5th Seminar Nasional Mahasiswa Fakultas Teknologi Informasi (SENAFTI)
7 September 2024 – Jakarta, Indonesia
Volume 3, Nomor 2, September 2024 - ISSN 2962-8628 (*online*)

IMPLEMENTASI KRIPTOGRAFI UNTUK KEAMANAN DATA CV. *DOPE SUPPLY* INDONESIA MENGGUNAKAN METODE AES BERBASIS *WEBSITE*

Cut Alfath Dhuhana[1*], Wahyu Pramusinto[2]

[1,2]Teknik Informatika, Fakultas Teknologi Informasi, Universitas Budi Luhur, Jakarta Selatan, Indonesia

Email: [1*]2311510909@student.budiluhur.ac.id, [2]wahyu.pramusinto@budiluhur.ac.id
(* : *corresponding author*)

Abstrak-Teknologi yang semakin canggih salah satunya di bidang komputer, memberikan kemudahan dalam pelayanan di segala aspek kehidupan menjadi lebih efisien, akurat, dan cepat . Saat ini teknologi komputer telah mengalami pertumbuhan yang pesat dan telah menjadi salah satu aspek penting bagi setiap orang, karena besarnya jumlah pekerjaan yang cepat terselesaikan dengan adanya teknologi tersebut. Meskipun demikian, kemajuan teknologi juga mengalami berbagai dampak negatif, salah satu akibat buruk dari pertumbuhan teknologi yaitu adanya pencurian data. CV. *Dope Supply* Indonesia Indonesia merupakan industri yang terfokus dalam penyediaan barang dan jasa memiliki aset data yang termasuk privasi. Kriptografi adalah teknik menyandikan atau mengamankan data atau informasi, seperti integritas, kerahasiaan, dan autentikasi data, antara lain, agar orang yang tidak berhak memilikinya tidak dapat mengetahuinya. Akan tetapi perusahaan masih belum melengkapi dengan keamanan yang baik, sehingga data tersebut dapat dengan mudah diakses dan disalahgunakan oleh pihak-pihak yang tidak bertanggung jawab. Maka dari itu, CV. *Dope Supply* Indonesia perlu menerapkan sistem yang dapat melindungi data. Kriptografi adalah proses enkripsi yang dapat mengubah teks atau data *plain* menjadi teks rahasia, dan proses dekripsi yang dapat mengembalikan teks rahasia menjadi data *plain*. Metode AES adalah salah satu algoritma kriptografi yang bisa digunakan untuk mengamankan data. Dalam implementasi ini, dokumen yang dapat digunakan adalah dokumen dengan format doc,xls, pdf, serta txt. Tujuan dari penelitian dan pengujian menerapkan metode AES untuk menjaga keamanan data pada CV. *Dope Supply* Indonesia agar data tidak rusak dan terjaga autentikasinya.

Kata Kunci: *Advanced Encription Standart* (AES), Keamanan Data, Kriptografi, *Website*

IMPLEMENTATION OF CRYPTOGRAPHY FOR DATA SECURITY AT CV. DOPE SUPPLY INDONESIA USING THE ADVANCED ENCRYPTION STANDARD (AES) METHOD BASED ON WEBSITE

Abstract- *The rapid growth of technology, particularly in computers, provides convenience in services across all aspects of life, making them more efficient, accurate, and fast. Currently, computer technology has experienced rapid growth and has become an important aspect for everyone, due to the large volume of work that can be completed quickly with this technology. However, technological advancements also come with various negative impacts, one of the adverse effects of technological growth being data theft. CV. Dope Supply Indonesia is an industry focused on providing goods and services that have data assets, including privacy. Cryptography is a technique for encoding or securing data or information, such as integrity, confidentiality, and data authentication, among others, so that unauthorized individuals cannot access it. However, the company has not yet implemented with good security measures, allowing this data to be easily accessed and misused by irresponsible parties. Therefore, CV. Dope Supply Indonesia needs to implement a system that can protect its data. Cryptography is an encryption process that can transform plain text or data into chypertext, and a decryption process that can revert from chypertext into plain text or data. The AES method is one of the cryptographic algorithms that can be used to secure data. In this implementation, the documents that can be used are those in doc, xls, pdf, and txt formats. This research and testing aim to apply the AES method to maintain data security at CV. Dope Supply Indonesia, ensures that the data remains intact and its authentication is preserved.*

Keywords*: Advanced Encryption Standard (AES), Data Security, Cryptography, Website*

1. PENDAHULUAN

Teknologi yang semakin canggih salah satunya di bidang komputer memberikan kemudahan dalam pelayanan di segala aspek kehidupan menjadi lebih efisien, akurat, dan cepat [1] . Saat ini teknologi komputer telah bertumbuh dengan pesat dan menjelma sebagai salah satu aspek penting bagi setiap orang, karena besarnya jumlah pekerjaan yang cepat terselesaikan dengan adanya teknologi tersebut. Meskipun demikian, kemajuan teknologi juga mengalami berbagai dampak negatif, salah satu akibat buruk dari pertumbuhan teknologi yaitu

adanya pencurian data [2].

