

IMPLEMENTASI ALGORITMA KRIPTOGRAFI AES 128 DAN VIGENERE CIPHER PADA *COFFEE SHOP* NGOPI DENGAN APLIKASI BERBASIS WEB

Firda Nur Syahrani¹, Wahyu Pramusinto^{2*}

^{1,2}Teknik Informatika, Fakultas Teknologi Informasi, Universitas Budi Luhur, Jakarta, Indonesia

Email: ¹2011501810@student.budiluhur.ac.id, ^{2*}wahyu.pramusinto@budiluhur.ac.id
(* : corresponding author)

Abstrak- Kemajuan teknologi komputer dan telekomunikasi sekarang ini menjadi kebutuhan yang penting bagi setiap orang, tetapi dengan keuntungan tersebut ada juga dampak negatif yang muncul. Salah satu dampak *negatif* perkembangan teknologi adalah pencurian data. Dengan maraknya pencurian data tersebut sangatlah diperlukan sebuah sistem pengamanan, dalam hal ini adalah kedai kopi NgoPi. NgoPi adalah salah satu kedai kopi yang memiliki *file-file* data yang lumayan rentan untuk dimanipulasi, seperti data keuangan, data penjualan, dan lain-lain. Oleh karena itu, pada penelitian ini dibuat sebuah sistem pengamanan *file* dengan menggunakan teknik kriptografi enkripsi dekripsi agar tidak terjadi pencurian data pada *coffee shop* ini. Penggunaan algoritma *hybrid* antara *Vigenere Cipher*, *Advance Encryption Standard (AES)* dengan bit 128, serta *Hashing* menggunakan MD5 sebagai autentikasi menjadi pilihan pada penelitian ini. *Vigenere Cipher* adalah salah satu algoritma kriptografi simetris klasik, sedangkan *Advance Encryption Standard (AES)* adalah algoritma kriptografi modern dengan kunci simetris lainnya. Dengan kombinasi dua algoritma kriptografi simetris tersebut, diharapkan dapat mencapai tingkat keamanan yang optimal untuk menjaga kerahasiaan *file* pada kedai NgoPi. Selain itu, hasil penelitian ini menunjukkan bahwa sistem pengamanan *file* yang dikembangkan menggunakan kombinasi algoritma *Vigenere Cipher* dan *Advance Encryption Standard (AES)* dengan bit 128 ini menghasilkan durasi proses berdasarkan *size file* yang ingin dilakukan proses enkripsi dan dekripsi. Dimana semakin besar *size file* nya, maka semakin lama juga proses enkripsi dan dekripsi nya. Seperti contoh *file* menu.docx dengan *size* 18 kb, dapat menyelesaikan proses enkripsi dan dekripsi dengan waktu 0,49 detik. Sedangkan *file* rekap-sale-mei.xlsx dengan *size* 54 kb menyelesaikan proses enkripsi dan dekripsi dengan waktu 1,45 detik.

Kata Kunci: Kriptografi, AES-128, *Vigenere Cipher*, *File*

IMPLEMENTATION OF AES 128 AND VIGENERE CIPHER CRYPTOGRAPHIC ALGORITHMS IN NGOPI COFFEE SHOP WITH WEB-BASED APPLICATIONS

Abstract- Advances in computer and telecommunications technology are now an important necessity for everyone, but with these benefits there are also negative impacts that arise. One of the negative impacts of technological development is data theft. With the rise of data theft, a security system is needed, in this case the NgoPi coffee shop. NgoPi is one of the coffee shops that has data files that are quite vulnerable to manipulation, such as financial data, sales data, and others. Therefore, in this research, a file security system is created using decryption encryption cryptography techniques to prevent data theft in this coffee shop. The use of a hybrid algorithm between *Vigenere Cipher*, *Advance Encryption Standard (AES)* with 128 bits, and *Hashing* using MD5 as authentication is an option in this research. *Vigenere Cipher* is one of the classic symmetric cryptography algorithms, while *Advance Encryption Standard (AES)* is a modern cryptography algorithm with another symmetric key. With the combination of the two symmetric cryptography algorithms, it is expected to achieve an optimal level of security to maintain the confidentiality of files at the NgoPi shop. In addition, the results of this study show that the file security system developed using a combination of the *Vigenere Cipher* and *Advance Encryption Standard (AES)* algorithms with 128 bits produces a process duration based on the size of the file you want to encrypt and decrypt. Where the larger the file size, the longer the encryption and decryption process. For example, the menu.docx file with a size of 18 kb, can complete the encryption and decryption process in 0.49 seconds. While the rekap-sale-mei.xlsx file with a size of 54 kb completes the encryption and decryption process in 1.45 seconds.

