JNATIA Volume 3, Nomor 1, November 2024 p-ISSN: 2986-3929
Jurnal Nasional Teknologi Informasi dan Aplikasinya e-ISSN: 3032-1948

Enkripsi Resep Dokter untuk Meminimalisir Penyalahgunaan Obat Menggunakan Algoritma AES Mode CBC

Komang Wahyu Agastya[a1], AAIN Eka Karyawati[a2]

[a]Program Studi Informatika, Fakultas Matematika dan Ilmu Pengetahuan Alam,
Universitas Udayana
Jalan Raya Kampus UNUD, Bukit Jimbaran, Kuta Selatan, Badung, Bali, Indonesia
[1]wahyuagastyakomang@gmail.com
[2]eka.karyawati@unud.ac.id

Abstract

Patient safety has always been a top priority, and medication error is a significant concern in this domain. Prescriptions are a crucial factor that can elevate the risk of medication errors. A study by Prof. Dr. Nurul Idrus involving 1,200 drug users revealed that a substantial number of respondents misused prescriptions and experimented with obtained medications to substitute for those they couldn't easily access. To address this issue and enhance patient safety, we propose utilizing the AES encryption algorithm to safeguard the confidentiality of prescriptions. AES encryption offers robust protection against unauthorized access and data breaches. Furthermore, employing the CBC (Cipher Block Chaining) mode provides an additional layer of security. In CBC mode, each block of the message is encrypted not only with the encryption key but also with the ciphertext of the previous block, resulting in a unique encrypted message even for identical plaintexts. This combination of AES encryption and CBC mode effectively safeguards prescription data, minimizing the potential for prescription misuse and medication errors, ultimately contributing to improved patient safety.

Keywords: *Prescription misuse, AES, CBC*

1. Pendahuluan

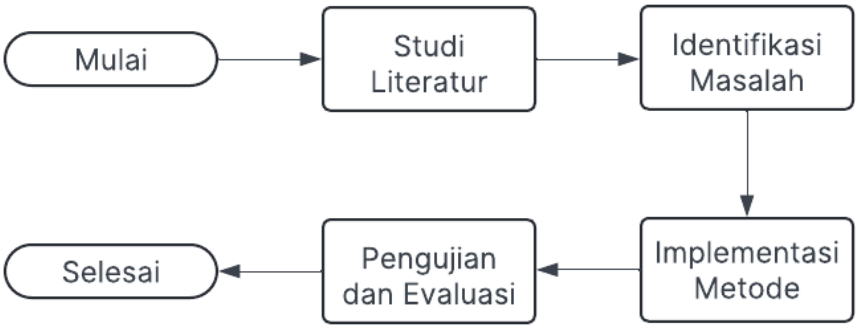
Patient safety telah menjadi perhatian bagi setiap tenaga kesehatan di seluruh dunia sejak dahulu. Kesalahan pengobatan (medication error), yang seharusnya dapat dicegah, masih di bawah kontrol atau tanggung jawab tenaga kesehatan, adalah salah satu hal yang terkait erat dengan patient safety [1]. Pada fase komunikasi non-verbal antara dokter dan apoteker tentang pengobatan pasien, dapat terjadi medication error [2]. Salah satu faktor yang dapat meningkatkan kemungkinan medication error adalah resep. Sebuah laporan dari Institut Kedokteran Amerika menunjukkan bahwa antara 44,000 dan 98,000 orang telah meninggal karena medication error, atau sekitar 7000 orang meninggal setiap tahun sebagai akibat dari medication error yang sering terjadi. [3]. Penyalahgunaan resep dokter marak terjadi dengan dalih mencari alternatif dari obat-obatan yang dilarang keras peredarannya. Dari 1.200 pengguna narkoba yang dipilih untuk penelitian oleh Prof. Dr. Nurul Idrus, sebagian mengatakan bahwa mereka bereksperimen menggunakan obat yang diresepkan dokter sebagai pengganti obat yang sulit mereka dapatkan. [4]. Resep adalah alat komunikasi profesional antara dokter (penulis resep), APA (penyedia/pembuat obat), dan pasien. [5] oleh karena itu, hendaknya resep bersifat rahasia agar tidak dapat dilihat oleh orang yang tidak berhak. Dengan melakukan enkripsi terhadap resep, maka kerahasiaan resep dapat ditingkatkan serta penyalahgunaan resep dapat dikurangi. Enkripsi AES-CBC adalah algoritma enkripsi simetris yang kuat dan aman yang dapat membantu meningkatkan keamanan data resep dan mengurangi penyalahgunaan obat. AES bekerja dengan memecah pesan menjadi blok-blok dan mengenkripsinya menggunakan kunci rahasia. Mode CBC menambahkan lapisan keamanan ekstra dengan menggabungkan setiap blok pesan dengan blok acak (Initialization Vector) sebelum dienkripsi, sehingga menghasilkan pesan terenkripsi yang unik setiap kali meski pesan aslinya sama. Proses algoritma enkripsi AES terdiri

