3rd Seminar Nasional Mahasiswa Fakultas Teknologi Informasi (SENAFTI)
30 Agustus 2023 – Jakarta, Indonesia
Volume 2, Nomor 2, September 2023 - ISSN 2962-8628 (*online*)

PENGAMANAN *FILE* PENTING PADA PT. CANGKEMAN UTAMA KREASI MENGGUNAKAN ALGORITMA AES-128

Muhammad Ihsan Imanuddin[1*], Rizky Pradana[2]

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

Email: [1*]emihsan87@email.com, [2]rizky.pradana@budiluhur.ac.id
(* : corresponding author)

Abstrak-Dalam era di mana teknologi informasi dan komunikasi memainkan peran sentral, data yang dianggap penting harus dijaga kerahasiaannya dengan menerapkan tindakan-tindakan keamanan yang dapat mencegah akses yang tidak diinginkan. PT. Cangkeman Utama Kreasi merupakan sebuah perusahaan yang beroperasi dalam sektor Telekomunikasi dan Informasi menyadari betapa krusialnya perlindungan data organisasi dari potensi ancaman siber dan akses yang tidak sah. Permasalahannya adalah perusahaan ini masih menyimpan data yang berisi informasi tagihan, laporan laba rugi perusahaan yang berupa arsip dokumen digital di dalam suatu folder pada komputer tanpa adanya sistem pengamanan data. Untuk meminimalkan kemungkinan terjadinya tindak kejahatan data ini, diperlukan pengamanan data atau informasi tersebut. Penelitian ini bertujuan untuk membuat aplikasi enkripsi dan dekripsi dengan metode algoritma *Advanced Encryption Standard* (AES)-128 sebagai solusi dalam meningkatkan keamanan data di lingkungan perusahaan. Dengan penerapan metode enkrispi dan dekripsi AES-128, perusahaan PT. Cangkeman Utama Kreasi dapat terhindar dari resiko dengan menerapkan metode ini dan mencapai tingkat keamanan yang lebih tinggi dalam menghadapi ancaman siber baik dari dalam maupun dari luar dan potensi kebocoran data. Hal ini memberikan *key*akinan kepada manajemen dan pemangku kepentingan bahwa data perusahaan dijaga dengan baik dan mencegah akses yang tidak sah. Penggunaan algoritma AES-128 memberikan tingkat keamanan yang tinggi dan kinerja yang optimal dalam melindungi data sensitive. Dapat disimpulkan bahwa implementasi aplikasi kriptografi AES-128 di perusahaan ini telah berhasil meningkatkan keamanan data mereka. Implementasi ini membentuk dasar yang kokoh dalam menjaga keamanan data perusahaan di era digital yang penuh dengan tantangan.

Kata Kunci: Kriptografi, Enkripsi, Dekripsi, AES-128

SECURING IMPORTANT FILES AT PT. CANGKEMAN UTAMA KREASI USING AES-128 ALGORITHM

Abstract-*In an era where information and communication technology plays a central role, data that is considered important must be kept confidential by implementing security measures to prevent unauthorized access. PT. Cangkeman Utama Kreasi is a company operating in the Telecommunication and Information sector, and they are aware of the crucial need to protect organizational data from potential cyber threats and unauthorized access. The issue is that this company still stores data containing billing information and company income statements in the form of digital document archives within a folder on the computer without any data security system. To minimize the possibility of data crimes, it is necessary to secure the data or information. This research aims to create an encryption and decryption application using the Advanced Encryption Standard (AES)-128 algorithm as a solution to enhance data security within the company's environment.*
By implementing the AES-128 encryption and decryption methods, PT. Cangkeman Utama Kreasi can mitigate risks, achieve a higher level of security against both internal and external cyber threats, and potential data leaks. This provides confidence to the management and stakeholders that the company's data is well-protected and safeguards against unauthorized access. The use of AES-128 algorithm provides a high level of security and optimal performance in protecting sensitive data. In conclusion the implementation of the AES-128 cryptography application in this company has successfully enhanced their data security. This implementation forms a strong foundation for maintaining the company's data security in the challenging digital era.

