

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 Fakultas Teknik 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

	Halaman
ABSTRAK	ii
KATA PENGANTAR	iv
DAFTAR ISI	vi
DAFTAR TABEL	viii
DAFTAR GAMBAR	xiv
BAB I PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah	6
1.3 Batasan Masalah	7
1.4 Tujuan Penelitian	7
1.5 Manfaat Penelitian	8
1.6 Sistematika Penulisan	8
BAB II TINJAUAN PUSTAKA	7
2.1 Kriptografi	7
2.7.1 Pengertian Kriptografi	7
2.7.2 Tujuan Kriptografi	8
2.7.3 Elemen Sistem Kriptografi	8
2.7.4 Enkripsi dan Dekripsi	9
2.2 <i>Diffie-Hellman Key Exchange</i> (DHE)	9
2.3 <i>Advance Encryption Standard</i> (AES)	12
2.4 <i>Pesan End-To-End</i>	13
2.5 <i>Flowchart</i>	16
BAB III METODOLOGI PENELITIAN	19
3.1 Alat dan Bahan yang digunakan	19
3.2 Teknik Pengumpulan Data	19
3.3 <i>Flowchart</i> Algoritma <i>Diffie-Hellman Key Exchange</i> (DHE)	20
3.4 <i>Flowchart</i> Enkripsi Algoritma <i>Advanced Encryption Standard</i> (AES)	22

3.5 <i>Flowchart</i> Dekripsi Algoritma <i>Advanced Encryption Standard</i> (AES)	24
3.6 Penerapan Algoritma DHE dan AES	25
3.6.1 Contoh Penerapan Algoritma DHE	25
3.6.2 Penerapan Algoritma AES	27
3.6.3 Studi Kasus Penerapan Algoritma DHE dan AES	27
3.7 Perancangan Sistem	65
3.7.1 <i>Flowchart</i> Sistem	65
3.8 Perancangan Tabel	67
3.9 Perancangan Antarmuka	67
BAB IV HASIL DAN PEMBAHASAN	71
4.1 Hasil Penelitian	71
4.2 Implementasi Aplikasi	72
BAB V KESIMPULAN DAN SARAN	77
5.1 Kesimpulan	77
5.2 Saran	77
DAFTAR PUSTAKA	79

DAFTAR TABEL

Tabel 2.1 Tabel Bentuk dan Simbol <i>Flowchart</i>	20
Tabel 3.1 Tabel Plainteks	31
Tabel 3.2 Tabel Plainteks Hexadesimal	31
Tabel 3.3 Tabel Chiper Key	31
Tabel 3.4 Tabel Hasil P XOR K	32
Tabel 3.5 Tabel Kunci Round 1	33
Tabel 3.6 Tabel Kunci Round 2	33
Tabel 3.7 Tabel Kunci Round 3	33
Tabel 3.8 Tabel Kunci Round 4	33
Tabel 3.9 Tabel Kunci Round 5	33
Tabel 3.10 Tabel Kunci Round 6	33
Tabel 3.11 Tabel Kunci Round 7	34
Tabel 3.12 Tabel Kunci Round 8	34
Tabel 3.13 Tabel Kunci Round 9	34
Tabel 3.14 Tabel Kunci Round 10	34
Tabel 3.15 tabel S-Box	34
Tabel 3.16 Tabel Hasil Subbye Round 0	35
Tabel 3.17 Tabel Hasil Shift Row Round 0	35

Tabel 3.18 Tabel Matriks AES	35
Tabel 3.19 Tabel Hasil Matriks	35
Tabel 3.20 Tabel Hasil Add Roun Key Round 0	36
Tabel 3.21 Tabel Hasil Subbye Round 1	36
Tabel 3.22 Tabel Hasil Shift Row Round 1	37
Tabel 3.23 Tabel Hasil Matriks Round 1	37
Tabel 3.24 Tabel Hasil Add Round Key Round 1	38
Tabel 3.25 Tabel Hasil Subbye Round 2	38
Tabel 3.26 Tabel Hasil Shift Row Round 2	38
Tabel 3.27 Tabel Hasil Matriks Round 2	38
Tabel 3.28 Tabel Hasil Add Roun Key Round 2	39
Tabel 3.29 Tabel Hasil Subbye Round 3	39
Tabel 3.30 Tabel Hasil Shift Row Round 3	40
Tabel 3.31 Tabel Hasil Matriks Round 3	40
Tabel 3.32 Tabel Hasil Subbye Round 4	41
Tabel 3.33 Tabel Hasil Shift Row Round 4	41
Tabel 3.34 Tabel Hasil Matriks Round 4	41
Tabel 3.35 Tabel Hasil Add Roun Key Round 4	42
Tabel 3.36 Tabel Hasil Subbye Round 5	42

Tabel 3.37 Tabel Hasil Shift Row Round 4	43
Tabel 3.38 Tabel Hasil Matriks Round 5	43
Tabel 3.39 Tabel Hasil Add Roun Key Round 5	44
Tabel 3.40 Tabel Hasil Subbye Round 6	44
Tabel 3.41 Tabel Hasil Shift Row Round 6	44
Tabel 3.42 Tabel Hasil Matriks Round 6	44
Tabel 3.43 Tabel Hasil Add Roun Key Round 6	45
Tabel 3.43 Tabel Hasil Subbye Round 7	45
Tabel 3.44 Tabel Hasil Shift Row Round 7	46
Tabel 3.45 Tabel Hasil Matriks Round 7	46
Tabel 3.46 Tabel Hasil Add Roun Key Round 6	47
Tabel 3.47 Tabel Hasil Subbye Round 8	47
Tabel 3.48 Tabel Hasil Shift Row Round 8	47
Tabel 3.49 Tabel Hasil Matriks Round 8	47
Tabel 3.50 Tabel Hasil Add Roun Key Round 8	48
Tabel 3.51 Tabel Hasil Subbye Round 9	48
Tabel 3.52 Tabel Hasil Shift Row Round 9	49
Tabel 3.53 Tabel Hasil Matriks Round 9	49
Tabel 3.54 Tabel Hasil Add Roun Key Round 8	50