dari empat kategori transformasi byte yaitu SubBytes, ShiftRows, MixColumns, dan AddRoundKey. [6] [7]. Input plaintext akan mempertahankan transformasi byte AddRoundKey pada langkah pertama enkripsi. Pada langkah-langkah berikutnya, state akan mengalami transformasi SubBytes, ShiftRows, MixColumns, dan AddRoundKey berulang sebanyak Nr. State tidak akan mengalami transformasi MixColumns lagi pada putaran terakhir. [8].

2. Metode Penelitian

2.1. Diagram Alir Penelitian

Penelitian ini dimulai dengan melakukan studi literatur tentang penelitian terkait dengan enkripsi AES mode CBC, selanjutnya memahami permasalahan yang ingin diselesaikan, lalu mengimplementasikan algoritma kedalam sistem, dan terakhir dilakukan pengujian dan evaluasi.



Gambar 1. Diagram Alir Penelitian

2.2 Studi Literatur

Langkah pertama dalam penelitian ini adalah melakukan tinjauan pustaka untuk mempelajari kriptografi dan Algoritma AES serta mode CBC. Hal ini dilakukan dengan cara membaca dan memahami berbagai sumber seperti jurnal ilmiah, makalah, dan referensi lainnya. Tujuannya adalah untuk mendapatkan informasi yang mendalam dan akurat yang diperlukan untuk penelitian ini.

2.3 Identifikasi Masalah

Pada tahap ini, dilakukan identifikasi masalah untuk memahami permasalahan utama yang ingin diselesaikan. Permasalahan dalam penelitian ini adalah penyalahgunaan resep dokter sehingga maraknya penyalahgunaan obat-obatan yang dilarang keras peredarannya. Maka dari itu, pengenkrepsian file resep dokter menjadi salah satu solusi yang efektif dalam menjaga kerahasiaan isi resep pasien.

2.4 Implementasi Metode

Tahap ini adalah pengimplementasian algoritma AES mode CBC ke dalam sistem. Sistem nantinya akan berjalan pada web, digunakan bahasa HTML, CSS, dan javascript untuk membangun sistem. Algoritma AES mode CBC akan diterapkan menggunakan bahasa pemrograman javascript. Proses enkripsi dan dekripsi akan menggunakan satu kata sandi yang sama berjumlah delapan karakter atau lebih untuk memastikan keamanan dan kesamaan data.

2.5 Pengujian dan Evaluasi

Pada tahap ini dilakukan pengujian jalannya algoritma AES mode CBC yang telah diterapkan, apakah algoritma telah berjalan baik atau ada kendala. Selanjutnya dilakukan evaluasi apabila masih terdapat kekurangan dalam sistem.

2.6 Kriptografi

Kriptografi adalah bidang yang mempelajari cara menyandikan pesan dalam bentuk yang tidak dapat dipahami lagi untuk menjaga kerahasiaan pesan [9]. Kriptografi terdiri dari proses enkripsi dan proses dekripsi. Proses enkripsi adalah mengonversikan informasi yang dapat dibaca (plaintext) menjadi informasi yang tidak terbaca (ciphertext), sedangkan proses dekripsi adalah membalikkan dari informasi yang tidak terbaca (ciphertext) menjadi informasi yang dapat dibaca (plaintext).

2.7 Advanced Encryption Standard

AES, atau Advanced Encryption Standard, adalah algoritma simetri dan cipher blok yang dikenal sebagai Rijndael, yang ditemukan oleh Dr. Vincent Rijmen dan Dr. Joan Daemen [10]. Setiap cipher mengenkripsi dan mendekripsi data dalam blok 128-bit menggunakan kunci kriptografi masing-masing 128, 192, dan 256 bit. Kunci 128-bit, 192-bit, dan 256-bit menjalani 10, 12, dan 14 putaran enkripsi, secara berurutan. Satu putaran terdiri dari beberapa langkah pemrosesan termasuk substitusi, transposisi, dan pencampuran input teks biasa untuk mengubahnya menjadi output ciphertext akhir. Semakin banyak putaran, semakin sulit untuk memecahkan enkripsi, dan semakin aman informasi asli. Baik dalam enkripsi maupun dekripsi, algoritma ini menggunakan satu kunci yang sama, dan input serta outputnya berupa blok sejumlah bit tertentu. Algoritma AES terdiri dari empat proses transformasi byte yaitu SubBytes, ShiftRows, MixColumns, dan AddRoundKey. [6] [7].

