

DAFTAR PUSTAKA

- Agus, I., Destiawati, F., & Dhika, H. (2019). Perbandingan Cloud Computing Microsoft Onedrive, Dropbox, dan Google Drive. *Faktor Exacta*, 12(1). <https://doi.org/10.30998/faktorexacta.v12i1.3631>
- Ahmad Halimi, Abu Tholib, & Moh. Ainol Yaqin. (2024). OPTIMASI KEAMANAN DATA PENERIMAAN MAHASISWA MENGGUNAKAN AES-256, SHA-256, DAN BASE64. *JUSTIFY: Jurnal Sistem Informasi Ibrahimy*, 3(1), 38–45. <https://doi.org/10.35316/justify.v3i1.5107>
- Amin, M. M. (2017). IMPLEMENTASI KRIPTOGRAFI KLASIK PADA KOMUNIKASI BERBASIS TEKS. *Pseudocode*, 3(2). <https://doi.org/10.33369/pseudocode.3.2.129-136>
- Ariesta, A., Dewi, Y. N., Sariasih, F. A., & Fibriany, F. W. (2021). PENERAPAN METODE AGILE DALAM PENGEMBANGAN APPLICATION PROGRAMMING INTERFACE SYSTEM PADA PT XYZ. *Jurnal CoreIT: Jurnal Hasil Penelitian Ilmu Komputer Dan Teknologi Informasi*, 7(1). <https://doi.org/10.24014/coreit.v7i1.12635>
- Arradian, D. (2024, May 6). 61 Juta Serangan Bruteforce Terjadi di Indonesia selama 2023, Kedua Tertinggi di Asia Tenggara. https://Tekno.Sindonews.Com/Read/1371729/207/61-Juta-Serangan-Bruteforce-Terjadi-Di-Indonesia-Selama-2023-Kedua-Tertinggi-Di-Asia-Tenggara-1714961102#goog_rewarded. https://tekno.sindonews.com/read/1371729/207/61-juta-serangan-bruteforce-terjadi-di-indonesia-selama-2023-kedua-tertinggi-di-asia-tenggara-1714961102#goog_rewarded
- Bagus, I. A. D., Sukarsa, I. M., & Buana, W. P. (2022). Pemanfaatan Dropbox Cloud Storage dan Dropbox API Sebagai Media Penyimpanan dan Pertukaran Data pada Sistem Informasi Berbasis Web. *JITTER-Jurnal Ilmiah Teknologi Dan Komputer*, 3(1).
- Berisha, B., Mëziu, E., & Shabani, I. (2022). Big data analytics in Cloud computing: an overview. *Journal of Cloud Computing*, 11(1). <https://doi.org/10.1186/s13677-022-00301-w>
- Calvin Christian, Sampe Hotlan Sitorus, & Irma Nirmala. (2023). IMPLEMENTASI ALGORITMA RSA DAN ONE TIME PASSWORD (OTP) UNTUK PENGAMANAN DATA PENGGUNA DAN PROSES TRANSAKSI PADA WEBSITE E-COMMERCE. *Coding : Jurnal Komputer Dan Aplikasi*, 11, 62–72.
- Fachry, M., Kusyanti, A., & Amron, K. (2018). Pengamanan Data pada Media Penyimpanan Cloud Menggunakan Teknik Enkripsi dan Secret Sharing.

