Jurnal Unitek
Vol.17 No.2 Juli - Desember 2024
e-ISSN: 2580-2582, p-ISSN: 2089-3957

Algoritma AES 128 dalam Mengenkripsikan Berkas Bansos Kecamatan Tigabinanga Berbasis Web

Yusril Agita Prayoga Tarigan[1], Rachmat Aulia[2], Andi Marwan Elhanafi[3]
[1,2,3)] Program Studi Teknik Informatika, Universitas Harapan Medan
Jl. H.M. Jhoni No. 70 C Medan
Email: yusriltarigan@gmail.com[1], jackm4t@gmail.com[2],
andimarwanelhanafi@gmail.com[3]

ABSTRAK

Kegiatan pembagian bantuan sosial (bansos) sering dilakukan pemerintah untuk membantu warga, di Kecamatan Tigabinanga pembagian dilakukan secara rutin untuk mendukung masyarakat. Namun, seiring dengan perkembangan teknologi, data digital seringkali menghadapi risiko keamanan, termasuk kemungkinan pengubahan atau akses tidak sah oleh pihak yang tidak bertanggung jawab. Untuk mengatasi masalah ini, diperlukan metode yang efektif untuk melindungi data. Salah satu solusi yang dapat diterapkan adalah teknik kriptografi. Penelitian ini mengusulkan penggunaan Algoritma AES (Advanced Encryption Standard) 128 untuk mengenkripsi file bansos. Aplikasi berbasis web ini dikembangkan menggunakan bahasa pemrograman PHP untuk memastikan keamanan data. Dengan penerapan Algoritma AES 128, aplikasi ini dapat menjaga kerahasiaan dan integritas data bansos, mencegah kebocoran informasi, dan melindungi data dari pencurian. Proses enkripsi yang diterapkan akan menghasilkan output yang tidak dapat diakses atau dibaca oleh pihak yang tidak berwenang. Dengan menggunakan aplikasi keamanan berkas, berkas-berkas bansos yang terdapat pada kecamatan Tigabinanga akan menjadi lebih aman dan akan mengurangi terjadinya kebocoran data.

Kata kunci: *Bansos, Algoritma AES 128, PHP*

ABSTRACT

Social assistance distribution activities are often carried out by the government to help residents, in Tigabinanga District, distribution is carried out routinely to help the community. However, along with technological developments, digital data often faces security risks, including the possibility of changes or access by irresponsible parties. To overcome this problem, an effective method is needed to protect data. One solution that can be applied is cryptography techniques. This study proposes the use of the AES (Advanced Encryption Standard) 128 Algorithm to encrypt social assistance files. This web-based application is developed using the PHP programming language to ensure data security. By implementing the AES 128 Algorithm, this application can maintain the confidentiality and integrity of social assistance data, prevent information leakage, and protect data from theft. The encryption process applied will produce output that cannot be accessed or read by unauthorized parties. By using the file security application, social assistance files in Tigabinanga District will be more secure and will reduce data leakage.

Keywords: *Social assistance, Algoritma AES 128, PHP*

Jurnal Unitek
Vol.17 No.2 Juli - Desember 2024
e-ISSN: 2580-2582, p-ISSN: 2089-3957

Pendahuluan

Kecamatan Tiga Binanga, yang terletak di Kabupaten Karo, memiliki luas wilayah 160,38 km², atau sekitar 7,45 persen dari luas total kabupaten. Dengan populasi sekitar 19.476 jiwa, dan berada pada ketinggian 490-700 meter di atas permukaan laut, kecamatan ini memiliki suhu rata-rata 19 °C dan curah hujan tahunan 2500 mm, yang termasuk dalam iklim tropis (Hartati, 2019). Pada 24 Februari 2021, jumlah penduduk Tiga Binanga meningkat menjadi 20.346 jiwa dengan kepadatan penduduk 127 jiwa/km². Tingginya kepadatan penduduk dan berbagai kegiatan sosial, termasuk distribusi bantuan sosial (bansos), menambah kompleksitas dalam pengelolaan data Bansos adalah layanan publik yang diberikan kepada penduduk dan rumah tangga yang sangat miskin, terutama dengan menggunakan prinsip solidaritas vertikal karena tidak mempertimbangkan kontribusi ataupun premi dari penerima manfaat (Fadilah, 2021). Proses distribusi bansos sering menggunakan format digital seperti Microsoft Excel, Word, atau PDF, yang berisiko terhadap keamanan data, untuk melindungi data dari kebocoran atau pencurian, diperlukan solusi yang efektif. Salah satu metode yang dapat diterapkan adalah kriptografi. Kriptografi mengubah data dari format yang dapat dibaca menjadi format yang sulit dipahami untuk melindungi informasi (Pramudito & Kusumaningsih, 2018).