2.8 Cipher Block Chaining

CBC (singkatan dari cipher-block chaining) adalah mode block cipher AES yang lebih unggul dari mode ECB dalam hal menyembunyikan pola pada plaintext. Mode CBC mencapai hal ini dengan melakukan XOR antara blok plaintext pertama (B_1) dengan initialization vector sebelum dienkripsi. CBC juga menggunakan chaining blok di mana setiap blok plaintext selanjutnya di-XOR dengan ciphertext dari blok sebelumnya. Jika dituliskan dalam notasi matematis, rumusnya akan menjadi:

$$C_i = E_K (B_i \oplus C_{i-1}) \quad (1)$$

di mana E_K menunjukkan algoritma enkripsi blok menggunakan kunci K, dan C_{i-1} adalah cipher yang sesuai dengan B_{i-1}. Untuk dekripsinya secara matematis akan menjadi:

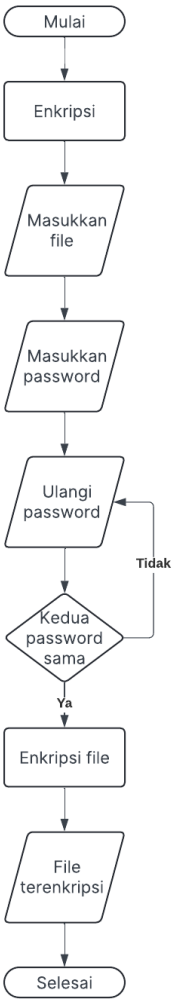
$$B_i = D_K (C_i) \oplus (C_{i-1}) \quad (2)$$

di mana D_K menunjukkan algoritma enkripsi blok menggunakan kunci K.

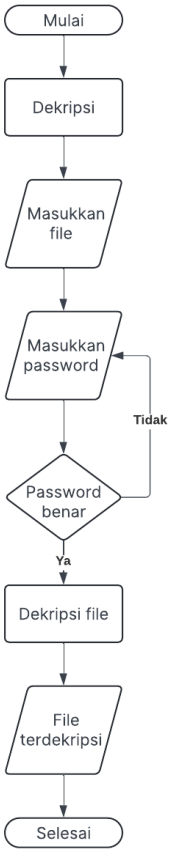
2.9 Desain Sistem

Sistem akan terdiri dari dua proses yaitu proses enkripsi dan proses dekripsi. Masing-masing proses dapat dilihat pada Gambar 2 dan Gambar 3. Proses Enkripsi dapat dilihat pada Gambar 2, dimulai dari memasukkan file resep yang hendak dienkripsi, selanjutnya dilanjutkan dengan membuat password enkripsi dan mengulangi password yang sama. Sistem akan mengecek apakah kedua password telah sama dan memenuhi persyaratan. Jika kedua password telah sama dan memenuhi persyaratan, akan muncul tombol untuk mengenkripsi file resep. Jika kedua password tidak sama/belum memenuhi persyaratan, maka dilakukan pengulangan untuk memasukkan password. Selanjutnya sistem akan mengenkripsi file resep menggunakan algoritma AES dengan mode CBC, lalu file resep yang telah dienkripsi dapat diunduh. Proses dekripsi dapat dilihat pada Gambar 3, dimulai dari memasukkan file resep yang telah dienkripsi sebelumnya, lalu dilanjutkan dengan memasukkan password yang telah digunakan untuk melakukan enkripsi sebelumnya. Sistem akan mengecek apakah password yang dimasukkan sama dengan password yang digunakan untuk melakukan enkripsi, jika salah maka dapat dilakukan penginputan password lagi, dan jika benar maka file resep terenkripsi akan didekripsi oleh sistem, lalu file terdekripsi dapat diunduh.