Keywords: Cryptography, AES-128, *Vigenere Cipher*, *File*

1. PENDAHULUAN

Kemajuan teknologi komputer dan telekomunikasi sekarang ini menjadi kebutuhan yang penting bagi setiap orang, tetapi dengan keuntungan tersebut ada juga dampak *negatif* yang muncul. Salah satu dampak *negatif* dari kemajuan teknologi adalah pembajakan. Pencurian data adalah tentang berbagi informasi dan perlindungan data.

Beberapa informasi terpenting adalah informasi keuangan, keuangan, dan sensitif. Untuk itu diperlukan sebuah sistem yang mampu untuk mengamankan data sensitif tersebut.

Kriptografi adalah cara yang dapat diimplementasikan dalam menjaga keamanan data atau pesan dengan mengenkripsinya dengan enkripsi yang tidak dapat dibaca. Hanya orang yang berwenang yang dapat membaca atau mengenali formulir terenkripsi ini. Kriptografi sendiri memiliki beberapa jenis algoritma yang dapat diterapkan, seperti algoritma simetris (kunci tunggal) dan algoritma asimetris (kunci ganda).

NgoPi merupakan salah satu *coffee shop* di daerah Bintaro yang memiliki masalah dalam hal penyimpanan data salah satunya data keuangan, dimana penyimpanan data yang dilakukan hanyalah secara manual saja tanpa adanya pengamanan apapun. Pengamanan data yang minim tersebut memiliki kerentanan bagi data tersebut untuk dapat dimanipulasi ataupun dicuri oleh pihak yang tidak bertanggung jawab, seperti contoh pada awal pembukaan *coffee shop* ini terjadi manipulasi data pada *file* keuangan yang dilakukan oleh pihak yang tidak bertanggung jawab. Maka dari itu penulis bermaksud untuk membuat suatu aplikasi berbasis web untuk mengamankan *file* dokumen dengan menggunakan metode algoritma *Advanced Encryption Standard (AES-128)* dan algoritma *Vigenere Cipher*, serta dilakukan *Hashing* menggunakan MD5.

Pada Penelitian sebelumnya dengan judul “Implementasi Super Enkripsi AES dan RSA Pada Pengamanan Data Rekam Medis Pasien” [1] kombinasi 2 algoritma kriptografi digunakan untuk mengamankan data rekam medis pasien. “Implementasi Metode *Advanced Encryption Standard (AES 128 Bit)* Untuk Mengamankan Data Keuangan” [2] hanya menggunakan algoritma *Advanced Encryption Standard (AES 128 Bit)* saja. “Penerapan *Algoritme* Kriptografi RC6 Untuk Mengamankan File Penjualan Dan Gambar Produk Alisan” [3] menggunakan algoritma RC6 pada proses enkripsi dan dekripsi nya. “Penerapan Kriptografi *Caesar Cipher* dan *Vigenere Cipher* untuk Mengamankan Database Barang Belting pada PT. Multi Mitra Usaga Bersama” [4] menggunakan kombinasi *Vigenere Cipher* dan *Caesar Cipher* untuk proses algoritma nya. Maka dari itu, pada penelitian ini penulis juga menggunakan 2 kombinasi algoritma kriptografi simetris, yaitu algoritma *Advanced Encryption Standard (AES-128)* dan *Vigenere Cipher*, serta dilakukan *Hashing* menggunakan MD5. Diharapkan dengan kombinasi algoritma kriptografi ini dapat memiliki tingkat keamanan yang cukup tinggi untuk menjaga keamanan dan kerahasiaan data.