- Jurnal Pengembangan Teknologi Informasi Dan Ilmu Komputer*, 2(11), 4863–4869. <http://j-ptiik.ub.ac.id>
- Fatimatuazzahro'. (2021). Penerapan Kriptografi Hibrida menggunakan Algoritma Hill Cipher dan Rivest Shamir Adleman (RSA) Pada Pengamanan pesan Teks. *Universitas Islam Negeri Maulana Malik Ibrahim Malang*.
- Gaffney, K. P., Hipp, D. R., Prammer, M., Kennedy, D., Brasfield, L., & Patel, J. M. (2022). SQLite: Past, Present, and Future. *Proceedings of the VLDB Endowment*, 15(12). <https://doi.org/10.14778/3554821.3554842>
- Gamnis, S., VanderLinden, M., & Mailewa, A. (2022). Analyzing Data Encryption Efficiencies for Secure Cloud Storages: A Case Study of Pcloud vs OneDrive vs Dropbox. *Advances in Technology*, 2(1). <https://doi.org/10.31357/ait.v2i1.5526>
- Georgi, P., Wei, Q., Sain, B., Schlickriede, C., Wang, Y., Huang, L., & Zentgraf, T. (2021). Optical secret sharing with cascaded metasurface holography. *Science Advances*, 7(16). <https://doi.org/10.1126/sciadv.abf9718>
- Hariharan, N. K. (2021). Financial Data Security in Cloud Computing. *International Journal of Engineering, Science and Mathematics*, 10(1).
- Herdianto, L. B. (2023). Evaluasi Sistem E-Learning PT Otak Kanan Melalui Pengujian Blackbox Testing dan System Usability Scale (SUS). *Jurnal Informatika Dan Teknik Elektro Terapan (JITET)*, 11(3).
- Hts, D. I. G., Aldizar, M. R., Nasution, I. F., & Nasution, M. F. (2023). Perbandingan Algoritma Kriptografi Simetris dan Asimetris. *UNES Journal of Information System*, 8(1).
- Ivanov, F., Kreschuk, A., & Krouk, E. (2020). On the secret sharing scheme based on supercodes decoding. *IFAC-PapersOnLine*, 53(2). <https://doi.org/10.1016/j.ifacol.2020.12.260>
- John Swatrahadi, Permana, Hendrana, & Rinaldi Munir. (2024). MENGAMANKAN FILE RAHASIA MENGGUNAKAN HYBRID KRIPTOGRAFI. *Jurnal Review Pendidikan Dan Pengajaran*, 7.
- Nanda, N. A., Silalahi, S. M. S., Patricia Nasution, D., Sari, M., & Gunawan, I. (2023). Kriptografi dan Penerapannya Dalam Sistem Keamanan Data. *Jurnal Media Informatika*, 4(2). <https://doi.org/10.55338/jumin.v4i2.428>
- Novianty, D. (2021, November 16). Waduh! Serangan Brute Force di Indonesia Paruh Pertama 2021 Naik 2 Digit. <https://www.suara.com/tekno/2021/11/16/160100/Waduh-Serangan-Brute-Force-Di-Indonesia-Paruh-Pertama-2021-Naik-2-Digit>. <https://www.suara.com/tekno/2021/11/16/160100/waduh-serangan-brute-force-di-indonesia-paruh-pertama-2021-naik-2-digit>

- Oktaviani, S., Rizky, F., & Gunawan, I. (2023). Analisis Keamanan Data Dengan Menggunakan Kriptografi Modern Algoritma Advance Encryption Standar (AES). *Jurnal Media Informatika*, 4(2). <https://doi.org/10.55338/jumin.v4i2.435>
- Putri, G. G., Setyorini, W., & Rahayani, R. D. (2018). Analisis Kriptografi Simetris AES dan Kriptografi Asimetris RSA pada Enkripsi Citra Digital. *ETHOS (Jurnal Penelitian Dan Pengabdian)*, 6(2). <https://doi.org/10.29313/ethos.v6i2.2909>
- Putri, W. C. U., Marwati, R., & Gozali, S. M. (2023). PENGABUNGAN KRIPTOGRAFI RIVEST SHAMIR ADLEMAN (RSA) DAN ADVANCED ENCRYPTION STANDARD (AES) PADA APLIKASI PENGIRIM E-MAIL. *INTERVAL: Jurnal Ilmiah Matematika*, 3(2), 92–101.
- Ramalinda, D., Jayadi, & Raharja, A. R. (2024). Strategi Perlindungan Data Menggunakan Sistem Kriptografi Dalam Keamanan Informasi. *Journal of International Multidisciplinary Research*, 2, 665–671. <https://journal.banjaresepacific.com/index.php/jimr>
- Rismanto. (2017, January). *Makna/Kegunaan Kode ASCII Beserta Tabel*. <https://Blogger-Programer.Blogspot.Com/2017/01/MaknaKegunaan-Kode-Ascii-Beserta-Tabel.Html>.
- Safitri, K., & Nasution, I. P. (2023). Analisis Penggunaan Aplikasi Google Drive Sebagai Media Penyimpanan Data. *Jurnal Sains Dan Teknologi (JSIT)*, 3(3). <https://doi.org/10.47233/jsit.v3i2.891>
- Sebastian, N. (2024, August 16). *Usage & Trends of Personal Cloud Storage: GoodFirms Research*. <https://Www.Goodfirms.Co/Resources/Personal-Cloud-Storage-Trends>.
- Selimis, G. N., Kakarountas, A. P., Fournaris, A. P., Milidonis, A., & Koufopavlou, O. (2007). A Low Power Design for Sbox Cryptographic Primitive of Advanced Encryption Standard for Mobile End-Users. *Journal of Low Power Electronics*, 3(3). <https://doi.org/10.1166/jolpe.2007.139>
- Siska Narulita, Ahmad Nugroho, & M. Zakki Abdillah. (2024). Diagram Unified Modelling Language (UML) untuk Perancangan Sistem Informasi Manajemen Penelitian dan Pengabdian Masyarakat (SIMLITABMAS). *Bridge : Jurnal Publikasi Sistem Informasi Dan Telekomunikasi*, 2(3), 244–256. <https://doi.org/10.62951/bridge.v2i3.174>
- Sofian, N., Wicaksana, A., & Hansun, S. (2019). LSB steganography and AES encryption for multiple PDF documents. *Proceedings of 2019 5th International Conference on New Media Studies, CONMEDIA 2019*. <https://doi.org/10.1109/CONMEDIA46929.2019.8981842>