p-ISSN: 2986-3929
e-ISSN: 3032-1948



Gambar 2. Diagram Alir Enkripsi



Gambar 3. Diagram Alir Dekripsi

3. Hasil dan Diskusi

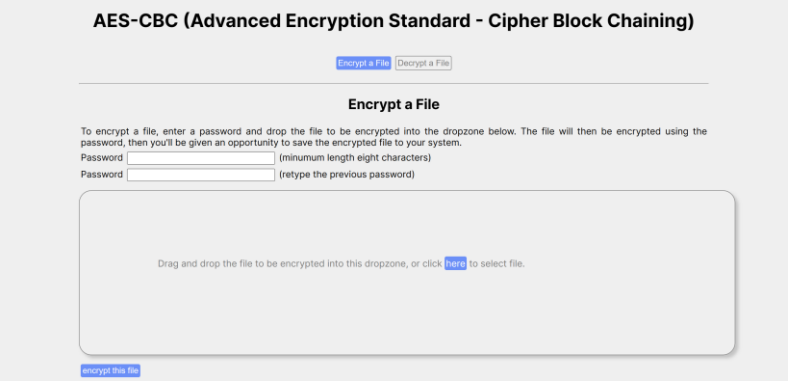
3.1. Implementasi Sistem

Sistem ini akan terbagi menjadi dua bagian yaitu proses enkripsi dan dekripsi. Masing-masing proses akan berjalan di web tanpa memerlukan koneksi internet agar dapat memastikan bahwa tidak ada data yang bocor dan tersebar ke internet.

3.1.1. Tampilan Proses Enkripsi

Saat hendak melakukan proses enkripsi, dibutuhkan file resep berupa file berformat .txt, .doc, .jpg, .png ataupun .pdf. Selanjutnya dapat memasukkan password dan perulangan password. Jika sudah, dapat dilakukan proses enkripsi. Proses enkripsi akan menghasilkan file berformat sama dengan format asli yang ditambahkan format.enc. Gambar 4 merupakan tampilan proses enkripsi resep dokter.

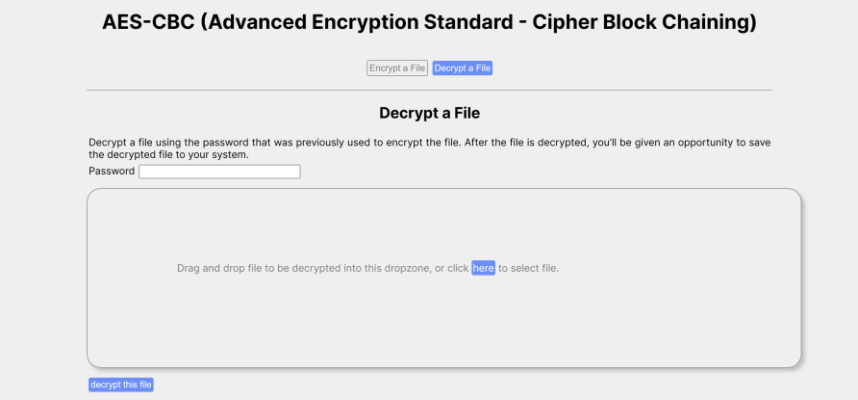
p-ISSN: 2986-3929
e-ISSN: 3032-1948



Gambar 4. Tampilan Proses Enkripsi

3.1.2. Tampilan Proses Dekripsi

Saat hendak melakukan proses dekripsi, dibutuhkan file resep terenkripsi berupa file berformat .txt, .doc, .jpg, .png ataupun .pdf yang telah ditambahkan format. enc sebelumnya. Selanjutnya dapat memasukkan password yang telah dibuat sebelumnya. Jika sudah, dapat dilakukan proses dekripsi. Proses dekripsi akan menghasilkan file berformat sama dengan format asli yang ditambahkan format.dec. Gambar 5 merupakan tampilan untuk proses dekripsi resep dokter.



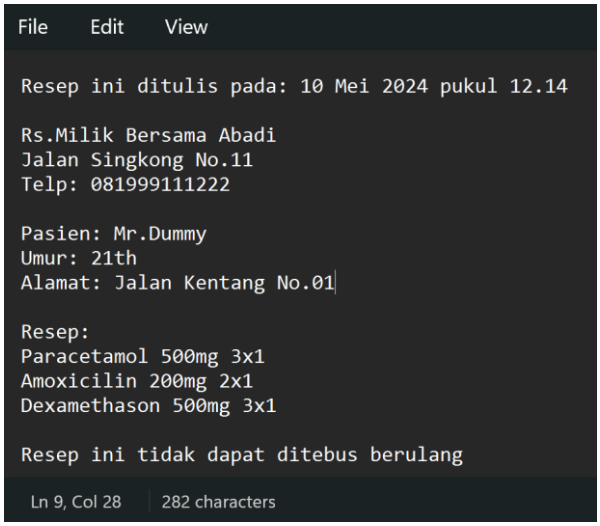
Gambar 5. Tampilan Proses Dekripsi

3.2. Pengujian Sistem

3.2.1. Pengujian Enkripsi AES mode CBC

Pengujian enkripsi algoritma AES dengan mode CBC pada penelitian ini menggunakan data resep dummy yang telah peneliti buat sebelumnya dengan harapan untuk menguji apakah algoritma AES mode CBC berhasil diterapkan atau tidak.

