Impementasi Algoritma AES untuk Enkripsi Data Dokumen Pada Kantor Desa Seren Selimbau

Nurmala[1], Noviyanti. P[2]

Program Studi Teknologi Informasi, Institut Shanti Bhuana, Bengkayang, Jl. Bukit Karmel, No. 1, Bengkayang, Indonesia [1,2]

nurmala@shantibhuana.ac.id[1], noviyanti@shantibhuana.ac.id[2]

Abstrak – Kantor desa Seren Selimbau memiliki banyak dokumen penting yang perlu dilindungi dari akses yang yang tidak sah. Selama belum ada perlindungan khusus yang dilakukan oleh Kantor Desa Seren Selimbau terhadap dokumen yang dimiliki sehingga rawan terjadi kebocoran informasi. Implementasi dari algoritma *Advanced Encription Standard* atau dikenal dengan AES bertujuan untuk memberikan keamanan data dokumen yang dimiliki serta melakukan pencegahan terhadap kebocoran informasi.Penelitian ini membahas tentang implementasi sistem enkripsi data dokumen di Kantor Desa Seren Selimbau. Penggunaan Algoritma AES sebagai algoritma untuk enkripsi data digunakan karena algoritma ini memiliki proses pengamanan yang tinggi dan telah menjadi standar enkripsi data yang diakui secara internasional. Sistem enkripsi data dokumen ini dikembangkan menggunakan bahasa pemrograman C#. Sistem ini memungkinkan pengguna untuk mengenkripsi dokumen dengan mudah dan aman.

Kata Kunci – Algoritma AES, Dokumen, Kantor Desa, Keamanan data

Abstract - The Seren Selimbau village office has many important documents that need to be protected from unauthorized access. As long as there is no special protection carried out by the Seren Selimbau Village Office for the documents held, it is prone to information leaks. The implementation of the Advanced Encryption Standard algorithm, known as AES, aims to provide security for owned document data and prevent information leaks. This research discusses the implementation of the document data encryption system at the Seren Selimbau Village Office. The use of AES algorithm as an algorithm for data encryption is used because this algorithm has a high-security process and has become an internationally recognized data encryption standard. This document data encryption system was developed using the C# programming language. This system allows users to encrypt documents easily and securely.

Key Words – AES Algorithm, Data security, Document, Vilage Office

I. PENDAHULUAN

Di era digital yang berkembang sangat pesat ini, keamanan data, termasuk keamanan data dari dokumen menjadi semakin penting dan perlu diperhatikan dengan serius. Hal ini dikarenakan data-data dalam dokumen sangat krusial karena berkaitan dengan kerahasiaan informasi karyawan, saham dan lainnya, kepatuhan terhadap regulasi, resiko adanya pencurian identitas, kerugian finansial, maupun integritas dokumen itu sendiri. Mengingat pentingnya peran dari dokumen itu sendiri maka dokumen dinyatakan sebagai salah satu elemen terpenting dalam sebuah organisasi guna mendukung kegiatan administrasi sebuah organisasi[1]. Dokumen adalah sebuah rekaman informasi yang dapat berupa tulisan, gambar, suara,video,atau kombinasi dari semuannya.Dokumen digunakan sebagai bukti atau keterangan untuk berbagai keperluan.Untuk itu, agar dokumen tersebut tetap aman tentunya perlu dilindungi dari akses yang tidak sah. Pencurian dan penyadapan dokumen saat ini menjadi sangat rentan sehingga dapat mengakibatkan banyak kerugian bagi pemilik dokumen. Velumadhaca

Rao dan Selvamani (2015) dalam [2] menyatakan bahwa kehilangan atau kebocoran data dapat memiliki dampak serius pada bisnis, merk, dan kepercayaan sebuah organisasi. Oleh karena itu, perlindangan data dan keamanan informasi menjadi sangat penting bagi setiap organisasi. Salah satu hal yang mendukung perlindungan data dan keamanan informasi adalah adanya teknologi keamanan data yang mutakhir, sehingga dapat meminimalisir kehilangan maupun kecurian data.

Kantor Desa Seren Selimbau adalah pusat administrasi dan pelayanan masyarakat untuk wilayah Desa Seren Selimbau. Sebagai bagian dari struktur pemerintahan di tingkat desa, kantor ini bertanggung jawab untuk menyediakan berbagai layanan administratif kepada penduduk desa tersebut. Dalam menyimpan data, kantor desa ini menggunakan arsip dokumen digital yang terdapat dalam suatu folder pada komputer tanpa adanya sistem pengaman data yang efektif. Untuk itu kantor desa tersebut memerlukan solusi untuk memastikan data dokumen digital dimiliki aman dari kehilangan atau kebocoran data[2]. Melalui sistem ini diharapkan bisa mengamankan dokumen-dokumen penting lainnya. Untuk mengakses sistem ini di kantor desa,tidak perlu memerlukan akses internet karena proses enkripsi sepenuhnya dilakukan di komputer atau perangkat lokal. Untuk mencegah dari kebocoran dan kehilangan data, perlu mengimplementasikan tahap-tahap keamanan data yang Tangguh dan kuat, termasuk enkripsi data, serta kontrol akses yang ketat.