Keywords*: Cryptography, Encryption, Decryption, AES-128*

1. PENDAHULUAN

Dengan pesatnya perkembangan teknologi, manusia kini dapat berkomunikasi dan berbagi informasi dengan cepat, efektif, dan efisien tanpa adanya batasan jarak dan waktu. Informasi dapat disebar atau disampaikan ke berbagai negara, kota bahkan sampai pelosok bukan suatu kendala lagi untuk itu tuntutan keamanan kerahasiaan informasi tersebut juga semakin meningkat. Dalam era di mana teknologi informasi dan komunikasi memainkan peran sentral, data yang dianggap penting harus dijaga kerahasiaannya dengan menerapkan tindakan-tindakan keamanan yang dapat mencegah akses yang tidak diinginkan.

PT. Cangkeman Utama Kreasi adalah perusahaan yang bergerak di bidang Telekomunikasi dan Informasi. Permasalahannya adalah perusahaan ini masih menyimpan data yang berisi informasi tagihan, laporan laba rugi perusahaan yang berupa dokumen digital diarsipkan di dalam sebuah folder pada komputer tanpa adanya sistem keamanan data. Untuk mengatasi permasalahan ini, solusinya adalah dengan menerapkan pengamanan *file* menggunakan metode kriptografi yang dapat mengenkripsi isi data-data sehingga data-data tersebut menjadi lebih aman [1]. Pengamanan *file* adalah proses krusial untuk menjamin keamanan, kerahasiaan, dan mencegah kebocoran informasi perusahaan yang dapat berdampak buruk jika jatuh ke tangan pihak yang tidak berkepentingan. [2].

Kriptografi adalah bidang ilmu yang mempelajari teknik-teknik matematika terkait dengan keamanan data dan informasi, termasuk validitas data, integritas data, dan otentikasi data [3]. Secara keseluruhan, kriptografi adalah teknik pengamanan informasi yang melibatkan pengolahan informasi awal (*plaintext*) menggunakan kunci (*key*) tertentu dengan metode enkripsi tertentu, sehingga menghasilkan informasi baru yang disebut (*Ciphertext*), yang tidak dapat dibaca secara langsung [4]. *Ciphertext* tersebut dapat dikembalikan menjadi informasi awal (*plaintext*) melalui proses dekripsi [5].

Metode enkripsi dan dekripsi AES-128 (*Advanced Encryption Standard* – 128) merupakan algoritma kriptografi simetri dimana kunci yang digunakan untuk enkripsi dan dekripsi pesan [6]. Pemilihan algoritma ini didasarkan pada tingkat keamanan pertukaran informasi yang sangat baik, yakni mempunyai panjang kunci 128 bit. AES-128 menawarkan tingkat keamanan yang tinggi, karena algoritma ini termasuk di antara yang paling aman dan sulit untuk ditembus oleh serangan *brute force* atau teknik kriptanalis terbaru. Penggunaan kunci 128 bit dalam algoritma ini memberikan tingkat keamanan yang sangat kuat. AES-128 menunjukkan efisiensi dan kinerja yang baik, meskipun tingkat keamanannya tinggi. Proses enkripsi dan dekripsi berlangsung dengan cepat dan efisien, sehingga tidak memerlukan sumber daya yang berlebihan dalam penerapannya.

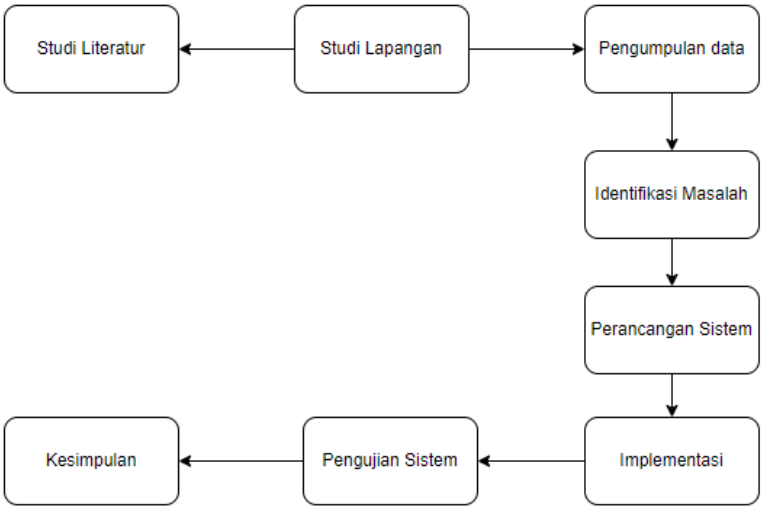
Oleh karena itu, tujuan dari penelitian ini adalah untuk menciptakan sebuah alat bantu berupa perangkat lunak yang menggunakan metode *Advanced Encryption Standard* (AES-128) guna menjaga keamanan dokumen PT. Cangkeman Utama Kreasi dari pihak yang seharusnya tidak memiliki kewenangan atas dokumen tersebut. Dalam penelitian ini, dilakukan pengujian pada *file* dokumen untuk mengevaluasi waktu respons dan mengukur perbandingan ukuran *file* sebelum dan setelah proses enkripsi.

