2nd Seminar Nasional Mahasiswa Fakultas Teknologi Informasi (SENAFTI)
21 Maret 2023 – Jakarta, Indonesia
Volume 2, Nomor 1, April 2023 - ISSN 2962-8628 (*online*)

IMPLEMENTASI ALGORITME AES-128 UNTUK ENKRIPSI DAN DEKRIPSI DOKUMEN BERBASIS WEB PADA PT. BNG CONSULTING

Ahmad Riyad[1*], Gunawan Pria Utama[2], Dolly Virgian Shaka Yudha Sakti[3], Sejati Waluyo[4]

[1,2,3,4] Teknik Informatika, Fakultas Teknologi Informasi, Universitas Budi Luhur, DKI Jakarta, Indonesia

Email: [1*]ahmadriyad46@gmail.com, [2]gunawan.priautama@budiluhur.ac.id, [3]dolly.virgianshaka@budiluhur.ac.id, [4]sejati.waluyo@budiluhur.ac.id
(* : *corresponding author*)

Abstrak- Pengamanan data adalah langkah penting dalam suatu instansi atau perusahan baik swasta maupun pemerintahan untuk mencegah tindak kejahatan digital. Tingginya kasus kebocoran data pribadi di dunia digital yang disalahgunakan oleh oknum yang tidak bertanggung jawab untuk dijual. Rendahnya kualitas keamanan dari suatu *file* menjadi permasalahan yang sering terjadi. Dalam perusahaan PT BNG CONSULTING terdapat banyak data seperti, seperti laporan pajak, laporan keuangan, dan data SPT pajak. *File* yang ada belum terjaga keamanannya yang karena masih disimpan dalam folder komputer atau flash disk. Tujuan penelitian ini dengan membuat aplikasi dalam pengamanan file melalui proses perubahan terhadap isi *file* dari yang bisa dibaca menjadi tidak bisa dibaca (encryption) dan dari *file* tidak bisa dibaca kembali bisa dibaca seperti semula (decryption). Pengimplementasian aplikasi pengamanan terhadap *file* dengan menggunakan algoritme kriptografi berbasis web. Algoritme yang digunakan untuk mengamankan file menggunakan algoritme Advanced Encryption Standard (AES-128). Hasil yang didapat adalah pada saat proses enkripsi dan dekripsi *file*, *file* tidak terjadi kerusakan sebelum dan sesudah enkripsi maupun dekripsi. Metode yang digunakan dalam penelitian ini adalah *black box texting* yaitu metode untuk menemukan kesalahan dan pengujian fungsional pada aplikasi sesuai input yang diterima dengan benar dan output yang dihassilkan sesuai dengan yang diharapkan. Hasil penelitian dari menggunakan metode *black box texting* dengan data yang diuji jika pengujian tidak sesuai maka hasilnya error, dan jika sesuai hasilnya valid.

Kata Kunci: Kriptografi, Enkripsi, Dekripsi, Keamanan File, AES-128.

IMPLEMENTATION OF AES-128 ALGORITHM FOR WEB-BASED DOCUMENT ENCRYPTION AND DECRYPTION AT PT. BNG CONSULTING

Abstract- *Data security is an important step in an agency or company both private and government to prevent digital crime. High cases of personal data leakage in the digital world are being abused by irresponsible people for sale. The low security quality of a file is a frequent problem. In PT BNG CONSULTING companies there are many data such as tax reports, financial statements, and tax revenue data. Existing file have not been maintained for security because they are still stored in a computer folder or flash disk. The purpose of this study was to create an application in file security through the process of changing the contents of the file from readable to non-readable (encryption) and from readable (decryption) file. Implementation of file security applications using web-based cryptographic algorithms. The algorithm used to secure file uses the Advanced Encryption Standard (AES-128) algorithm. The result is that during the file encryption and decryption process, file do not break before and after encryption or decryption. The result obtained is that during the file encryption and decryption process, the file does not occur damage before and after encryption or decryption. The method used in this study is black box texting, which is a method for finding errors and functional testing in applications according to correctly received inputs and outputs that are incited as expected. The results of the study from using the black box texting method with seven data tested if the test is not appropriate then the results are errors, and if according to the results are valid.*

Keywords*: Cryptographic, Encryption, Decryption, File Security, AES-128.*

1. PENDAHULUAN

Pada era teknologi informasi saat ini telah mempengaruhi seluruh aspek kehidupan manusia yang dapat dengan mudah bertukar informasi dalam berbagai format tanpa batasan ruang dan waktu [1]. Oleh karena itu keamanan data sangat penting sehingga hanya orang yang berwenang yang mengetahui penyimpanan data yang bersifat rahasia [2]. Banyaknya pencurian data oleh oknum yang tidak bertanggung jawab di dunia digital disebabkan tingginya nilai jual data pribadi. Masalah lain yang mengkhawatirkan adalah rendahnya sistem keamanan untuk file-file penting yang dimiliki oleh suatu instansi/perusahan pemerintah. Oleh karena itu, keamanan data diperlukan untuk melindungi *file* rahasia [3].

