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

PENGAMANAN DATA ANGGOTA POLRI DENGAN AES-128 DAN BASE64 PADA PUSLITBANG POLRI BOGOR

Agung Docman Priatama[1*], Painem[2]

[1,2]Teknik Informatika, Fakultas Teknologi Informasi, Universitas Budi Luhur, Jakarta, Indonesia
Email: [1*]1911501318@student.budiluhur.ac.id, [2]painem@budiluhur.ac.id
(: corresponding author)*

Abstrak- Manfaat keamanan data menggunakan algoritme kriptografi metode AES-128 dan Base64 sangat baik dalam tingkat kemanan file agar tidak dicuri oleh pihak yang tidak berwenang. Keamanan data pada saat ini, data disimpan dalam box penyimpanan arsip dan menggunakan Microsoft Word tanpa perlindungan keamanan. Solusi pencegahan untuk mencegah potensi pencurian dan penyalahgunaan data anggota Polri adalah memastikan keamanan data tersebut, sehingga informasi tersebut tidak jatuh ke tangan yang tidak sah dan tidak digunakan untuk merugikan Puslitbang Polri.. Solusi Mengatasi masalah ini, digunakan dua metode keamanan pada *file*, yaitu AES-128 dan base64.Proses enkripsi dimulai dengan metode AES-128 dan dilanjutkan dengan base64. Namun, saat melakukan dekripsi, dilakukan secara berkebalikan, yaitu base64 terlebih dahulu, kemudian AES-128. Aplikasi ini telah diuji menggunakan metode black box dan berjalan dengan baik. Hasil penelitian menunjukkan bahwa ukuran *file* asli sebelum dienkripsi lebih kecil daripada setelah dienkripsi. Semakin besar ukuran *file* yang dienkripsi dan didekripsi, maka waktu yang dibutuhkan untuk proses tersebut juga semakin lama. Hasil akhir pengujian menunjukkan bahwa rata-rata ukuran hasil enkripsi berkisar antara 64500 byte, dengan durasi waktu 915 milidetik. Demikian pula, rata-rata ukuran hasil dekripsi berada dalam kisaran 48250 byte, dengan waktu 895 milidetik.

Kata Kunci: Kriptografi, *encryption, decryption, file, Advanced Encryption Standard* (AES-128), Base64.

SECURITY OF POLRI MEMBER DATA *FILE*S USING AES-128 AND BASE64 METHOD, PUSLITBANG POLRI BOGOR.

Abstract- *The benefits of data security using the AES-128 and Base64 cryptographic algorithms are highly effective in maintaining file security to prevent unauthorized access. Currently, data security involves storing information in archive storage boxes and utilizing Microsoft Word without security protection. A preventive solution to counter the potential risks of data theft and misuse is to ensure data security, thus preventing unauthorized access and misuse detrimental to Puslitbang Polri. To address this issue, two security methods are employed on the files, namely AES-128 and Base64. The encryption process begins with the AES-128 method and is then followed by Base64. However, during decryption, the reverse process is applied; Base64 is decoded first, followed by AES-128 decryption. The application has been thoroughly tested using a black box method and functions effectively. Research findings indicate that the original file size is smaller before encryption compared to the size post-encryption. The larger the encrypted and decrypted file size, the longer the processing time required. The final test results reveal that the average size of the encrypted output ranges around 64,500 bytes, with a processing duration of 915 milliseconds. Similarly, the average size of the decrypted output falls within the range of 48,250 bytes, with a processing time of 895 milliseconds.*

Keywords*:* Kriptografi, *encryption, decryption, file, Advanced Encryption Standard* (AES-128), Base64.

1. PENDAHULUAN

Menjaga keamanan data merupakan hal yang sangat penting, terutama bagi pengguna yang sering berbagi in*form*asi rahasia. Oleh karena itu, perlu dilakukan proses penyandian data agar tidak dapat diakses oleh pihak yang tidak berwenang. Salah satu cara untuk meningkatkan keamanan data adalah dengan menggunakan kriptografi, yaitu ilmu yang mempelajari cara menjaga keamanan pesan atau data saat dikirimkan dari pengirim ke penerima tanpa gangguan dari pihak ketiga. Salah satu teknik kriptografi yang digunakan adalah mengenkripsi pesan menjadi karakter acak yang tidak dimengerti oleh pihak yang tidak berwenang, dan untuk mendapatkan pesan asli, dilakukan proses mendeskripsi dengan kunci yang tepat.