p-ISSN: 2986-3929
e-ISSN: 3032-1948



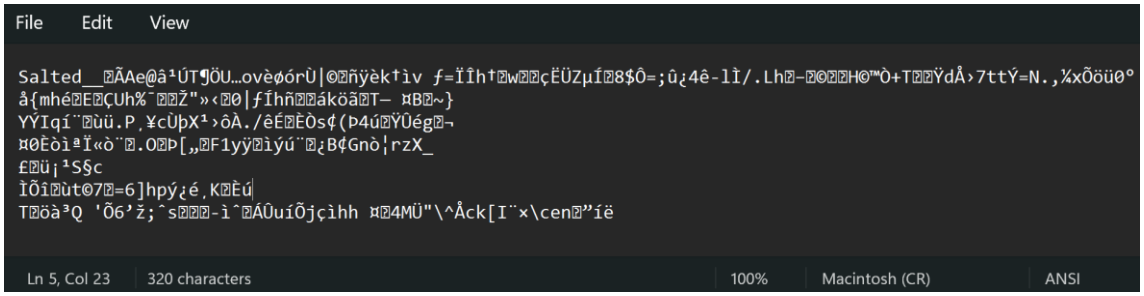
Gambar 6. Data Dummy Plaintext Berformat .txt

Gambar 6 merupakan salah satu contoh data dummy berupa plaintext, data resep tersebut ditulis dalam bahasa Indonesia yang dapat dibaca dan dipahami oleh seseorang. Data dummy adalah informasi yang tidak mengandung data berguna apapun, tetapi berfungsi untuk memesan ruang di mana data nyata secara nominal hadir. Data dummy dapat digunakan sebagai placeholder untuk tujuan pengujian dan operasional. Untuk pengujian, data dummy juga dapat digunakan sebagai stub atau pad untuk menghindari masalah pengujian perangkat lunak dengan memastikan bahwa semua variabel dan bidang data terisi. Data dummy resep dokter untuk pengujian algoritma AES adalah data buatan yang menyerupai resep dokter asli, namun tidak mengandung informasi pasien yang sebenarnya. Data ini digunakan untuk menguji kinerja algoritma AES dalam mengenkripsi dan mendekripsi data medis sensitif.

Gambar 7. Proses Enkripsi

Gambar 7 menunjukkan proses untuk melakukan enkripsi file resep. File dummy bernama “Resep Obat Mr.Dummy.txt” berukuran 297 Bytes telah dimasukkan ke sistem. Pengguna telah memasukkan password yang valid dan file resep telah terenkripsi dilihat dari pemberitahuan “File Encrypted” yang berwarna hijau.