2. METODOLOGI PENELITIAN

2.1 Data Penelitian

Data yang akan digunakan dalam penelitian ini berasal dari *file* dokumen penjualan dan *file* dokumen lainnya yang ada di Ngopi. Peneliti mendapatkan data secara langsung dari *coffee shop* NgoPi tanpa menggunakan perantara, dimana data-data dibawah ini adalah dengan persetujuan langsung dari manager Ngopi kepada peneliti. Berikut adalah beberapa contoh data yang akan digunakan.

Table 1. Data Penelitian

Nama <i>file</i>	Jenis <i>file</i>	Ukuran <i>file</i>
Rekap penjualan	.xlsx	367 kb
Stok opname	.xlsx	25 kb
Resep menu	.docx	9 kb
Data lain lain	.docx	10 kb

2.2 Metode Pembandingan

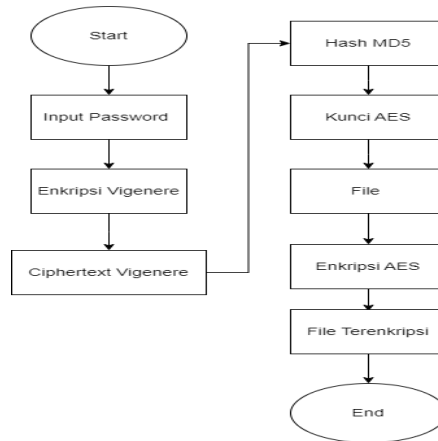
Pada metode pembandingan penelitian terdahulu dengan penelitian yang sekarang, terdapat beberapa perbedaan yang signifikan. Perbedaan dengan penelitian terdahulu terdapat pada perancangan algoritma yang digunakan, dimana pada penelitian terdahulu metode yang digunakan adalah kombinasi antara algoritma simetris dan asimetris, yaitu algoritma AES dan RSA [1]. Dengan 2 kombinasi tersebut diharapkan *file* yang akan diproses lebih bisa dienkripsi dengan aman karena prosesnya melalui dua algoritma. Dan untuk pembandingan dengan penelitian ini adalah jenis algoritma yang digunakan, yaitu algoritma AES dan *Vigenere Cipher*. Kombinasi yang dilakukan pada penelitian ini adalah antar sesama algoritma simetris.

2.3 Penerapan Metode

Teknik penerapan metode yang digunakan oleh penulis adalah kombinasi antara algoritma kriptografi *Advanced Encryption Standard (AES)* dan *Vigenere Cipher*, serta dilakukan *Hashing* menggunakan MD5. Pada kombinasi algoritma ini digunakan algoritma *Vigenere Cipher* statis [5], pemilihan *Vigenere Cipher* statis

ditujukan agar hasil program nantinya tidak membuat pengguna menjadi bingung karena harus memasukan 2 jenis kalimat, yaitu *plaintext* dan juga *key (password)*. Alasan *userfriendly* lah yang menjadi putusan penulis menggunakan *Vigenere Cipher* statis [6].

