**SKRIPSI**

# PENERAPAN FUNGSI HASH PADA *SECURE HASH ALGORITHM-256*

# *THE APPLICATION OF HASH FUNCTION IN SECURE HASH ALGORITHM-256*

ANGGREKA BRILIANNA NOVITASARI
24010119130076

**DEPARTEMEN MATEMATIKA**
**FAKULTAS SAINS DAN MATEMATIKA**
**UNIVERSITAS DIPONEGORO**
**SEMARANG**
**2026**

**SKRIPSI**

# PENERAPAN FUNGSI HASH PADA *SECURE HASH ALGORITHM-256*

## *THE APPLICATION OF HASH FUNCTION IN SECURE HASH ALGORITHM-256*

Diajukan untuk memenuhi salah satu syarat memperoleh derajat
Sarjana Matematika (S.Mat.)

ANGGREKA BRILIANNA NOVITASARI
24010119130076

**DEPARTEMEN MATEMATIKA**
**FAKULTAS SAINS DAN MATEMATIKA**
**UNIVERSITAS DIPONEGORO**
**SEMARANG**
**2026**

**HALAMAN PENGESAHAN**

**SKRIPSI**

**PENERAPAN FUNGSI HASH PADA *SECURE HASH ALGORITHM-256***

Telah dipersiapkan dan disusun oleh:

ANGGREKA BRILIANNA NOVITASARI
24010119130076

Telah dipertahankan di depan Tim Penguji
pada tanggal 6 Maret 2026

Susunan Tim Penguji

Pembimbing II/Penguji,

Solikhin, S.Si., M.Sc
NIP. 198506302012121001

Penguji,

Dr. Dra. Titi Udjiani, S.R.R.M., M.Si.
NIP. 196402231991022001

Mengetahui,
Ketua Departemen Matematika,

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

Pembimbing I/Penguji,

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

# ABSTRAK

## PENERAPAN FUNGSI HASH PADA *SECURE HASH ALGORITHM-256*

oleh

Anggreka Brilianna Novitasari
24010119130076

Diberikan keluarga hash $(\mathcal{A}, \mathcal{B}, \mathcal{K}, \mathcal{H})$. Fungsi hash tanpa kunci adalah keluarga hash dengan $|\mathcal{K}| = 1$. Pada Tugas Akhir ini, analisis keamanan berfokus pada sifat *collision resistant*. Konstruksi Merkle–Damgård adalah konstruksi yang menunjukkan bahwa sifat *collision resistant* dari fungsi hash iteratif $\mathbb{H}$ bergantung pada fungsi kompresi $h$. Algoritma *Secure Hash Algorithm-256* (SHA-256) adalah algoritma yang dibangun dari konstruksi Merkle–Damgård. Untuk meningkatkan kesulitan dalam menukan *collision* pada SHA-256, digunakan operasi $\wedge$ pada fungsi kompresi $h$ untuk merusak struktur grup serta digunakan fungsi $Choose$ dan fungsi $Majority$ pada fungsi kompresi $h$ untuk meningkatkan kompleksitas algoritma karena fungsi tersebut bukan homomorfisma grup.

**Kata kunci:** fungsi hash, *collision resistant*, Merkle–Damgård, SHA-256, struktur aljabar.

## ABSTRACT

***THE APPLICATION OF HASH FUNCTION IN SECURE HASH ALGORITHM-256***

by

Anggreka Brilianna Novitasari
24010119130076

Given a hash family $(\mathcal{A}, \mathcal{B}, \mathcal{K}, \mathcal{H})$, an unkeyed hash function is defined as a hash family with $|\mathcal{K}| = 1$. In this Final Project, the security analysis is focused on the collision resistant property. The Merkle–Damgård construction is a construction that shows collision resistant property of iterative hash function $\mathbb{H}$ depends on compression function $h$. The Secure Hash Algorithm–256 (SHA-256) is an algorithm that is constructed based on the Merkle–Damgård construction. To increase the difficulty of finding collisions in SHA-256, the $\wedge$ operation is used in compression function $h$ to break the group structure, also the $Choose$ and $Majority$ functions are used in compression function $h$ to enhance the complexity of the algorithm, as these functions are not group homomorphisms.



**Keywords:** hash function, *collision resistant*, Merkle–Damgård, SHA-256, algebraic structure.