Berkas atau file merupakan kumpulan data yang berkaitan dengan suatu objek yang disimpan di sistem komputer. Yusfrizal (2019) menyatakan bahwa berkas berfungsi sebagai identitas dari data yang dapat diakses dan diatur oleh pengguna. Setiap berkas memiliki nama unik, atribut yang menyertai informasi tentang berkas, ukuran fisik dan logis, serta memerlukan manajemen berkas untuk pengaturan dan akses yang efisien. Kriptografi adalah teknik pengamanan informasi dengan menyandikan teks asli menggunakan algoritma tertentu untuk menghasilkan teks yang tidak dapat dibaca tanpa kunci khusus. Andrian Lesmana (2018) menjelaskan bahwa kriptografi mencakup proses enkripsi untuk mengubah teks asli menjadi ciphertext, dan dekripsi untuk mengembalikannya ke bentuk semula. Kriptografi telah digunakan sejak zaman kuno, dimulai dari bangsa Mesir dan Mesopotamia, hingga penggunaannya yang lebih kompleks pada masa Romawi dan Perang Dunia II. Sejarahnya mencakup metode klasik seperti substitusi dan transposisi, yang terus berkembang hingga era modern dengan alat dan teknik enkripsi yang lebih canggih (Pramudito & Kusumaningsih, 2018) (Azhari et al., 2022).

Algoritma AES *(Advanced Encryption Standard)* adalah metode enkripsi blok yang menggunakan panjang blok 128 bit. AES menggantikan DES *(Data Encryption Standard)* dan dikenal karena keamanannya yang lebih tinggi. Proses enkripsi dan dekripsi dalam AES melibatkan beberapa ronde transformasi, yang mencakup operasi seperti substitusi byte, pergeseran baris, pencampuran kolom, dan operasi XOR dengan kunci (Mustika, 2020).

PHP *(Hypertext Preprocessor)* adalah bahasa pemrograman yang digunakan untuk mengolah data pada server web. XAMPP adalah paket perangkat lunak yang

menggabungkan server Apache, MySQL, dan PHP untuk mempermudah pembuatan dan pengelolaan situs web dinamis (Putra & Nita, 2019).

Python adalah bahasa pemrograman berbasis objek yang dikenal karena kemudahan penggunaannya dan fleksibilitas dalam berbagai aplikasi. Sublime Text adalah editor teks yang mendukung berbagai bahasa pemrograman, termasuk PHP dan Python, serta menyediakan fitur-fitur canggih untuk meningkatkan produktivitas pengembang (Triono et al., 2023).

Penelitian ini berjudul "Algoritma AES 128 dalam Mengenkripsi Berkas Bansos pada Kecamatan Tiga Binanga Berbasis Web" bertujuan untuk mengembangkan aplikasi berbasis web dengan menggunakan Algoritma AES *(Advanced Encryption Standard)* 128 untuk mengenkripsi data bansos. Penelitian ini terinspirasi oleh penelitian sebelumnya oleh Bagas Putra Pratama dan Wasis Haryono, yang mengeksplorasi aplikasi kriptografi untuk dokumen pengarsipan menggunakan algoritma Triple DES (Pratama & Haryono, 2020), dengan menerapkan Algoritma AES 128, diharapkan aplikasi ini dapat meningkatkan keamanan data bansos dan melindungi informasi penting dari akses yang tidak sah. Penggunaan bahasa pemrograman PHP dalam pengembangan aplikasi ini bertujuan untuk memastikan perlindungan data secara efektif.