Pencurian berupa aset data maupun informasi yang bersifat privasi bisa saja terjadi, sudah sepatutnya dalam penyimpanan data penting tersebut perlu dilengkapi dengan keamanan yang baik, sehingga data tersebut memungkinkan untuk diakses dan disalahgunakan oleh pribadi-pribadi yang tidak berkewajiban. Maka dari itu, perlu menerapkan sistem yang mampu mengamankan data agar data tersebut tidak bisa diubah secara sewenang-wenang oleh pihak yang tidak berkepentingan.

Kriptografi adalah teknik menyandikan atau melindungi data atau informasi, seperti kerahasiaan, integritas dan autentikasi data, antara lain, agar orang yang tidak berhak memilikinya tidak dapat mengetahuinya. Kriptografi adalah proses enkripsi yang dapat mengubah teks biasa atau data menjadi teks rahasia, dan proses deskripsi yang dapat memulihkan teks rahasia menjadi teks biasa atau data [3]. Metode AES ialah salah satu algoritma kriptografi yang dapat difungsikan sebagai metode pengamanan data [4].

Metode pembanding digunakan untuk membandingkan metodologi penelitian ini dengan yang diterapkan dalam penelitian sebelumnya. Metode pembanding dilakukan dengan penelitian sebelumnya yaitu penelitian dengan judul "Pengamanan Data Gaji Karyawan Dengan Menggunakan Metode *Advanced Encryption Standard* (AES)" [5]. Tujuannya adalah untuk mengidentifikasi perbedaan antara penelitian yang dilakukan saat ini dengan penelitian sebelumnya. Perbedaan utama antara kedua penelitian ini terletak pada objek yang digunakan. Penelitian sebelumnya menggunakan hanya berfokus pada gaji karyawan saja. Sedangkan, penelitian yang akan dilakukan berfokus pada seluruh dokumen yang terdapat pada CV. *Dope Supply* Indonesia dengan berextention txt, doc, xls, pdf dan ukuran maksimal 4 MB.

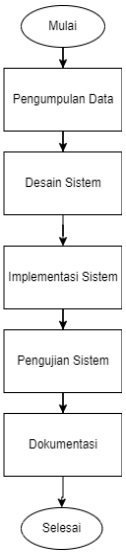
Bersumber dari uraian di atas, maka dalam penelitian ini tujuan mengimplementasikan kriptografi berbasis website untuk mengetahui konsep kriptografi menggunakan metode *Advanced Encryption Standard* (AES). Pada penelitian ini aplikasi diimplementasikan berbasis website dengan menerapkan bahasa pemrograman *python* dengan framework flask dan database MySQL. Hasil penelitian yaitu aplikasi kriptografi berbasis *website* yang dapat mengerjakan enkripsi dan dekripsi file data yang setelah diuji berhasil dapat mengamankan serta melindungi data dari orang yang tidak berkepentingan di CV. *Dope Supply* Indonesia.

2. METODE PENELITIAN

2.1 Tahapan Penelitian

Metode pembanding digunakan untuk membandingkan metodologi penelitian ini dengan yang diterapkan dalam penelitian sebelumnya dengan tujuan untuk mengidentifikasi perbedaan antara penelitian yang dilakukan saat ini dengan penelitian sebelumnya.

Perbedaan utama antara kedua penelitian ini terletak pada objek yang digunakan. Penelitian sebelumnya menggunakan hanya berfokus pada gaji karyawan saja. Sedangkan, penelitian yang akan dilakukan berfokus pada seluruh dengan berextention txt, doc, xls, pdf dan ukuran maksimal 4 MB. Penerapan metode penelitian digambarkan dalam bentuk diagram proses penelitian, seperti yang ditunjukkan Gambar 1.