Dalam proses enkripsi, pesan yang semula akan dikirim diubah atau di enkripsi dengan kunci menjadi informasi acak. Kunci ini adalah kunci yang hanya dapat diketahui oleh pengirim dan penerima. Kunci ini dapat digunakan untuk mengubah ciphertext kembali ke plaintext penerima [4].

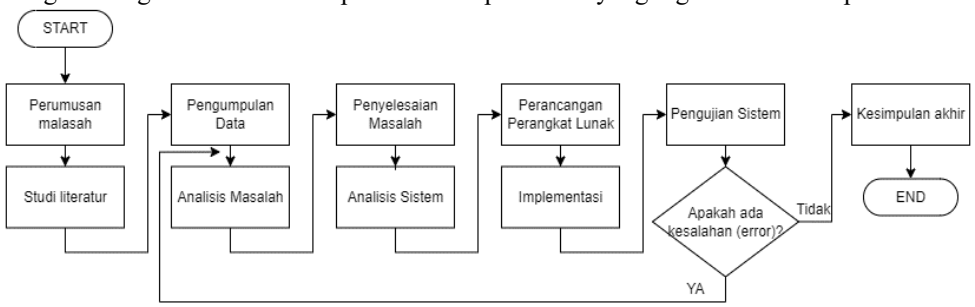
Orang internal juga berpengaruh pada kerahasiaan file-file penting tersebut, misalnya memiliki niat buruk terhadap data tersebut. Kasus pencurian data pribadi seperti dokumen elektronik, dimana pada tahun 2014 jumlah pelanggaran 1225 di tingkat penyidikan adalah 790, jadi presentasenya 64%, ditahun 2015 jumlah pelanggaran di tingkat penyidikan adalah 1569 dengan sebesar 851 dari 54% kasus, dan pada tahun 2016, jumlah total kejahatan adalah 1207, sedangkan investigasi kriminal adalah 699, dan presentasenya 57%, sehingga kasus kejahatan didunia digital Keamanan data sangat penting di masa perkembangan teknologi [5].

Tujuan berdasarkan penelitian adalah untuk mengetahui konsep kriptografi mengamankan informasi berbasis *file* menggunakan algoritme AES. Algoritme AES dipilih karena dapat mengenkripsi dan mendekripsi data dengan panjang kunci yang berbeda yaitu 128 bit, 192 bit dan 256 bit, dan perbedaan panjang kunci tersebut mempengaruhi jumlah putaran dari algoritme AES [6]. Pada tahap perencanaan aplikasi proteksi file digunakan bahasa pemrograman berbasis web PHP dengan bantuan database MySQL. Hasil implementasi dapat disimpulkan bahwa aplikasi mampu mendukung file survey yang semula dalam format clear text menjadi teks terenkripsi, dimana hasil akhirnya berupa file yang maknanya tidak dapat dibaca lagi.

Dalam penelitian lain, penelitian sebelumnya juga sudah banyak yang menggunakan algoritme Advanced Encryption Standard Penerapan Algoritme AES dan RSA. Karena menurut penelitian sebelumnya pengujian data waktu rata-rata enkripsi yang dibutuhkan RSA kurang dari 8ms, hal ini menunjukan AES membutuhkan waktu yang lebih lambat untuk melakukan sebuah enkripsi data. Uji dekripsi data proses AES lebih cepat dibandingkan dengan RSA [7]. Algoritme kriptografi simetris dibagi menjadi 2 kategori yaitu algoritme aliran (Stream Ciphers) dan algoritme blok (Block Ciphers). Pada algoritme aliran, proses penyandiannya berorientasi pada satu bit atau satu byte data. Sedang pada algoritme blok, proses penyandiannya berorientasi pada sekumpulan bit atau byte data (per blok). Contoh algoritme kunci simetris adalah DES (Data Encryption Standard), blowfish, twofish, MARS, IDEA, 3DES (DES diaplikasikan 3 kali), AES (Advanced Encryption Standard) yang bernama asli Rijndael. Enkripsi AES menggunakan proses berulang yang disebut round. Jumlah putaran yang digunakan oleh AES bergantung pada panjang kunci yang digunakan. Setiap putaran membutuhkan kunci putaran dan masukan dari putaran berikutnya. Kunci round dihasilkan berdasarkan kunci yang ditentukan[10].

2. METODE PENELITIAN

Metode penelitian ini memakai metode *waterfall* yang diawali dengan perumusan masalah penelitian, setelah itu dilakukan Penelitian dengan membaca hasil penelitian sebelumnya serta dokumen pendukung Slainnya, sehingga diperoleh hasil dibuat untuk. tidak berbeda dengan tujuan yang dicapai sebelumnya. Gambar 1 menunjukkan langkah-langkah untuk menerapkan metode penelitian yang digunakan dalam penelitian ini.