p-ISSN: 2986-3929
e-ISSN: 3032-1948

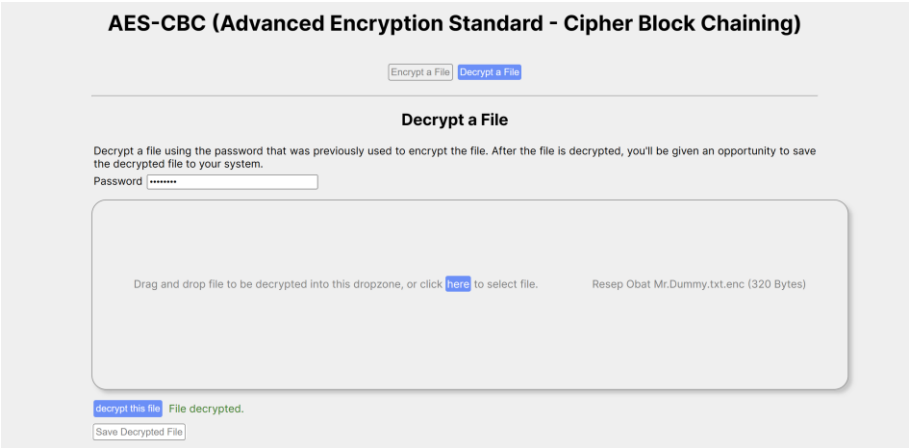


Gambar 8. File Terenkripsi berupa Chipertext

Gambar 8 menunjukkan hasil enkripsi berupa chipertext yang sudah tidak dapat terbaca lagi. Chipertext hasil dari enkripsi resep dokter menggunakan algoritma AES adalah string teks yang tidak dapat dipahami yang mewakili resep dokter asli. Chipertext ini dihasilkan dengan menggabungkan resep dokter asli dengan kunci enkripsi AES. Algoritma AES menggunakan serangkaian substitusi dan permutasi yang kompleks untuk mengubah data asli menjadi chipertext.

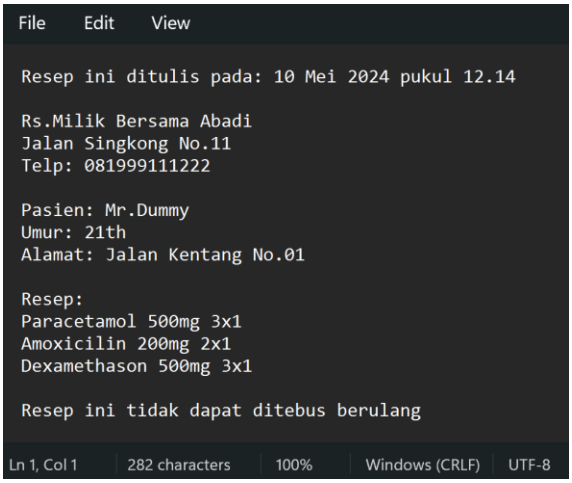
3.2.2. Pengujian Dekripsi AES mode CBC

Pengujian dekripsi algoritma AES dengan mode CBC pada penelitian ini menggunakan data resep dummy yang telah peneliti buat dan dekripsi sebelumnya dengan harapan untuk menguji apakah algoritma AES mode CBC berhasil diterapkan atau tidak. Gambar 9 menunjukkan proses untukl melakukan dekripsi. File dummy bernama “Resep Obat Mr.Dummy.txt.enc” berukuran 320 Bytes telah dimassukan ke sistem. Pengguna telah memasukkan password enkripsi yang valid dan file resep telah berhasil didekripsi, dapat dilihat dari pemberitahuan “File decrypted” yang berwarna hijau. Gambar 10 menunjukkan hasil dekripsi resep dokter berupa plaintext yang dapat terbaca dengan berbahasa Indonesia sesuai dengan plaintext asli sebelum dienkripsi. Ini menunjukkan bahwa proses enkripsi serta dekripsi telah berhasil dilakukan tanpa mengubah informasi dalam file resep asli. File hasil dekripsi yang diperoleh berukuran 297 Bytes sama dengan file asli namun file hasil dekripsi berukuran 320 Bytes menunjukkan ada peningkatan ukuran dalam file hasil dekripsi.



Gambar 9. Proses Dekripsi

p-ISSN: 2986-3929
e-ISSN: 3032-1948



Gambar 10. Plaintext Hasil Dekripsi

3.3. Pengujian Akurasi Sistem

Menguji tingkat keberhasilan sistem akan dilakukan pengujian terhadap 20 file resep dokter berbeda.

3.3.1. Pengujian Akurasi Enkripsi

Tabel 1. Hasil Pengujian Enkripsi

No	Nama File	Ukuran Asli	Nama File Terenkripsi	Ukuran File Terenkripsi	Keterangan
1	Resep Obat Dummy.txt	297 Bytes	Resep Obat Dummy.txt.enc	320 Bytes	Berhasil
2	presc1.txt	146 Bytes	presc1.txt.enc	176 Bytes	Berhasil
3	presc2.txt	147 Bytes	presc2.txt.enc	176 Bytes	Berhasil
4	presc3.txt	144 Bytes	presc3.txt.enc	176 Bytes	Berhasil
5	presc4.txt	282 Bytes	presc4.txt.enc	304 Bytes	Berhasil
6	presc5.txt	353 Bytes	presc5.txt.enc	384 Bytes	Berhasil
7	presc6.txt	342 Bytes	presc6.txt.enc	368 Bytes	Berhasil
8	presc7.txt	880 Bytes	presc7.txt.enc	912 Bytes	Berhasil
9	presc8.txt	491 Bytes	presc8.txt.enc	512 Bytes	Berhasil
10	presc9.txt	246 Bytes	presc9.txt.enc	272 Bytes	Berhasil
11	presc10.txt	517 Bytes	presc10.txt.enc	544 Bytes	Berhasil
12	presc11.txt	140 Bytes	presc11.txt.enc	160 Bytes	Berhasil
13	presc12.txt	349 Bytes	presc12.txt.enc	368 Bytes	Berhasil
14	presc13.txt	703 Bytes	presc13.txt.enc	720 Bytes	Berhasil
15	presc14.txt	401 Bytes	presc14.txt.enc	432 Bytes	Berhasil
16	presc15.txt	331 Bytes	presc15.txt.enc	352 Bytes	Berhasil
17	presc16.txt	355 Bytes	presc16.txt.enc	384 Bytes	Berhasil