Gambar 1. Tahap Penelitian

Berdasarkan Gambar 1 tahapan penelitian dapat dijabarkan antara lain:

a. Pengumpulan Data
   Dalam tahap ini, meminta manajer dan staff IT memberikan informasi mengenai keamanan data yang diterapkan pada perusahaan melalui wawancara. Selain itu, observasi langsung terhadap sistem yang sedang berjalan dilakukan, disertai dengan studi pustaka tentang teknik kriptografi dan keamanan data.
b. Desain Sistem
   Tahap berikutnya sistem keamanan informasi dirancang dengan menerapkan metode *Advanced Encryption Standard* (AES). Aktivitas pada tahap ini mencakup menentukan spesifikasi teknis dan arsitektur sistem, termasuk detail mengenai bagaimana metode AES akan diterapkan dalam sistem.
c. Implementasi Sistem
   Dalam tahap ini, sistem keamanan data dikembangkan menggunakan pemrograman *Python* dengan *framework* flask dan database MySQL berdasarkan dengan desain yang telah dirancang.
d. Pengujian Sistem
   Aktivitas pada tahap ini meliputi pengujian *Black Box Testing* untuk memastikan semua fitur dan fungsi sistem berjalan sesuai harapan, serta uji keamanan untuk mengukur efektivitas enkripsi dan dekripsi data.
e. Dokumentasi
   Tahapan terakhir melibatkan penyusunan dokumentasi lengkap yang mencakup semua tahapan penelitian, mulai dari pengumpulan data hingga pengujian sistem.

2.2 Keamanan Data

Melindungi data dari akses, perusakan yang tidak sah, pengungkapan, penggunaan, modifikasi, gangguan, atau sangatlah penting, karena dapat setiap individu atau organisasi harus memastikan akan kemanan data masing-masing [6]. Terdapat 3 prinsip untuk kemanan data yaitu kerahasiaan yang menegaskan bahwa data hanya bisa diakses oleh individu maupuan kelompok yang memiliki izin. Integritas menegaskan bahwa data tetap akurat dan tidak diubah oleh pihak ataupun aspek yang tidak berwenang. Dan yang ketiga adalah ketersediaan memastikan bahwa data selalu tersedia untuk pengguna berwenang saat diperlukan [7].

Salah satu Undang-Undang yang memiliki keterkaitan dengan keamanan data adalah terdapat pada Pasal 26 ayat (1) Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) yang berisi "*Kecuali ditentukan lain oleh Peraturan Perundang-undangan, penggunaan setiap informasi melalui media elektronik yang menyangkut data pribadi seseorang harus dilakukan atas persetujuan orang yang bersangkutana"*[8].

2.3 Kriptografi

Kriptografi yaitu ilmu yang memuat tentang mempertahankan kerahasiaan data atau informasi dengan proses mengirimkan data atau informasi tersebut dalam bentuk kode dengan menerapkan algoritma khusus dengan tujuan agar tidak dapat terbaca oleh siapapun selain pengirim dan penerima informasi atau data tersebut yang disebut enkripsi. Sedangkan untuk sebaliknya yaitu mengubah kode yang telah dikirimkan menjadi informasi dengan format awal adalah deskripsi [9].

2.4 *Cybersecurity*

Cybersecurity merupakan suatu mekanisme yang dibangun untuk melindungi suatu integritas, kerahasiaan, dan ketersediaan informasi [10]. *Cybercrime* adalah sebuah kejahatan di ruang siber yang dilakukan oleh individu atau kelompok yang melakukan penyerangan sistem keamanan komputer atau data dengan berbagai alasan yang dapat mengakibatkan kerugian ekonomi atau politik bagi individu atau kelompok tersebut [11].

