

SKRIPSI

**MODIFIKASI PEMBANGKIT PERTUKARAN KUNCI ALGORITMA
DIFFIE-HELLMAN DALAM KRIPTOSISTEM KOMBINASI VIGENERE
CIPHER DAN OPERASI XOR**

*MODIFICATION OF THE DIFFIE-HELLMAN KEY EXCHANGE
ALGORITHM IN CRYPTOSYSTEM OF COMBINATION OF VIGENERE
CIPHER AND XOR OPERATION*



MUHAMMAD RIZAL INDRASTA

24010119140101

**DEPARTEMEN MATEMATIKA
FAKULTAS SAINS DAN MATEMATIKA
UNIVERSITAS DIPONEGORO
SEMARANG**

2023

HALAMAN PENGESAHAN

SKRIPSI

**MODIFIKASI PEMBANGKIT PERTUKARAN KUNCI ALGORITMA
DIFFIE-HELLMAN DALAM KRIPTOSISTEM KOMBINASI VIGENERE
CIPHER DAN OPERASI XOR**

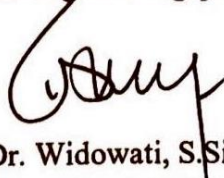
Telah dipersiapkan dan disusun oleh :

MUHAMMAD RIZAL INDRASTA
24010119140101

Telah dipertahankan di depan Tim Penguji
pada tanggal 6 April 2023

Susunan Tim Penguji

Pembimbing II / Penguji



Prof. Dr. Widowati, S.Si., M.Si
NIP. 196902141994032002

Penguji,



Dr. Nikken Prima Puspita, S.Si., M.Sc
NIP. 198604132009122007

Mengetahui,

Ketua Departemen Matematika



Dr. Sursilo Hariyanto, S.Si., M.Si
NIP. 197410142000121001

Pembimbing I / Penguji



Suryoto, S.Si., M.Si
NIP. 196807141994031004

ABSTRAK

MODIFIKASI PEMBANGKIT PERTUKARAN KUNCI ALGORITMA DIFFIE-HELLMAN DALAM KRITOSISTEM KOMBINASI VIGENERE CIPHER DAN OPERASI XOR

oleh

Muhammad Rizal Indrasta
24010119140101

Kriptografi merupakan cabang ilmu sains yang mempelajari seni penyandian pesan agar pesan tersebut tetap aman. Dalam kriptografi diperlukan suatu teknik matematika guna membuat suatu algoritma di dalamnya. Terdapat suatu algoritma pembangkit kunci dalam kriptografi, yaitu pembangkit pertukaran kunci Algoritma Diffie-Hellman. Vigenere Cipher dan Operasi XOR merupakan dua dari berbagai algoritma kriptografi. Pada skripsi ini membahas mengenai modifikasi pembangkit pertukaran kunci Algoritma Diffie-Hellman dengan membentuk suatu kunci yang baru dan kemudian kunci tersebut diterapkan dalam kritosistem kombinasi Vigenere Cipher dan Operasi XOR. Terdapat dua langkah dalam proses enkripsi pada kritosistem ini, langkah pertama adalah menggunakan Vigenere Cipher dan langkah kedua adalah menggunakan dengan Operasi XOR. Sebaliknya, dalam proses dekripsi, langkah pertama dekripsi adalah menggunakan Operasi XOR dan langkah kedua dekripsi menggunakan Vigenere Cipher.

Kata kunci : Kriptografi, Enkripsi, Dekripsi, Pertukaran Kunci Diffie-Hellman, *Vigenere Cipher*, Operasi XOR.

Pembimbing I/Penguji



Suryoto, S.Si., M.Si.
NIP. 196807141994031004

Pembimbing II/Penguji



Prof. Dr. Widowati, S.Si., M.Si.
NIP. 196902141994032002