p-ISSN: 2986-3929
e-ISSN: 3032-1948

No	Nama File	Ukuran Asli	Nama File Terenkripsi	Ukuran File Terenkripsi	Keterangan
18	presc17.txt	510 Bytes	presc17.txt.enc	528 Bytes	Berhasil
19	presc18.txt	245 Bytes	presc18.txt.enc	272 Bytes	Berhasil
20	presc19.txt	385 Bytes	presc19.txt.enc	416 Bytes	Berhasil

Telah dilakukan pengujian enkripsi dengan dua puluh file resep berbeda. Pada tabel 1 dapat dilihat bahwa ukuran file asli mengalami perubahan setelah dilakukan enkripsi. Algoritma enkripsi AES CBC (Cipher Block Chaining) membutuhkan blok data input yang memiliki panjang yang kelipatan dari ukuran blok AES (biasanya 128 bit). Jika panjang data input tidak kelipatan dari ukuran blok, maka data input harus dipad dengan bit tambahan agar panjangnya menjadi kelipatan dari ukuran blok. Bit padding ini akan meningkatkan ukuran file setelah enkripsi. Selain itu format file juga akan berubah setelah dienkripsi, sistem akan menambahkan format. enc pada file terenkripsi. Pengujian enkripsi terhadap kedua puluh file tersebut berhasil dilakukan.

Tabel 2. Hasil Pengujian Dekripsi

No	Nama File	Ukuran	Nama FileTerdekripsi	Ukuran File Terdekripsi	Keterangan
1	Resep Obat Dummy.txt	320 Bytes	Resep Obat Dummy.txt.enc	297 Bytes	Berhasil
2	presc1.txt.enc	176 Bytes	presc1.txt.enc.dec	146 Bytes	Berhasil
3	presc2.txt.emc	176 Bytes	presc2.txt.enc.dec	147 Bytes	Berhasil
4	presc3.txt.enc	176 Bytes	presc3.txt.enc.dec	144 Bytes	Berhasil
5	presc4.txt.enc	304 Bytes	presc4.txt.enc.dec	282 Bytes	Berhasil
6	presc5.txt.enc	384 Bytes	presc5.txt.enc.dec	353 Bytes	Berhasil
7	presc6.txt.enc	368 Bytes	presc6.txt.enc.dec	342 Bytes	Berhasil
8	presc7.txt.enc	912 Bytes	presc7.txt.enc.dec	880 Bytes	Berhasil
9	presc8.txt.enc	512 Bytes	presc8.txt.enc.dec	491 Bytes	Berhasil
10	presc9.txt.enc	272 Bytes	presc9.txt.enc.dec	246 Bytes	Berhasil
11	presc10.txt.enc	544 Bytes	presc10.txt.enc.dec	517 Bytes	Berhasil
12	presc11.txt.enc	160 Bytes	presc11.txt.enc.dec	140 Bytes	Berhasil
13	presc12.txt.enc	368 Bytes	presc12.txt.enc.dec	349 Bytes	Berhasil
14	presc13.txt.enc	720 Bytes	presc13.txt.enc.dec	703 Bytes	Berhasil
15	presc14.txt.enc	432 Bytes	presc14.txt.enc.dec	401 Bytes	Berhasil
16	presc15.txt.enc	352 Bytes	presc15.txt.enc.dec	331 Bytes	Berhasil
17	presc16.txt.enc	384 Bytes	presc16.txt.enc.dec	355 Bytes	Berhasil
18	presc17.txt.enc	528 Bytes	presc17.txt.enc.dec	510 Bytes	Berhasil
19	presc18.txt.enc	272 Bytes	presc18.txt.enc.dec	245 Bytes	Berhasil
20	presc19.txt.enc	416 Bytes	presc19.txt.enc.dec	385 Bytes	Berhasil