Puslitbang Polri adalah singkatan dari Pusat Penelitian dan Pengembangan Polri yang berada di Lembaga pemerintah yaitu Polisi Republik Indonesia (POLRI). Pusat Penelitian dan Pengembangan (Puslitbang) adalah elemen penting dalam penelitian, evaluasi, dan pengembangan di tingkat Mabes Polri yang dikelola oleh Kapolri.

Tugas utama Puslitbang adalah merencanakan dan menyusun program penelitian, evaluasi, dan pengembangan, baik dalam pembinaan maupun operasional kepolisian melalui kegiatan inovatif dan rekayasa, serta melakukan pengawasan dan uji coba terhadap materiil, fasilitas, dan layanan yang digunakan oleh satuan kerja kepolisian lainnya dalam organisasi.

.Puslitbang Polri sebagai kantor Lembaga pemerintah yang memiliki data penting, salah satunya adalah data anggota kepolisian. Data anggota polisi saat ini berupa *file* word yang tersimpan dalam komputer tetapi belum ada keamanan data. Untuk meminimalisasi kebocoran data maka berdasarkan latar belakang dan permasalah diatas dibuatkan aplikasi keamanan *file* atau data dengan menggunakan metode tertentu. Salah satu aplikasi keamanan *file* yang akan dibuat pada penelitian ini adalah kriptografi dengan menggunakan metode AES-128 dan Base 64, Data Anggota tersebut hanya di simpan di komputer atau di *file* biasa tidak ada keamanan yang lebih untuk mengamankan data tersebut, sehingga rentannya kehilangan data tersebut. Data tersebut harus memiliki sistem keamanan yang baik, karena data tersebut sangatlah penting dan tidak boleh sampai hilang. Arsip data anggota Polri juga diarsipkan dengan menggunakan box pengarsipan. Puslitbang Polri tidak memiliki sistem keamanan data yang baik sekarang, sehingga bisa terjadi kebocoran data yang dilakukan oleh pihak yang tidak bertanggung jawab dan mudah di akses oleh orang lain.

Untuk mencegah dampak merugikan pada Puslitbang Polri, perlindungan data menjadi hal yang sangat penting dan harus diterapkan dengan hati-hati. Untuk menghindari kehilangan atau penyalahgunaan data, perlu adanya sistem keamanan *file* yang kuat di Puslitbang Polri. Dengan menerapkan algoritme kriptografi AES-128 dan Base64 berbasis web, dapat dipastikan bahwa data-data tersebut akan terlindungi secara aman dan terjaga dari ancaman yang mungkin timbul.

Penelitian terkait dengan kriptografi dilakukan oleh [1] menggunakan metode AES untuk mengamankan data keuangan. Sedangkan Implementasi kriptografi algoritma IDEA pada kemanan data teks berbasis android dilakukan oleh [2]. Algoritma simetris, juga dikenal sebagai algoritma kriptografi konvensional, bekerja dengan kunci yang identik untuk melakukan enkripsi dan dekripsi. Algoritma kriptografi simetris terbagi menjadi dua jenis: algoritma aliran (Stream Ciphers) dan algoritma blok (Block Ciphers)[3]. Dalam proses enkripsi dan dekripsi kriptografi dengan kunci simetris, penggunaan kunci yang identik memastikan kerahasiaan dan keamanan kunci. Keunggulan algoritma simetris termasuk penggunaan daya komputasi yang minim dan kecepatan tinggi dalam melakukan enkripsi data[4]. Berikutnya Impementasi Kriptografi pada pengamanan data pembayaran piutang pelanggan menggunakan Vigenere Cipher dilakukan oleh [5]. Dan penerapan Kriptografi untuk pengamanan data penjualan sepatu dengan metode AES*(Advanced Encryption Standard*) dilakukan oleh [6]. Kata kriptografi berasal dari bahasa Yunani "kryptos" yang berarti menyembunyikan, dan graphein yang berarti menulis. Kriptografi adalah ilmu dan seni untuk menjaga kerahasian pesan dengan cara menyandikannya ke dalam bentuk yang tidak dapat dimengerti lagi maknanya. [7]