Metode Penelitian

Metode dalam penelitian ini akan melakukan beberapa tahapan yakni sebagai berikut

1. Analisis Keamanan Berkas
    1. Tampilan web menarik.
    2. Tidak terlalu sulit untuk dipahami dan digunakan.
    3. Memiliki detai file dengan lengkap.
    4. Dapat mengamankan berkas bansos dari kebocoran data.
    5. Dapat digunakan pada format docx,xls,txt,ppt,dan pdf.
    6. Dapat digunakan pada berkas hingga ukuran 3MB.

2. Analisis Kebutuhan Sistem
    1. Loptop Asus core i5
    2. Sistem Operasi Windows 11
    3. XAMPP Control Panel V 3.2.2
    4. Python
    5. Sublime Text / Visual Studio Code
    6. Browser Google Chrome
    7. Software pembuat berkas Notepad dan Microsoft Office.

3. Contoh Perhitungan AES 128

Proses Enkripsi

Contoh enkripsi yang akan berikan adalah seperti di bawah ini dengan:

PLAINTEXT: COBAALGORITMAAES
CHIPERKEY: YUSRILTARIGANAES
PLAINTEXT: 34 4F 42 41 41 4C 47 4F 52 49 54 4D 41 41 45 53
CHIPERKEY: 59 55 53 52 49 4C 54 41 52 49 47 41 4E 41 45 53

Proses selanjutnya yang akan dilakukan adalah AddRound Key yaitu dengan cara mengxorkan plainteks dengan chiperteks yang kemudian akan digunakan untuk proses enkripsi. Jika semua proses sudah dilaksalanakan maka akan mendapat hasil seperti tabel 1 round 0- 1 dibawah ini.

Tabel 1. AddRound Key proses enkripsi round 0-1

Round 0				Round 1			
59	49	52	DB	92	C0	8E	4E
55	4C	49	3B	77	3E	7F	41
53	54	47	BE	EA	AD	E8	45
52	41	41	7D	3C	7D	2E	53

Cara yang sama juga berlaku untuk round 2 -10. Hasil dari seluruh round dapat dilihat pada Tabel 2 seperti dibawah ini.

Tabel 2. AddRound Key proses enkripsi round 2-4

Round 2				Round 3				Round 4			
0B	99	59	D7	9F	06	5F	88	9F	99	C6	4E
A0	D7	E9	96	17	C0	29	BF	B2	72	5B	E4
8F	65	C8	20	A4	C1	09	29	38	F9	F0	D9
64	58	25	0B	6A	32	17	1C	AE	9C	8B	97
Round 5				Round 6				Round 7			
E6	7F	B9	F7	10	6F	D6	21	0A	65	B3	92
87	F5	AE	4A	57	A2	0C	46	1D	BF	B3	F5
B0	49	B9	60	CC	85	3C	5C	37	B2	8E	D2
81	1D	96	01	E9	F4	62	63	14	E0	82	E1
Round 8				Round 9				Round 10			
6C	09	BA	28	A6	AF	15	3D	39	96	83	BE
A8	17	A4	51	55	42	E6	B7	29	6B	8D	3A
CF	7D	F3	21	AE	D3	20	01	38	EB	CB	CA

5B	BB	39	D8	6F	D4	ED	35	48	9C	71	44

Dari hasil enkripsi aes 128 di atas maka akan mendapatkan hasil seperti di bawah ini.

Hex : B2E8EB3B6BB2132BAC3F96AAFD5E412B
Chiper Text : sujrO2uyEyusP5aq/V5BKw==

Proses Deskripsi

Contoh deskripsi yang akan diberikan adalah seperti di bawah ini dengan:

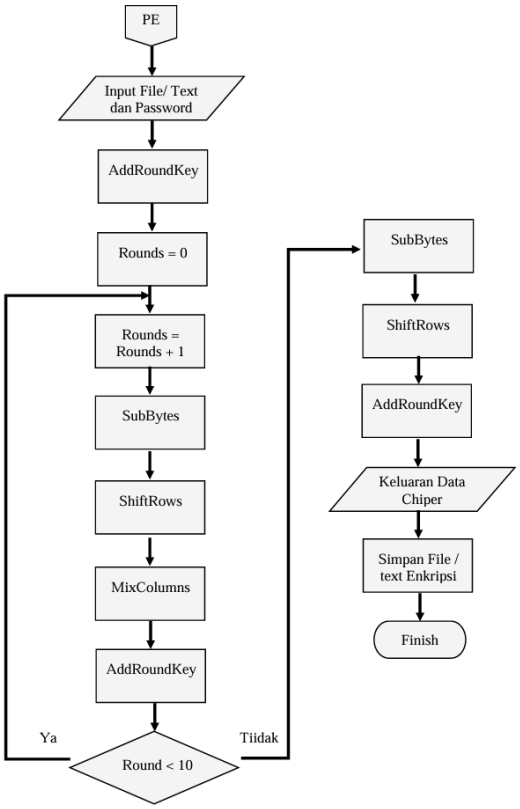
Chipertext : B2 E8 EB 3B 6B B2 13 2B AC 3F 96 AA FD 5E 41 2B
Roundkey 10 : 39 29 38 48 96 6B EB 9C 83 8D CBB 71 BE 3A CA 44
Jadi hasil = B2 E8 EB 3B 6B B2 13 2B AC 3F 96 AA FD 5E 41 2B

Round key 10 akan digunakan untuk round pertama di dalam deskripsi, pada proses deskripsi prosesnya akan di balik. Round 1 dalam deskripsi akan menggunakan roundkey ke 9 untuk round 2 menggunakan roundkey ke 8 sampai round ke 10 menggunakan roundkey ke 1.

Hex : 43 4F 42 41 41 4C 47 4F 52 49 54 4D 41 41 45 53
Plain Text : COBAALGORITMAAES

Flowchart dari proses kegiatan enkripsi AES 128 dapat dilihat pada gambar 1 berikut

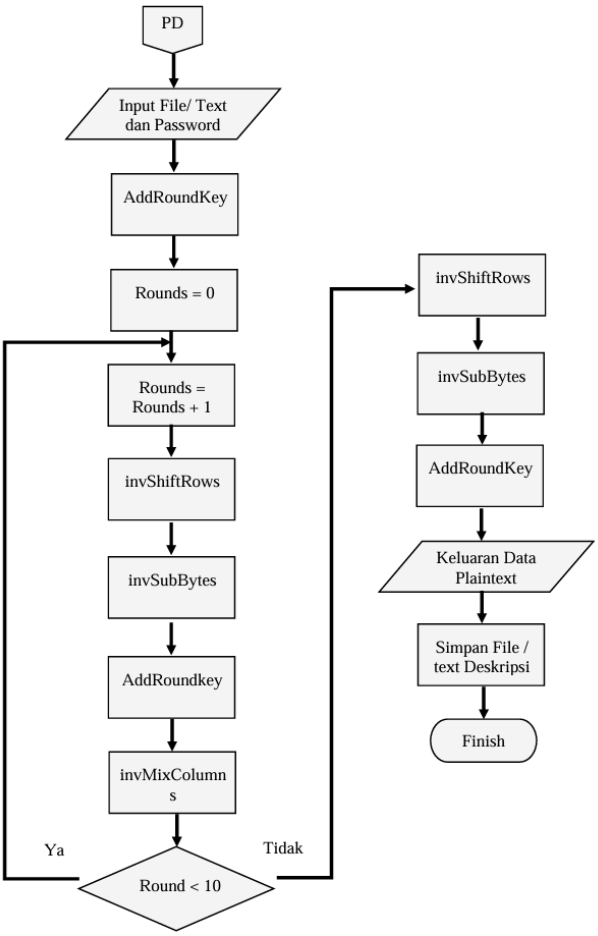
Flowchart Proses Enkripsi AES 128



Gambar 1. Proses Enkripsi AES 128

Flowchart dari proses kegiatan enkripsi AES 128 dapat dilihat pada gambar 2 berikut

Flowchart Proses Deskripsi AES 128



Gambar 2. Proses Deskripsi AES 128

4. Desain Sistem

Bentuk desain sistem yang penulis buat menggunakan beberapa bentuk diagram dari Unified Modeling Language yaitu Use Cace Diagram, Activity Diagram danSequence.