2.3.1. Proses Enkripsi

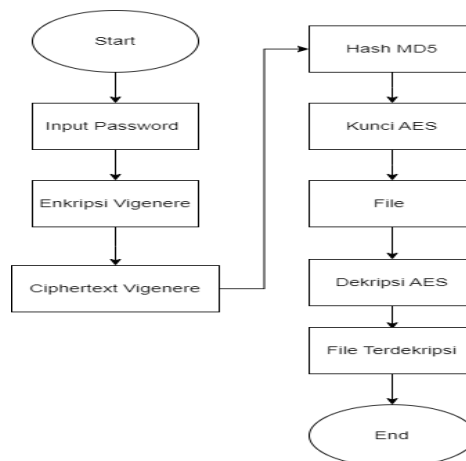


Gambar 1. Proses Enkripsi

Proses enkripsi *file* yang dilakukan pada aplikasi ini diawali dengan penginputan *password*, dimana *password* yang diinput ini akan digunakan sebagai kunci dari algoritma *Vigenere Cipher* untuk mengenkripsi *plaintext* yang terdapat pada *backend*, *plaintext* nya adalah \$text = "qwertyuiop". Lalu setelah melakukan proses enkripsi menggunakan algoritma *Vigenere Cipher*, *ciphertext* yang didapatkan akan dilakukan proses *Hashing* menggunakan MD5.

Lalu, hasil dari proses *Hashing* dengan MD5 tersebutlah yang akan dijadikan kunci algoritma *Advanced Encryption Standard (AES)* untuk mengenkripsi *file*.

2.3.2. Proses Dekripsi



Gambar 2. Proses Dekripsi

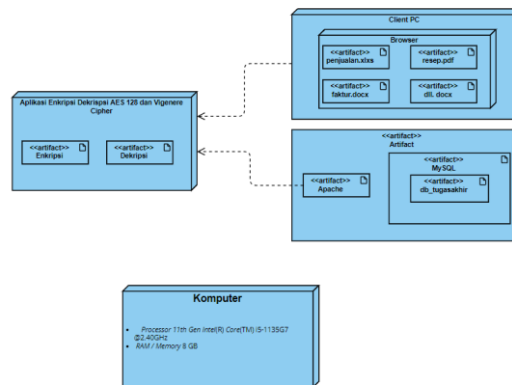
Proses dekripsi *file* yang dilakukan pada aplikasi ini diawali dengan menginputkan *password* yang sama sesuai pada saat proses enkripsi. Lalu akan dilakukan proses enkripsi *Vigenere Cipher* terhadap *plaintext* dan *key (password)* yang tadi diinputkan), setelah itu hasil *ciphertext* dari proses enkripsi *Vigenere Cipher* kan dilakukan *Hashing* menggunakan MD5.

Lalu, hasil dari proses *Hashing* menggunakan MD5 tersebut akan disamakan dengan *password* yang tersimpan pada *database*, setelah *password* nya benar maka akan dilakukan proses dekripsi dengan algoritma *Advanced Encryption Standard (AES)* pada *file* yang akan didekripsi.

3. HASIL DAN PEMBAHASAN

3.1 Lingkungan Percobaan

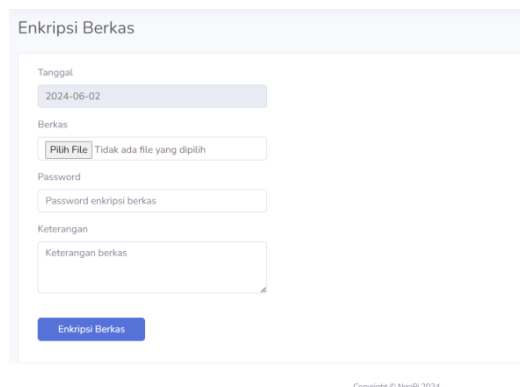
Dalam penelitian ini, lingkungan pengujian mencakup perangkat keras (*hardware*) dan perangkat lunak (*software*) yang digunakan untuk penelitian dan alat pengembangan aplikasi. Kondisi percobaan yang digunakan dalam penelitian ini adalah sebagai berikut.:



Gambar 3. Lingkungan Percobaan

3.2 Implementasi Metode

3.2.1. Proses Enkripsi



The screenshot shows a web form titled 'Enkripsi Berkas'. The form includes the following fields:

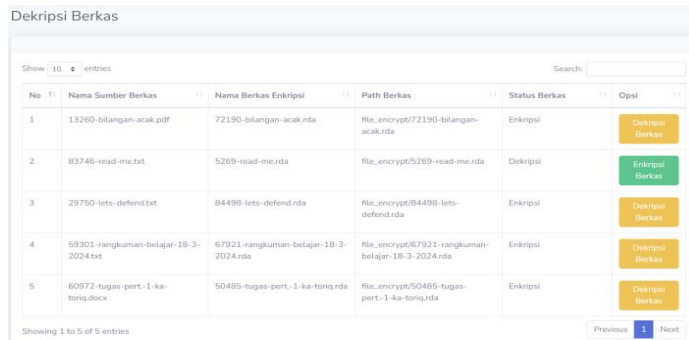
- Tanggal:** 2024-06-02
- Berkas:** A file selection area with a 'Pilih File' button and the text 'Tidak ada file yang dipilih'.
- Password:** A text input field labeled 'Password enkripsi berkas'.
- Keterangan:** A text area labeled 'Keterangan berkas'.
- Enkripsi Berkas:** A blue button to initiate the encryption process.

Gambar 4. Implementasi Metode Proses Enkripsi

Untuk memulai proses enkripsi, pengguna harus masuk ke menu *form* enkripsi yang ada di bagian sub menu berkas, kemudian pengguna hanya perlu menginput *file* dokumen yang akan dienkripsi lalu memasukan *password* dan juga keterangan pada *file* dokumen tersebut. Sebagaimana dapat dilihat pada Gambar 4.

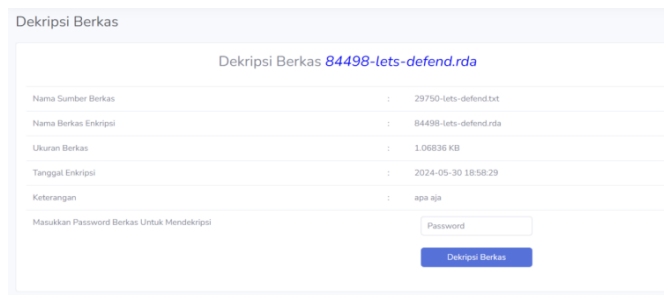
Lalu proses enkripsi akan dimulai dengan memasuki proses *Vigenere Cipher* terlebih dahulu, dimana *password* yang dimasukan oleh pengguna akan dienkripsi dengan algoritma *Vigenere Cipher*, lalu setelah mendapatkan *ciphertext* dari hasil *Vigenere Cipher* proses yang akan dilakukan selanjutnya adalah *Hashing* menggunakan MD5. Setelah mendapatkan hasil dari *Hashing* MD5, *ciphertext* tersebut akan dipotong menjadi 16 karakter untuk dijadikan sebagai *key* dalam proses enkripsi *file* dengan algoritma AES 128 dan *file* akan berhasil terenkripsi [7].

3.2.2. Proses Dekripsi



No	Nama Sumber Berkas	Nama Berkas Enkripsi	Path Berkas	Status Berkas	Opsi
1	13260-bilangan-acak.pdf	72190-bilangan-acak.rda	file_encrypt/72190-bilangan-acak.rda	Enkripsi	Dekripsi Berkas
2	83746-read-me.txt	5269-read-me.rda	file_encrypt/5269-read-me.rda	Dekripsi	Enkripsi Berkas
3	29750-lets-defend.txt	84498-lets-defend.rda	file_encrypt/84498-lets-defend.rda	Enkripsi	Dekripsi Berkas
4	59301-rangkuman-belajar-18-3-2024.txt	67921-rangkuman-belajar-18-3-2024.rda	file_encrypt/67921-rangkuman-belajar-18-3-2024.rda	Enkripsi	Dekripsi Berkas
5	60972-tugas-pert-1-ka-tonig.docx	50485-tugas-pert-1-ka-tonig.rda	file_encrypt/50485-tugas-pert-1-ka-tonig.rda	Enkripsi	Dekripsi Berkas

Gambar 5. Implementasi Metode Proses Dekripsi



Dekripsi Berkas **84498-lets-defend.rda**

Nama Sumber Berkas : 29750-lets-defend.txt
 Nama Berkas Enkripsi : 84498-lets-defend.rda
 Ukuran Berkas : 1.06836 KB
 Tanggal Enkripsi : 2024-05-30 18:58:29
 Keterangan : apa aja