- Srivastava, A. K. (2022). Django , The Python Web Framework. *INTERANTIONAL JOURNAL OF SCIENTIFIC RESEARCH IN ENGINEERING AND MANAGEMENT*, 06(05). <https://doi.org/10.55041/ijrsrem13183>
- Swinhoe, D. (2020, June 23). *Brute-force attacks explained, and why they are on the rise*. <https://Www.Csoonline.Com/Article/569513/Brute-Force-Attacks-Explained-and-Why-They-Are-on-the-Rise.Html>.
<https://www.csoonline.com/article/569513/brute-force-attacks-explained-and-why-they-are-on-the-rise.html>
- Tantowi, L., & Wijayanti, L. (2023). PELUANG DAN TANTANGAN PENYIMPANAN CLOUD STORAGE PADA DOKUMEN DIGITAL. *Shaut Al-Maktabah: Jurnal Perpustakaan, Arsip Dan Dokumentasi*, 15(1). <https://doi.org/10.37108/shaut.v15i1.803>
- Thabit, F., Can, O., Alhomdy, S., Al-Gaphari, G. H., & Jagtap, S. (2022). A Novel Effective Lightweight Homomorphic Cryptographic Algorithm for data security in cloud computing. *International Journal of Intelligent Networks*, 3. <https://doi.org/10.1016/j.ijin.2022.04.001>
- Thales. (2023, July 5). *Cloud assets the biggest targets for cyberattacks, as data breaches increase*. <https://Cpl.Thalesgroup.Com/about-Us/Newsroom/2023-Cloud-Security-Cyberattacks-Data-Breaches-Press-Release>.
- Tulim, A., & Helman, H. (2022). Keuntungan dan Kerugian Pemanfaatan Aplikasi Dropbox dalam Sinkronisasi Data. *All Fields of Science Journal Liaison Academia and Society*, 2(4). <https://doi.org/10.58939/afosj-las.v2i4.469>
- Turrahmi K, A., Askar, A., & Mashud, M. (2023). SISTEM INFORMASI BADAN USAHA MILIK DESA (BUMDES) BINA MANDIRI DESA MINASA BAJI KECAMATAN BANTIMURUNG KABUPATEN MAROS. *Jurnal Publikasi Manajemen Informatika*, 3(1). <https://doi.org/10.55606/jupumi.v3i1.700>
- Yang, P., Xiong, N., & Ren, J. (2020). Data Security and Privacy Protection for Cloud Storage: A Survey. In *IEEE Access* (Vol. 8). <https://doi.org/10.1109/ACCESS.2020.3009876>

LAMPIRAN

Lampiran 1 Source code

<https://github.com/AzzahraBeladinaShaff/Code-Skripsi-Kripto>



Lampiran 2 Data yang digunakan

<https://drive.google.com/drive/folders/1Ur5SUNTW1DFM5chGwsH1CXtGePUG5UvX>

Lampiran 3 *Source code* pengujian hasil dekripsi menggunakan SHA-256

```
import hashlib

# Fungsi untuk menghitung hash tanpa chunk pertama dan mencetak hash
setiap chunk
def calculate_hash_with_chunks(file_path, chunk_size=4096):
    sha256_hash = hashlib.sha256()
    chunks = []
    with open(file_path, "rb") as f:

        f.read(chunk_size)

        i = 1
        while chunk := f.read(chunk_size):
            sha256_hash.update(chunk)
            chunk_hash = hashlib.sha256(chunk).hexdigest() # Hash
setiap chunk
            chunks.append(chunk_hash)
            print(f"Chunk {i}: {chunk_hash}")
            i += 1
        return sha256_hash.hexdigest(), chunks

# Fungsi untuk menghitung persentase kesamaan
def calculate_similarity(original_file, decrypted_file,
chunk_size=4096):
    _, chunks_original = calculate_hash_with_chunks(original_file,
chunk_size)
    _, chunks_decrypted = calculate_hash_with_chunks(decrypted_file,
chunk_size)

    # Bandingkan chunk b
    matching_chunks = sum(1 for i in range(len(chunks_original)) if
chunks_original[i] == chunks_decrypted[i])
    total_chunks = len(chunks_original)

    # Hitung persentase chunk yang cocok
    return (matching_chunks / total_chunks) * 100 if total_chunks > 0
else 0

# Ganti dengan path file asli dan file hasil dekripsi
original_file = "anggaran.docx"
decrypted_file = "reconstructed_file.docx"

# Hitung hash dan tampilkan hasil per chunk
print("Original file:")
view_hash_original, _ = calculate_hash_with_chunks(original_file)

print("\nDecrypted file:")
```

```
view_hash_decrypted, _ = calculate_hash_with_chunks(decrypted_file)

# Tampilkan hash keseluruhan
print(f"\nHash Original: {view_hash_original}")
print(f"Hash Decrypted: {view_hash_decrypted}")

# Hitung persentase kesamaan
similarity = calculate_similarity(original_file, decrypted_file)
print(f"\nSimilarity Percentage : {similarity:.2f}%")
```