Gambar 1. Tahapan Penelitian

1. Studi Literatur

Tahapan studi literatur ini dengan melakukan *review* berbagai penelitian sebelumnya, diantaranya adalah penelitian dengan metode AES bit 128 dengan pengembangan system RAD, AES 128 dengan Teknik Steganografi *End Of File* (EOF), kombinasi AES 128 dengan RSA, AES 128 dengan memakai SQL Injection, AES 256, algoritme RC5 dan RC6. Studi ini juga dilakukan dengan menangani masalah terkait yaitu kriptografi, khususnya metode kriptografi dengan menggunakan algoritme *Advanced Encryption Standard* (AES) 128, memberikan referensi yang kuat kepada penulis untuk menentukan metode yang digunakan untuk memecahkan masalah yang diteliti.

2. Tahapan Pengumpulan Data

Wawancara (*Interview*). Proses wawancara dilakukan seperti wawancara tatap muka dan sesi tanya jawab dengan pihak kepentingan pengembangan aplikasi dan perangkat lunak untuk mengetahui tentang aplikasi dan perlindungan yang ada. Observasi (*Observation*). Pada PT.BNG *Consulting* untuk mengetahui keadaan

sebenarnya dari objek penelitian. Tujuannya adalah untuk memperoleh penjelasan tentang informasi dan data yang diperlukan untuk penelitian.

3. Analisa Sistem

a. Analisis Data

Salah satu langkah untuk mengatasi masalah keamanan ini, dalam analisis data dilakukan pengumpulan *file* yang digunakan untuk mendapatkan informasi yang diperlukan untuk merancang program. Pengumpulan *file* sesuai dengan jenisnya. Dekripsi file menentukan langkah-langkah yang digunakan untuk membuat aplikasi yang mudah dipahami.

b. Anlisa Penerapan Algoritme

Setelah langkah pengumpulan data dan monitoring pengoperasian sistem. Kemudian dibuat implementasi alias dari algoritme tersebut. Analisis aplikasi algoritme menjelaskan langkah-langkah penerapan metode enkripsi *Advanced Encryption Standard* (AES) untuk proses perlindungan data penting. Maka dilakukan:

1) Menentukan kunci yang akan digunakan untuk proses enkripsi dan dekripsi *file.*
2) Proses enkripsi file dengan kunci enkripsi, yaitu proses mengubah suatu file yang akan dienkripsi menjadi ciphertext dengan menggunakan kunci enkripsi.
3) Proses dekripsi ciphertext menggunakan kunci yang sama dengan kunci enkripsi, yaitu proses mengubah ciphertext menjadi pesan yang dapat dibaca kembali (plaintext).

c. Analisis Sistem

Keamanan yang digunakan pada sistem adalah proses enkripsi isi *file*. Enkripsi dilakukan untuk mengamankan isi *file* yang bersifat rahasia (hanya pihak berwenang yang bisa akses). Karena itu membutuhkan modul untuk melakukan enkripsi data tersebut. Modul pengenkripsian ditempatkan pada aplikasi yang akan dipanggil ketika pengguna mengamankan isi *file.* Sedangkan modul pendekripsi dipanggil ketika pengguna ingin melihat isi *file.*

4. Perancangan Perangkat Lunak

Pada tahap perancangan sesuai dengan hasil analisis sistem terutama pada perancangan enkripsi dan dekripsi. Selain itu, dukungan tambahan diintegrasikan ke dalam aplikasi dan desain antarmuka pengguna. Pengembangan sistem ini menggunakan metode waterfall, model ini harus dijalankan satu per satu secara lengkap sebelum melanjutkan ke langkah berikutnya, dan hasil dari setiap langkah harus didokumentasikan dengan baik.

5. Implementasi

Pada proses implementasi ini dilakukan pembuatan yang telah dirancang dalam tahap perancangan ke dalam Bahasa pemograman tertentu. Dalam hal ini aplikasi ini digunakan:

a) Perangkat lunak yang digunakan dalam proses penerapan pengamanan data *file* menggunakan bahasa pemograman php serta DBMS yang digunakan adalah PHPMyAdmin.
b) Perangkat keras yang digunakan Prosesor Intel Core i7, RAM 4GB DDR3, SSD 128GB.

6. Pengujian Sistem

Metode pengujian adalah *blackbox* yang digunakan untuk memeriksa kesalahan dan, saat dijalankan, fungsi aplikasi untuk mengklarifikasi apakah masukan diterima dengan benar dan apakah hasil yang dihasilkan demikian.

7. Kesimpulan

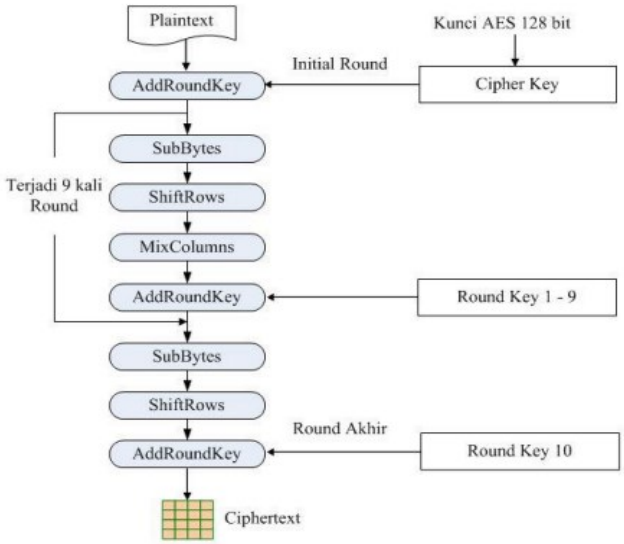
Tahapan terakhir ini di mana disimpulkan bahwa penerapan metode kriptografi *Advanced Encyption Standard* (AES) 128, berfungsi dengan baik dan dapat mengamankan *file* pada bagian *Accounting* pada PT BNG Consulting dengan aman dan pada tahapan ini ada saran untuk perkembangan pada sistem ini