Penelitian sebelumnya yang berjudul "Implementasi Keamanan File Menggunakan Metode Kriptografi Base-64 dan Steganografi Least Significant Bit (LSB) Random 2-Bit Berbasis Web" [7] mengeksplorasi cara mengamankan data digital dengan menggabungkan teknik kriptografi Base-64 dan steganografi LSB 2-Bit di lingkungan web. Pendekatan ini bertujuan untuk melindungi dan menyembunyikan informasi sensitif dalam format digital. Penelitian lainnya yang berjudul "Implementasi Kriptografi Pada Pengamanan Data Pembayaran Piutang Pelanggan Menggunakan Vigenere Cipher" [8] menerapkan kriptografi Vigenere untuk melindungi informasi pembayaran piutang. Maka dari itu peneliti pada penelitian ini menggunakan algoritma AES-128 untuk melindungi file penting pada PT. Cangkeman Utama Kreasi dengan penelitian yang berjudul "Pengamanan File Penting Pada Pt. Cangkeman Utama Kreasi Menggunakan Algoritma AES-128".

2. METODE PENELITIAN

2.1 *Flowchart* Penelitian

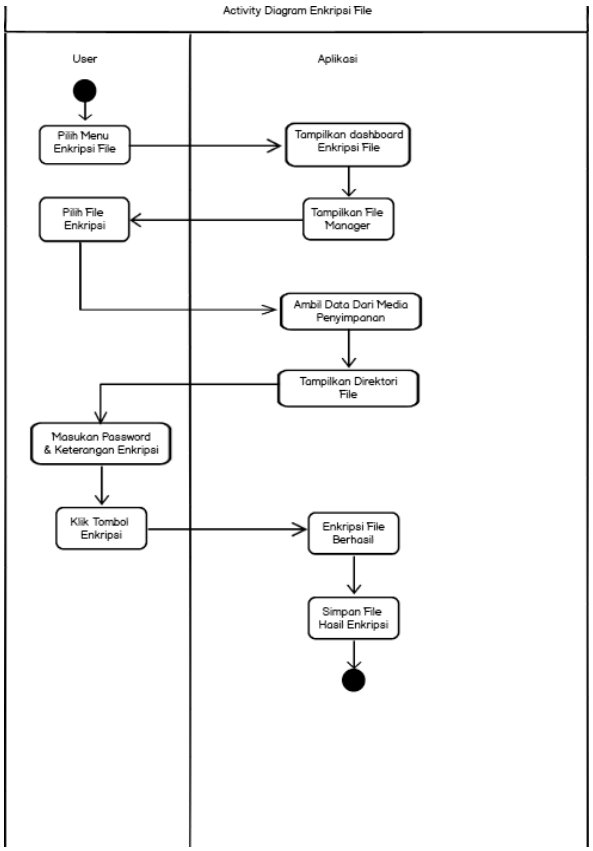
Pada tahap ini penulis melakukan penelitian dengan menggunakan metode *waterfall* dan juga sebagai pedoman agar penelitian ini mempunyai tujuan yang jelas dan tidak keluar pada jalurnya. Pada Gambar 1 berikut menunjukkan tahapan penerapan metode penelitian yang digunakan dalam penelitian ini.