Lampiran 4 Hasil pengujian hash

KECIL 1

PROBLEMS	OUTPUT	TERMINAL	PORTS	GITLENS	DEVGR	COMMENTS
PS F:\Django\zahrakrip-base> py test_decryption.py						
Original File:						
Chunk 1:	78a5f383a6ff65d2e94a4c4823af75cfdc8154f5243448c73438255797684c9c					
Chunk 2:	5f27bec1ac3468ab5a6b6c3bc33f3d378d1a0f99136293c889580bf3f6					
Chunk 3:	d239f4c1e6de93965026371f3c624da672c53c53307a283be1bde9ec					
Chunk 4:	96e5cc35f3ac3ad4b1a10e2e0d96719a55e154bf7a3766a09c7642d-fb35d					
Decrypted File:						
Chunk 1:	78a5f383a6ff65d2e94a4c4823af75cfdc8154f5243448c73438255797684c9c					
Chunk 2:	5f27bec1ac3468ab5a6b6c3bc33f3d378d1a0f99136293c889580bf3f6					
Chunk 3:	d239f4c1e6de93965026371f3c624da672c53c53307a283be1bde9ec					
Chunk 4:	96e5cc35f3ac3ad4b1a10e2e0d96719a55e154bf7a3766a09c7642d-fb35d					
Hash Original:	f4b545c2dd4968fe44f6f8d3249ab11ecfc628c5ed7af96997f71gab25f5ea6					
Hash Decrypted:	f4b545c2dd4968fe44f6f8d3249ab11ecfc628c5ed7af96997f71gab25f5ea6					
Similarity Percentage : 100.00%						

KECIL 2

PROBLEMS	OUTPUT	TERMINAL	PORTS	GITLENS	DEVGR	COMMENTS
PS F:\Django\zahrakrip-base> py test_decryption.py						
Original File:						
Chunk 1:	33daef55148e23ff34818647c89635ff4fad88735e5e052459936661189737b					
Chunk 2:	4947ab8afeebdcfa26c95fad72c33144f213f08b9f2ea406dc559da5d1b07					
Chunk 3:	355dd5de0e1b63b8a4c46f1c71e7017169fd9c3231f08b7222c2baec50fd8a3					
Chunk 4:	aa661e28efdc6f6c18ae992df6a4088b04367e8dd166d7cc33ceab188308082					
Chunk 5:	e5d93654af7a5c99a6272ff61c089262b27b9bc334b6c1dfc5cc644e1e457832					
Chunk 6:	ce1a1cdcc30f9c07c273bb7280b0fd7d195333941fe618be2b5fb7154faa8					
Chunk 7:	385e067ba699a1eedfed81568a7b2cecc6aba399f8c2de39854a8fa5fdec39ea					
Decrypted File:						
Chunk 1:	33daef55148e23ff34818647c89635ff4fad88735e5e052459936661189737b					
Chunk 2:	4947ab8afeebdcfa26c95fad72c33144f213f08b9f2ea406dc559da5d1b07					
Chunk 3:	355dd5de0e1b63b8a4c46f1c71e7017169fd9c3231f08b7222c2baec50fd8a3					
Chunk 4:	aa661e28efdc6f6c18ae992df6a4088b04367e8dd166d7cc33ceab188308082					
Chunk 5:	e5d93654af7a5c99a6272ff61c089262b27b9bc334b6c1dfc5cc644e1e457832					
Chunk 6:	ce1a1cdcc30f9c07c273bb7280b0fd7d195333941fe618be2b5fb7154faa8					
Chunk 7:	385e067ba699a1eedfed81568a7b2cecc6aba399f8c2de39854a8fa5fdec39ea					
Hash Original: 513b2b7b25a2c2f9dce288dcad2098665c5535c460bf8267872dd7b6348e						
Hash Decrypted: 513b2b7b25a2c2f9dce288dcad2098665c5535c460bf8267872dd7b6348e						
Similarity Percentage : 100.00%						