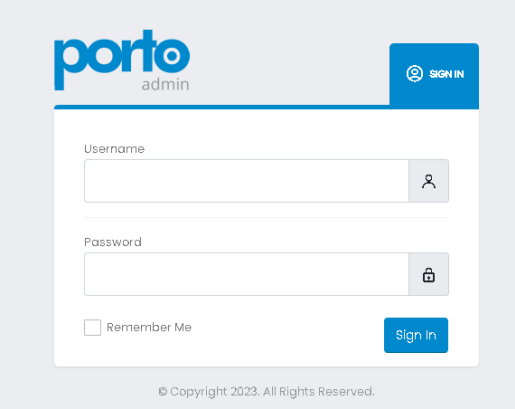
5. Perancangan Interface

Perancangan interface merupakan perancangan untuk melihat desain awal dari sebuah system. Berikut adalah perancangan system interface dari perancangan aplikasi.

Hasil dan Pembahasan

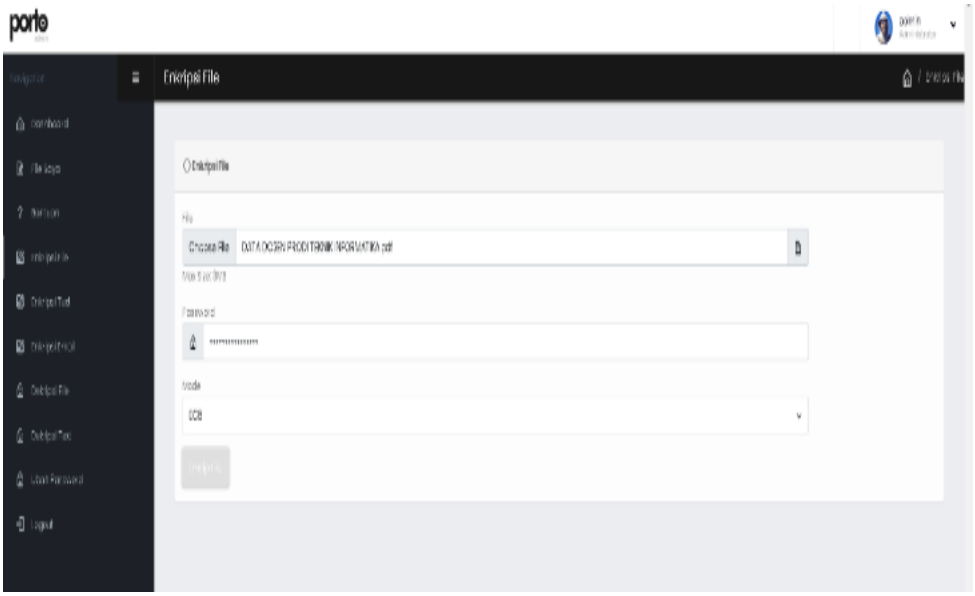
Hasil dari rancangan optimasi algoritma aes 128 dalam mengenkripsikan berkas bansos pada kecamatan Tigabinanga berbasis web.

1. Tampilan Login
   Tampilan login digunakan untuk masuk pada aplikasi yang menggunakan akun admin. seperti pada Gambar 3 di bawah ini.