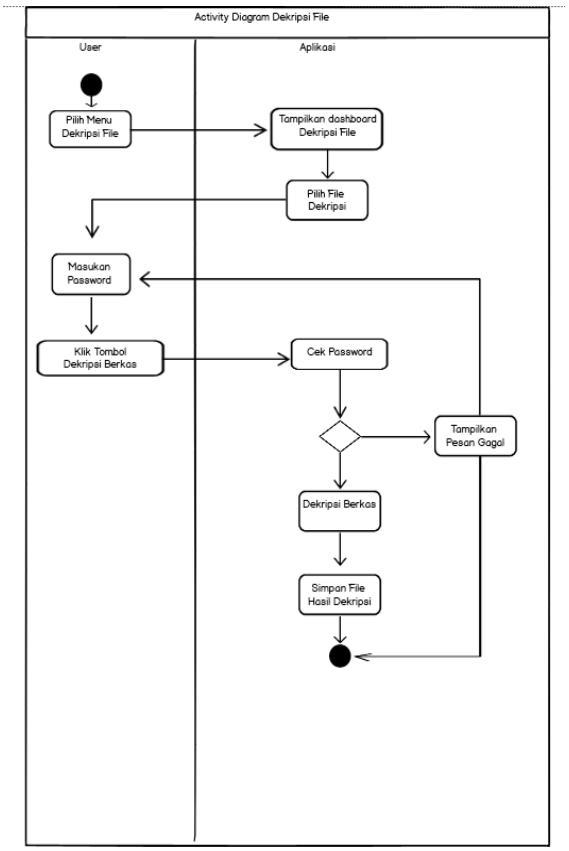
Gambar 1. *Flowchart* Penelitian

2.2 Flowchart Enkripsi *File* dan Dekripsi *File*

Flowchart digunakan untuk menggambarkan alur dari sebuah program yang dibuat. Setiap langkah atau alur dalam program tersebut digambarkan dalam bentuk diagram dan dihubungkan dengan garis. Berikut pada Gambar 2 tahapan *flowchart form* enkripsi dan pada Gambar 3 yaitu, *flowchart form* dekripsi.



Gambar 2. Activity Diagram Enkripsi AES-128



Gambar 3. Activity Diagram Dekripsi AES-128

2.3 Pengumpulan Data

Pada tahap ini, dilakukan pengumpulan data dan informasi yang relevan terkait dengan permasalahan yang ada. Proses pengumpulan data dan informasi dilakukan melalui wawancara dan observasi. Dalam wawancara ini, pertanyaan diajukan kepada pihak perusahaan yang terkait dengan pengamanan dokumen yang dilakukan oleh direktur perusahaan PT. Cangkeman Kreasi Utama. Data yang diperoleh dari wawancara digunakan sebagai percobaan untuk diproses pada aplikasi enkripsi dan dekripsi menggunakan metode AES-128 ditununjukan pada Tabel 1.

Tabel 1. Data Penelitian

Nama *File*	**Jenis *File***	**Ukuran *File***
Nib dan sertif	.docx	590 KB
Hasil Assessment	.docx	1.60 MB
Salinan data member	.xlsx	239 KB
Perjanjian program magang	.pdf	74.9 KB
Config HA 1	.txt	1.85 KB
Config HA 2	.txt	9.63 KB
Config Fix	.txt	3. 96 KB

2.4 Kriptografi

Dalam menurut istilah, kriptografi merupakan ilmu yang digunakan untuk menjaga keaslian sebuah pesan agar orang lain tidak mudah menyalahgunakan. Menurut Menezes dalam [9], kriptografi adalah sebuah ilmu yang membahas teknik matematis yang berkaitan dengan topik keamanan informasi. Para ahli kriptografi terlibat dalam mengembangkan algoritma dan metode enkripsi yang dapat mengamankan data dan menjaga kerahasiaannya. Mereka juga menganalisis keamanan sistem yang ada dan berusaha untuk meningkatkan keamanan dalam menghadapi tantangan yang terus berkembang di dunia siber. Berikut adalah unsur-unsur dalam dunia kriptografi meliputi :

a. *Plaintext* (pesan asli) adalah pesan asli yang akan dikirimkan dan dijaga keamanannya.
b. *Ciphertext* (pesan terenkripsi) adalah pesan yang sudah dilakukan pengkodean dan sudah siap untuk dikirimkan.
c. *Cipher key* (kunci) informasi rahasia yang digunakan dalam proses enkripsi dan dekripsi. Kunci ini menentukan bagaimana data diubah menjadi *Ciphertext* dan dikembalikan menjadi *plaintext*. Enkripsi (encryption) yakni tahap yang bertujuan untuk memberikan sandi *plaintext* sehingga menjadi *Ciphertext*.
d. Enkripsi (enkripsi): Adalah proses mengubah teks biasa (*plaintext*) menjadi teks yang diacak (*Ciphertext*) menggunakan kunci kriptografi tertentu.
e. Dekripsi (*decryption*) proses mengubah *Ciphertext* kembali menjadi *plaintext* menggunakan kunci yang sama yang digunakan dalam proses enkripsi.