KECIL 3

PROBLEMS	OUTPUT	TERMINAL	PORTS	GITLENS	DEVGR	COMMENTS
py test_decryption.py						
Original File:						
Chunk 1:	0fa089d78140c39e9b3994852a9ae9a702bc86d239c54b136835850ba492e					
Chunk 2:	0f3e1fd8da4e949e93a1a9cb684f6cb07c1f124395959c81205d690ea386					
Chunk 3:	7bdc7f6d516cabe8a8efb1536fc3be3fed4225b672d557410e11b2f17cb478					
Chunk 4:	2aa13772d313e0991eca9fd259fd690bab3912b718a80aa2fdda9a4496f7b					
Chunk 5:	7bf71ec361f25c5e1cebb9c111939620a4d62da279208c51cbf728925b4c6660					
Chunk 6:	8a6d72af8bb50c4e15d65762ab4349b38604b97366387d1d522fefe19350a					
Chunk 7:	6c310850a10272af674b0591c5b532da4185584db7b50b0f6ae5f185590d0					
Chunk 8:	31ea7f6572457f0f7339c45fec0624ccdb8909e54a43fea2ccf8d51df2f10					
Chunk 9:	2ccf4d940ab0f8c8d1923b39462d2c34faee7b72e8568f8b6230f5117759294					
Chunk 10:	4ae768e2a643bd72577d31e7a56be17d73f967beec275147b3cc8538ba8b2					
Chunk 11:	53931806c17805f43904fc466170715434c51386aa244f9c5d8115d8afe					
Chunk 12:	8c659d31b2178ec704d58491f3ce10083a4979420618c72e088dd3b0a0					
Decrypted File:						
Chunk 1:	0fa089d78140c39e9b3994852a9ae9a702bc86d239c54b136835850ba492e					
Chunk 2:	0f3e1fd8da4e949e93a1a9cb684f6cb07c1f124395959c81205d690ea386					
Chunk 3:	7bdc7f6d516cabe8a8efb1536fc3be3fed4225b672d557410e11b2f17cb478					
Chunk 4:	2aa13772d313e0991eca9fd259fd690bab3912b718a80aa2fdda9a4496f7b					
Chunk 5:	7bf71ec361f25c5e1cebb9c111939620a4d62da279208c51cbf728925b4c6660					
Chunk 6:	8a6d72af8bb50c4e15d65762ab4349b38604b97366387d1d522fefe19350a					
Chunk 7:	6c310850a10272af674b0591c5b532da4185584db7b50b0f6ae5f185590d0					
Chunk 8:	31ea7f6572457f0f7339c45fec0624ccdb8909e54a43fea2ccf8d51df2f10					
Chunk 9:	2ccf4d940ab0f8c8d1923b39462d2c34faee7b72e8568f8b6230f5117759294					
Chunk 10:	4ae768e2a643bd72577d31e7a56be17d73f967beec275147b3cc8538ba8b2					
Chunk 11:	53931806c17805f43904fc466170715434c51386aa244f9c5d8115d8afe					
Chunk 12:	8c659d31b2178ec704d58491f3ce10083a4979420618c72e088dd3b0a0					
Hash Original: cca7912829897723c1891f5d0f9cdaeb7902f58c3743bc5c0da2a1e0446c						
Hash Decrypted: cca7912829897723c1891f5d0f9cdaeb7902f58c3743bc5c0da2a1e0446c						
Similarity Percentage : 100.00%						