2.5 Metode AES

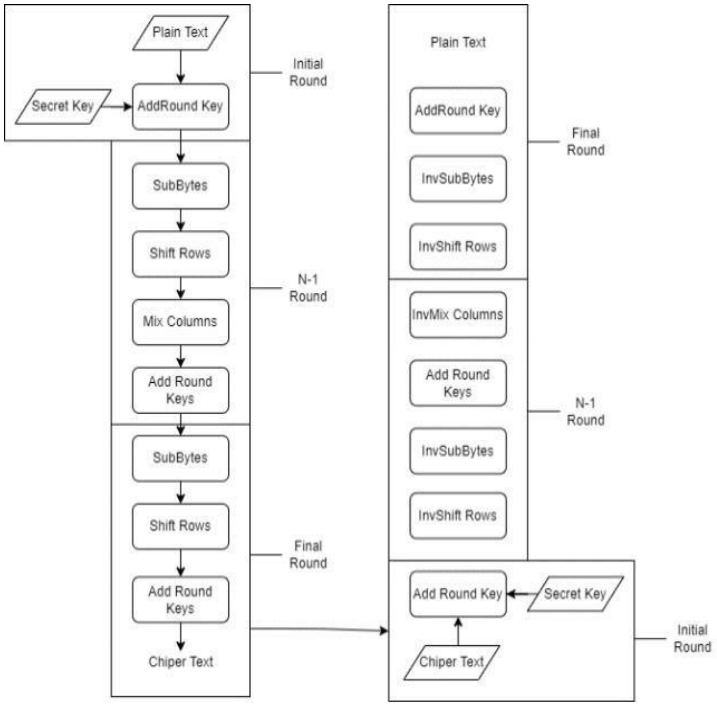
AES sendiri memiliki sifat simetris yang hanya memanfaatkan satu kunci simetris pada waktu enkripsi dan deskripsi yang termasuk dalam algoritma *block chiper* [12]. AES atau *Advanced Encryption Standard* diperkenalkan untuk menggantikan metode DES (*Data Encryption Standard)* karena DES sendiri memiliki algoritma yang lambat dan kunci enkripsi yang sangat kecil [13]. Perbedaan panjang kunci dapat memberikan dampak pada jumlah perputaran yang dilakukan oleh AES sendiri, seperti yang ditunjukan Tabel 1 [14].

Tabel 1. Urutan Data AES

	Panjang Kunci	Panjang Blok	Jumlah Putaran
AES-128	4	4	10
AES-129	6	4	12
AES-256	8	4	14

Menurut Endar algoritma AES mempunyai 3 parameter di antaranya adalah [15]:
a. Data masukan atau *input* yang ada pada array berukuran 16-bit yaitu *plaintext.*
b. Hasil enkripsi yang ada pada array berukuran sama 16-bit yaitu *ciphertext.*
c. Dan yang ketiga merupakan kunci *chipering* atau *chiper key* yang ada pada array ukuran sama yaitu *Key.*

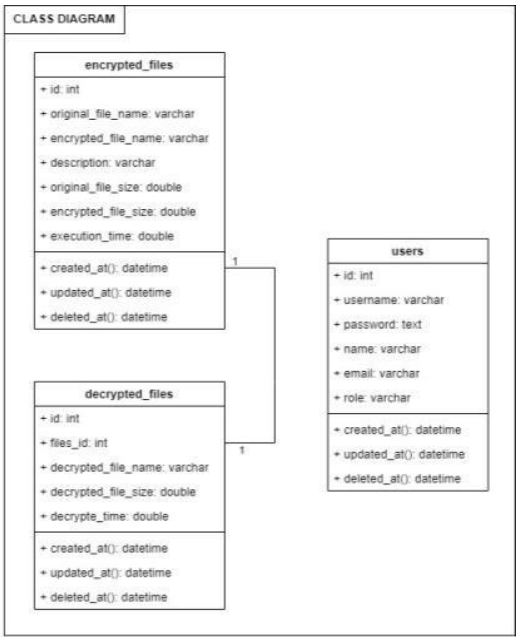
Tahapan utama menerapakan metode aes terdapat 3 tahap utama yaitu *initial round, N-1 round,* dan *Final Round,* seperti berikut [15]:



Gambar 2. Tahap AES

2.6 Rancangan Basis Data

Sistem keamanan informasi dirancang dengan menerapkan metode *Advanced Encryption Standard* (AES). Aktivitas pada tahap ini mencakup menentukan spesifikasi teknis basis data sistem dengan menggunakan *class diagram.*



Gambar 3. *Class Diagram*

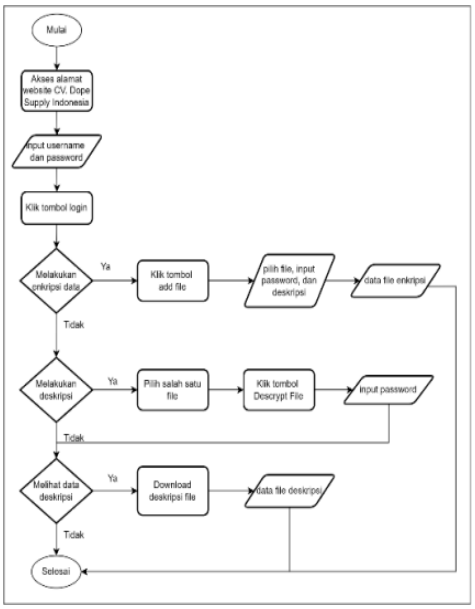
3. HASIL DAN PEMBAHASAN

3.1 *Flowchart*

Gambar *flowchart* membantu merancang aktivitas kerja, yang menjelaskan berbagai aktivitas, prosedur, dan proses yang terjadi. *Flowchart* yang dibuat berdasarkan hasil rancangan sistem.