AES (Advanced Encryption Standard) adalah sebuah metode kriptografi yang menggunakan algoritma chiper blok. Metode ini melibatkan teknik substitusi, permutasi, dan beberapa putaran pada setiap blok yang akan dienkripsi dan didekripsi[8]. Ukuran tiap jenis data akan diujikan dengan ukuran yang seragam untuk memastikan perbandingan yang objektif. Ukuran berkas yang akan diuji adalah 100 KB, 200 KB, 500 KB, 1000 KB, dan 5000 KB untuk format dokumen dan gambar. Untuk berkas audio dan video, waktu yang diukur adalah 1 menit, 2 menit, 3 menit, 4 menit, dan 5 menit. Parameter kinerja yang diambil meliputi kecepatan komputasi atau waktu yang diperlukan serta biaya enkripsi dalam hal penggunaan memori saat algoritma AES melakukan proses enkripsi dan dekripsi[9].

Pada penelitian yang yang sudah dilakukan, hampir semua penelitian hanya menggunakan satu metode saja. Sedangkan pada penelitian ini menggunakan dua metode yaitu (*Advanced Encryption Standard*) AES-128 dan Base64. Kelebihan menggunakan AES-128 dan Base64 sendiri yaitu dari segi tingkat kemanan yang yang lebih tinggi dan lebih baik jika dibandingkan dengan menggunakan satu metode, pada AES sendiri memiliki ketahanan yang kuat terhadap serangan *exhaustive key* search atau teknik dasar dari mencoba setiap kemungkinan kunci secara berturut-turut hingga kunci yang benar ditemukan sedangkan Base64 adalah untuk mengubah data biner menjadi bentuk teks agar dapat ditransmisikan secara aman melalui media yang hanya mendukung karakter teks. Jika algoritme kriptografi metode AES-128 dan Base64 tidak digunakan maka akan berakibat kehilangan dan kecurian data, seperti data anggota bisa dipalsukan orang lain bisa karena sangat bahaya. Dan berdampak sangat besar seperti kehilangannya kepercayaan terhadap keamanan data Polri. Karena ini data dari pemerintah seperti *file* data Anggota Polri.

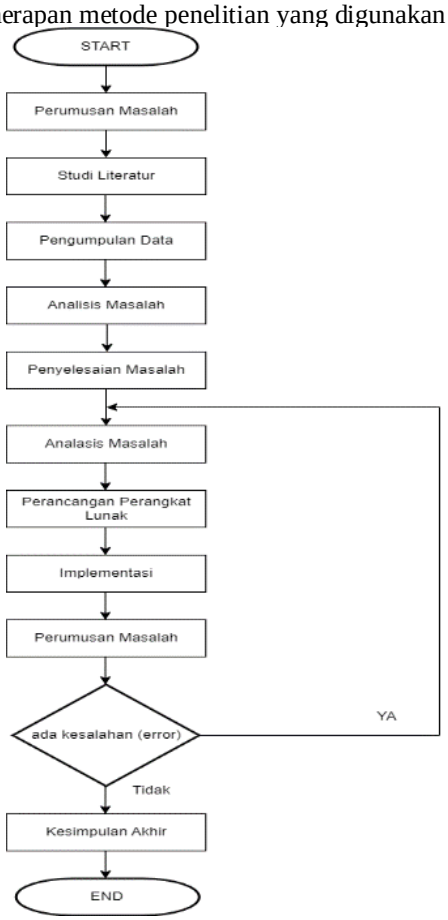
Base64 adalah metode enkode dan dekode data ke format ASCII dengan menggunakan sistem bilangan dasar 64. Ini berfungsi untuk menerjemahkan data biner menjadi teks ASCII. Base64 umumnya diterapkan dalam berbagai aplikasi seperti e-mail melalui MIME, data XML, atau untuk tujuan enkode URL[10].