KECIL 4

PROBLEMS	OUTPUT	TERMINAL	PORTS	GITLENS	DEVGR	COMMENTS
Original File:						
Chunk 1:	9844dc8b13e61f43168aad834df462deb14d8277ddada38cccfcd820256f					
Chunk 2:	72840bd78cab0f066138563a2e44f30d43437c4564cc7a8c283a0b9699730					
Chunk 3:	abc3c6f3c14247544fcdbeae5e332f6e1e585057f62841ac8a2d8b6135					
Chunk 4:	3a747db150b22824e77f8c623c87151e14875104cfd8b47681ed7808f3187					
Chunk 5:	1f8f687b56d27e45d6a49c7f836c6389138d806e3528fbf7345967ad2418e					
Chunk 6:	7c37beca1a08f4e049574920847857ee8a4086c269d2f58e6706abfd9f87					
Chunk 7:	e9323b1c38d17b5dbf618f5b487807b35ee4a4086c269d2f58e6706abfd9f87					
Chunk 8:	bd698ef9aa246d901fd069981d1447f78da0e81301c57d6843b18c4dfdf369					
Chunk 9:	8a73cb74e29f4a62f6e56a40abf9a348b4c29a396a6c4ff3f169406630					
Chunk 10:	f5485f4c1193d884c8c8a70e02b7540af8d1c23b6d9157699759237					
Chunk 11:	71989b43462fc6a23fbc1c380aa84723f6f4c62b3401e57f080f503801b					
Chunk 12:	ace767802f35b5f3eb404c78956ef8ab16f8d279e0f4ee663cc25a7e4f					
Chunk 13:	a7d7f1eddbef2fbc21e4586e055c456a1011cdaf379e55d8f7a76f2b6a43					
Chunk 14:	ddb94d669778733a56ad308bd514fd369776f5e12344c4bb175d1d555075					
Chunk 15:	b9a69a8e56ecaba327f499f4c4e078f8f7e7267680b6c3156fbcd43d2a24					
Chunk 16:	a42170f41a8764ea881ab8a2a1b0bd120c8ba06634c24fcf81df1cca36d518					
Chunk 17:	e6569ef56830c27a8771cbb28b1887b30599c3e950c24f61649688e119794					
Decrypted File:						
Chunk 1:	9844dc8b13e61f43168aad834df462deb14d8277ddada38cccfcd820256f					
Chunk 2:	72840bd78cab0f066138563a2e44f30d43437c4564cc7a8c283a0b9699730					
Chunk 3:	abc3c6f3c14247544fcdbeae5e332f6e1e585057f62841ac8a2d8b6135					
Chunk 4:	3a747db150b22824e77f8c623c87151e14875104cfd8b47681ed7808f3187					
Chunk 5:	1f8f687b56d27e45d6a49c7f836c6389138d806e3528fbf7345967ad2418e					
Chunk 6:	7c37beca1a08f4e049574920847857ee8a4086c269d2f58e6706abfd9f87					
Chunk 7:	e9323b1c38d17b5dbf618f5b487807b35ee4a4086c269d2f58e6706abfd9f87					
Chunk 8:	bd698ef9aa246d901fd069981d1447f78da0e81301c57d6843b18c4dfdf369					
Chunk 9:	8a73cb74e29f4a62f6e56a40abf9a348b4c29a396a6c4ff3f16940630					
Chunk 10:	f5485f4c1193b40884c8c8a70e02b7540af8d1c23b6d9157699759237					
Chunk 11:	71989b43462fc6a23fbc1c380aa84723f6f4c62b3401e57f080f503801b					
Chunk 12:	ace767802f35b5f3eb404c78956ef8ab16f8d279e0f4ee663cc25a7e4f					
Chunk 13:	a7d7f1eddbef2fbc21e4586e055c456a1011cdaf379e55d8f7a76f2b6a43					
Chunk 14:	ddb94d669778733a56ad308bd514fd369776f5e12344c4bb175d1d555075					
Chunk 15:	b9a69a8e56ecaba327f499f4c4e078f8f7e7267680b6c3156fbcd43d2a24					
Chunk 16:	a42170f41a8764ea881ab8a2a1b0bd120c8ba06634c24fcf81df1cca36d518					
Chunk 17:	e6569ef56830c27a8771cbb28b1887b30599c3e950c24f61649688e119794					
Hash Original: 60743cea29e553d7c57ea8a2942ef55728f887f25948a5d978991a3170a36b						
Hash Decrypted: 60743cea29e553d7c57ea8a2942ef55728f887f25948a5d978991a3170a36b						
Similarity Percentage : 100.00%						

SEDANG 3

[illegible]

SEDANG 4

[illegible]

[illegible]

[illegible][illegible][illegible][illegible][illegible]

BESAR 10

[illegible]

Lampiran 5 Daftar hadir dan surat penugasan seminar hasil



KEMENTERIAN PENDIDIKAN, KEBUDAYAAN
RISET DAN TEKNOLOGI
UNIVERSITAS HASANUDDIN
FAKULTAS TEKNIK
DEPARTEMEN TEKNIK INFORMATIKA
Kampus Fakultas Teknik Unhas, Jl. Poros Malino, Gowa
<http://eng.unhas.ac.id/informatika>, Email : informatika@unhas.ac.id

DAFTAR HADIR SEMINAR HASIL

Nama/Stambuk : Azzahra Beladina Shaff D121201017

Judul Skripsi/T.A : **“ Implementasi Hybrid Cryptography dan Secret Sharing untuk Menjaga Kerahasiaan Data pada Cloud Storage “**

Hari/Tanggal : Rabu, 30 Oktober 2024

Jam : 10.30 Wita – Selesai

Tempat : Ruang Lab. UBICON Departemen Teknik Informatika Gowa

No.	Jabatan	Nama Dosen	Tanda Tangan
L.	Pembimbing I	1. Dr.Eng. Ady Wahyudi Paundu,ST.,M.T	1.
II.	Anggota Penguji	2. Dr.Eng. Ir. Zulkifli Tahir,ST.,M.Sc	2.
		3. Mukarramah Yusuf, B.Sc.,M.Sc.,Ph.D	3.

