MENINGKATKAN KEAMANAN KUNCI MENGGUNAKAN PERTUKARAN KUNCI DIFFIE-HELLMAN DENGAN KRIPTOGRAFI SIMETRIS

SKRIPSI

untuk memenuhi persyaratan
dalam menyelesaikan program sarjana Strata-1 Matematika

Oleh:

NANDA ROSSIANA ZAHWARI
NIM. 1911011320010

PROGRAM STUDI S1-MATEMATIKA
FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM
UNIVERSITAS LAMBUNG MANGKURAT
BANJARBARU

2024

SKRIPSI

MENINGKATKAN KEAMANAN KUNCI MENGGUNAKAN PERTUKARAN KUNCI DIFFIE-HELLMAN DENGAN KRIPTOGRAFI SIMETRIS

Oleh:

Nanda Rossiana Zahwari

NIM. 1911011320010

telah dipertahankan di depan Dosen Penguji pada tanggal 12 Februari 2024.
Susunan Dosen Penguji:

Pembimbing I

Dr. Mochammad Idris., S.Si., M.Si.
NIP. 197702142005011001

Pembimbing II

Saman Abdurrahman, S.Si., M.Sc.
NIP. 197807132005011002

Dosen Penguji:

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

Banjarbaru, 29 Februari 2024

Wakil Dekan Bidang Akademik,

Dr. Gunawan, S.Si., M.Si.
NIP. 19791012005011002

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, 29 Februari 2024

Nanda Rossiana Zahwari
NIM. 1911011320010

ABSTRAK

MENINGKATKAN KEAMANAN KUNCI MENGGUNAKAN PERTUKARAN KUNCI DIFFIE-HELLMAN DENGAN KRIPTOGRAFI SIMETRIS (Oleh: Nanda Rossiana Zahwari; Pembimbing: Mochammad Idris, Saman Abdurrahman; 2024; 49 halaman)

Kriptografi sangat diperlukan dalam masalah keamanan pesan atau data. Kriptografi merupakan ilmu, seni, atau teknik dalam memecahkan sebuah *ciphertext*. Kriptografi berguna dalam menjaga keamanan informasi atau kerahasiaan data, integritas data, autentikasi individu, dan autentikasi sumber data. Kriptografi simetris merupakan kriptografi yang menggunakan satu buah kunci rahasia yang sama dalam proses enkripsi dan dekripsi. Penelitian ini bertujuan untuk menentukan proses enkripsi pada kriptografi simetris dapat menggunakan formula dekripsi dan proses dekripsi dapat menggunakan formula enkripsi. Selain itu, penelitian ini juga bertujuan untuk meningkatkan keamanan pesan dengan menerapkan pertukaran kunci Diffie-Hellman menggunakan kriptografi simetris dan melakukan simulasi numerik. Kriptografi simetris yang digunakan dalam penelitian ini adalah Caesar *cipher*, *affine cipher*, dan Vigenere *cipher*. Hasil dari penelitian ini adalah diperoleh kunci rahasia bersama. Pada pertukaran kunci Diffie-Hellman, dengan memilih kunci rahasia dan menyepakati kunci publik maka diperoleh kunci rahasia bersama yang kemudian akan digunakan sebagai kunci rahasia pada kriptografi simetris. Simulasi numerik yang disajikan adalah dengan menginput kunci, *plaintext*, dan *ciphertext* sehingga diperoleh hasil dari enkripsi dan dekripsi.

Kata Kunci: Caesar *Cipher*, *Affine Cipher*, Vigenere *Cipher*, Pertukaran Kunci Diffie-Hellman.

ABSTRACT

IMPROVING KEY SECURITY USING DIFFIE-HELLMAN KEY EXCHANGE WITH SYMMETRIC CRYPTOGRAPHY (By: Nanda Rossiana Zahwari; Thesis Advisor: Mochammad Idris, Saman Abdurrahman; 2024; 49 pages)

Cryptography is indispensable in message or data security issues. Cryptography is the science, art, or technique of cracking a ciphertext. Cryptography is useful in maintaining information security or data confidentiality, data integrity, individual authentication, and data source authentication. Symmetric cryptography is cryptography that uses the same secret key in the encryption and decryption process. This research aims to determine the encryption process in symmetric cryptography can use the decryption formula and the decryption process can use the encryption formula. In addition, this research also aims to improve message security by applying Diffie-Hellman key exchange using symmetric cryptography and performing numerical simulations. The symmetric cryptography used in this research are Caesar cipher, affine cipher, and Vigenere cipher. The result of this research is that a shared secret key is obtained. In Diffie-Hellman key exchange, by selecting the secret key and agreeing on the public key, a shared secret key is obtained which will then be used as the secret key in symmetric cryptography. The numerical simulation presented is by inputting the key, plaintext, and ciphertext so that the results of encryption and decryption are obtained.

