

**IMPLEMENTASI KEAMANAN MENGGUNAKAN KRIPTOGRAFI
POST-QUANTUM KYBER768 PADA PROTOKOL *TRANSPORT LAYER*
*SECURITY***

Skripsi



Disusun oleh

Syifalita Hidawani

21SA3056

**PROGRAM STUDI TEKNOLOGI INFORMASI
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM PURWOKERTO
PURWOKERTO**

2025

**IMPLEMENTASI KEAMANAN MENGGUNAKAN KRIPTOGRAFI
POST-QUANTUM KYBER768 PADA PROTOKOL *TRANSPORT LAYER*
*SECURITY***

Skripsi

Untuk memenuhi sebagian persyaratan mencapai derajat Sarjana S1
pada Program Studi Teknologi Informasi Fakultas Ilmu Komputer



Disusun oleh

Syifalita Hidawani

21SA3056

**PROGRAM STUDI TEKNOLOGI INFORMASI
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM PURWOKERTO
PURWOKERTO**

2025

PERSETUJUAN

Skripsi

IMPLEMENTASI KEAMANAN MENGGUNAKAN KRIPTOGRAFI *POST-QUANTUM* KYBER768 PADA PROTOKOL *TRANSPORT LAYER* *SECURITY*

Yang dipersiapkan dan disusun oleh

Syifalita Hidawani

21SA3056

telah disetujui oleh dosen pembimbing Skripsi
Pada tanggal 18 Januari 2025

Dosen Pembimbing 1,

Dosen Pembimbing 2,

Didit Suhartono, M.Kom.
NIDN. 0626018004

Khairunnisak Nur Isnaini, M.Kom.
NIDN. 0624049402

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer (S.Kom.)
Tanggal 07 Februari 2025

Mengetahui,

Fakultas Ilmu Komputer
Dekan,

Kaprodi Teknologi Informasi

Dr. Eng., Ir. Imam Tahyudin, M.M.
NIK. 2012.09.1.009

Dr. Rujianto Eko Saputro, M.Kom.
NIK. 2014.02.1.018

PENGESAHAN

Skripsi

**IMPLEMENTASI KEAMANAN MENGGUNAKAN KRIPTOGRAFI
POST-QUANTUM KYBER768 PADA PROTOKOL *TRANSPORT LAYER*
*SECURITY***

Yang dipersiapkan dan disusun oleh

Syifalita Hidawani

21SA3056

Telah dipertahankan di depan dewan penguji
Pada tanggal 07 Februari 2025

Dr. Purwadi, M.Kom.
NIDN. 0628018101

Dani Arifudin, M.Kom.
NIDN. 0609109202

Khairunnisak Nur Isnaini, M.Kom.
NIDN. 0624049402

Skripsi ini telah disahkan sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer (S.Kom.)
Tanggal 07 Februari 2025

Mengetahui,

Fakultas Ilmu Komputer
Dekan

Dr. Eng., Ir. Imam Tahyudin, M.M.
NIK. 2012.09.1.009

SURAT PERNYATAAN KEASLIAN PENELITIAN

Yang bertanda tangan dibawah ini :

Nama Mahasiswa : Syifalita Hidawani
NIM : 21SA3056
Program Studi : Teknologi Informasi
Fakultas : Ilmu Komputer
Perguruan Tinggi : Universitas Amikom Purwokerto

Menyatakan bahwa Skripsi Sebagai Berikut:

Judul Skripsi : Implementasi Keamanan Menggunakan Kriptografi *Post Quantum* Kyber768 pada Protokol *Transport Layer Security*

Dosen Pembimbing 1 : Didit Suhartono, M.Kom.

Dosen Pembimbing 2 : Khairunnisak Nur Isnaini, M.Kom.

Adalah benar-benar **ASLI** dan **BELUM PERNAH** dibuat orang lain, kecuali yang diacu dalam daftar pustaka pada Skripsi ini.

Demikian pernyataan ini saya buat, apabila ini di kemudian hari terbukti bahwa saya melakukan penjiplakan karya orang lain, maka saya bersedia menerima **SANKSI AKADEMIK**.

Purwokerto, 18 Januari 2025

Yang menyatakan,

Bermaterai

10000

Syifalita Hidawani

NIM. 21SA3056

HALAMAN PERSEMBAHAN

Dengan rendah hati, penulis menyampaikan terima kasih kepada semua pihak yang terlibat, di antaranya:

1. Keluarga penulis yang tidak ada hentinya dalam mendoakan, mendukung, dan memfasilitasi penulis selama perjalanan studi.
2. Diri sendiri yang mampu melewati seluruh rangkaian perjalanan menulis skripsi ini.
3. Bapak Didit Suhartono, M.Kom., selaku dosen pembimbing skripsi I dan Ibu Khairunnisak Nur Isnaini, M.Kom., selaku dosen pembimbing skripsi II yang senantiasa sabar membimbing penulis, memberi waktu, arahan, saran, dukungan materiil maupun emosional hingga penulis dapat menyelesaikan penelitian ini.
4. Pemilik NIM 21SA3017 yang senantiasa menemani dan memberikan dukungan moral, motivasi, serta kesabaran tanpa batas kepada penulis selama perjalanan studi.
5. Teman-teman pengurus Forum Asisten 23/24 dan 24/25 serta anggota Forum Asisten yang telah banyak memberi dukungan kepada penulis.
6. Teman-teman kelas TI21B khususnya Delia, Vina, Lidiya dan Afi yang telah kebersamai penulis dari semester 1.
7. Rekan-rekan kuliah maupun seluruh pihak lain yang turut membantu dalam penyusunan skripsi ini yang tidak bisa penulis sebutkan satu persatu.