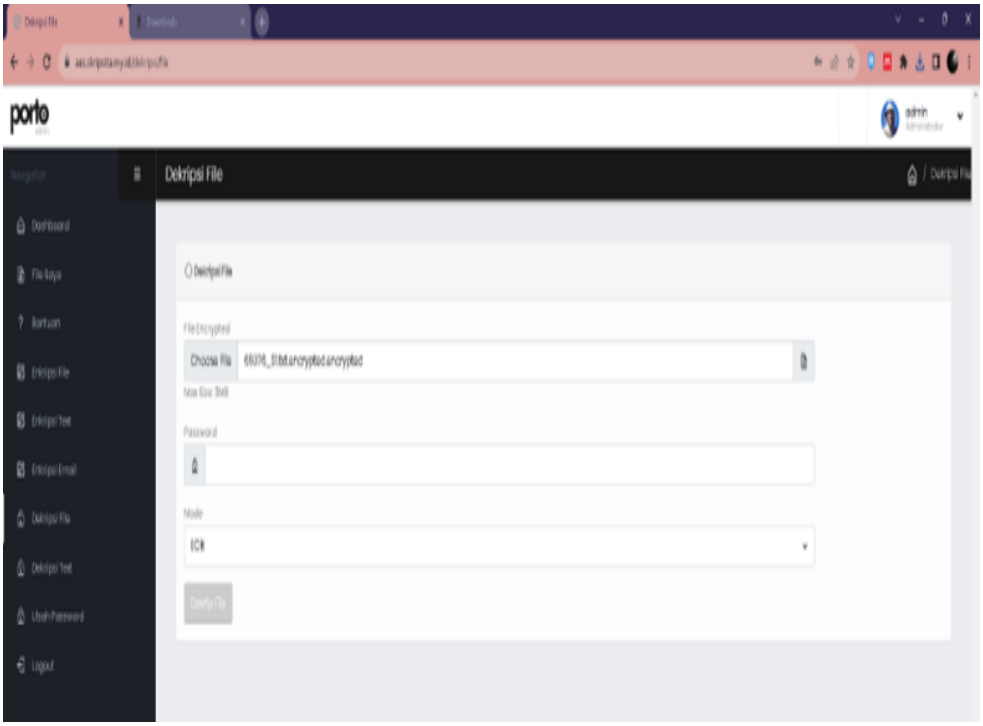
Gambar 3. Tampilan Login

2. Tampilan Enkripsi Berkas
   Menu ini merupakan menu yang berfungsi untuk mengenkripsikan dengan cara mengambil berkas dari komputer dan memasukkan *password*. Seperti pada Gambar 4 di bawah ini.



Gambar 4. Tampilan Enkripsi Berkas

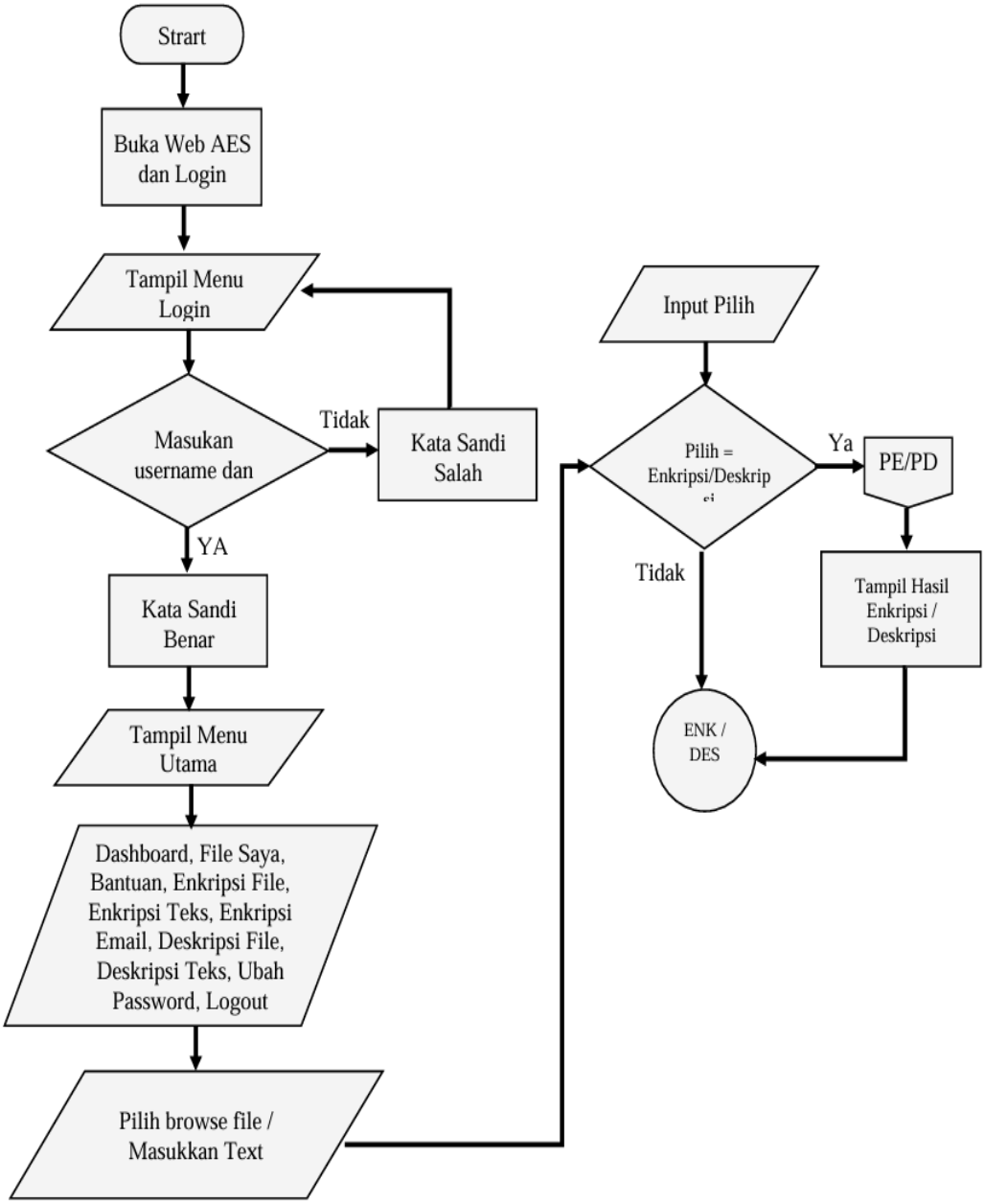
3. Tampilan Deskripsi Berkas
   Menu deskripsi email adalah menu yang berfungsi untuk mendeskripsikan file yang sudah terenkripsi dengan memasukkan password sesuai dengan enkripsi. Seperti pada Gambar 5 di bawah ini.



