Journal of Information Technology and Computer Science (INTECOMS)
Volume 7 Nomor 3, Tahun 2024
e-ISSN : 2614-1574
p-ISSN : 2621-3249

IMPLEMENTASI PENGAMANAN AKSES REPORTING BUDGET DEALER MENGGUNAKAN ALGORITMA KRIPTOGRAFI ADVANCED ENCRYPTION STANDARD (AES) PADA MICROSOFT POWERAPPS

IMPLEMENTATION OF DEALER BUDGET REPORTING ACCESS SECURITY USING ADVANCED ENCRYPTION STANDARD (AES) CRYPTOGRAPHY ALGORITHM ON MICROSOFT POWERAPPS

Wieko[1], Kemal Adnan[2], Eka Putri Aprillia[3], Dadang Mulyana Iskandar[4]
[1,2,3,4]Program Studi Sistem Informasi, Sekolah Tinggi Ilmu Komputer, Jakarta, Indonesia
wieko04@gmail.com[1], adnkml17@gmail.com[2], Ekaaaaprillia8@gmail.com[3],
mahvin2012@gmail.com[4]

ABSTRACT

Information security is a critical aspect in the digital environment, especially in data management and exchange. This research aims to implement an additional layer of security in Microsoft Power Apps using the Advanced Encryption Standard (AES) cryptographic algorithm to check the encrypted text and the encryption results will be sent via email, so as to secure dealer budget reporting access. The research methodology involves an in-depth understanding of AES concepts, security requirements analysis, and technical implementation on Microsoft Power Apps. The research results show that AES integration in Microsoft Power Apps is able to increase the security level of automation processes involving text. AES encryption implemented at this level provides protection against unauthorized access and prevents the risk of information leakage. This implementation is relevant for organizations that rely on Microsoft Power Apps in their business workflows, especially in environments where information security is a top priority. To ensure the protection of reporting data so that it cannot be accessed easily, the AES cryptographic algorithm is needed, the encryption results will be sent via private email, so that not just any user gets the password keys

Keywords: *Information Security, Cryptography, Advanced Encryption Standard (AES), Microsoft Power Apps.*

ABSTRAK

Keamanan informasi menjadi aspek kritis dalam lingkungan digital, khususnya dalam manajemen dan pertukaran data. Penelitian ini bertujuan untuk mengimplementasikan lapisan keamanan tambahan pada Microsoft Power Apps menggunakan algoritma kriptografi Advanced Encryption Standard (AES) untuk melakukan pengecekan text yang di enkripsi dan hasil enkripsi tersebut akan dikirimkan melalui email, sehingga dapat mengamankan akses reporting budget dealer. Metodologi penelitian melibatkan pemahaman mendalam terhadap konsep AES, analisis kebutuhan keamanan, dan implementasi teknis pada Microsoft Power Apps. Hasil penelitian menunjukkan bahwa integrasi AES pada Microsoft Power Apps mampu meningkatkan tingkat keamanan proses otomatisasi yang melibatkan teks. Enkripsi AES yang diimplementasikan pada level ini memberikan perlindungan terhadap akses yang tidak sah dan mencegah risiko kebocoran informasi.Penerapan ini relevan untuk organisasi yang mengandalkan Microsoft Power Apps dalam alur kerja bisnis mereka, terutama di lingkungan di mana keamanan informasi merupakan prioritas utama. Untuk menjamin perlindungan data reporting agar tidak dapat diakses dengan mudah, maka diperlukan algoritma kriptografi AES, hasil enkripsi tersebut akan dikirimkan melalui email pribadi, sehingga tidak sembarang pengguna yang mendapatkan password keys tersebut.

Kata Kunci: Pengamanan Informasi, Kriptografi, Advanced Encryption Standard (AES), Microsoft Power Apps

PENDAHULUAN

Dalam era digital yang terus berkembang, pertukaran informasi melalui media elektronik telah menjadi unsur krusial dalam berbagai aspek kehidupan, baik dalam konteks bisnis maupun pribadi. Namun, pertumbuhan pesat ini juga memunculkan tantangan baru terkait keamanan data dan informasi. Keamanan informasi merupakan cabang studi dari teknologi informasi yang mengkhususkan diri untuk mempelajari metode dan teknik untuk melindungi informasi dan sistem informasi dari akses, penggunaan, penyebaran, perusakan, perubahan, dan penghancuran tanpa otorisasi yang sah[1].

