IMPLEMENTASI ALGORITMA *DIFFIE-HELLMAN KEY EXCHANGE* (DHE) DAN AES DALAM ENKRIPSI PESAN *END-TO-END*

SKRIPSI

Oleh

M. Khairi Nasution

71220915064

PROGRAM STUDI TEKNIK INFORMATIKA

FAKULTAS TEKNIK

UNIVERSITAS ISLAM SUMATERA UTARA

MEDAN

2025

KATA PENGANTAR

Assalamu'alaikum Warahmatullahi Wabarakatuh

Alhamdulillah, segala puji dan syukur penulis ucapkan kepada Allah Subhanahu wa ta"ala, yang telah memberikan Rahmat dan Karunia-Nya kepada penulis sehingga dapat menyelesaikan penyusunan Skripsi ini dengan judul **"Implementasi Algoritma *Diffie-Hellman Key Exchange* (DHE) Dan AES Dalam Enkripsi Pesan *End-to-end*".** Tidak lupa Shalawat beserta salam penulis ucapkan kepada Nabi Muhammad Shallallahu „alaihi wa sallam yang telah membawa kita dari alam kebodohan ke alam yang penuh dengan ilmu pengetahuan seperti saat sekarang ini.

Dalam penyelesaian Skripsi penulisan ini, penulis banyak mendapatkan bimbingan dan bantuan dari pihak lain berupa materi, spiritual, dan informasi secara langsung maupun tidak langsung. Pada kesempatan ini penulis mengucapkan terima kasih yang sebesar-besarnya kepada :

1. Ibu Dr. Safrida, S.E, M.Si selaku Rektor Universitas Islam Sumatera Utara.
2. Ibu Ir. Darlina Tanjung, MT selaku Dekan FakultasTeknik Universitas Islam Sumatera Utara.
3. Bapak Muhammad Zulfansyuri Siambaton, S.T, M.Kom, selaku Ketua Program Studi Fakultas Teknik Informatika Universitas Islam Sumatera Utara.
4. Bapak Rahmat Aulia, S.T, M.Scom.IT, selaku dosen pembimbing I yang sudah bersedia membantu penulis dalam menyelesaikan skripsi.

5. Bapak Antoni, S.Kom, M.Kom, selaku dosen pembimbing II yang sudah bersedia membantu penulis dalam menyelesaikan skripsi.
6. Seluruh Dosen dan Staff pengajar Program Studi Teknik Informatika Universitas Islam Sumatera Utara yang telah banyak memberikan ilmu pengetahuannya kepada penulis.
7. Semua pihak yang tidak dapat disebutkan satu persatu.

Penulis menyadari bahwa penulisan skripsi ini masih jauh dari sempurna, untuk itu penulis mohon saran dan kritikan pembaca agar kedepannya bisa lebih baik lagi dan semoga tulisan ini bermanfaat bagi kita semua.

Medan, 2025

Penulis,

M. Khairi Nasution
NPM : 71220915064

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR PUSTAKA

Adyan, A. Q., Susilo, B., & Andreswari, D. (2020). Sistem Pendukung Keputusan Penempatan Praktik Kerja Lapangan Berdasarkan Nilai Kompetensi Dasar Dan Nilai Sikap Siswa Menggunakan Metode Pembobotan Rank Order Centroid Dan Metode Profile Matching. Jurnal Rekursif, 8(1), 11–22.

Azhari, M., Mulyana, D. I., Perwitosari, F. J., & Ali, F. (2022). Implementasi Pengamanan Data pada Dokumen Menggunakan Algoritma Kriptografi Advanced Encryption Standard (AES). Jurnal Pendidikan Sains Dan Komputer, 2(1), 163–171. https://doi.org/10.47709/jpsk.v2i01.1390

Aziz, Nur. (2022). ANALISIS PERANCANGAN SISTEM INFORMASI. Edited by Wahyuni, Neneng S. Widina Media Utama. 1st ed. ed. Neneng Sri Wahuni. Bandung: Widina Bhakti Bandung.

Cristy, N., & Riandari, F. (2021). Implementasi Metode Advanced Encryption Standard (AES 128 Bit) untuk Mengamankan Data Keuangan. JIKOMSI (Jurnal Ilmu Komputer Dan Sistem Informasi), 4(2), 75–85. https://ejournal.sisfokomtek.org/index.php/jikom/article/view/181%0A

Gunawan, H., Budi, A. S., & Primananda, R. (2022). Penerapan Algoritma Diffie-Hellman Key Exchange dalam Komunikasi Data Antarnode pada Wireless Sensor Network. Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer (J-PTIIK), 6(1), 197–203. Fakultas Ilmu Komputer, Universitas Brawijaya.

Haji, B. T. A. (2020). Pengertian Implementasi. LAPORAN AKHIR, 31.

Hidayatulloh, N. W., dkk. (2023). Mengenal Advance Encryption Standard (AES) sebagai Algoritma Kriptografi dalam Mengamankan Data. Digital Transformation Technology (Digitech), 3(1), 1–10.

Kadir. 2021 . "Algoritma: Journal Of Mathematcs". Fakultas Ilmu Pendidikan UIN Syarif Hidayatullah Jakarta. Vol. III.

Lie, I. R., & Alamsyah, D. (2023). Penerapan Algoritma Diffie-Hellman pada Steganografi Least Significant Bit. MDP Student Conference 2023, Universitas Multi Data Palembang. E-ISSN: 2985-7406.

Mhatre, S., Khatode, O., Thakre, S., & Karche, S. (2024). Securing Text Files: A Comprehensive Study on AES and Diffie-Hellman Encryption. International Journal for Research in Applied Science & Engineering Technology (IJRASET), 12(6), 2192–2199. https://doi.org/10.22214/ijraset.2024.63457

Rizka, M. (2021). Perpaduan Diffie Hellman dan Blowfish sebagai Sistem Keamanan Dokumen. *Jurnal Infomedia: Teknik Informatika, Multimedia & Jaringan*, 6(2), 86–90.

Sa'diyah, A. Z., Safitri, D., & Sujarwo. (2024). Implementasi pendidikan inklusif di SMP Negeri 259 Jakarta. Sindoro: Cendikia Pendidikan, 4(12), 51–60.

Sinambela, R. G., Fauzi, A., & Khair, H. (2024). Enhancing AES Key Generation Using Diffie-Hellman Method for Image Security. Journal of Artificial Intelligence and Engineering Applications, 3(3), 359–363. https://ioinformatic.org/

Sitepu, D. A., Nurhayati, & Khair, H. (2022). Implementasi Pengamanan Data Koperasi Menggunakan Algoritma Advanced Encryption Standard (AES). Jurnal Ilmiah Kaputama (JIKA), 6(1), 49–58. https://citisee.amikompurwokerto.ac.id/assets/proceedings/paper/8__Amikom_Purwokerto_Implementasi_Pengamanan_Data_Koperasi_Menggunakan_Algoritma_Advanced_Encryption_Standard_(Aes).pdf

Tharisa amalia. (2020). Konsep dasar dalam mempelajari mata kuliah algoritma pemprograman. 1–23.

Ziliwu, K. B., Maslan, A., & Kremer, H. (2022). Implementasi Caesar Cipher pada Algoritma Kriptografi dalam Penyandian Pesan Whatsapp. Jurnal Comasie, 7(2), 117–125.