3.1.1 *Flowchart* Tampilan Layar Pengguna

Saat masuk dalam sistem sebagai pengguna melakukan enkripsi data dengan memilih fitur "*Add File*" dan melakukan unggah dokumen yang akan dienkripsi beserta menginputkan *password*. Demikian pula proses deskripsi *file* yang akan dienkripsi sehingga didapatkan *output* berupa data dokumen terenkripsi. Alur akses pengguna pada sistem ditunjukkan oleh *flowchart* sistem di Gambar 4.



Gambar 4. *Flowchart* Tampilan Layar – Pengguna

3.2 Tampilan Layar Aplikasi

Proses pembuatan sistem untuk memenuhi kebutuhan CV. *Dope Supply* Indonesia telah selesai, seperti yang terlihat pada tampilan aplikasi berikut ini.

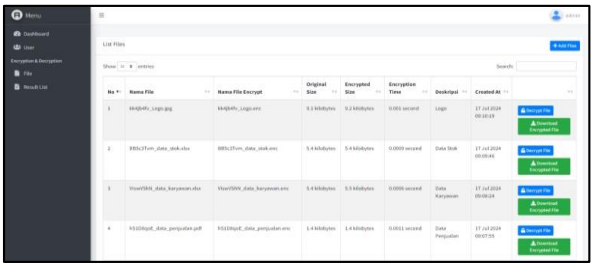
3.2.1 Tampilan Layar Halaman *Login*

Halaman *login* merupakan halaman yang pertama kali akan ditampilkan oleh sistem pada pengguna. Pada halaman ini pengguna diminta memasukkan *username* dan *password* yang telah terdaftar. Tampilan layarnya seperti Gambar 5.

Gambar 5. Tampilan Layar Halaman *Login*

3.2.2 Tampilan Layar Halaman Proses Enkripsi dan Deskripsi

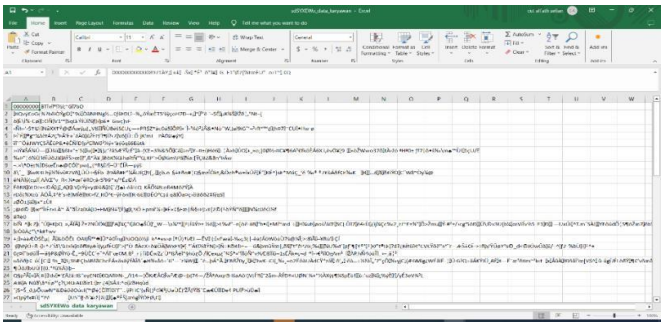
Gambar 6, menunjukkan tampilan halaman proses enkripsi dan deskripsi dimana pengguna dapat melakukan proses enkripsi data dan deskripsi data pada halaman ini.



Gambar 6. Tampilan Kayar Halaman Proses Enkripsi Dan Deskripsi

3.2.3 Tampilan Layar Hasil Proses Enkripsi

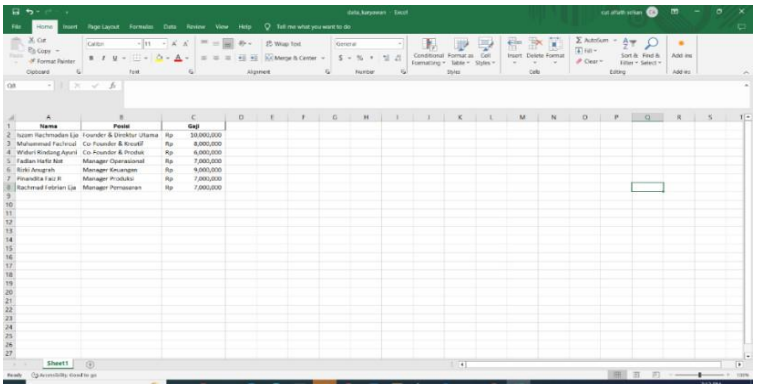
Hasil proses enkripsi data yang mengubah data menjadi kode data yang telah diproses oleh sistem ditunjukkan oleh Gambar 7.



Gambar 7. Tampilan Layar Hasil Proses Enkripsi

3.2.4 Tampilan Layar Hasil Proses Dekripsi

Sedangkan untuk proses dekripsi yaitu mengubah data enkripsi menjadi data awal, hasilnya ditunjukkan oleh Gambar 8.