2.1 *Advanced Encryption Standard*

AES adalah cipher blok simetris menggantikan algoritma DES (*Data Encryption Standard*). Algoritma AES memiliki ukuran blok tetap 128 bit dengan panjang kunci yang berbeda. Kunci AES 128 menggunakan proses pengulangan yang disebut putaran, yang melibatkan 10 lintasan pola matriks 4 x 4, setiap pola matriks terdiri dari 1 byte atau 8 bit untuk enkripsi dan dekripsi [8].

2.2 Proses Enkripsi

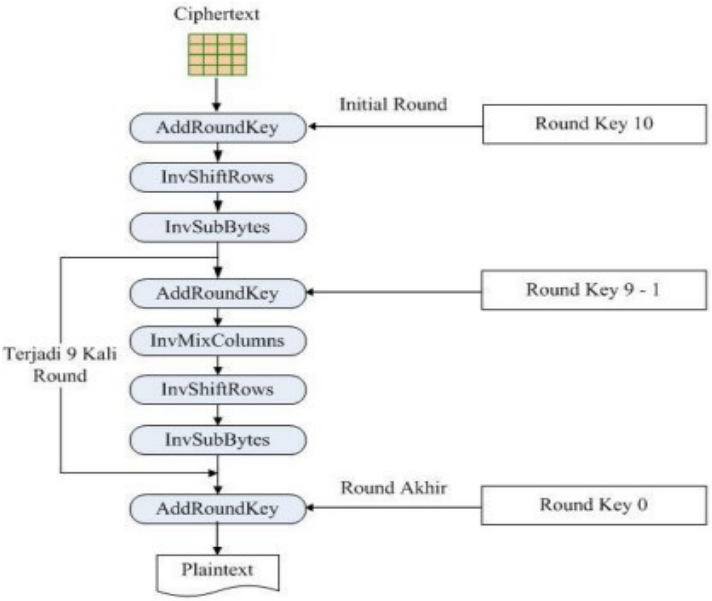
Proses enkripsi algoritma AES 128 terdiri dari empat jenis byte transformasi yaitu SubBytes, ShiftRows, MixColumns dan AddRoundKey. Pada awal proses emkripsi, state akan mengalami transformasi SubBytes, ShiftRows, MixColumns, dan AddRoundKey secara berulang sebanyak Nr (Nilai Round). Proses ini disebut *round function.* Proses enkripsi AES dilihat pada Gambar 2. Berikut:



Gambar 2. Enkripsi AES 128

2.3 Proses Dekripsi

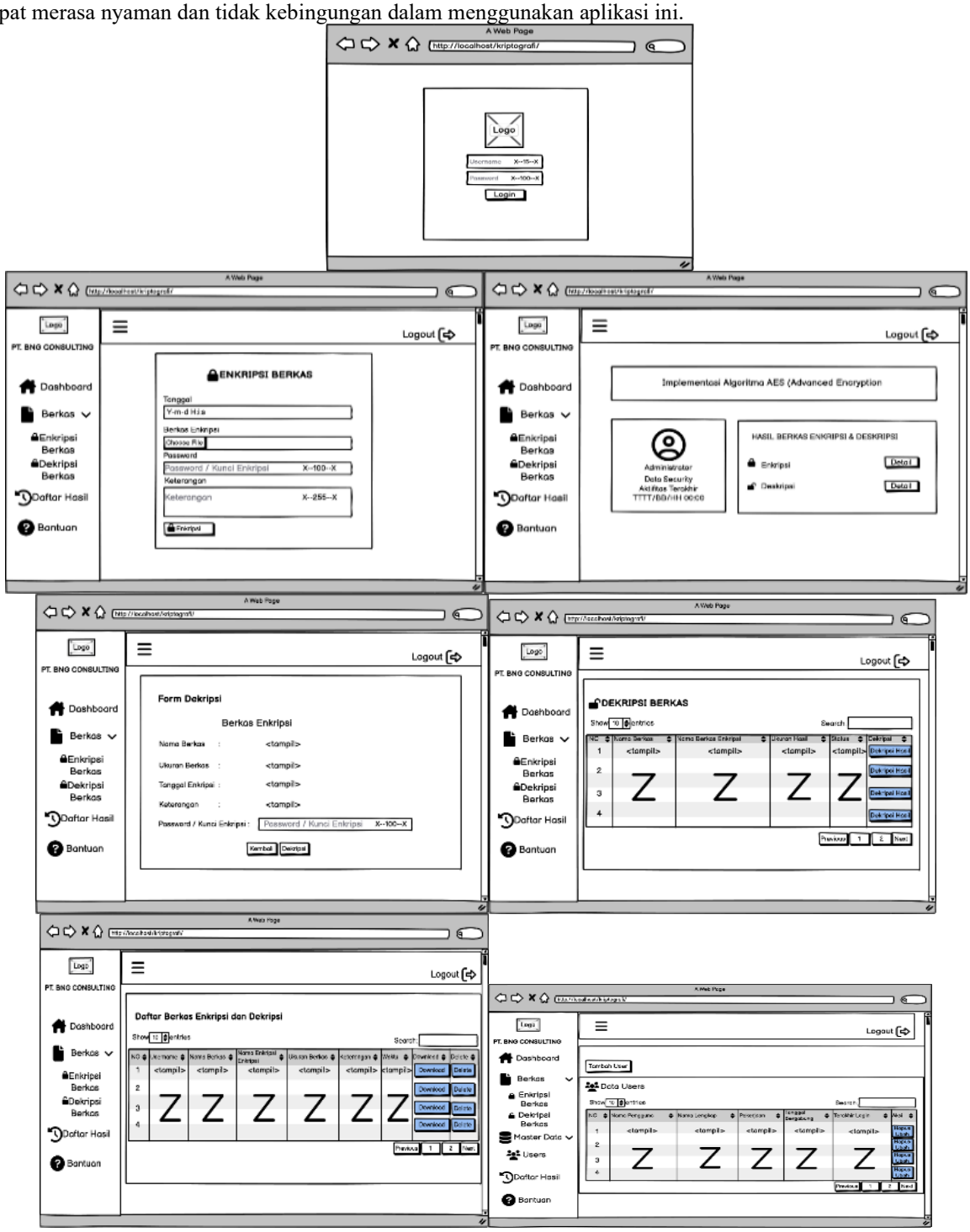
Pada proses dekripsi AES 128 Enkripsi harus dibalik untuk mendapatkan enkripsi terbalik dengan langkah-langkah berikut: InvShiftRows, InvSubBytes, InvMixColumns, dan AddRoundKey. dekripsi ditunjukkan pada Gambar 3 di bawah ini

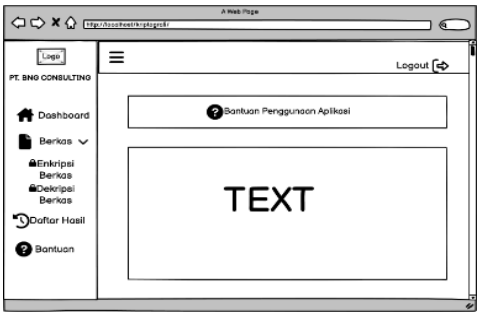


Gambar 3. Dekripsi AES 128

2.4 Rancangan Layar

Dalam pembuatan suatu aplikasi, sangat diperlukan tahap perancangan layar sebagai bentuk dasar dalam membuat desain aplikasi yang diinginkan. Rancangan layar harus mudah dimengerti, tujuannya agar pengguna dapat merasa nyaman dan tidak kebingungan dalam menggunakan aplikasi ini.