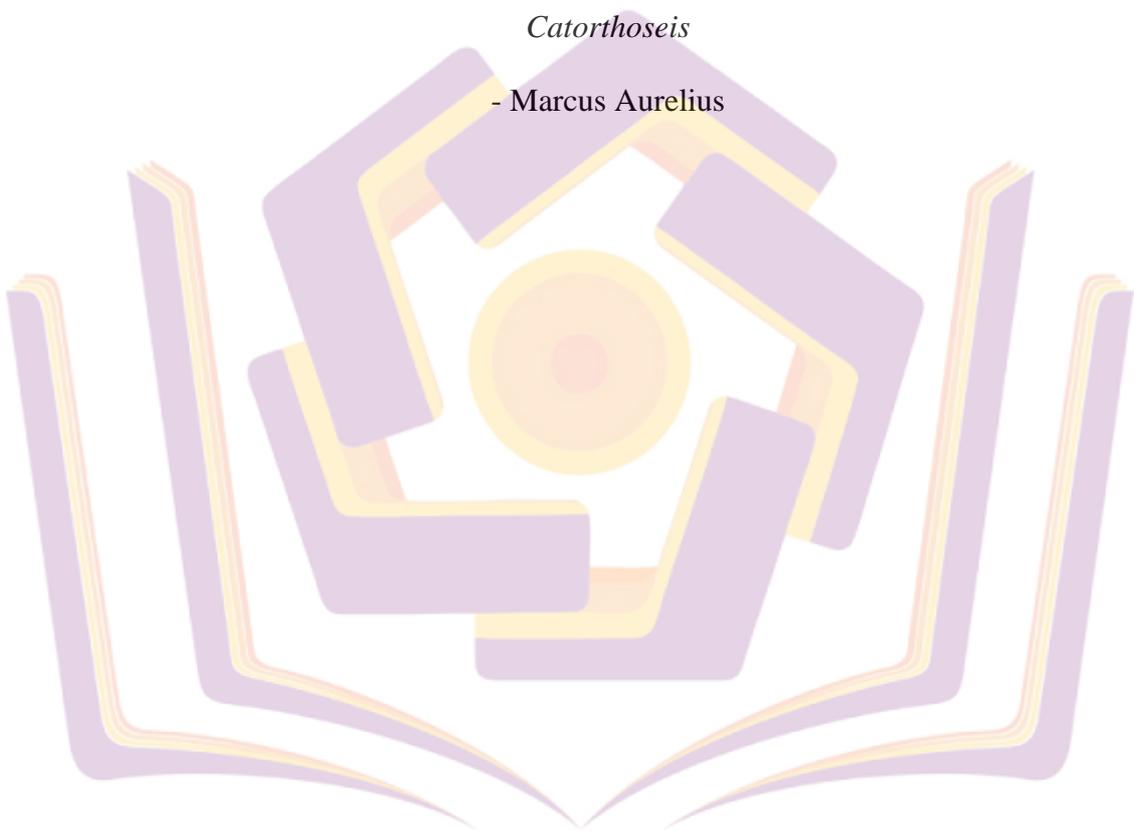
HALAMAN MOTTO

Jangan menjelaskan tentang dirimu kepada siapapun. Karena yang menyukaimu tidak membutuhkan itu, dan yang membencimu tidak mempercayai itu.

– Ali bin Abi Thalib

Catorthoseis

- Marcus Aurelius



KATA PENGANTAR

Puji syukur penulis ucapkan kepada Allah SWT, yang telah memberikan kesehatan dan karunia-Nya kepada penulis serta kekuatan untuk menyelesaikan skripsi yang berjudul Implementasi Keamanan Menggunakan Kriptografi *Post-Quantum* Kyber768 Pada Protokol *Transport Layer Security*. Tidak lupa penulis mengucapkan shalawat dan salam kepada junjungan Nabi Besar Muhammad SAW. Penyelesaian skripsi ini tidak terlepas dari bantuan berbagai pihak baik yang terkait secara langsung atau yang tidak langsung. Penulis menyadari bahwa dalam proses penyusunan skripsi ini melibatkan banyak pihak. Oleh sebab itu dalam kesempatan ini, penulis ingin mengucapkan banyak terima kasih kepada:

1. Dr. Berlilana, M.Kom., M.Si., selaku Rektor Universitas Amikom Purwokerto.
2. Dr. Eng., Ir. Imam Tahyudin, M.M., selaku Dekan Fakultas Ilmu Komputer.
3. Dr. Rujianto Eko Saputro, M.Kom., selaku Kepala Program Studi Teknologi Informasi.
4. Didit Suhartono, M.Kom., selaku dosen pembimbing I dan Khairunnisak Nur Isnaini, M.Kom., selaku dosen pembimbing II yang telah memberikan arahan, ilmu dan saran selama proses pembuatan skripsi ini hingga akhirnya bisa terselesaikan.
5. Chyntia Raras Ajeng Widiawati, S.Kom., M.Eng., selaku dosen pembimbing akademik yang selalu memberikan ilmu dan pengarahan selama kuliah di

Universitas Amikom Purwokerto.

6. Dan seluruh pihak yang turut membantu penyusunan skripsi ini yang tidak dapat disebutkan satu persatu.

Dalam pembuatan skripsi ini dilakukan dengan segala usaha semaksimal mungkin.

Namun tentunya masih ada banyak kekurangan dan keterbatasan dalam skripsi ini.

Oleh karena itu, diharapkan segala saran dan kritik untuk membangun kesempurnaan tulisan ini.

Purwokerto, 15 Januari 2025

Penulis