2.5 AES- 128

AES-128 adalah singkatan dari *Advanced Encryption Standard* dengan kunci 128 bit. Ini adalah salah satu algoritma kriptografi yang paling umum digunakan untuk melindungi data dalam bidang keamanan komputer [10]. AES-128 menggunakan blok *plaintext* dengan ukuran 128 bit dan mengenkripsi data dengan menggunakan kunci 128 bit yang sama, AES-128 memiliki 10 putaran dalam tiap proses enkripsi dan dekripsinya. Algoritma ini terdiri dari serangkaian transformasi yang kompleks dan terbukti aman dalam menjaga kerahasiaan dan integritas data. AES-128 telah diterima secara luas di industri dan digunakan dalam berbagai aplikasi yang memerlukan tingkat keamanan yang tinggi.

2.6 Spesifikasi *Database*

Di bawah ini adalah struktur-struktur dari spesifikasi *database* yang digunakan dalam pembuatan aplikasi ini. Tabel 2 berisi spesifikasi *database file*, sementara Tabel 3 berisi spesifikasi *database users*.

Tabel 2. *Database File*

Nama	Tipe Data	Keterangan	Keterangan
Id_*file*	Int	11	Nama Id *File*
Username	Varchar	15	Username
*File*_name_source	Varchar	255	Nama *File* asli
*File*_name_finish	Varchar	255	Nama Hasil *File*
*File*_url	Varchar	255	Lokasi Penyimpanan
*File*_size	Float	-	Ukuran *File*
Password	Varchar	16	Password *file*
Tgl_upload	TimeStamp	-	Tanggal Upload
Status	Enum	(„1“,“2“)	Status User
Keterangan	Varchar	255	Keterangan *File*

Tabel 3. *Database users*

Nama	Tipe Data	Ukuran	Keterangan
Username	Varchar	15	Nama *Username*
Password	Varchar	100	Kata Sandi
Fullname	Varchar	50	Nama Aslo
Job_tittle	Varchar	50	Keterangan Pekerjaan
Join_date	Timestamp	-	Tanggal Mendaftar
Last_activity	Timestamp	-	Aktifitas Terakhir
Status	Enum	(„1“,“2“)	Status Pengguna

3. HASIL DAN PEMBAHASAN

3.1 Lingkungan Percobaan

Dalam implementasi aplikasi, spesifikasi perangkat yang digunakan harus mendukung fasilitas operasi kerja aplikasi sesuai dengan harapan. Beberapa spesifikasi berikut ini dapat mendukung pengoperasian sistem ini, antara lain:

a. Spesifikasi Perangkat Lunak (*Software*) yang digunakan pada aplikasi di PT. Cangkeman Utama Kreasi adalah Sistem Operasi Windows 10, XAMPP *Control Panel* v5.6.40-1, Google Chrome, MySQL dan Bahasa pemrograman PHP.
b. Spesifikasi Perangkat Keras (*Hardware*) yang dipakai untuk menjalankan program ini di PT. Cangkeman Utama Krease adalah Laptop dengan Prosesor Intel(R) Core(TM) i5-1035G1 CPU @ 1.00GHz (8 CPUs), *Memory* 8192MB, dan *Storage Solid-state 512* GB.

3.2 Perancangan Perangkat Lunak

Pada tahap ini, akan dilakukan perancangan yang sejalan dengan hasil analisis sistem, terutama perancangan untuk enkripsi dan dekripsi. Selain itu, fitur pendukung lainnya akan digabungkan dengan aplikasi, dan perancangan antarmuka akan direncanakan. Pengembangan perangkat lunak ini akan menggunakan metode *waterfall*, di mana setiap tahapan harus diselesaikan secara berurutan sebelum melanjutkan ke tahap berikutnya.