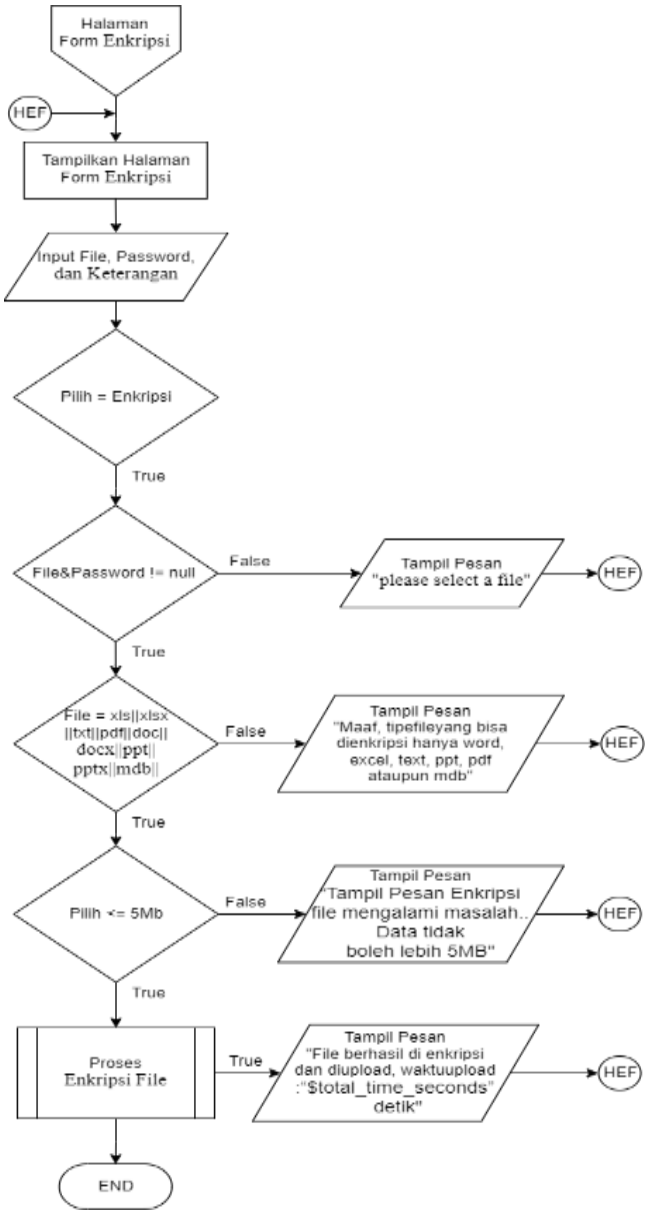
Gambar 4. Rancangan Layar

3. HASIL DAN PEMBAHASAN

Pada bagian ini adalah penjelasan dari implementasi algoritme enkripsi AES 128 untuk enkripsi dan dekripsi *file*. Bagian ini menjelaskan tentang *flowchart*, algoritme, proses dan hasil enkripsi dan dekripsi dokumen dalam sebuah aplikasi.

3.1 *Flowchart* Menu Berkas (Enkripsi)

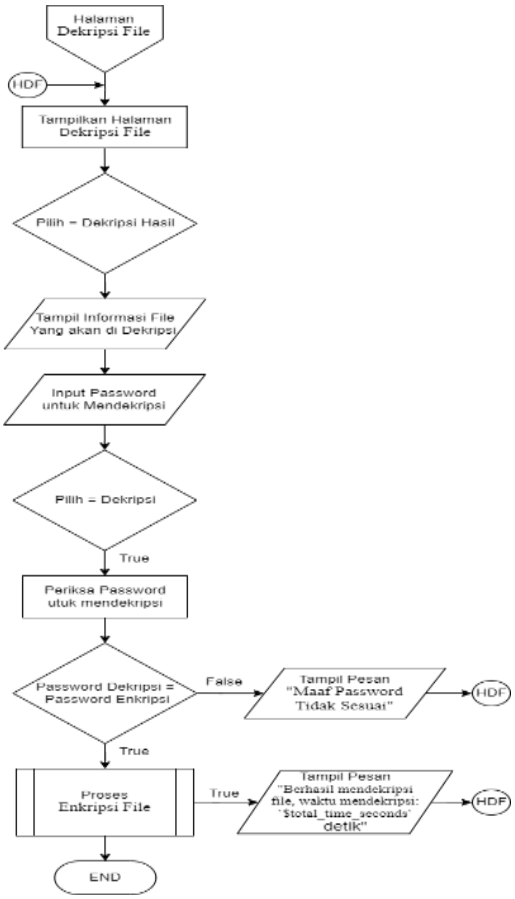
Pada Gambar 5 merupakan *flowchart* dari halaman form enkripsi, dimana *flowchart* ini menjelaskan tentang melakukan enkripsi *file*, dalam menenkripsi *file* admin dan user haru memasukkan *password*, setelah itu program akan memproses enkripsi.



Gambar 5. *Flowchart* Enkripsi

3.2 *Flowchart* Menu Berkas (Dekripsi)

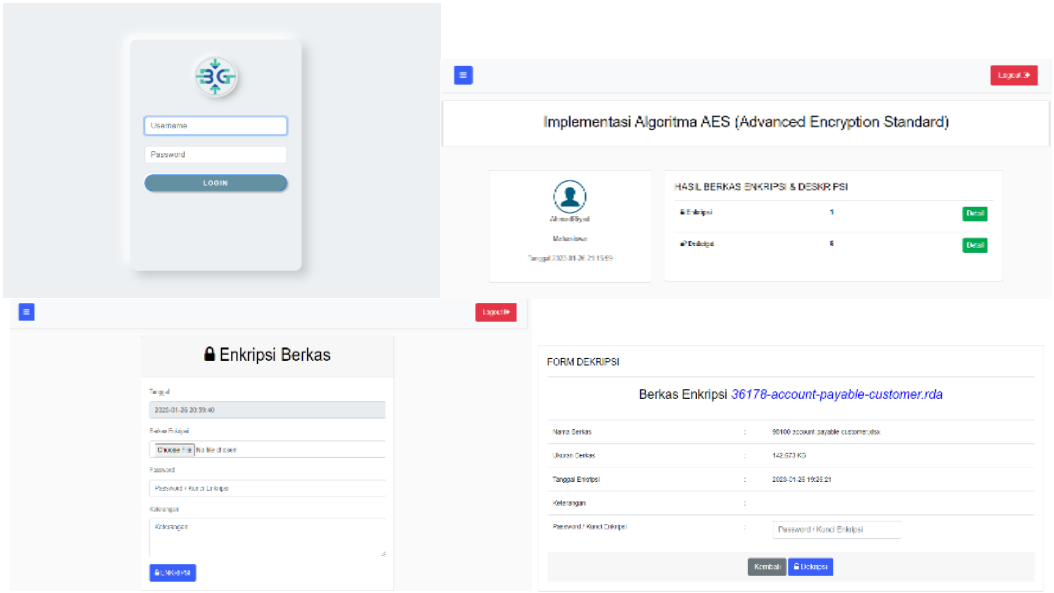
Pada Gambar 6 merupakan *flowchart* dari halaman *form* dekripsi, dimana *flowchart* ini menjelaskan tentang melakukan dekripsi *file*, dalam dekripsi *file* pengguna harus memasukkan password yang sesuai dengan password enkripsi, setelah itu program akan memproses dekripsi.