Gambar 5. Tampilan Deskripsi Berkas

Flowchart Aplikasi AES 128 Berbasis web

Pada flowchart di bawah ini , akan menampilkan proses masuk ke dalam web.dan memilih *file* doc,docx,xls, txt, dan pdf untuk di enkripsi. Flowchart dapat dilihat pada Gambar 4.



Gambar 6. Flowchart Aplikasi AES 128 Berbasis Web

Hasil Uji Coba

Tabel 3. Hasil Pengujian Aplikasi

No	Pengujian	Proses	Status
1	Login menggunakan *username* dan *Password* yang sesuai.	Berhasil masuuk ke dalam *dashboard* web.	Berhasil
2	Login menggunakan *username* dan *password* yang tidak sesuai.	Tidak dapat masuk ke dalam web.	Berhasil
3	Melakukan enkripsi menggunakan plaintext "COBAALGORITMAAES" dan dengan chiperkey "YUSRILTARIGANAES".	Text akan berubah menjadi "sujrO2uyEyusP5aq/V5BKwLaPH jTJLJjb0i1xn6x wVg="	Berhasil
4	Melakukan deskripsi pada hasil test pengujian ke 3 dengan *password* yang sesuai.	"sujrO2uyEyusP5aq/V5BKwLaPH jTJLJjb0i1xn6x wVg=" akan Kembali menjadi "COBAALGORITMAAES"	Berhasil
5	Melakukan deskripsi pada hasil test pengujian ke 3 dengan *password* yang tidak sesuai pada saat enkripsi.	Text tidak akan berubah karena *password* salah.	Berhasil
6	Melakukan enkripsi file "Contoh Data.pdf" berukuran 3.468 kb	Tidak dapat mengenkripsi berkas.	Berhasil.
7	Melakukan enkripsi fiile "S1.txt" berukuran 1kb.	Dapat melakukan enkripsi terhadaf file, nama dan isi file akan berubah. Format file berubah menjadi "69376_S1.txt.encrypted.encrypted".	Berhasil
8	Melakukan deskripsi file "69376_S1.txt.encrypted.encrypted" Dengan *password* yang sesuai saat enkripsi.	Dapat melakukan deskripsi terhadap file, nama dan isi file akan Kembali seperti semula.	Berhasil
10	Menggunakan menu enkripsi email.	Tidak berhasil melakukan enkripsi dan mengirim email.	Gagal

Kelebihan Sistem

Berikut ini merupakan kelebihan yang terdapat pada system :

1. Memiliki fitur login menggunakan admin.
2. Tampilan dan penggunaan yang sederhana.
3. Prosesenkripsi dan deskripsi berjalan dengan cepat.
4. Memiliki detail berkas yang diperlukan.

Dapat mengenkripsi file dengan format *.txt, *.pdf, *.doc, *.docx, *.xls, dan *.xlsx.