Selanjutnya dilakukan pengujian dekripsi dengan dua puluh file resep berbeda yang telah dienkripsi sebelumnya. Pada tabel 2 dapat dilihat bahwa ukuran file mengalami perubahan ke ukuran file asli sebelum di enkripsi. Saat data dienkripsi dengan AES CBC, padding yang

ditambahkan pada langkah enkripsi dihapus pada langkah dekripsi. Hal ini mengembalikan panjang data ke ukuran semula. Mode CBC AES menambahkan blok ciphertext dari blok sebelumnya ke blok plaintext saat ini sebelum enkripsi. Saat data didekripsi, operasi ini dibalik, sehingga blok ciphertext pertama didekripsi menggunakan kunci enkripsi saja, dan blok ciphertext selanjutnya didekripsi dengan menggunakan blok ciphertext sebelumnya dan kunci enkripsi. Hal ini mengembalikan data ke format plaintext asli, dengan panjang yang sama dengan plaintext sebelum enkripsi. Sistem menambahkan format. dec pada file hasil dekripsi. Pada kedua puluh file yang dilakukan pengujian, semua file berhasil didekripsi.

4. Kesimpulan

Dapat disimpulkan bahwa enkripsi dan dekripsi menggunakan AES-CBC untuk mengamankan resep dokter berhasil dilakukan. Hasil enkripsi menunjukkan bahwa resep dokter yang telah dienkripsi tidak dapat dibaca oleh pihak yang tidak berwenang. Hal ini dibuktikan dengan tidak terbacanya pesan yang telah dienkripsi. Proses dekripsi juga berhasil dilakukan, dimana resep dokter yang telah didekripsi kembali menjadi pesan yang sama dengan resep asli. Hal ini menunjukkan bahwa proses enkripsi dan dekripsi tidak merusak data resep dokter. Secara keseluruhan, penelitian ini menunjukkan bahwa AES-CBC merupakan metode yang efektif untuk mengamankan resep dokter dan meminimalisir penyalahgunaan obat.

Daftar Pustaka

[1] M. R. COHEN, "Medication Errors," American Journal of Pharmaceutical Education, 2007.

[2] M. J. Rantucci, Komunikasi Apoteker-Pasien Panduan Konseling Pasien, Jakarta: EGC, 2009.

[3] I. Lisni, N. E. Gumilang and E. Kusumahati, "Potensi Medication error Pada Resep di Salah Satu Apotek di Kota Kadipaten," Jurnal Sains dan Kesehatan, vol. 3, no. 4, pp. 558-568, 2021.

[4] Admin, "Universitas Gadjah Mada," Universitas Gadjah Mada, 7 January 2014. [Online]. Available: https://ugm.ac.id/id/berita/8575-pemakai-narkoba-gunakan-obat-terlarang-dari-resep-dokter/. [Accessed 9 May 2024].

[5] C. S. Lestari, Seni Menulis Resep, Jakarta: PT Perca, 2002.

[6] T. M. Kumar and P. Karthigaikumar, "FPGA implementation of an optimized key expansion module of AES algorithm for secure transmission of personal ECG signals," Design Automation for Embedded Systems, vol. 22, no. 1-2, pp. 13-24, 2018.

[7] H. M. Mohammad and A. A. Abdullah, "Enhancement process of AES: a lightweight cryptography algorithm-AES for constrained devices," TELKOMNIKA (Telecommunication Computing Electronics and Control), vol. 20, no. 3, pp. 551-560, 2022.

[8] F. P. Utama, G. Wijaya, R. Faurina and A. Vatresia, "Implementasi Algoritma Aes 256 Cbc, Base 64, Dan Sha 256 Dalam Pengamanan Dan Validasi Data Ujian Online," Jurnal Teknologi Informasi dan Ilmu Komputer (JTIIK), vol. 10, no. 5, pp. 945-954, 2014.

[9] M. Azhari, D. I. Mulyana, F. J. Perwitosari and F. Ali, "Implementasi Pengamanan Data pada Dokumen Menggunakan Algoritma Kriptografi AdvancedEncryption Standard(AES)," Jurnal Pendidikan Sains dan Komputer, vol. 2, no. 1, 2022.

[10] Henry, A. H. Kridalaksana and Z. Arifin, "Kriptografi Aes Mode Cbc Pada Citra Digital," Prosiding Seminar Ilmu Komputer dan Teknologi Informasi , vol. 1, no. 1, 2016.