunawan, S.Si., M.Si.

NIP. 197911012005011002

Koordinato 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, 5 Januari 2024

Muhammad Fikri Ilhami
NIM. 1611011210012

ABSTRAK

MENGEMBANGKAN *HIBRID CAESAR CIPHER* DAN *VIGENERE CIPHER* YANG DIMODIFIKASI UNTUK KOMUNIKASI DATA YANG AMAN (Oleh: Muhammad Fikri Ilhami; Pembimbing: Thresye, S.Si, M.Si, Akhmad Yusuf, S.Si, M.Kom,2023; 66 halaman)

Pengamanan data dilakukan dengan teknik enkripsi dan dekripsi yang merupakan proses dalam kriptografi. Enkripsi merupakan proses penyandian plainteks menjadi cipherteks dan dekripsi merupakan proses sebaliknya. Penelitian ini bertujuan untuk meningkatkan keamanan data melalui pendekatan hibrid menggunakan Caesar cipher dan Vigenere cipher. Kombinasi dari kedua cipher klasik ini dengan modifikasi untuk mencakup huruf, angka, dan simbol diharapkan dapat memaksimalkan keamanan data. Keamanan pertama terletak dari tingkat keamanan enkripsi data *caesar cipher* yang bergantung pada pergeseran karakter yang digunakan. Selanjutnyta keamanan kedua, data yang sudah disandikan akan dienkripsi sekali lagi menggunakan *vigenere cipher* sehingga membuat data semakin sulit dipecahkan. Penelitian ini mengkaji bagaimana pembentukan algoritma *hibrid caesar cipher* dan *vigenere cipher* yang telah dimodifikasi dan bagaimana perbandingan *hibridcaesar cipher* dan *vigenere cipher* yang menggunakan substitusi alfabet dan ASCII pada program Matlab.

Kata Kunci:*Hibrid, Caesar cipher, Vigenere cipher*.

ABSTRACT

DEVELOPING A MODIFIED HYBRID CAESAR CIPHER AND VIGENERE CIPHER FOR SECURE DATA COMMUNICATION (By : Muhammad Fikri Ilhami; Advisors: Thresye, S.Si, M.Si, Akhmad Yusuf, S.Si, M.Kom,2023; 66 pages)

Data security is carried out with encryption techniques and descriptions which are the process in cryptography. Encryption is the process of encoding plaintext into ciphertext and decryption is the reverse process. This research aims to improve data security through a hybrid approach using the Caesar cipher and the Vigenere cipher. The combination of these two classic ciphers with modifications to include letters, numbers and symbols is expected to maximize data security. The first security lies in the security level of caesar cipher data encryption that depends on the character shift used. Furthermore, the second security, the data that has been encouraged will be encrypted once again using the vigenere cipher so as to make the data more difficult to solve. This study examines how the formation of the modified hybrid caesar cipher and vigenere cipher algorithm and how to compare hybrid caesar cipher and vigenere cipher that uses the alphabet and ASCII substitution in the matlab program.

Keywords: Hybrid, Caesar cipher, Vigenere cipher.

PRAKATA

Alhamdulillhah, puji syukur kepada Tuhan Yang Maha Esa yang telah melimpahkan rahmat dan karunia-Nya kepada penulis, sehingga penulis dapat menyelesaikan skripsi yang berjudul **"MENGEMBANGKAN *HIBRID CAESAR CIPHER* DAN *VIGENERE CIPHER* YANG DIMODIFIKASI UNTUK KOMUNIKASI DATA YANG AMAN"**. Penyesuaian skripsi ini dimaksudkan untuk memenuhi salah satu persyaratan dalam rangka menyelesaikan program sarjana Strata-1 Matematika di Program Studi Matematika Fakultas Matematika dan Ilmu Pengetahua Alam Universitas Lambung Mangkurat.

Pada kesempatan ini, 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 yang telah sabar membimbing, meluangkan waktu, memberikan bantuan, dan motivasi yang sangat berharga dari awal sampai akhir penyusunan skripsi ini.
3. Ibu Thresye, S.Si., M.Si. selaku dosen pembimbing I dan Bapak Akhmad Yusuf, S.Si., M.Kom. selaku dosen pembimbing II yang telah bersabar membinmbing , meluangkan waktu dan mendampingi dari awal sampai akhir penyusunan skripsi ini.
4. Bapak Oni Soesanto, S.Si., M.Si. selaku dosen penguji I dan Pardi Affandi, S.Si., M.Sc. selaku dosen penguji II yang telah memberikan masukan dalam penyusunan skripsi ini.
5. Dosen-dosen pengajar dan staff administrasi Program Studi Matematika yang telah memberikan bantuan, bimbingan, motivasi dan ilmu yang bermanfaan.
6. 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.

7. Kedua orang tua, saudara, serta keluarga tercinta yang senantiasa mendo'akan, nasehat, motivasi, dan dukungan.
8. Sahabat-sahabat saya yang selama ini menempuh perkuliahan dan pengalaman yang luar biasa bersama-sama akan menjadi momen yang tidak terlupakan dan sangat dirindukan.
9. Teman-teman seperjuangan Program Studi Matematika yang telah memberikan dukungan serta semangat luar biasa selama perkuliahan.

Penulis menyadari akan kekurangan dalam menyusun skripsi ini. Oleh karena itu, penulis mengharapkan saran dan kritik demi penyempurnaan skripsi ini. Akhir kata, penulis berharap semoga skripsi ini dapat bermanfaat bagi semua pihak dan khususnya mahasiswa Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Lambung Mangkurat Banjarbaru. Aamiiiin.

Banjarbaru, 5 Januari 2024

Muhammad Fikri Ilhami
NIM. 1611011210012

DAFTAR ISI

Halaman

DAFTAR GAMBAR

Halaman

DAFTAR TABEL

Halaman

ARTI LAMBANG DAN SINGKATAN

Simbol	Arti
$\mathbb{Z}$	: notasi himpunan bilangan bulat
$a \mid b$	: a *membagi* b
$a \nmid b$	: $a$tidak membagi b
mod	: module
$a \equiv b$	: $a$kongruen b
$C_n = E_n(P)$	: enkripsi cipherteks dari plainteks
$P_n = D_n(C)$	: dekripsi plainteks dari cipherteks
K_n	: kunci
SM	: Sebelum Masehi
ASCII	: American Standard Code for Information Interchange
DES	: Data Encryption Standard
IDEA	: International Data Encryption Algorithm
AES	: Advanced Encryption Standard
OTP	: One Time Pad
MAC	: Message Authentication Code
RC	: Ron Code / Rivest's Cipher
IBM 437	: Kode asli IBM Personal Computer
■	: Bukti Selesai