Menurut [11] proses enkripsi dan dekripsinya melalui proses awal menggunakan metode Base64 terlebih dahulu dan setelahnya baru dilakukan proses menggunakan metode AES-128 dan akan menghasilnya ASCII berbentuk *ChiperText*.

kontribusi penelitian dengan alur berbeda pada penelitian ini menggunakan AES-128 terlebih dahulu, lalu proses selanjutnya Base64 yang akan menghasilkan output karakter dari hasil Base64. Kelebihan dari penelitian ini adalah pendekatan yang berbeda dalam alur proses. Proses enkripsi dan dekripsi dimulai dengan penerapan AES-128 terlebih dahulu, diikuti oleh tahap berikutnya menggunakan metode Base64, yang menghasilkan keluaran berupa karakter dari hasil Base64. Pendekatan ini memberikan kontribusi baru dalam pengolahan data keamanan dengan urutan langkah yang berlawanan, memberikan alternatif pendekatan yang lebih efektif seperti mudah dimengerti, karena file hasil enkripsi akan menjadi karakter-karakter yang mudah dimengerti.

2. METODE PENELITIAN

Pada Tahap ini berperan sebagai panduan untuk menjalankan penelitian agar hasilnya tetap sesuai dengan tujuan yang telah ditetapkan sebelumnya. Berikut adalah gambaran metode yang digunakan dalam penelitian ini. Gambar 1 menggambarkan langkah-langkah penerapan metode penelitian yang digunakan dalam penelitian ini.



Gambar 1. Metodologi Penelitian

Pada gambar 1 menampilkan proses penerapan metode penelitian yang digunakan dalam penelitian ini.

2.1 Pengumpulan Data

Pada langkah ini, data dikumpulkan sesuai dengan metode yang telah disebutkan sebelumnya. Proses pengumpulan data melibatkan wawancara dan observasi sebagai metode utama. Proses Wawancara dilakukan proses tanya jawab langsung kepada yang bersangkutan atau berhubungan pada peneletian ini agar mendapatkan informasi tentang data yang akan kami teliti. Proses Observasi digunakan untuk menghimpun atau mendapatkan informasi yang terdapat di Pusat Penelitian dan Pengembangan Kepolisian Republik Indonesia di Bogor. Tujuannya adalah untuk memperoleh penjelasan tentang data dan in*form*asi yang terkait dengan penelitian ini.

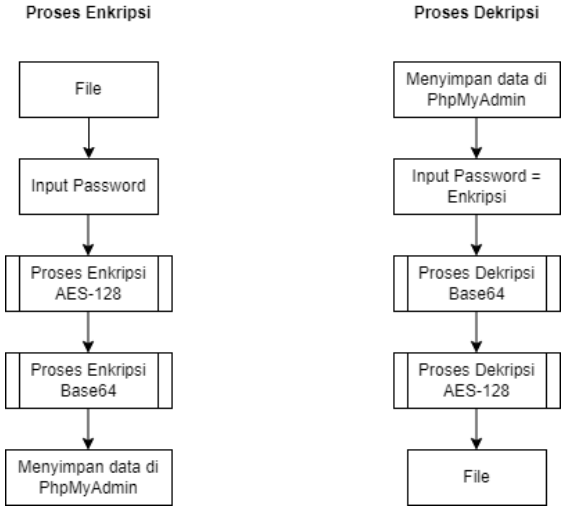
2.2 Pengujian Sistem

Dalam tahap pengujian sistem, tujuannya adalah untuk memastikan bahwa sistem yang telah dibuat sesuai dengan hasil analisis dan perancangan, serta dapat menghasilkan kesimpulan apakah sistem tersebut sesuai dengan yang diharapkan. Oleh karena itu, penting untuk menggunakan metode pengujian yang memperhitungkan ukuran

atau parameter tertentu, sehingga dapat ditarik kesimpulan tentang keberhasilan sistem. Metode pengujian yang digunakan adalah blackbox, yang fokus pada penemuan kesalahan dan demonstrasi fungsionalitas aplikasi saat dijalankan. Metode ini memeriksa apakah input diterima dengan benar dan apakah output yang dihasilkan sesuai dengan harapan. Dengan demikian, pengujian blackbox membantu memverifikasi bahwa sistem berjalan sesuai dengan tujuan yang telah ditetapkan.