PANITIA UJIAN

Ketua,

Dr.Eng. Ady Wahyudi Paundu,ST.,M.T



**KEMENTERIAN PENDIDIKAN, KEBUDAYAAN,
RISET, DAN TEKNOLOGI
UNIVERSITAS HASANUDDIN
FAKULTAS TEKNIK
DEPARTEMEN TEKNIK INFORMATIKA**

Kampus Fakultas Teknik Unhas, Jl. Poros Malino, Gowa
<http://eng.unhas.ac.id/informatika>, Email : informatika@unhas.ac.id

Nomor : 1743/UN4.7.7/TD.06/2024
Lamp : -
Hal : Penerbitan Surat Penugasan Panitia/Penguji
Seminar Hasil Strata Satu (S1)

Kepada Yth :

Wakil Dekan Bidang Akademik dan Kemahasiswaan
Fakultas Teknik Universitas Hasanuddin

Di-

Gowa

Dengan hormat,
Berdasarkan Persetujuan Pembimbing Mahasiswa, Bersama ini diusulkan susunan Panitia/Penguji Seminar Hasil Strata Satu (S1) bagi mahasiswa Departemen Teknik Informatika Fakultas Teknik tersebut di bawah ini :

Nama / Stambuk : Azzahra Beladina Shaff D121201017
Judul TA : Implementasi Hybrid Cryptography dan Secret Sharing untuk
Menjaga Kerahasiaan Data pada Cloud Storage

Dengan ini kami sampaikan Susunan Panitia Seminar Hasil Program Strata Satu (S1) Departemen Teknik Informatika Fakultas Teknik Universitas Hasanuddin dengan susunan sebagai berikut :

Pembimbing I/ Ketua : 1. Dr.Eng. Ady Wahyudi Paundu, ST., M.T
Penguji / Anggota : 2. Dr.Eng. Ir. Zulkifli Tahir, ST., M.Sc
3. Mukarramah Yusuf, B.Sc., M.Sc., Ph.D

Untuk dapat diterbitkan surat penugasannya

Demikian penyampaian kami, atas perhatian dan kerjasamanya diucapkan terima kasih.

Gowa, 28 Oktober 2024
Ketua Departemen Tek.Informatika,



Prof. Dr. Ir. Indrabayu, ST, MT., M.Bus.Sys., IPM, ASEAN.Eng
Nip.19750716 200212 1 004

Tembusan :

1. Arsip

Hari/Tanggal : Rabu, 30 Oktober 2024

Waktu : 10.30 - selesai

Tempat : Lab. Ubicam





KEMENTERIAN PENDIDIKAN, KEBUDAYAAN,
RISET, DAN TEKNOLOGI
UNIVERSITAS HASANUDDIN
FAKULTAS TEKNIK

Jalan Poros Malino Km. 6 Bontomarannu, Gowa, 92171, Sulawesi Selatan
☎ +62811 4420 909, E-mail: teknik@unhas.ac.id, <https://eng.unhas.ac.id>

SURAT PENUGASAN

No. 31059/UN4.7.1/TD.06/2024

Dari : Dekan Fakultas Teknik Universitas Hasanuddin.

Kepada : Mereka yang tercantum namanya di bawah ini.

Isi : 1. Bahwa merujuk kepada Peraturan Rektor Universitas Hasanuddin Nomor : 29/UN4.1/2023 tentang Penyelenggaraan Program Sarjana Universitas Hasanuddin, dengan ini menugaskan Saudara sebagai **PENGUJI/PANITIA UJIAN SARJANA** Program Strata Satu (S1) Departemen Teknik Informatika Fakultas Teknik Universitas Hasanuddin dengan susunan sebagai berikut :

Pembimbing / Ketua : 1. Dr.Eng. Adi Wahyudi Paundu, ST., M.T.
Penguji / Anggota : 2. Dr.Eng. Ir. Zulkifli Tahir, ST., M.Sc
3. Mukarramah Yusuf, B.Sc., M.Sc., Ph.D

untuk menguji bagi mahasiswa tersebut di bawah ini :

Nama/NIM : Azzahra Beladina Shaff D121201017
Program Studi : Teknik Informatika
Judul Thesis/Skripsi : Implementasi Hybrid cryptography dan Secret Sharing untuk Menjaga Kerahasiaan Data pada Cloud Storage
2. Waktu Ujian ditetapkan oleh Panitia Ujian Sarjana Program Strata Satu (S1).
3. Agar Surat penugasan ini dilaksanakan sebaik-baiknya dengan penuh rasa tanggung jawab.
4. Surat penugasan ini berlaku sejak tanggal ditetapkan sampai dengan berakhirnya Ujian Sarjana tersebut, dengan ketentuan bahwa segala sesuatu akan ditinjau dan diperbaiki sebagaimana mestinya apabila dikemudian hari ternyata terdapat kekeliruan dalam keputusan ini.