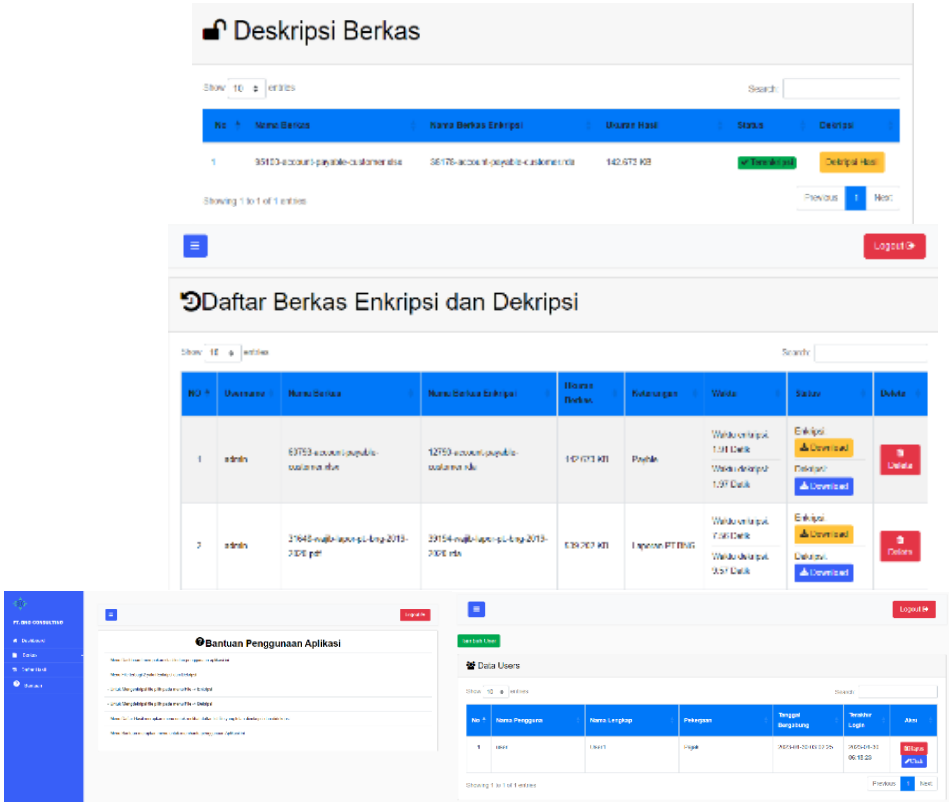
Gambar 6. *Flowchart* Dekripsi

3.3 Tampilan Layar

Pada Gambar 7 dan 8, terdapat tampilan layar aplikasi keamanan berkas. Pada Gambar 7, terdapat tampilan aplikasi login hingga enkripsi berkas, Pada Gambar 8 terdapat tampilan aplikasi untuk dekripsi berkas.



Gambar 7. Tampilan Layar Aplikasi (Login dan Proses Enkripsi Berkas)



Gambar 8. Tampilan Layar

3.4 Pengujian

Dari pengujian yang telah dilakukan terhadap sisi kecepatan dan hail enkripsi yang berupa banyak karakter dan beberapa ukuran data sebelum dan sesudah dienkripsi menggunakan algoritme kriptografi AES 128. Tabel 1 dan Tabel 2 menunjukan hasil pengujian dilakukan.

Tabel 1. Hasil Pengujian Dekripsi

No	Nama File Awal	Ukuran File	Nama File Hasil Enkripsi	Ukuran File Setalah Enkripsi	Status	
					Durasi Enkripsi	Keterangan
1	Account Payable Customer.xlsx	143 KB	12790-account-payable-customer.rda	143 KB	1.91 detik	Berhasil
2	Wajib Lapor PT. BNG 2019-2020.pdf	540 KB	39194-wajib-lapor-pt.-bng-2019-2020.rda	540 KB	7.56 detik	Berhasil
3	PPH 23 JAN - DES TAHUN 2022.xlsx	936 KB	88958-pph-23-jan---des-tahun-2022.rda	936 KB	14.48 detik	Berhasil
4	Pajak Penghasilan Pasal 24.docx	16 KB	69738-pajak-penghasilan-pasal-24.rda	16 KB	0.21 detik	Berhasil
5	PPH 21 KEPCO.mdb	1.108 KB	90163-pph-21-kepco.rda	1.108 KB	15.21 detik	Berhasil
6	Tutorial pengisian 1770 SS dengan efilling.pptx	2.569 KB	87369-tutorial-pengisian-1770-ss-dengan-efilling.rda	2.569 KB	37.62 detik	Berhasil
7	Jadwal Verifikasi Dokumen dan Pengambilan SKDP BNG Consulting.jpg	248 KB	Maaf, tipe file yang bisa dienkripsi hanya word, excel, text, ppt, pdf ataupun mdb			Gagal