Keamanan menjadi suatu hal yang mendesak untuk dipertimbangkan, terutama untuk akses reporting.

Dalam konteks ini, penelitian ini bertujuan untuk mengatasi kekhawatiran keamanan dengan mengimplementasikan lapisan keamanan tambahan menggunakan algoritma kriptografi Advanced Encryption Standard (AES) pada Microsoft Power Apps. Permasalahan kunci yang dipecahkan meliputi bagaimana mengintegrasikan AES secara efisien dalam alur kerja otomatisasi untuk melindungi teks dan file yang dihasilkan dari proses enkripsi dan dekripsi data. Enkripsi dilakukan saat pengiriman data dengan cara mengubah data menjadi data rahasia. Sedangkan dekripsi merupakan merubah data rahasia tadi menjadi data asli, Sehingga proses pertukaran informasi hanya dapat dilihat oleh sipemegang kunci tersebut[2]

Tujuan utama dari penelitian ini merupakan mengimplementasikan dan mengevaluasi efektivitas keamanan yang diperoleh melalui penggunaan AES pada Microsoft Power Apps. Dengan demikian, diharapkan dapat memberikan solusi yang handal dalam melindungi data sensitif dari ancaman keamanan yang mungkin timbul selama proses otomatisasi

METODE

Kriptografi

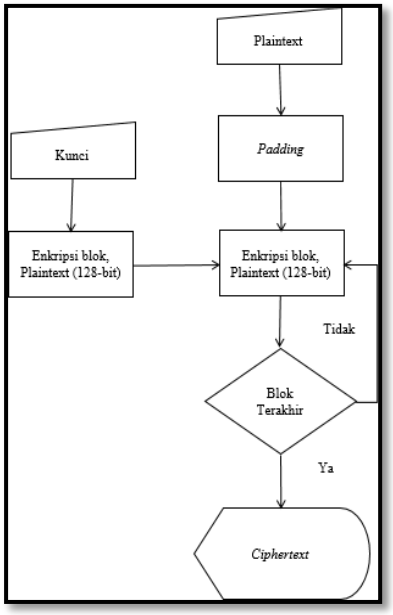
Kriptografi merupakan ilmu menjaga kerahasiaan pesan dengan cara menyandikannya dalam bentuk yang tidak dapat dipahami lagi. Dalam kriptografi terdapat dua proses yaitu enkripsi dan dekripsi. Pesan terenkripsi disebut plaintext. Disebut demikian karena informasi ini dapat dengan mudah dibaca dan dipahami oleh siapa saja.[3]. Oleh karena itu, kriptografi dapat dianggap sebagai ilmu yang mempelajari keamanan pesan.

Tujuan kriptografi:

kriptografi bertujuan untuk menyediakan layanan keamanan seperti melindungi komunikasi dari akses yang tidak sah, Integritas data memastikan bahwa pesan dan transmisi asli dan otentikasi digunakan untuk memverifikasi identitas. Identitas dikaitkan dengan ini. komunikator tidak dapat menolak pesan atau tindakan yang dikirim.

Algoritma AES (Advanced Encryption Standard)

Advanced Encryption Standard (AES) merupakan algoritma enkripsi yang berfungsi untuk mengamankan data. Algoritma AES merupakan blok ciphertext simetris yang mampu melakukan enkripsi dan dekripsi. Enkripsi merupakan mengubah data asli menjadi data yang tidak terbaca atau disebut ciphertext, berbeda dengan enkripsi yang bersifat decoding, decoding mengubah data yang tidak terbaca menjadi data yang dapat dibaca seperti semula atau disebut teks versi murni. Aes menggunakan kunci 128, 192, dan 256-bit untuk mengenkripsi dan mendekripsi data[3]. Enkripsi dilakukan saat pengiriman data dengan cara memiliki tingkat keamanan data yang berbeda-beda serta memiliki kelebihan dan kekurangan tersendiri [4].