Gambar 8. Tampilan Layar Hasil Proses Deskripsi

3.3 Hasil Pengujian Enkripsi dan Dekripsi

Berikut ini pengujian hasil enkripsi dan dekripsi yang dilakukan pada fitur menu pada proses melakukan enkripsi dan dekripsi file dokumen CV. Dope Supply Indonesia seperti ditampilkan pada Tabel 2 dan Tabel 3 berikut.

3.3.1 Hasil Pengujian Enkripsi

Tabel 2 menunjukkan hasil pengujian enkripsi dimana semua file yang diuji telah berhasil diubah menjadi bentuk enkripsi. Terdapat empat file yang diujikan dalam proses enkripsi dengan berbagai format dan ukuran. Untuk hasil proses enkripsi ukuran file yang diproses tidak mengalami perubahan yang signifikan. Sedangkan untuk durasi proses enkripsi terjadi sangat cepat berkisar 0.0006 hingga 0.0503 detik. Nama file yang dienkripsi mengalami penambahan karakter dan kode serta berextention enc yang dimana menandakan dokumen sudah mengalami proses enkripsi. Dengan demikian dapat disimpulkan bahwa proses enkripsi berjalan sukses atau berhasil dengan waktu relatif cepat dan untuk ukuran file tidak mengalami perubahan signifikan.

Tabel 2. Hasil Pengujian Enkripsi

No	Nama *File* Awal	Ukuran *File* Awal	Nama *File* Setelah Enkripsi	Ukuran *File*	Status	
					Enkripsi	Durasi (*Second*)
1	laporan_penjualan.pdf	1.4 kb	hS1D8qoE_data_penjualan.enc	1.4 kb	Berhasil	0.0011
2	data_karyawan.xls	5.4 kb	VIswVShN_data_karyawan.enc	5.5 kb	Berhasil	0.0006
3	data_stok. xls	5.4 kb	BB5c3Tvm_data_stok.enc	5.4 kb	Berhasil	0.0009
4	Cut Alfath_FullBAB	2,712 kb	GyrEmkaq_Cut_Alfath_FullBAB.enc	2,6 Mb	Berhasil	0.0503

3.3.2 Hasil Pengujian Dekripsi

Tabel 3 menunjukkan hasil pengujian enkripsi dimana semua *file* yang diuji telah berhasil diubah menjadi bentuk dekripsi. Terdapat empat file yang diujikan dalam proses dekripsi dengan berbagai format dan ukuran. Untuk hasil proses dekripsi ukuran file yang diproses tidak mengalami perubahan serta durasi proses dekripsi terjadi juga relatif cepat berkisar 0.0015 hingga 0.0343 detik. Nama *file* yang dekripsi terdapat penambahan karakter dan kode tertentu namun dengan extention seperti file sebelum di enkripsi dimana menandakan dokumen sudah kembali dengan format awal. Dengan demikian dapat disimpulkan bahwa proses dekripsi berjalan sukses atau berhasil dengan waktu relatif cepat, ukuran file tidak mengalami perubahan serta dokumen kembali ke format awal walau dengan judul ada penambahan karakter atau kode tertentu.

Tabel 3. Hasil Pengujian Dekripsi

No	Nama File Awal	Ukuran *File* Awal	Nama *File* Setelah Enkripsi	Ukuran *File*	Status	
					Dekripsi	Durasi (*Second*)
1	hS1D8qoE_data_penjualan.enc	1.4 kb	hXAg1LoS_BB5c3Tvm_data_stok.xlsx	1.4 kb	Berhasil	0.0018
2	VIswVShN_data_karyawan.enc	5.4 kb	MPTNGEyu_VIswVShN_data_karya wan.xlsx	5.4 kb	Berhasil	0.0015
3	BB5c3Tvm_data_stok.enc	5.4 kb	hXAg1LoS_BB5c3Tvm_data_stok.xlsx	5.4 kb	Berhasil	0.0033
4	GyrEmkaq_Cut_Alfath_FullBAB.enc	2,6 Mb	SqRMv4vZ_GyrEmkaq_Cut_Alfath_FullBAB.docx	2.6 Mb	Berhasil	0.0343

3.4 Hasil Pengujian *Black Box*

Pengujian black box ini dilakukan untuk memastikan fungsi dari semua sistem telah berjalan dengan baik. Hasil pengujiannya ditampilkan oleh Tabel 4.