3.3 Implementasi

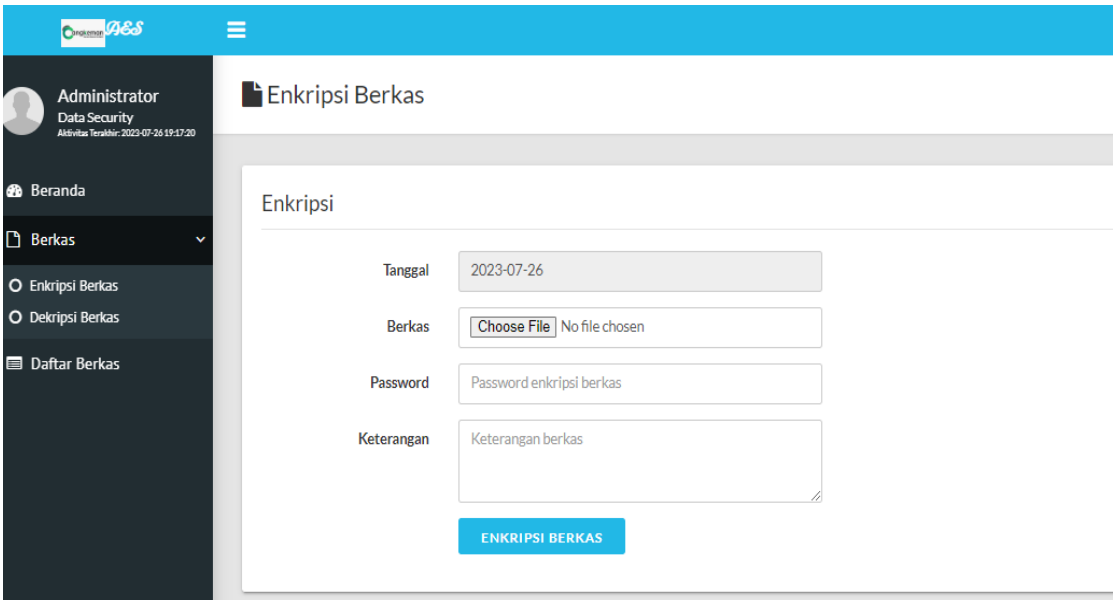
Dala fase ini Sistem akan memastikan bahwa data terenkripsi dan hanya dapat diakses oleh pihak yang berwenang dengan menggunakan kunci rahasia yang aman. Implementasi aplikasi kriptografi ini akan meningkatkan keamanan data perusahaan dan memberikan kepercayaan kepada manajemen bahwa informasi mereka terlindungi dengan baik. Sistem dibangun menggunakan bahasa pemrograman PHP serta *Database* yang digunakan adalah MySQL dan *Hardware* yang digunakan mempunyai spesifikasi Prosesor Intel Core i5, RAM 8 GB dan mempunyai kapasitas *storage* SSD 512 GB.

3.4 Pengujian Sistem

Pada tahap ini, dilakukan pengujian pada sistem yang telah dibuat untuk memastikan bahwa sistem tersebut sesuai dengan hasil analisis dan perancangan yang telah dilakukan, serta berfungsi sesuai yang diharapkan. Metode pengujian yang digunakan adalah blackbox testing, yaitu sebuah metode pengujian perangkat lunak yang menguji fungsionalitas aplikasi tanpa mengetahui struktur internalnya.

3.5 Form *Web Interface* Enkripsi

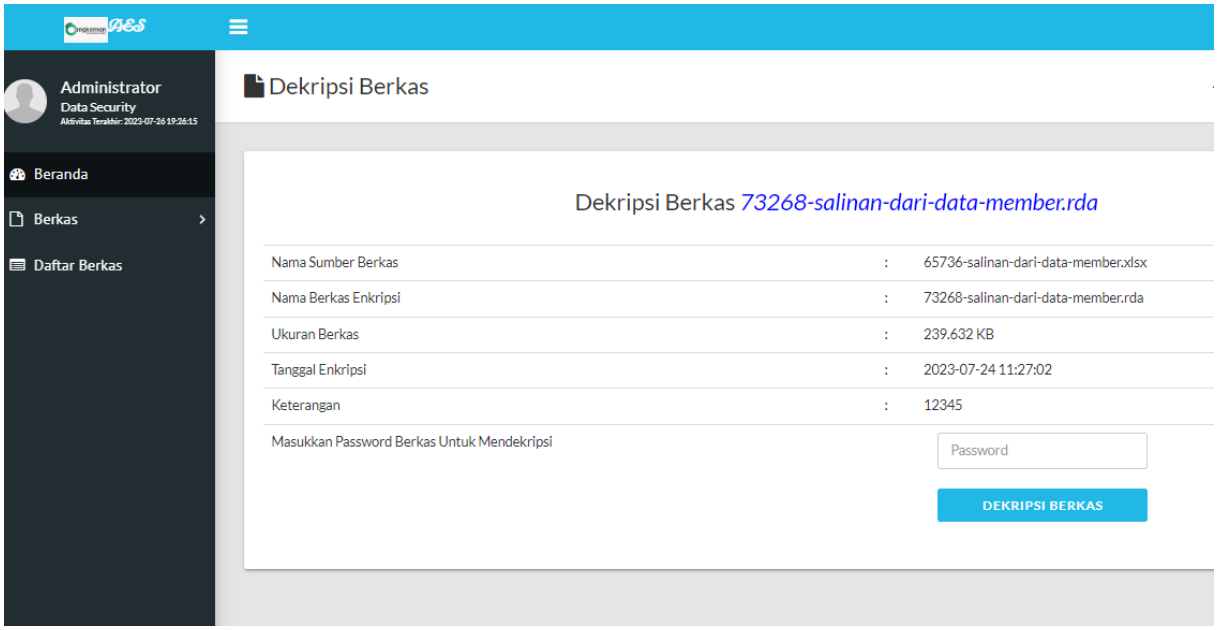
Pada Gambar 4 adalah tampilan web *interface* untuk memproses *file plaintext.* Pada proses ini tahap pertama adalah masuk ke halaman enkripsi berkas dan memilih *file* yang akan dienkripsi. Selanjutnya, pilih *file* yang ingin dienkripsi, beri sandi dan keterangan pada *file* tersebut. Setelah itu, klik tombol 'Enkripsi Berkas'. Jika berkas berhasil dienkripsi, akan muncul *pop-up* yang menampilkan pesan "Berhasil" dan waktu proses enkripsi.