Tabel 3.55 Tabel Hasil Subbyte Round 10	50
Tabel 3.56 Tabel Hasil Shift Row Round 10	50
Tabel 3.57 Tabel Hasil Add Round Key Round 10	51
Tabel 3.58 Tabel Hasil Round 0	51
Tabel 3.59 Tabel Hasil Invers Shift row Round 1	52
Tabel 3.60 Tabel Invers S-Box	52
Tabel 3.61 Hasil Dari Invers Subbyte Round 1	52
Tabel 3.62 Hasil Invers Add Round Key Round 1	53
Tabel 3.63 Tabel Invers Column	53
Tabel 3.64 Tabel Hasil Invers Mix Column Round 1	53
Tabel 3.65 Tabel Hasil Invers Shift row Round 2	54
Tabel 3.66 Hasil Dari Invers Subbyte Round 2	54
Tabel 3.67 Hasil Invers Add Round Key Round 2	54
Tabel 3.68 Tabel Hasil Invers Mix Column Round 2	54
Tabel 3.69 Tabel Hasil Invers Shift row Round 3	55
Tabel 3.70 Hasil Dari Invers Subbyte Round 3	55
Tabel 3.71 Hasil Invers Add Round Key Round 3	56
Tabel 3.72 Tabel Hasil Invers Mix Column Round 3	56
Tabel 3.73 Tabel Hasil Invers Shift row Round 4	56

Tabel 3.74 Hasil Dari Invers Subbyte Round 4	57
Tabel 3.75 Hasil Invers Add Round Key Round 4	57
Tabel 3.76 Tabel Hasil Invers Mix Column Round 4	57
Tabel 3.77 Tabel Hasil Invers Shift row Round 5	58
Tabel 3.78 Hasil Dari Invers Subbyte Round 5	58
Tabel 3.79 Hasil Invers Add Round Key Round 5	58
Tabel 3.80 Tabel Hasil Invers Mix Column Round 5	58
Tabel 3.81 Tabel Hasil Invers Shift row Round 6	59
Tabel 3.82 Hasil Dari Invers Subbyte Round 6	59
Tabel 3.83 Hasil Invers Add Round Key Round 6	60
Tabel 3.84 Tabel Hasil Invers Mix Column Round 6	60
Tabel 3.85 Tabel Hasil Invers Shift row Round 7	60
Tabel 3.86 Hasil Dari Invers Subbyte Round 7	61
Tabel 3.87 Hasil Invers Add Round Key Round 7	61
Tabel 3.88 Tabel Hasil Invers Mix Column Round 7	61
Tabel 3.89 Tabel Hasil Invers Shift row Round 8	62
Tabel 3.90 Hasil Dari Invers Subbyte Round 8	62
Tabel 3.91 Hasil Invers Add Round Key Round 8	62
Tabel 3.92 Tabel Hasil Invers Mix Column Round 8	62

Tabel 3.93 Tabel Hasil Invers Shift row Round 8	63
Tabel 3.94 Hasil Dari Invers Subbyte Round 8	63
Tabel 3.95 Hasil Invers Add Round Key Round 8	64
Tabel 3.96 Tabel Hasil Invers Mix Column Round 8	64
Tabel 3.97 Tabel Hasil Invers Shift row Round 9	64
Tabel 3.98 Hasil Dari Invers Subbyte Round 9	65
Tabel 3.99 Hasil Invers Add Round Key Round 9	65
Tabel 3.100 Tabel Hasil Invers Mix Column Round 9	65
Tabel 3.101 Tabel Hasil Invers Shift row Round 10	66
Tabel 3.102 Hasil Dari Invers Subbyte Round 10	66
Tabel 3.103 Hasil Invers Add Round Key Round 10	66
Tabel 3.104 Tabel Hasil Plaintext Akhir	66
Tabel 3.105 Perancangan Tabel <i>User</i>	70
Tabel 3.106 Perancangan Tabel Hasil Pesan	70
Tabel 4.1 Tabel Hasil Pesan	76

DAFTAR GAMBAR

Gambar 2.1 Ilustrasi Kriptografi	7
Gambar 2.2 Konsep Dasar Enkripsi End-To-End	16
Gambar 3.1 Flowchart Algoritma Diffie-Hellman Key Exchange (DHE)	20
Gambar 3.2 Flowchart Enkripsi Algoritma Advanced Encryption Standard (AES)	22
Gambar 3.3 Flowchart Dekripsi Algoritma Advanced Encryption Standard (AES)	24
Gambar 3.4 Gambar Rcon	31
Gambar 3.5 Flowchart Sistem	65
Gambar 3.6 Perancangan Antarmuka Halaman Login Pengguna	70
Gambar 3.7 Perancangan Antarmuka Halaman Registrasi	71
Gambar 3.8 Perancangan Antarmuka Halaman Fitur Chat	71
Gambar 4.1 Tampilan Halaman Login	72
Gambar 4.2 Tampilan Halaman Login Gagal	72
Gambar 4.3 Tampilan Halaman Registrasi	73
Gambar 4.4 Tampilan Halaman Registrasi Gagal	74
Gambar 4.5 Tampilan Halaman Chat	75

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-PTIHK)*, 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](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 pemrograman. 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.