Keywords: Caesar Cipher, Affine Cipher, Vigenere Cipher, Diffie-Hellman Key Exchange

PRAKATA

Alhamdulillahirabbil'alamin, puji syukur kepada Allah subhanahu wa ta'ala yang telah memberikan ridha, rahmat, karunia, serta izin-Nya, sehingga penulis dapat menyelesaikan skripsi dengan judul "Meningkatkan Keamanan Kunci Menggunakan Pertukaran Kunci Diffie-Hellman dengan Kriptografi Simetris". Shalawat serta salam tak lupa tercurahkan kepada junjungan Nabi Muhammad shalallahu 'alaihi wasallam beserta keluarga, sahabat, serta pengikut beliau hingga akhir zaman. 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.

Pada proses penyusunan skripsi ini tidak terlepas dari bantuan dan dukungan dari berbagai pihak. Selesainya penulisan skripsi ini secara khusus 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.

3. Ibu Thresye, S.Si., M.Si. selaku dosen pembimbing akademik yang telah memberikan bimbingan, arahan, dan motivasi selama perkuliahan.

4. Bapak Dr. Mochammad Idris, S.Si., M.Si. dan Bapak Saman Abdurrahman, S.Si., M.Sc. selaku dosen pembimbing yang telah bersedia meluangkan waktu, membimbing dan mendampingi selama penyusunan skripsi ini hingga akhirnya skripsi ini dapat terselesaikan.

5. Bapak Akhmad Yusuf, S.Si., M.Kom. dan Ibu Dr. Na'imah Hijriati, S.Si., M.Si. selaku dosen penguji yang telah memberikan masukan dan saran sehingga penulisan skripsi ini dapat menjadi lebih baik.

6. Dosen-dosen pengajar dan Staf Program Studi Matematika yang telah memberikan ilmu, arahan, dan bantuan dalam kelengkapan administrasi dalam rangka penyusunan skripsi ini.

7. Orang tua, adik, dan keluarga yang selalu menjadi penyemangat dan selalu memberikan dukungan, kasih sayang, doa, pengertian, dan nasihat kepada penulis. Penulis berharap dapat menjadi anak yang baik dan dapat dibanggakan di dunia maupun di akhirat kelak.

8. Seluruh sahabat, teman, dan rekan mahasiswa matematika angkatan 2019 yang telah menjadi teman seperjuangan selama perkuliahan, memberikan kesenangan, canda tawa, motivasi, keluh kesah, saran dalam penulisan skripsi ini.

Dalam penyusunan skripsi ini tentunya terdapat kekurangan, sehingga penulis mengharapkan kritik dan saran untuk dijadikan masukan dan pembelajaran. Akhir kata, semoga skripsi ini dapat bermanfaat bagi semua pihak, terutama mahasiswa Program Studi Matematika Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Lambung Mangkurat. Aamiin.

Banjarbaru, 29 Februari 2024

Nanda Rossiana Zahwari
NIM. 1911011320010

DAFTAR ISI

DAFTAR TABEL

Tabel Halaman

DAFTAR GAMBAR

Gambar Halaman

ARTI LAMBANG DAN SINGKATAN

$\mathbb{N}$	:	himpunan bilangan asli
$\in$	:	anggota atau elemen
$\notin$	:	bukan anggota atau bukan elemen
$=$	:	sama dengan
$\neq$	:	tidak sama dengan
$<$	:	kurang dari
$>$	:	lebih dari
$\leq$	:	kurang dari atau sama dengan
$\geq$	:	lebih dari atau sama dengan
$a \mid b$	:	a membagi habis b
$a \nmid b$	:	a tidak membagi habis b
FPB	:	faktor persekutuan terbesar
$FPB(a, b)$	:	faktor persekutuan terbesar dari a dan b
$\equiv$	:	kongruen
$a \equiv b \ (mod\ m)$	:	a kongruen dengan b modulo m
a^{-1}	:	invers dari a
A_m	:	himpunan bilangan modulo