Gambar 4. Tampilan Enkripsi

3.6 Form *Web Interface* Dekripsi

Pada Gambar 5 menampilkan halaman dekripsi yang digunakan untuk mendekripsi *file*. Jika pengguna mengklik tombol "Dekripsi Berkas" maka akan diarahkan ke halaman form dekripsi. Di halaman tersebut, untuk melanjutkan proses dekripsi, pengguna diminta memasukkan *password* yang sesuai dengan *password* enkripsi.



Gambar 5. Tampilan Dekripsi Berkas

3.7 Pengujian

Pada tahap ini, dilakukan pengujian pada aplikasi yang telah dibuat untuk mengetahui ukuran *file* hasil dari proses enkripsi dan dekripsi menggunakan metode *Advanced Encryption Standard* (AES-128). Tujuan pengujian ini adalah untuk memastikan apakah ukuran *file* hasil enkripsi dan dekripsi berbeda atau sama. Selain itu, juga dilakukan pengukuran waktu proses enkripsi dan dekripsi *file* untuk mengetahui berapa lama waktu yang dibutuhkan dalam kedua proses tersebut. Berikut adalah hasil dari proses enkripsi serta dekripsi yang diperoleh dari pengujian tersebut. Pada Table 4. Adalah hasil pengujian enkripsi *file*

Tabel 4. Enkripsi *File*

No	Nama *File*	Waktu	Ukuran awal	Ukuran setelah	PresentaseKenaikan	Status
1	Nib	42,00	603.810	603,824	0,2317%	BERHASIL
2	Assesment	73,00	1679,450	1679,456	0,036%	BERHASIL
3	Perjanjian magang	6,00	76,741	76,752	0,0143%	BERHASIL
4	Config HA 1	1.30	10,087	10,096	0,0891%	BERHASIL
5	Config HA 2	1.07	9,865	9,872	0,0709%	BERHASIL
6	Config Fix	00.87	4,060	4,064	0,0984%	BERHASIL

Pada table 5 adalah hasil dari dekripsi *file.*

Tabel 5. Dekripsi *File*

No	Nama *File*	Waktu (detik)	Ukuran awal (bytes)	Ukuran Setelah (bytes)	Hasil
1	Nib	42,00	603,824	603,824	Tidak Berubah
2	Assesment	78,00	1679,456	1679,456	Tidak Berubah
3	Perjanjian magang	6,00	76,752	76,752	Tidak Berubah
4	Config HA 1	0,94	10,096	10,096	Tidak Berubah
5	Config HA 2	0,87	9,872	9,872	Tidak Berubah
6	Config Fix	0.87	4,064	4,064	Tidak Berubah