Masukkan Password Berkas Untuk Mendekripsi

Password

Dekripsi Berkas

Gambar 6. Implementasi Metode Proses Dekripsi

Untuk memulai proses dekripsi, pengguna hanya perlu menuju sub menu berkas, lalu klik bagian deskripsi berkas. Selanjutnya, pengguna hanya perlu memilih *file* yang ingin didekripsi seperti pada Gambar 5. Kemudian pengguna akan diarahkan ke halaman dekripsi berkas, seperti pada Gambar 6, dihalaman tersebut pengguna akan diminta untuk memasukkan *password* untuk selanjutnya *file* tersebut akan didekripsi [8].

Lalu proses dekripsi akan dimulai dengan memasuki proses *Vigenere Cipher* terlebih dahulu, dimana *password* yang dimasukan oleh pengguna akan dienkripsi dengan algoritma *Vigenere Cipher*, lalu setelah mendapatkan *ciphertext* dari hasil *Vigenere Cipher* proses yang akan dilakukan selanjutnya adalah *Hashing* menggunakan MD5. Setelah mendapatkan hasil dari *Hashing* MD5, *ciphertext* tersebut akan dipotong menjadi 16 karakter dan akan disamakan dengan *password* yang tersimpan pada *database*, lalu selanjutnya memasuki proses dekripsi *file* dengan algoritma AES 128 dan *file* akan berhasil terdekripsi [9].

3.3 Analisa dan Pengujian

3.3.1. Tampilan Layar

Berikut adalah tampilan layar yang dimiliki oleh *website* enkripsi dan dekripsi dengan menggunakan algoritma AES 128 dan *Vigenere Cipher*.



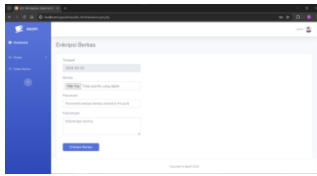
Gambar 7. Login
 Pada Gambar 7. memperlihatkan tampilan pada halaman *login* diaplikasi ini.



Gambar 8. Dashboard Admin
 Pada Gambar 10. memperlihatkan tampilan pada halaman *dashboard* admin diaplikasi ini.

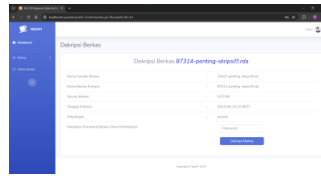


Gambar 9. Dashboard User
 Pada Gambar 10. memperlihatkan tampilan pada halaman *dashboard* *user* diaplikasi ini.



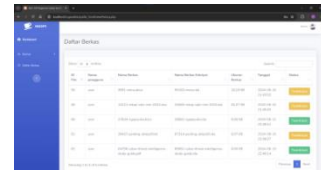
Gambar 10. Halaman Enkripsi

Pada Gambar 10. memperlihatkan tampilan pada halaman enkripsi diaplikasi ini.



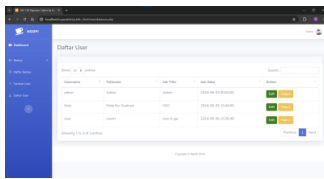
Gambar 11. Halaman Dekripsi

Pada Gambar 11. memperlihatkan tampilan pada halaman dekripsi diaplikasi ini.



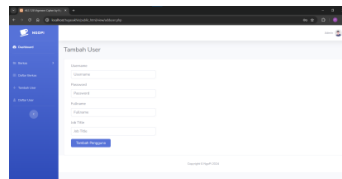
Gambar 12. Halaman Daftar Berkas

Pada Gambar 12. memperlihatkan tampilan pada halaman daftar berkas diaplikasi ini.



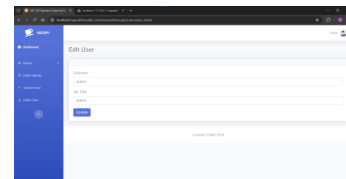
Gambar 13. Halaman Daftar User

Pada Gambar 13. memperlihatkan tampilan pada halaman daftar user diaplikasi ini.