Tabel 2. Hasil Pengujian Dekripsi

No	Nama File Enkripsi	Ukuran File Enkripsi	Nama File Hasil Dekripsi	Ukuran File Dekripsi	Status	
					Durasi Enkripsi	Keterangan
1	58110-account-payable-customer.rda	143 KB	31162-account-payable-customer.xlsx	143 KB	1.97 detik	Berhasil
2	39194-wajib-lapor-pt.-bng-2019-2020.rda	540 KB	31648-wajib-lapor-pt.-bng-2019-2020.pdf	540 KB	9.57 detik	Berhasil
3	88958-pph-23-jan---des-tahun-2022.rda	936 KB	40310-pph-23-jan---des-tahun-2022.xlsx	936 KB	16.57 detik	Berhasil
4	69738-pajak-penghasilan-pasal-24.rda	16 KB	13109-pajak-penghasilan-pasal-24.docx	16 KB	0.3 detik	Berhasil
5	90163-pph-21-kepco.rda	1.108 KB	58283-pph-21-kepco.mdb	1.108 KB	17.5 detik	Berhasil
6	87369-tutorial-pengisian-1770-ss-dengan-efilling.rda	2.569 KB	44825-tutorial-pengisian-1770-ss-dengan-efilling.pptx	143 KB	44.22 detik	Berhasil

4. KESIMPULAN

Kesimpulan penelitian ini adalah telah ditemukan penyebab dari kebocoran data di PT. BNG CONSULTING, yaitu cara penyimpanan data yang hanya dalam bentuk folder di komputer dan flashdisk. Pada penelitian ini telah dibuat sebuah program untuk meningkatkan keamanan data penting di PT. BNG CONSULTING dengan membuat sebuah program pengamanan data melalui proses enkripsi dan dekripsi metode kriptografi Algoritme *Advanced Encryption Standard* (AES–128). Pada penelitian selanjutnya sebaiknya melakukan pengembangan aplikasi berbasis *mobile* dengan menggunakan algoritma yang berbeda, dan dapat mengkompresi file agar durasi enkripsi dan dekripsi file lebih cepat walaupun dalam ukuran file yang besar, dan untuk perkembangan selanjutnya diharapkan mengkombinasikan 2 metode dalam aplikasi.

DAFTAR PUSTAKA

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

[2] D. Hulu, B. Nadeak, and S. Aripin, "Implementasi Algoritma AES (Advanced Encryption Standard) Untuk Keamanan File Hasil Radiologi di RSU Imelda Medan," *KOMIK (Konferensi …*, vol. 4, pp. 78–86, 2020, doi: 10.30865/komik.v4i1.2590.

[3] I. Dian Widyawan, "Pengamanan File Menggunakan Kriptografi Dengan Metode Aes-128 Berbasis Web Di Komite," vol. 4, no. 1, pp. 15–22, 2021.

[4] A. Eka Putri, A. Kartikadewi, and L. A. Abdul Rosyid, "Implementasi Kriptografi dengan Algoritma Advanced Encryption Standard (AES) 128 Bit dan Steganografi menggunakan Metode End of File (EOF) Berbasis Java Desktop pada Dinas Pendidikan Kabupaten Tangerang," *Appl. Inf. Syst. Manag.*, vol. 3, no. 2, pp. 69–78, 2021, doi: 10.15408/aism.v3i2.14722.

[5] M. Imron and A. Pratama, "Pengamanan E-Dokumen Berbasis Steganografi Dengan Kombinasi Advanced Encryption Standard (AES) 128 Bit," *InfoTekJar*, vol. 2, pp. 6–10, 2022.

[6] 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.

[7] A. Hermawan, E. Iman, H. Ujianto, T. Informasi, and U. Teknologi, "InfoTekJar : Jurnal Nasional Informatika dan Implementasi Enkripsi Data Menggunakan Kombinasi AES dan RSA," vol. 2, 2021.

[8] H. Wijaya, "Implementasi Kriptografi AES-128 Untuk Mengamankan URL (Uniform Resource Locator) dari SQL Injection," *Akad. J.*, vol. 17, no. 1, pp. 8–13, 2020.

[9] D. Pratomo, N. B. Nugroho, and R. I. Ginting, "Implementasi Kriptografi Untuk Mengamangkan Data Penjualanan di PT . Papparich Medan Menggunakan Metode AES 128," J. CyberTech, no. x, 2019.

[10] R. Toyib and A. Wijaya, "Analisis Perbandingan Algoritma Simetris Rivest Code 5 dengan Algoritma Simetris Rivest Code 6) (Studi Kasus:SMK Negeri Seluma)," J. Inform. Upgris, vol. 4, no. 2, pp. 203–209, 2019, doi: 10.26877/jiu.v4i2.2840.

[11] Yusfrizal, "Rancang Bangun Aplikasi Kriptografi Pada Teks Menggunakan Metode Reverse Chiper Dan Rsa Berbasis Android," J. Tek. Inform. Kaputama, vol. 3, no. 2, pp. 29–37, 2019.