Gambar 1. Algoritma AES

Implementasi Algoritma Enkripsi dan Dekripsi AES-128

Implementasi Algoritma Enkripsi dan Dekripsi AES-128. Pada mode ini, setiap blok secara individual dan independen yang berada pada plainteks dienkripsi, kelemahan mode ECB merupakan deterministic dikarenakan blok data yang sama selalu menghasilkan cipher yang sama juga[5]. Berikut merupakan diagram alur proses enkripsi AES dengan menggunakan modus ECB

Algoritma enkripsi AES diimplementasikan dengan mode ECB seperti gambar diatas. Langkah langkah proses enkripsi mode ECB pada AES merupakan:

1. Padding plaintext.
2. Ekspansi plaintext.
3. Enkripsi blok plaintext 128 bit.
4. Output [8]

Microsoft Power Apps

Power Apps merupakan sejumlah aplikasi, layanan, dan konektor, serta platform data, yang menyediakan lingkungan pengembangan cepat untuk membangun aplikasi kustom untuk kebutuhan bisnis Anda. Menggunakan Power Apps, Anda dapat dengan cepat membuat aplikasi bisnis kustom yang terhubung ke data bisnis yang tersimpan di platform data[6].

Aplikasi yang dibuat menggunakan Power Apps menyediakan logika bisnis kaya dan kemampuan alur kerja untuk mentransformasi operasi bisnis manual Anda menjadi proses digital dan otomatis. Terlebih lagi, aplikasi yang dibuat menggunakan Power Apps memiliki desain responsif dan dapat berjalan mulus di browser dan di perangkat seluler (ponsel atau tablet). Power Apps "mendemokratisasi" pengalaman membangun aplikasi bisnis dengan memungkinkan pengguna membuat aplikasi bisnis kustom kaya fitur tanpa menulis kode.

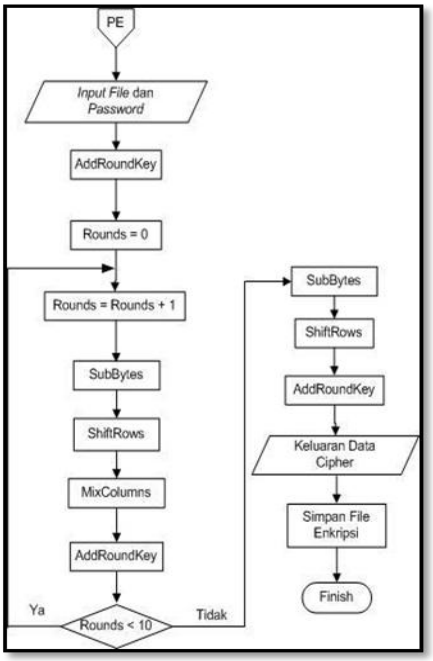
Power Apps juga menyediakan platform yang dapat diperpanjang yang memungkinkan pengembang pakar berineraksi dengan program dengan data dan metadata, menambahkan logika bisnis, membuat penghubung khas, dan berintegrasi dengan data eksternal[6].

Flowchart Proses Enkripsi AES

Untuk membuat jadwal kunci, AES memperluas kunci sandi menjadi K. Kata Nb(Nr+1) dibuat dengan ekstensi kunci. Strategi ini membutuhkan Nb kata kunci di awal dan Nb kata kunci di setiap putaran.

Array linier gaya [wi] kata-kata empat byte dibuat oleh jadwal kunci. Untuk menghasilkan kata keluaran, fungsi SubWord menerapkan S-Box ke masing-masing empat byte masukan. RotWord menghasilkan [a0, a1, a2, a3, a0] dari [a0, a1, a2, a3] setelah permutasi siklik. Nilai [xi-1], {00}, {00}, dan {00} terdiri dari Rcon[i], dengan x diwakili sebagai {02} pada kolom GF(28).