Ditetapkan di Gowa,
Pada tanggal 22 Nopember 2024
a.n. Dekan
Wakil Dekan Bidang Akademik dan Kemahasiswaan
Fakultas Teknik Unhas



Prof. Dr. Ir. Amil Ahmad Ilham, ST., M.IT
NIP.197310101998021001

Tembusan :

1. Dekan Fak. Teknik Unhas
2. Ketua Departemen Teknik Informatika FT-UH
3. Kasubag. Umum dan Perlengkapan FT-UH



Balai
Sertifikasi
Elektronik

• Dokumen ini telah ditandatangani secara elektronik menggunakan sertifikat elektronik yang diterbitkan BSrE

• UU ITE No 11 Tahun 2008 Pasal 5 Ayat 1

"Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah"



Lampiran 6 Daftar hadir dan surat penugasan ujian skripsi



KEMENTERIAN PENDIDIKAN, KEBUDAYAAN
RISET DAN TEKNOLOGI
UNIVERSITAS HASANUDDIN
FAKULTAS TEKNIK
DEPARTEMEN TEKNIK INFORMATIKA
Kampus Fakultas Teknik Unhas, Jl. Poros Malino, Gowa
<http://eng.unhas.ac.id/informatika>, Email : informatika@unhas.ac.id

DAFTAR HADIR UJIAN SKRIPSI MAHASISWA
FAKULTAS TEKNIK UNHAS

Nama/Stambuk : 1. Azzahra Beladina Shaff D121201017

Judul Skripsi/T.A : “ Implementasi Hybrid Cryptography dan Secret Sharing untuk Menjaga Kerahasiaan Data pada Cloud Storage“

Hari/Tanggal : Rabu, 28 November 2024

Jam : 09- 00 Wita – Selesai

Tempat : Ruang Lab. UBICON Departemen Teknik Informatika Gowa

No.	Jabatan	Nama Dosen	Tanda Tangan
L.	Pembimbing I	1. Dr.Eng. Ady Wahyudi Paundu,ST.,M.T	1.....
II.	Anggota Penguji	2. Dr.Eng. Ir. Zulkifli Tahir,ST.,M.Sc	2.....
		3. Mukarramah Yusuf, B.Sc.,M.Sc.,Ph.D	3.....

PANITIA UJIAN

Ketua

Dr. Eng. Ady Wahyudi Paundu, ST.,M.T



KEMENTERIAN PENDIDIKAN, KEBUDAYAAN,
RISET, DAN TEKNOLOGI
UNIVERSITAS HASANUDDIN
FAKULTAS TEKNIK
DEPARTEMEN TEKNIK INFORMATIKA

Kampus Fakultas Teknik Unhas, Jl. Poros Malino, Gowa
<http://eng.unhas.ac.id/informatika>, Email : informatika@unhas.ac.id

Gowa, 22 Nopember 2024

Nomor : 2088/UN4.7.7.1/TD.06/2024
Lamp : -
Hal : Usulan Susunan Panitia/Penguji Ujian Sarjana
Yth. : Bapak Wakil Dekan Bidang Akademik dan Kemahasiswaan
Fakultas Teknik Unhas
Di
Gowa

Dalam rangka penyelesaian studi pada Departemen Teknik Informatika Fakultas Teknik Unhas, bersama ini kami usulkan susunan Panitia/Penguji Ujian Sarjana Program Strata Satu (S1) bagi mahasiswa Departemen Teknik Informatika Fakultas Teknik Universitas Hasanuddin atas nama :

Pembimbing / Ketua : 1. Dr.Eng. Adi Wahyudi Paundu, ST., M.T.
Penguji / Anggota : 2. Dr.Eng. Ir. Zulkifli Tahir, ST., M.Sc
3. Mukarramah Yusuf, B.Sc., M.Sc., Ph.D

Untuk Bertugas sebagai Penguji/ Penanggap Ujian Sarjana bagi Mahasiswa :

Nama : Azzahra Beladina Shaff
Stambuk : D121 20 1017

Dengan Judul Skripsi :

“Implementasi Hybrid cryptography dan Secret Sharing untuk Menjaga Kerahasiaan Data pada Cloud Storage “

Pada : ~~Kamis~~
Hari/Tanggal : ~~Sabtu~~, 20 Nopember 2024
Jam : 09.00 Wita - Selesai
Tempat : Ruang Sidang Lab. Ubicom

Demikian penyampaian kami, atas perhatiannya diucapkan terimah kasih.

Ketua Departemen Tek.Informatika,



Prof. Dr. Ir. Indrabayu.,ST, MT, M.Bus.Sys., IPM, ASEAN.Eng
Nip.197507016 200212 1 004

Tembusan :
1. Arsip

Handwritten: Hari/Tanggal : Kamis, 28 Nov 2024

Handwritten: Waktu : 13.00 - selesai



Dipindai dengan CamScanner