Tabel 4. Hasil Pengujian *Black Box* – Pengguna

No	Butir Uji	Skenario Pengujian	Hasil Yang Diharapkan	Hasil Uji
1	Melakukan *login*	Mengisi *username* dan *password* kemudian klik *Login*	*Username* dan *password valid* dan sistem menampilkan halaman *dashboard* pengguna	Sesuai
		Tidak mengisi data *login* dengan lengkap dan sesuai	Sistem tidak memberikan akses pemberitahuan berupa pesan kesalahan *login*	Sesuai
2	*Input* Data	Klik menu data	Sistem menampilkan halaman daya	Sesuai
		Memasikkan data untuk dienkripsi	Data berhasil dienkripsi dan disimpan	Sesuai
3	Melihat data yang terenkripsi	Melihat data enkripsi	Menampilkan terenkripsi	Sesuai

4. KESIMPULAN

Pada penelitian ini telah dilakukan implementasi kriptografi menggunakan metode *Advanced Encryption Standart* (AES) untuk meningkatkan keamanan data pada CV. *Dope Supply* Indonesia berbasis website. Berdasarkan hasil penelitian dan pengujian yang telah dilakukan, dapat disimpulkan bahwa proses implementasi metode AES pada sistem keamanan data CV. *Dope Supply* Indonesia berhasil diterapkan dengan baik dengan melindungi data sensitif dari akses yang tidak sah berdasarkan hasil pengujian data enkripsi dan data deskripsi metode AES yang telah dilakukan. Serta berdasarkan pengujian tersebut menunjukkan, penggunaan metode AES telah meningkatkan keamanan data pada CV. *Dope Supply* Indonesia. Data yang telah dienkripsi menggunakan metode AES menjadi lebih sulit untuk dibobol, sehingga mengurangi risiko kebocoran data dan serangan *cyber*. Sedangkan untuk setiap fitur sistem telah diuji menggunakan pengujian *blackbox* menunjukkan bahwa sistem telah berjalan dengan baik dan sesuai dengan fungsi masing-masing fitur. Saran yang dapat dibagikan untuk pengembangan dan penelitian lebih lanjut yaitu meskipun metode AES merupakan metode yang kuat dalam melindungi atau meningkatkan keamanan data, terdapat beberapa metode pengembangan kriptografi lain yang dapat diterapkan untuk meningkatkan keamanan data lebih lanjut seperti RSA dan *Elliptic Curve Cryptography* (ECC). Dan untuk peningkatan keamanan tambahan dapat ditambahkan metode keamanan lain untuk meningkatkan lapisan keamanan data seperti *Secure Sockets Layer* (SSL) atau *Transport Layer Security* (TLS) agar dapat melindungi data berbasis *website*.

UCAPAN TERIMA KASIH

Semoga penelitian ini dapat bermanfaat pada masa yang akan datang. Maka, dari itu rasa terima kasih diucapkan kepada seluruh pihak-pihak terkait yang telah berkontribusi secara langsung maupui tidak langsung atas terlaksananya dan terselesaikannya penelitian ini tepat pada waktunya.

DAFTAR PUSTAKA

[1] S. Setti, I. Gunawan, B. E. Damanik, S. Sumarno, dan I. O. Kirana, "Implementasi Algoritma Advanced Encryption Standard dalam Pengamanan Data Penjualan Ramayana Department Store," *JURIKOM (Jurnal Ris. Komputer)*, vol. 7, no. 1, hal. 182, 2020, doi: 10.30865/jurikom.v7i1.1960.

[2] M. Azhari, D. I. Mulyana, F. J. Perwitosari, dan F. Ali, "Implementasi Pengamanan Data pada Dokumen Menggunakan Algoritma Kriptografi Advanced Encryption Standard (AES)," *J. Pendidik. Sains dan Komput.*, vol. 2, no. 01, hal. 163–171, 2022, doi: 10.47709/jpsk.v2i01.1390.

[3] F. A. Sitorus, N. B. Nugroho, dan U. F. S. S. Pane, "Implementasi Algoritma Advanced Encryption Standard (AES) 128 Bit untuk Keamanan Data Transaksi Penjualan Pada PT. Mitsubishi Electric Indonesia," *J. CyberTech*, no. x, hal. 1–15, 2020, [Daring]. Tersedia pada: https://ojs.trigunadharma.ac.id/

[4] A. Putra Ramadani Tarigan, P. S. Ramadhan, dan K. Ibnutama, "Penerapan Kriptografi Untuk Pengamanan Data Penjualan Sepatu Dengan Metode AES (Advanced Encryption Standard)," *J. Cyber Tech*, vol. 5, no. 1, hal. 26, 2023, doi: 10.53513/jct.v5i1.7851.