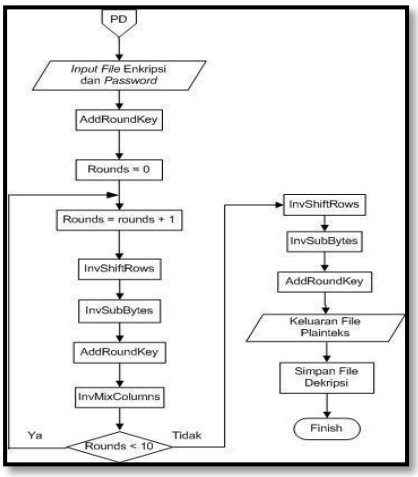
Flowchart ini merupakan alur jalannya proses enkripsi AES



Gambar 2. Flowchar Enkripsi

Flowchart Proses Dekripsi AES

Memanfaatkan InvShiftRows, InvSubBytes, InvMixColumns, dan AddRoundKey untuk mengubah byte, cipher invers AES dapat dihasilkan dengan membalikkan dan membalikkan transformasi cipher. Diagram flowchart proses dekripsi dapat digambarkan sebagai berikut:

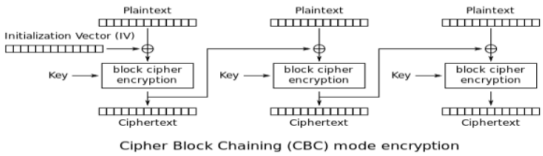


Gambar 3. Flowchart Dekripsi AES

Enkrispi menggunakan metode Cipher Block Chaining (CBC)

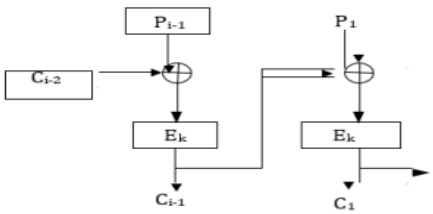
Algoritma Cipher Block Chaining (CBC) digunakan untuk mengenkripsi pesan plaintext dalam format teks.txt. Algoritma CBC membagi pesan biner ke dalam blok-blok dengan ukuran 8 bit setiap blok. Proses enkripsi CBC merupakan seperti berikut.

- Teks bebas dibagi menjadi beberapa blok yang berbeda secara ukuran.
- Blok pertama di-XOR-kan dengan vektor awal.
- Blok yang menghasilkan XOR dengan IV di-XOR-kan dengan kunci.
- Teks bebas yang menghasilkan XOR dengan kunci ini kemudian diubah menjadi IV pada blok berikutnya. e. Proses diulang sampai blok terakhir.



Gambar 4. Alur Proses Enkripsi Cipher Block Chaining

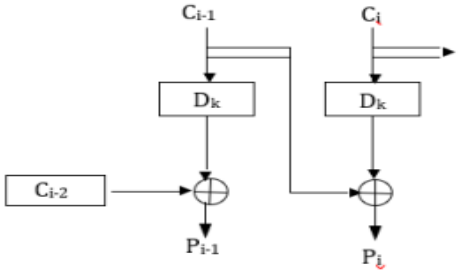
Menggunakan teknik umpan balik untuk blok bit, yang memungkinkan hasil enkripsi blok sebelumnya dikembalikan ke proses enkripsi blok saat ini. Ini dilakukan dengan mengXOR-kan blok plaintext saat ini dengan blok ciphertext hasil enkripsi sebelumnya. Kemudian, hasil pengXOR-an ini dimasukkan ke dalam fungsi enkripsi. Algoritma CBC membuat blok ciphertext bergantung pada blok plaintextnya dan seluruh blok plaintext sebelumnya. Dalam mode operasi cipher block chaining, proses enkripsi dilakukan pada setiap blok plaintext n-bit yang di-XOR dengan blok plaintext sebelumnya n-bit. Ini berlaku kecuali blok plaintext pertama di-XOR dengan cipher awal atau vektor awal (IV), yang berukuran n-bit. Metode enkripsi CBC



Gambar 5. Skema Enkripsi Mode Operasi CBC

Untuk dekripsi, blok ciphertext pertama di-XOR dengan blok ciphertext sebelumnya, yang menghasilkan blok

plaintext. Blok pertama di-XOR dengan blok IV, yang menghasilkan plaintext blok pertama. Gambar algoritma dekripsi CBC



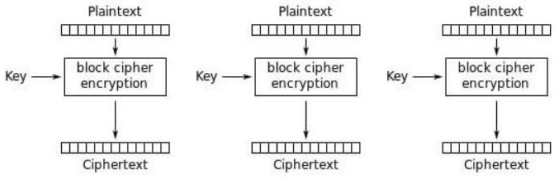
Gambar 6. Skema Dekripsi Mode Operasi CBC