Gambar 14. Halaman Tambah User

Pada Gambar 14. memperlihatkan tampilan pada halaman tambah user diaplikasi ini.



Gambar 15. Halaman Edit User

Pada Gambar 15. memperlihatkan tampilan pada halaman edit user diaplikasi ini.

3.3.2. Pengujian

Pengujian aplikasi ini tujuannya adalah untuk memeriksa hasil sistem *file* untuk keamanan. Pengujian enkripsi dekripsi *file* dan menjalankan kedua metode.

Table 2. Pengujian Enkripsi File

No.	Nama Asli File	Ukuran File Asli per (kb)	Nama File Setelah Di Enkripsi	Ukuran File Setelah Di Enkripsi per (kb)	Waktu per (detik)
1.	Menu.docx	18 kb	95163-menu.rda	19 kb	0.49 detik
2.	Rekap Sale-Mei 2024.xlsx	54 kb	34560-rekap-sale-mei-2024.rda	55 kb	1.45 detik
3.	Rekap stok Mei.xlsx	13 kb	9127-rekap-stok-mei.rda	14 kb	0.37 detik
4.	Sale-Item Mei 2024.xlsx	28 kb	84402-sale-item-mei--2024.rda	29 kb	0.76 detik
5.	bab 3 firda.docx	597,39 kb	79954-bab-3-firda.rda	598 kb	72.64 detik
6.	tugas akhir firda.docx	922,18 kb	18870-tugas-akhir-firda.rda	923 kb	110.52 detik

Pada tabel diatas menjelaskan hasil dari pengujian proses enkripsi *file* dengan perbandingan waktu setiap *file* yang diproses, dimana *file* yang ukurannya kecil cenderung melalui proses yang lebih singkat.

Sedangkan *file* yang ukurannya besar proses enkripsinya akan jauh lebih lambat. Sementara untuk ukuran *file* saat proses enkripsi akan berubah, yaitu bertambah menjadi 1 kb .

Table 3. Pengujian Dekripsi *File*

No.	Nama <i>File</i> Enkripsi	Ukuran Setelah Di Enkripsi per (kb)	Nama <i>File</i> Setelah Di Dekripsi	Ukuran <i>File</i> Setelah Di Dekripsi per (kb)	Waktu per (detik)
1.	95163-menu.rda	19 kb	Menu.docx	18 kb	0.48 detik
2.	34560-rekap-sale-mei-2024.rda	55 kb	Rekap Sale-Mei 2024.xlsx	54 kb	1.44 detik
3.	9127-rekap-stok-mei.rda	14 kb	Rekap stok Mei.xlsx	13 kb	0.37 detik
4.	84402-sale-item-mei--2024.rda	29 kb	Sale-Item Mei 2024.xlsx	28 kb	0.77 detik
5.	79954-bab-3-firda.rda	598 kb	bab 3 firda.docx	597,39 kb	72.64 detik
6.	18870-tugas-akhir-firda.rda	923 kb	tugas akhir firda.docx	922,18 kb	138.24 detik

Pada tabel diatas menjelaskan hasil dari pengujian proses dekripsi *file* dengan perbandingan waktu setiap *file* yang diproses, dimana *file* yang ukurannya kecil cenderung melalui proses yang lebih singkat. Sedangkan *file* yang ukurannya besar proses dekripsinya akan jauh lebih lambat. Sementara untuk ukuran *file* saat proses dekripsi akan kembali lagi seperti ukuran *file* semula aslinya [10].