2.3 Penerapan Metode AES-128 dan Base64

Pada penelitian ini untuk mengamankan *file* data Anggota Polri di Puslitbang Polri Bogor, Dengan Menggunakan Algoritme Kriptografi menggunakan metode AES-128 dan Base64. Dengan menggunakan dua metode maka untuk tingkat kemanannya lebih tinggi dibandingan dengan menggunaka satu metode saja. Karena proses pada enkripsi dan dekripsinya melalui proses dua kali, Ketika proses enkripsi maka akan melalui proses enkripsi pada AES-128 terlebih dahulu, kemudian dilanjutkan dengan metode kedua adalah Base64. Sebaliknya pada saat melakukan proses dekripsi maka melalui proses Base64 Terlebih dahulu, kemudian dilanjutkan dengan metode AES-128. Seperti pada gambar 4 menunjukan proses enkripsi dan dekripsi pada AES-128 dan Base64.



Gambar 2. Proses Enkripsi dan Dekripsi pada AES-128 dan Base64

Pada gambar 4 adalah proses enkripsi dan dekripsi menggunakan metode AES-128 dan Base64.

3. HASIL DAN PEMBAHASAN

Hasil dari penelitian ini mencakup data penelitian ini yaitu data Anggota Polri di Puslitbang Bogor, implementasi metode, dan pengujian *file* pada aplikasi menggunakan BlackBox Testing.

3.1 Data Penelitian

Data yang digunakan dalam penelitian ini merupakan data Anggota Polri dari Puslitbang Polri di Bogor, sebuah instansi pemerintahan. Dengan menerapkan algoritme kriptografi menggunakan metode AES-128 dan Base64, langkah ini bertujuan untuk mencegah dan melindungi data dari potensi kehilangan atau kecurian yang dapat disalahgunakan oleh pihak yang tidak bertanggung jawab. Data penelitian yang diperoleh dari tempat riset disajikan dalam Tabel 1 dan memiliki format yang berbeda pada *file-file* yang digunakan..

Tabel 1. Data Penelitian

No	Nama *File*	Ukuran *File*	Ekstensi
1	Data pers Kapus-Analis Puslitbang Polri	82 KB	pdf
2	Data pers Kapus-Analis Puslitbang Polri	11 KB	xlsx
3	Data pers Kapus-Analis Puslitbang Polri	85 KB	pptx
4	Data pers Kapus-Analis Puslitbang Polri	15 KB	docx

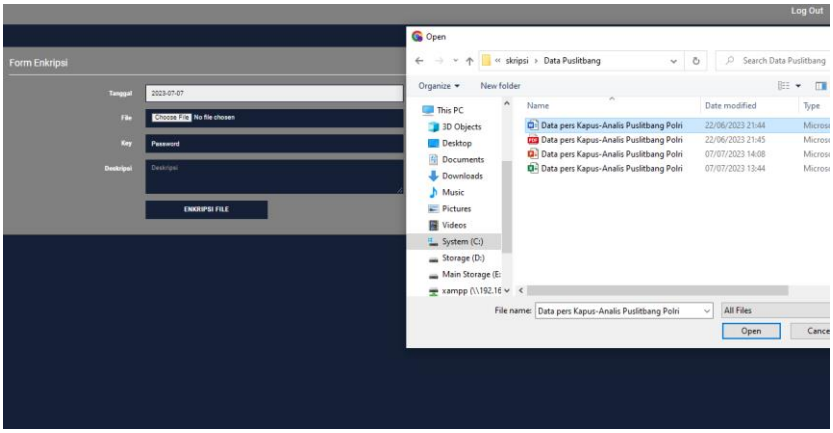
3.2 Implementasi Metode

Pada tahapan implementasi gabungan dua metode antara AES-128 dan Base64 tersebut, terdapat beberapa langkah yang perlu dilakukan, antara lain:

3.2.1 Proses Enkripsi

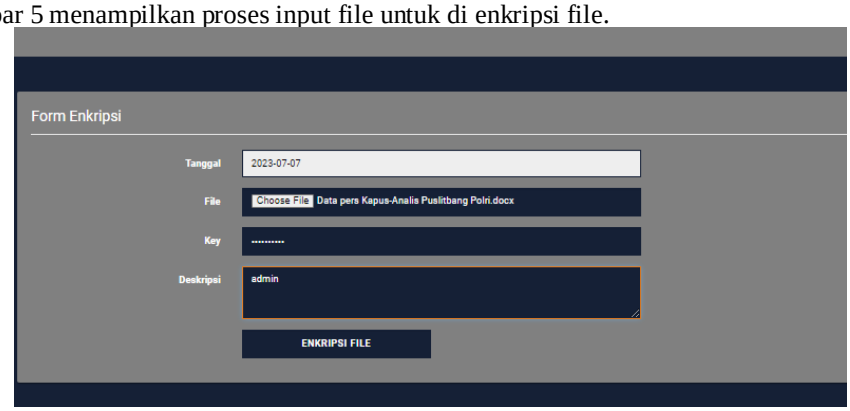
Pada proses Enkripsi pengguna memilih opsi "Enkripsi" dari menu utama aplikasi. Pengguna dapat memilih opsi ini untuk melanjutkan proses enkripsi data. Setelah memilih menu enkripsi, pengguna akan diminta untuk memilih *file* yang ingin dienkripsi. Proses pemilihan *file* bisa dilakukan dengan memilih dari direktori atau mengunggah *file* dari lokasi penyimpanan. Setelah *file* yang akan dienkripsi dipilih, langkah selanjutnya adalah memasukkan password atau kunci untuk mengamankan *file* tersebut. Pengguna diwajibkan untuk memasukkan password secara hati-hati dan disarankan menggunakan password yang kuat untuk meningkatkan keamanan *file* yang akan dienkripsi.

Setelah password dimasukkan, pengguna dapat menekan tombol "Enkripsi *File*" untuk memulai proses enkripsi. Aplikasi akan menjalankan proses enkripsi pada *file* yang dipilih dengan menggunakan gabungan dari dua metode algoritme, yaitu AES-128 dan Base64. Setelah proses enkripsi selesai, hasilnya akan ditampilkan dalam antarmuka aplikasi, mungkin melalui gambar-gambar seperti gambar 5, gambar 6, dan gambar 7.



Gambar 3. Proses Enkripsi Pemilihan *File*

Pada gambar 5 menampilkan proses input file untuk di enkripsi file.



Gambar 4. Proses Input Password Enkripsi

Pada gambar 6 menampilkan proses input password untuk proses enkripi file.

Gambar 5. *File* yang berhasil Dienkripsi

Pada gambar 7 menampilkan isi file yang sudah di enkripsi menjadi Bahasa yang tidak bisa dibaca.

3.2.2 Proses Deskripsi

Pada proses Dekripsi pengguna memilih opsi "Dekripsi" dari menu utama aplikasi. Setelah memilih menu "Dekripsi", pengguna diminta untuk memilih *file* yang akan didekripsi dari tabel dekripsi yang tersedia. Setelah *file* yang akan didekripsi dipilih, langkah selanjutnya adalah memasukkan password yang sama seperti yang digunakan saat melakukan proses enkripsi sebelumnya. Pengguna diharuskan untuk memasukkan password dengan hati-hati dan memastikan bahwa password yang dimasukkan benar agar proses dekripsi berhasil.

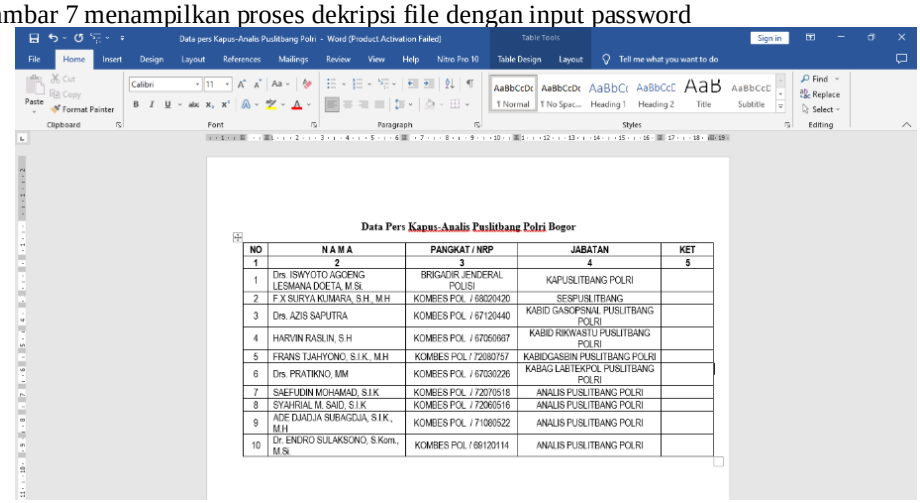
Setelah memasukkan password, pengguna dapat menekan tombol "Dekripsi *File*" untuk memulai proses dekripsi. Aplikasi akan melakukan proses dekripsi pada *file* yang dipilih dengan menggunakan kombinasi dari dua metode algoritme kriptografi, yaitu AES-128 dan Base64. Setelah proses dekripsi selesai, hasilnya akan ditampilkan dalam antarmuka aplikasi, mungkin melalui gambar-gambar seperti gambar 8, gambar 9, dan gambar 10.