Electronic Code Books

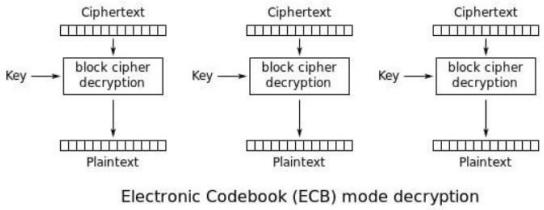
Elektronik Kode Buku (ECB) merupakan mode operasi sederhana yang menggunakan cipher blok untuk enkripsi kunci simetris yang merupakan metode langsung untuk memproses serangkaian blok pesan berurutan. Input plaintext terdiri dari banyak blok. Dengan menggunakan kunci enkripsi, blok dienkripsi secara individual dan independen (ciphertext). Akibatnya, setiap blok terenkripsi juga dapat didekripsi satu per satu. ECB dapat mendukung kunci enkripsi yang berbeda untuk setiap jenis blok. Nilai ciphertext untuk setiap blok plaintext berlaku, dan sebaliknya. Oleh karena itu, plaintext dengan kunci yang sama selalu dienkripsi ke ciphertext yang sama. Ini menunjukkan bahwa blok cipherteks keluaran selalu identik jika blok plainteks P1, P2, dan seterusnya dienkripsi beberapa kali di bawah kunci yang sama.

Dengan kata lain, nilai cipherteks selalu memiliki nilai yang sama. Ini juga berlaku untuk plainteks yang memiliki bagian yang identik sebagian. Sebuah contoh plainteks yang memiliki header surat yang sama dan dienkripsi dengan kunci yang sama akan memiliki bagian cipherteks yang identik sebagian.

ECB menjalankan operasinya dengan memecah plaintext menjadi blok yang berbeda yang masing-masing berukuran sesuai dengan blok sistem penyandian. Selanjutnya, algoritma enkripsi dan dekripsi yang sama digunakan untuk menyandi setiap blok. Untuk dekripsi ECB, algoritma dekripsi menggantikan algoritma enkripsi.



Gambar 7. Enkripsi Electronic Code Books



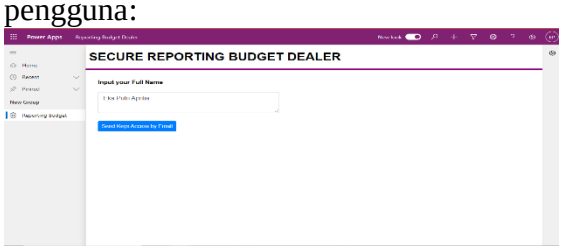
Gambar 8. Dekripsi Electronic Code Books

ECB tidak cocok untuk mode enkripsi identik dan ukuran blok kecil. Beberapa kata dan frasa mungkin digunakan kembali dalam teks biasa ketika ditulis dalam blok yang lebih kecil. Ini menunjukkan bahwa ciphertext dapat membawa dan mengkhianati pola plaintext yang sama, serta blok bagian berulang dari ciphertext yang sama dapat muncul. Pola plaintext memungkinkan aktor jahat untuk menebak dan menyerang buku kode. Meskipun keamanan ECB kurang, dapat ditingkatkan dengan menambahkan bit pad acak ke setiap blok. Blok yang lebih besar (64 bit atau lebih) mungkin memiliki cukup karakteristik unik (entropi) untuk mencegah serangan kodebook.

HASIL DAN PEMBAHASAN

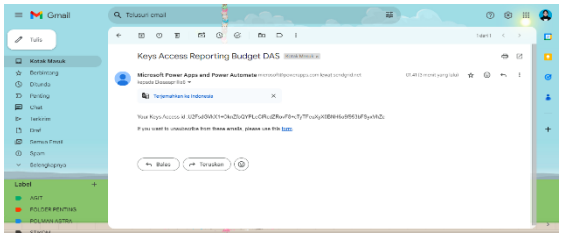
Tampilan program merupakan output dari program yang sudah dirancang dan akan digunakan untuk memberikan penjelasan lebih lanjut tentang tampilan yang ada dalam program aplikasi website. Pada tahap ini, penulis akan membahas peran masing-masing tampilan yang dihasilkan., program kriptografi ini dibuat untuk melindungi reporting budget dealer agar dapat dilihat hanya untuk karyawan yang memiliki keys khusus yang dikirimkan via email. Jika user belum tahu keys yang dimiliki, user perlu melakukan

permintaan keys untuk dikirimkan ke email pribadi. Berikut tampilan enkripsi text yang akan dikirimkan ke email pengguna:



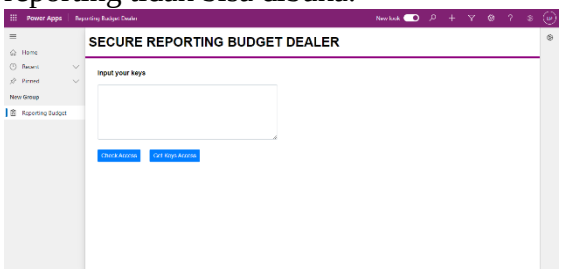
Gambar 9. Tampilan Form Enkripsi Text

System akan otomatis mengirimkan kode hasil enkripsi ke email pribadi user tersebut, sehingga dapat memperketat keamanan akses reporting data, karena keys tersebut hanya dikirim ke email user tersebut, Berikut hasil email inbox yang berisikan keys hasil enkripsi text.



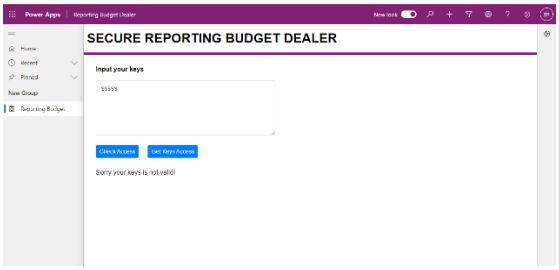
Gambar 10. Email Kode Enkripsi Text

Kemudian keys tersebut di copy kedalam system, untuk dilakukan dekripsi dan pengecekan validasi apakah hasil dekripsi tersebut sesuai dengan user login yang saat ini sedang login kedalam aplikasi, jika tidak sesuai, maka data reporting tidak bisa dibuka.



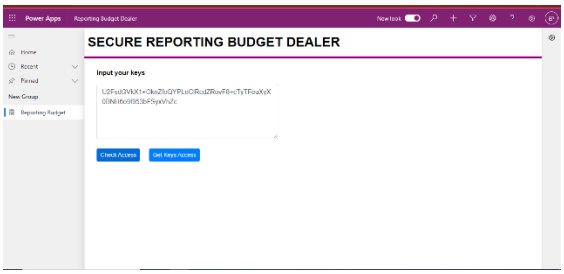
Gambar 11. Tampilan Awal Form Dekripsi Text

Berikut merupakan hasil jika user memasukan keys enkripsi yang tidak valid:



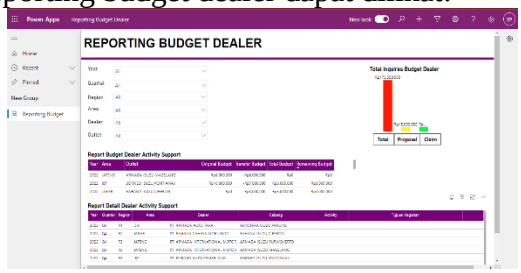
Gambar 12. Tampilan Validasi Keys Not Valid

Jika user sudah menginput keys yang sesuai dengan yang ada di email, maka user tersebut berhasil membuka reporting budget dealer.



Gambar 13. Tampilan Dekripsi Pengecekan Akses

Berikut merupakan tampilan jika user memasukan keys yang valid, maka reporting budget dealer dapat dilihat:



Gambar 14. Tampilan Reporting Budget Dealer

SIMPULAN

Implementasi enkripsi AES pada platform Microsoft Power Apps berjalan dengan baik, karena dapat melindungi akses data reporting budget dealer agar tidak dapat diakses dengan mudah, hasil enkripsi tersebut akan dikirimkan melalui email pribadi, sehingga tidak sembarang pengguna yang mendapatkan password keys tersebut. Program ini juga dapat memvalidasi jika user memasukan keys yang tidak valid maka user tersebut tidak bisa mengakses reporting budget dealer.