4. KESIMPULAN

Kesimpulan terkait kriptografi di PT. Cangkeman Utama Kreasi bahwa implementasi aplikasi kriptografi AES-128 telah berhasil meningkatkan keamanan data secara signifikan. Penggunaan algoritma AES-128 memberikan tingkat keamanan yang tinggi dan kinerja yang optimal dalam melindungi data sensitif perusahaan. Pengujian pengamanan *file* penting dengan metode AES-128 juga membuktikan bahwa data perusahaan dapat terhindar dari akses yang tidak sah. Dengan adanya sistem kriptografi yang kuat, perusahaan kami dapat menjaga integritas dan kerahasiaan informasi bisnis, mematuhi kebijakan keamanan, dan membentuk dasar yang kokoh untuk menghadapi tantangan keamanan data di era digital. Kriptografi telah membantu memastikan bahwa informasi perusahaan aman dari potensi ancaman siber dan akses yang tidak berwenang, sehingga kami dapat menjalin kemitraan bisnis yang lebih kuat dengan pelanggan dan mitra bisnis.

DAFTAR PUSTAKA

[1] H. D. Siregar, F. S. Sulaiman, dan N. Falih, "Literatur Review Permasalahan Pengamanan Pada Database," *Semin. Nas. Mhs. Ilmu Komput. dan Apl.*, vol. 2, no. 1, hal. 521–530, 2021.

[2] N. Chafid dan H. Soffiana, "Impelementasi Algoritma Kriptografi Klasik Caesar Untuk Rancang Bangun Aplikasi E-Voting Berbasis Web (Studi Kasus : Sman 10 Tangerang)," *J. Ilm. Sains dan Teknol.*, vol. 6, no. 2, hal. 133–145, 2022, doi: 10.47080/saintek.v6i2.2249.

[3] B. Zebua, P. Herwanto, dan R. Rosida, "Penggunaan Encripsi MD5 Untuk Pencegahan SQL Injection Pada Aplikasi Berbasis Web," *Pros. Semin. Nas. Inov. dan Adopsi Teknol.*, vol. 2, no. 1, hal. 22–31, 2022, doi: 10.35969/inotek.v2i1.206.

[4] Fatonah, M. Dadang Iskandar, A. P. Heryani, dan V. Khoirunnisa, "Implementasi Metode Rivest Shamir Adleman untuk Enkripsi dan Dekripsi Text," *J. Inform. dan Teknol. Komput. (J-ICOM)*, vol. 3, no. 1, hal. 32–39, 2022, doi: 10.33059/j-icom.v3i1.4990.

[5] R. Aulia dan R. Zulfi, "Rancang Bangun Aplikasi Kriptografi Untuk Pengamanan Dokumen Menggunakan Metode Shift Cipher Sekaligus Mengkompresikannya Dengan Metode Huffman," *InfoTekJar J. Nas. Inform. dan Teknol. Jar.*, vol. 6, no. 2, hal. 200–205, 2022, doi: https://doi.org/10.30743/infotekjar.v6i2.4763.

[6] M. F. Fachrozi dan H. Fahmi, "Penerapan Metode AES-128 Untuk Pengamanan Data Absensi FingerPrint," *JIKOMSI [Jurnal Ilmu Komput. dan Sist. Informasi]*, vol. 3, no. 3, hal. 1–8, 2021.

[7] A. Aryasanti, R. Ujiandari, dan ..., "Implementasi Keamanan File Menggunakan Metode Kriptografi Base-64 dan Steganografi Least Significant Bit (LSB) Random 2-Bit Berbasis Web," *J. Ticom ...*, vol. 11, hal. 113–118, 2023,

[Daring]. Tersedia pada: https://jurnal-ticom.jakarta.aptikom.or.id/index.php/Ticom/article/view/78.

[8] R. Risna, Y. Amaliah, dan S. Yunita, "Implementasi Kriptografi Pada Pengamanan Data Pembayaran Piutang Pelanggan Menggunakan Vigenere Cipher," *Sebatik*, vol. 26, no. 2, hal. 525–534, 2022, doi: 10.46984/sebatik.v26i2.2061.

[9] F. D. Hermawati *et al.*, "Keamanan E-Voting Di Indonesia Melalui Pemanfaatan Kriptografi Pada Sistem AES (Advance Encryption Standard)," *J. Tek. Mesin, Ind. Elektro Dan Inform.*, vol. 2, no. 2, hal. 45–56, 2023.

[10] S. Oktavani, F. Rizky, dan I. Gunawan, "Analisis Keamanan Data Dengan Menggunakan Kriptografi Modern Algoritma Advance Encryption Standar (AES) JURNAL MEDIA INFORMATIKA [JUMIN]," *J. MEDIA Inform. [JUMIN]*, vol. 4, no. 2, hal. 97–101, 2023.