[5] Sianipar, J. S., Nuugroho, N. B. dan Mariami, I. (2024) "Pengamanan Data Gaji Karyawan Dengan Menggunakan Metode Advanced Encryption Standard (AES)," Jurnal Sistem Informasi Tgd, 3(1), hal. 35–45.

[6] A. P. Triandari, "Studi Kepustakaan: Keamanan Informasi Di Perpustakaan Digital," *VISI PUSTAKA Bul. Jar. Inf. Antar Perpust.*, vol. 24, no. 3, hal. 237–250, 2022, doi: 10.37014/visipustaka.v24i3.3244.

[7] N. I. Putri, R. Komalasari, dan Z. Munawar, "Pentingnya Keamanan Data Dalam Intelijen Bisnis," *J. Sist. Inf.*, vol. 1, no. 2, hal. 41–49, 2020.

[8] CSA Teddy Lesmana, E. Elis, dan S. Hamimah, "Urgensi Undang-Undang Perlindungan Data Pribadi Dalam Menjamin Keamanan Data Pribadi Sebagai Pemenuhan Hak Atas Privasi Masyarakat Indonesia," *J. Rechten Ris. Huk. dan Hak Asasi Mns.*, vol. 3, no. 2, hal. 1–6, 2022, doi: 10.52005/rechten.v3i2.78.

[9] W. R. Maya, A. Azanuddin, dan E. Elfitriani, "Implementasi Kriptografi Pengamanan Data Nilai Siswa Menggunakan Algoritma DES," *J. SAINTIKOM (Jurnal Sains Manaj. Inform. dan Komputer)*, vol. 21, no. 1, hal. 1, 2022, doi: 10.53513/jis.v21i1.4764.

[10] M. R. Ramadhani dan A. R. Pratama, "Analisis Kesadaran Cybersecurity Pada Pengguna Media Sosial Di Indonesia," *Journal.Uii.Ac.Id*, vol. 1, no. 2, hal. 1–8, 2020, [Daring]. Tersedia pada: https://journal.uii.ac.id/AUTOMATA/article/download/15426/10219

[11] E. Budi, D. Wira, dan A. Infantono, "Strategi Penguatan Cyber Security Guna Mewujudkan Keamanan Nasional di Era Society 5.0," *Pros. Semin. Nas. Sains Teknol. dan Inov. Indones.*, vol. 3, no. November, hal. 223–234, 2021, doi: 10.54706/senastindo.v3.2021.141.

[12] B. E. Widodo dan A. S. Purnomo, "Implementasi Advanced Encryption Standard Pada Enkripsi Dan Dekripsi Dokumen Rahasia Ditintelkam Polda Diy," *J. Tek. Inform.*, vol. 1, no. 2, hal. 69–77, 2020, doi: 10.20884/1.jutif.2020.1.2.21.

[13] Melenia Bayu Aryanto, Muhlis Tahir, Silvia Irma Devita, Zuda Nuril Mustofa, Qurrotun Ainiyah, dan Shelviatus Sundoro, "Implementasi Enkrip Dan Dekrip File Menggunakan Metode Advance Encryption Standard (AES-128)," *J. Ilm. Sist. Inf. dan Ilmu Komput.*, vol. 3, no. 1, hal. 89–104, 2023, doi: 10.55606/juisik.v3i1.434.

[14] J. S. Sianipar, N. B. Nuugroho, dan I. Mariami, "Pengamanan Data Gaji Karyawan Dengan Menggunakan Metode Advanced Encryption Standard (AES)," *J. Sist. Inf. Tgd*, vol. 3, no. 1, hal. 35–45, 2024, [Daring]. Tersedia pada: https://doi.org/10.53513/jursi.v3i1.5653

[15] N. 'Endar, "Penerapan Steganografi File Gambar Menggunakan Metode Least Significant Bit (LSB) dan Algoritma Kriptografi Advanced Encryption Standard (AES) Berbasis Android," *J. Inform. Univ. Pamulang*, vol. 5, no. 1, hal. 37–37, 2020.

[16] R. F dan A. Anwar, "Implementasi Kriptografi Dengan Metode Advanced Encryption Standard (AES) Untuk Realtime Chat Berbasis Mobile Pada E-Learning Politeknik Negeri Lhokseumawe," *J. Artif. Intell. Softw. Eng.*, vol. 1, no. 2, hal. 92–99, 2021, doi: 10.30811/jaise.v1i2.2520.