DAFTAR PUSTAKA

[1] M. Azhari , D. I. Mulyana,F.J. Perwitosari, and F.Ali "ALGORITMA CAESAR CIPHER ATAU VIGENERE CIPHER PADA PENGENKRIPSIAN PESAN TEKS", *Journal on education*, vol. 5, no. 3, pp. 2655-1365, Mar-Apr. 2023, http://jonedu.org/index.php/joe

[2] R. Prasetyo and A. Suryana, "Aplikasi Pengamanan Data dengan Teknik Algoritma Kriptografi AES dan Fungsi Hash SHA-1 Berbasis Desktop," 2016.

[3] M. Azhari , D. I. Mulyana,F.J. Perwitosari, and F.Ali "IMPLEMENTASI PENGAMANAN DATA PADA DOKUMEN MENGGUNAKAN ALGORITMA KRIPTOGRAFI ADVANCED ENCRYPTION STANDARD (AES)," Jurnal Pendidikan Sains Dan Komputer, vol. 2, no. 1, pp. 2809-476, Feb. 2022, doi: 10.47709/jpsk.v2i1.1390

[4] B. Anwar, N. B. Nugroho, and R. Siregar, "J-SISKO TECH Jurnal Teknologi Sistem Informasi dan Sistem Komputer TGD Aplikasi Pengamanan Dokumen Penjualan Tiket Pesawat Di Pt. Benua Raya Jaya Tour And Travel Menggunakan Metode Advanced Encryption Standard AES)," vol. 3, no. 1, pp. 96–102, 2020.

[5] "175408-ID-implementasi advanced-encryption-standar".

[6] https://learn.microsoft.com/en-us/training/paths/create-app-models-business-processes/

[7] Ilham Saputra, Arief Nugroho, dan Muhammad Ilham (2023). "Implementasi Kriptografi Pada Fail Dokumen Menggunakan Algoritma AES-128"

[8] Dr. Ir. Mochammad Irfan, M.Eng., Dr. Ir. Asep Iwan Gunawan, M.Eng., dan Dr. Ir. Rini Nurhayati, M.T. (2022). "Penerapan Kriptografi Caesar Cipher Dan Hill Cipher dalam Pengiriman Pesan Rahasia Sebagai Media Pembelajaran Matematika Realist"

[9] Dadang Iskandar Mulyana. (2022). "Perancangan Aplikasi Enkripsi & Deskripsi pada Dokumen Dengan Algoritma Triple DES Berbasis Web"

[10] Dadang Iskandar Mulyana. (2022) "Implementasi Algoritma One Time menggunakan Algoritma Chiper Transposition Sebagai pengaman Rahasisa Pesan Rail Fence Cipher Dan Route Cipher Untuk Keamanan Fail"

[11] Dadang Iskandar Mulyana. (2023) "Algoritma Caesar Cipher atau Vigenere Cipher pada Pengenkripsian Pesan Teks"

[12] Dadang Iskandar Mulyana. (2022). "Pengamanan Transkrip Mahasiswa Menggunakan Kriptografi Playfair Cipher". Jurnal Teknik Elektro dan Komputasi (ELKOM).

[13] Stallings, W. (2006). "Cryptography and Network Security Principles and Practice." Fifth Edition. USA: Prentice Hall.

[14] Dadang Iskandar Mulyana. (2022). "Implementasi Metode Rivest Shamir Adleman untuk Enkripsi dan Dekripsi Text"

[15] Z. Jatmiko, "Implementation of Advanced Encryption Standard (Aes) Algorithm As a Security System for Archiving Data At Digital Library …," Elibrary.Unikom.Ac.Id, [Online]. Available: https://elibrary.unikom.ac.id/1350/15/22.10112441_ZAEN AL FIRDAUS_JURNAL DALAM BAHASA INGGRIS.pdf

[16] L. Mustika, "Implementasi Algoritma AES Untuk Pengamanan Login Dan Data Customer Pada E-Commerce Berbasis Web," JURIKOM (Jurnal Riset Komputer), vol. 7, no. 1, p. 148, 2020, doi: 10.30865/jurikom.v7i1.194.