Gambar 6. Dekripsi Berkas

Pada gambar 6 menampilkan form dekripsi.

Gambar 7. Proses Input Password Dekripsi

Pada gambar 7 menampilkan proses dekripsi file dengan input password



Gambar 8. Hasil Proses Dekripsi *File*

Pada gambar 8 menampilkan hasil proses dekripsi file.

3.3 Hasil Pengujian

Pada tahap ini, tabel hasil pengujian adalah hasil proses dari enkripsi *file* yang dikerjakan oleh sistem menggunakan aplikasi ini. Maka tabel berikut menunjukan hasil pengujian *file*.

Tabel 2. Hasil Pengujian *File* Proses Enkripsi

NO	Nama *File* Awal	Byte	Nama *File* Hasil Enkripsi	Byte	Kecepatan Enkripsi	Keterangan
1	Data pers Kapus-Analis Puslitbang Polri.docx	15000 Byte	13060-data-pers-kapus-analis-puslitbang-polri.rda	20000 Byte	450 Milidetik	BERHASIL
2	Data pers Kapus-Analis Puslitbang Polri.pdf	82000 Byte	63478-data-pers-kapus-analis-puslitbang-polri.rda	109000 Byte	1410 Milidetik	BERHASIL
3	Data pers Kapus-Analis Puslitbang Polri.pptx	85000 Byte	92714-data-pers-kapus-analis-puslitbang-polri.rda	114000 Byte	1590 Milidetik	BERHASIL
4	Data pers Kapus-Analis Puslitbang Polri.xlsx	11000 Byte	45207-data-pers-kapus-analis-puslitbang-polri.rda	15000 Byte	210 Milidetik	BERHASIL
	Rata-rata :	48250 Byte |		64500 Byte | 915 milidetik		

Tabel 3. Hasil Pengujian *File* Proses Dekripsi

NO	Nama *File* Enkripsi	Byte	Nama *File* Hasil Dekripsi	Byte	Status	
					Kecepatan Dekripsi	Keterangan
1	13060-data-pers-kapus-analis-puslitbang-polri.rda	20000 Byte	Data pers Kapus-Analis Puslitbang Polri.docx	15000 Byte	240 milidetik	BERHASIL
2	63478-data-pers-kapus-analis-puslitbang-polri.rda	109000 Byte	Data pers Kapus-Analis Puslitbang Polri.pdf	82000 Byte	1540 milidetik	BERHASIL
3.	92714-data-pers-kapus-analis-puslitbang-polri.rda	114000 Byte	Data pers Kapus-Analis Puslitbang Polri.pptx	85000 Byte	1590 milidetik	BERHASIL
4	45207-data-pers-kapus-analis-puslitbang-polri.rda	15000 Byte	Data pers Kapus-Analis Puslitbang Polri.xlsx	11000 Byte	210 milidetik	BERHASIL
	Rata-rata :	64500 Byte |		48250 Byte |	895 milidetik	

Hasil akhir pengujian menunjukkan bahwa rata-rata ukuran hasil enkripsi berkisar antara 64500 byte, dengan durasi waktu 915 milidetik. Demikian pula, rata-rata ukuran hasil dekripsi berada dalam kisaran 48250 byte, dengan waktu 895 milidetik.

4. KESIMPULAN

Hasil pengujian dengan metode AES -128 dan Base-64 *file* asli sebelum dilakukan proses enkripsi selalu lebih kecil dibandingkan dengan *file* yang sudah di dilakukan enkripsi. Dengan menggunakan dua metode AES-128 dan Base-64 maka pada saat melakukan proses enkripsi metode AES-128 yang akan dijalankan terlebih dahulu, kemudian dilanjutkan dengan metode kedua adalah Base-64. Sebaliknya pada saat melakukan proses dekripsi metode base-64 terlebih dahulu yang akan dijalan, kemudian dilanjutkan dengan metode AES-128. Pada saat melakukan enkripsi dan deskripsi waktu yang dibutuhkan adalah semakin besar ukuran *file* maka semakian lama proses enkrispi maupun proses dekripsi. Hasil pengujian aplikasi dengan menggunakan metode blackbox

adalah aplikasi yang dbuat sudah berjalan dengan baik. Hasil akhir pengujian menunjukkan bahwa rata-rata ukuran hasil enkripsi berkisar antara 64500 byte, dengan durasi waktu 915 milidetik. Demikian pula, rata-rata ukuran hasil dekripsi berada dalam kisaran 48250 byte, dengan waktu 895 milidetik.