Kekurangan Sistem

Berikut ini merupakan kekurangan yang terdapat pada system :

1. Tidak dapat melakukan enkripsi dan deskripsi pada berkas yang berukuran di atas 3 MB.
2. System belum 100% sempurna.
3. Tampilan kurang menarik.
4. Tidak Memiliki fitur Lupa *Password*.

Simpulan

Aplikasi keamanan berkas yang dibuat membuat berkas-berkas bansos yang terdapat pada kecamatan Tigabinanga menjadi lebih aman dan akan mengurangi terjadinya kebocoran data mengubah isi dari berkas tersebut yang dilakuakan oleh seseorang atau kelompok yang tidak bertanggung jawab. Proses yang diperlukan untuk melakukan login serta mengenkripsi dan deskripsi tidak terlalu lama.Tidak semua orang dapat mengenkripsi dan mendeskripsikan berkas karena hanya dapat dilakukan oleh orang yang mengetahui *username* dan *password*.

Daftar Pustaka

Azhari, M., Mulyana, D. I., Perwitosari, F. J., & Ali, F. (2022). *Jurnal Pendidikan Sains dan Komputer Implementasi Pengamanan Data pada Dokumen Menggunakan Algoritma Kriptografi Advanced Encryption Standard (AES) Jurnal Pendidikan Sains dan Komputer*. *2*(1), 163–171.

Fadilah, R. (2021). Bantuan Sosial Sembako dan Bantuan Sosial Tunai. *Jurnal El-Thawalib*, *2*(3), 167–179. https://doi.org/10.24952/el-thawalib.v2i3.3992

Hartati, C. D. (2019). Transformasi dan Kontinuitas Dalam Tradisi Penggunaan Bahan Bakar Limbah Jagung Untuk Memasak Skala Rumah Tangga, Studi Kasus Kecamatan Tiga Binanga Tanah Karo. *Jurnal Pendidikan Ilmu Sosial*, *28*(1), 8. https://doi.org/10.17509/jpis.v28i1.13299

Lesmana, A., & Shita, R. T. (2018). APLIKASI PENGAMANAN EMAIL BERBASIS ANDROID DENGAN ALGORITMA KRIPTOGRAFI AES-128 DAN RC4 PADAPT TIRTA INVESTAMA. *SKANIKA: Sistem Komputer dan Teknik Informatika*, *1*(2), 534-539..

Mustika, L. (2020). Implementasi Algoritma AES Untuk Pengamanan Login Dan Data Customer Pada E-Commerce Berbasis Web. *JURIKOM (Jurnal Riset Komputer)*, *7*(1), 148. https://doi.org/10.30865/jurikom.v7i1.1943

Pramudito, A. G., & Kusumaningsih, D. (2018). Implementasi Algoritma Aes 128 Dan Rc4 Untuk Pengamanan Email Pada Pt. Dinamika Hydro Engineering. *Skanika*, *1*(3), 869–876. http://jom.fti.budiluhur.ac.id/index.php/SKANIKA/article/view/2499

Pratama, B. P., & Haryono, W. (2020). Perancangan Aplikasi Kriptografi Pada Dokumen Pengarsipan Dengan Menggunakan Algoritma Triple Des Berbasis

Web. *Journal of Artificial Intelligence and Innovative Applications (JOAIIA)*, *1*(4), 204–212. http://www.openjournal.unpam.ac.id/index.php/JOAIIA/article/view/8288

Putra, A. B., & Nita, S. (2019). Perancangan dan Pembangunan Sistem Informasi E-Learning Berbasis Web (Studi Kasus Pada Madrasah Aliyah Kare Madiun). *Seminar Nasional Teknologi Informasi Dan Komunikasi 2019*, *1*(1), 81–85.

Triono, A., Budi, A. S., Abdillah, R., & Cipher, V. (2023). *Implementasi peretasan sandi vigenere chipher menggunakan bahasa pemrograman python*. *1*(1), 1–9.

Yusfrizal, Y. (2019). Rancang Bangun Aplikasi Kriptografi Pada Teks Menggunakan Metode Reverse Chiper Dan Rsa Berbasis Android. *Jurnal Teknik Informatika Kaputama (JTIK)*, *3*(2), 29–37.