4 KESIMPULAN

Berdasarkan uraian diatas dapat disimpulkan bahwa program aplikasi pengamanan *file* berbasis *web* untuk NgoPi dengan menggunakan kombinasi algoritma *Vigenere Cipher* dan *Advanced Encryption Standard (AES-128)* adalah sebagai berikut:

- Aplikasi sistem pengamanan *file* ini dibuat sebagai upaya dari tindakan pengamanan agar tidak dimanipulasi data oleh pihak yang tidak bertanggung jawab pada *coffee shop* NgoPi.
- Aplikasi ini dapat mengenkripsi *file* dengan beberapa jenis format, seperti *.doc, *.docx, *.xls, *.xlsx, *.ppt, *.pptx, dan *.pdf
- Proses enkripsi dan dekripsi tergantung pada ukuran *file* penyimpanan (semakin kecil ukuran *file* penyimpanan, semakin cepat waktu enkripsi dan dekripsi yang diperlukan untuk proses enkripsi dan dekripsi).
- File* maksimal yang dapat diproses pada aplikasi ini adalah 3MB.

DAFTAR PUSTAKA

- [1] Y. P. Putra, T. Mufizar, E. Alfiyani, and R. Medis, "Implementasi Super Enkripsi Aes Dan Rsa," no. 272, pp. 37–46.
- [2] N. Cristy and F. Riandari, "Implementasi Metode Advanced Encryption Standard (AES 128 Bit) Untuk Mengamankan Data Keuangan," *J. Ilmu Komput. dan Sist. Inf.*, vol. 4, no. 2, pp. 75–85, 2021.
- [3] B. H. Prasetyo, M. Anif, A. Saputro, D. Kusdiarto, and I. F. Akmaliah, "Penerapan Algoritme Kriptografi RC6 Untuk Mengamankan File Penjualan dan Gambar Produk Alisan," pp. 30–35.
- [4] M. Sari, H. D. Purnowo, and I. Sembiring, "Penerapan Kriptografi Caesar Cipher Dan Vigenere Cipher Untuk Mengamankan Database Barang Belting Pada Pt. Multi Mitra Usaha Bersama," *JIFOTECH J. Inf. Technol.*, vol. 2, no. 1, pp. 11–15, 2022.
- [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, 2022, doi:

- 10.46984/sebatik.v26i2.2061.
- [6] S. Vivi Wahdini, D. Hartama, I. Okta Kirana, Poningsih, and Sumarno, "Pengamanan Data Pelanggan dan Penjualan Menggunakan Implementasi Algoritma Kriptografi," *J. Informatics Manag. Inf. Technol.*, vol. 1, no. 3, pp. 101–107, 2021.
- [7] M. Fahri H Damanik, Indra Gunawan, Zulaini Masruo Nasution, Sumarno, and Ika Okta Kirana, "Pemanfaatan Algoritma Aes Untuk Keamanann Data Karyawan Pt. Telkom Indonesia Pematangsiantar," *STORAGE J. Ilm. Tek. dan Ilmu Komput.*, vol. 1, no. 1, pp. 32–37, 2022, doi: 10.55123/storage.v1i1.157.
- [8] E. Irianti, D. F. Surianto, Ainun Zahra Adistia, Muh. Juharman, and Jumadil Ahmad Safi'i, "Implementasi Kriptografi Vigenere Cipher untuk Keamanan Data Informasi Desa," *Progress. Information, Secur. Comput. Embed. Syst.*, vol. 1, no. 1, pp. 8–15, 2023, doi: 10.61255/pisces.v1i1.24.
- [9] H. Wijaya, "Jurnal Akademika Penerbit Implementasi Kriptografi Aes-128 Untuk Mengamankan Url (Uniform Resource Locator) Dari Sql Injection," *J. Akad.*, vol. 17, no. 1, pp. 8–13, 2020, [Online]. Available: <https://www.ejournal.lppmunidayan.ac.id/index.php/akd>
- [10] M. Azhari, D. I. Mulyana, F. J. Perwitosari, and F. Ali, "Implementasi Pengamanan Data pada Dokumen Menggunakan Algoritma Kriptografi Advanced Encryption Standard (AES)," *J. Pendidik. Sains dan Komput.*, vol. 2, no. 01, pp. 163–171, 2022, doi: 10.47709/jpsk.v2i01.1390.