Adapun saran yang dapat diberikan untuk penelitian ini yaitu Adanya inovasi baru untuk meningkatkan tingkat kemanan untuk lebih tinggi dan aman. Dikarenakan perkembangan teknologi sangat berkembang dengan cepat, maka harus ada perkembangan untuk program ini agar lebih aman. Mengimplementasikan fitur-fitur tambahan yang dapat meningkatkan keamanan pada data tersebut. Dapat lebih mempersingkat waktu untuk enkripsi dan dekripsi *file* agar lebih cepat dalam ukuran *file* yang besar.

DAFTAR PUSTAKA

[1] J. Prayudha, "Implementasi Keamanan Data Gaji Karyawan Pada Pt. Capella Medan Menggunakan Metode Advanced Encryption Standard (Aes)," Vol. 18, No. Saintikom, Pp. 119–129, 2019.

[2] J. Informasi And K. Logika, "Implementasi Kriptografi Algoritma Idea Pada Keamanan Data Teks Berbasis Android," Vol. 2, No. 1, 2021.

[3] I. Mu'alimin Arrijal, R. Efendi, And B. Susilo, "Penerapan Algoritma Kriptografi Kunci Simetris Dengan Modifikasi Vigenere Cipher Dalam Aplikasi Kriptografi Teks," 2016. [Online]. Available: Www.Ejournal.Unib.Ac.Id

[4] S. Suhandinata, R. A. Rizal, D. O. Wijaya, P. Warren, And S. Srinjiwi, "Analisis Performa Kriptografi Hybrid Algoritma Blowfish Dan Algoritma Rsa," *Jurteksi (Jurnal Teknologi Dan Sistem Informasi)*, Vol. 6, No. 1, Pp. 1–10, Dec. 2019, Doi: 10.33330/Jurteksi.V6i1.395.

[5] R. Risna, Y. Amaliah, And S. Yunita, "Implementasi Kriptografi Pada Pengamanan Data Pembayaran Piutang Pelanggan Menggunakan Vigenere Cipher," *Sebatik*, Vol. 26, No. 2, Pp. 525–534, Dec. 2022, Doi: 10.46984/Sebatik.V26i2.2061.

[6] A. Putra, R. Tarigan, P. S. Ramadhan, And K. Ibnutama, "Nomor 1, Edisi April," Vol. 5, 2023, [Online]. Available: Https://Ojs.Trigunadharma.Ac.Id/Index.Php/Jct/Index

[7] R. Munir, "Pengantar Kriptografi Bahan Kuliah If4020 Kriptografi."

[8] R. Nuari And N. Ratama, "Implementasi Algoritma Kriptografi Aes (Advanced Encryption Standard) 128 Bit Untuk Pengamanan Dokumen Shipping," 2020. [Online]. Available: Http://Openjournal.Unpam.Ac.Id/Index.Php/Joaiia

[9] R. Visdya, H. Chandra, A. Kusyanti, And M. Data, "Analisis Performa Proses Enkripsi Dan Dekripsi Menggunakan Algoritme Aes-128 Pada Berbagai Format File," 2019. [Online]. Available: Http://J-Ptiik.Ub.Ac.Id

[10] F. Musadat And J. Nur, "Aplikasi Kriptografi Keamanan Data Menggunakan Algoritma Base64," *Jurnal Informatika*, Vol. 7, No. 2, 2018, [Online]. Available: Http://Ejournal.Unidayan.Ac.Id/Index.Php/Jiu/Issue/View/10

[11] D. B. Nurcahyo And S. Amini, "Implementasi Kriptografi Dengan Algoritma Base64 Dan Advance Encryption Standard Untuk Mengamankan Data Email Berbasis Web," 2018.