Untuk menjaga data dokumen agar tetap aman yaitu dengan menerapkan algoritma Advanced Encryption Standard (AES). Algoritma AES sendiri merupakan algoritma kriptografi simetris. Kriptografi simetris merupakan sebuah kriptografi dimana kegiatan enkripsi dan dekripsinya menggunakan kunci yang sama[3]. Dengan demikian, sebuah informasi yang bersifat sensitive dapan di enkripsi menggukan sebuah kunci, dimana proses dekripsinya hanya bisa dilakukan oleh pihak yang memiliki kunci yang digunakan untuk melakukan enkripsi. Penggunaan algoritma AES pada penelitian ini didukung oleh penelitian yang dilakukan sebelumnya. Menurut [4] algoritma AES memiliki kemampuan untuk melakukan enkripsi serta melakukan dekripsi dengan Panjang kunci yang bervasiasi, yaitu 128 bit, 192 bit, maupun 256 bit. Perbedaan Panjang kunci pada algoritma AES akan mempengaruhi jumlah putaran pada proses enkripsi dan dekripsi. Semakin Panjang jumlah putarannya maka akan menawarkan keamanan yang lebih tinggi, tetapi sangat berpengaruh pada kinerja / waktu untuk melakukan proses enkripsi maupun dekripsi. Dari sini dapat disimpulkan bahwa algoritma AES menawarkan sebuah fleksibilatas dalam kegiatan enkripsi maupun dekripsinya. Pengetahuna tentang enkripsi muncul ketika pembahasan mengarah pada kriptografi, dimana kriptografi tersebut merupakan sebuah ilmu yang membahas tentang cara untuk melindungi informasi dengan melakukan perubahan pada teks asli atau dikenal dengan plain text menjadi sebuah teks yang sulit untuk dibaca atau dikenal dengan istilah chippertext. Ciri-ciri dari kriptografi adalah adanya proses enkripsi, proses dekripsi, kunci, serta keamanan informasi. Enkripsi adalah proses mengubah data plaintex (teks asli atau data yang dapat dibaca) menjadi ciphertext untuk melindungi informasi dari akses yang tidak sah[5], [6]. Plaintext merupakan informasi asli, dan ciphertext merupakan pesan yang telah diubah menjadi kode acak agar tidak mudah dibaca[7].

Karena memanfaatkan teknologi informasi, maka penelitian yang dilakukan adalah penelitian yang melibatkan dokumen-dokumen yang telah terdigitalisasi, yaitu dokumen yang plain text nya dalam bentuk file dengan ekstensi .pdf, .doc, dan .txt. sebagai referensi dari penelitian yang dilakukan saat ini adalah penelitian yang telah dilakukan sebelumnya oleh Delisman Hulu dkk, dengan judul Implementasi algoritma AES (Advanced Encryption Standard) untuk keamanan file hasil radiologi di RSU Imelda Medan. Penelitian ini memiliki tujuan yang sama dengan penelitian yang sedang berjalan yaitu melakukan perlindungan terhadap data dengan studi kasus yang berbeda[8]. Referensi berikutnya adalah penelitian yang dilakukan oleh Handrian dan Siswanto,yang berjudul Implementasi kriptografi dengan menggunakan metode RC-4 dan AES untuk mengamankan file dokumen pada PT Varnion Technologhy Semesta [9]. Berbeda dengan penelitian petama, penelitian yang dilakukan oleh

pISSN: 2252-486X
eISSN: 2548-4710

handrian dan Siswanto ini menggunakan dua algoritma sekaligus yaitu algoritma RC-4 dan algoritma AES. Dengan penggunaan dua algoritma tersebut hasil yang didapatkan lebih baik dari pada menggunakan algoritma AES saja. Referensi terakhir yang dijadi rujukan dalam penelitian ini adalah hasil penelitian dari Hoerul Fiji dan Noni Juliasari mengenai Implementasi Pengamanan Dokumen menggunakan Kriptografi dengan Advanced Encryption Standard 256 atau AES256 pada Celebes Kontruksindo PT. [10]. Penelitian yang menjadi rujukan terakhir ini bertujuan untuk melakukan proses keamanan data pada PT. Celebes Kontruksindo dengan menggunakan kunci yang paling Panjang yaitu kunci dengan panjang 256 bit, sehingga enkripsi yang dihasilkan lebih terjamin keamanannya.

I. TINJAUAN PUSTAKA

1. Keamana Data

Keamanan data pada dokumen saat ini sangat penting. Untuk itu data yang ada pada dokumen perlu dilindungi dan diamankan dari akses yang tidak sah. Pencurian dan penyadapan dokumen saat ini menjadi sangat rentan sehingga dapat mengakibatkan banyak kerugian bagi pemilik dokumen. Kerugian bagi pemilik dokumen dapat berupa kehilangan data ataupun kebocoran data. Survey yang dilakukan menunjukkan bahwa pencegahan terhadap data penting untuk dilakukan. Surveyor menyatakan perlindungan data sebesar 88% bersifat krisis dan sangat penting [2].

2. Dokumen

Dokumen adalah sebuah rekaman informasi yang dapat berupa tulisan, gambar, suara, video, atau kombinasi dari semuannya. Dokumen digunakan sebagai bukti atau keterangan untuk berbagai keperluan. Istilah dokumen berasal dari bahsa latin yaitu ‘documentum’ yang diartikan dalam Bahasa Indonesia sebagai sebuah bukti atau keterangan tertulis. Sehingga dokumen sering dijadikan sebagai bahan rujukan terhadap semuah proses atau kegiatan yang akan dilakukan. Sebuah perusahaan dikatakan memiliki administrasi yang baik jika perusahaan tersebut memiliki dokumen-dokumen yang dapat diakses dengan mudah dan dapat dipertanggungjawabkan dalam penggunaannya.

3. Algoritma advanced Encrytion Standard (AES)

Algoritma Advanced Encryption Standard (AES) adalah salah satu algoritma kriptografi yang digunakan secara luas untuk mengamankan data digital. Dikembangkan oleh dua kriptografer asal Belgia yaitu Joan Daemen dan Vincent Rijmen ini digunakan dan dipilih sebagai standar oleh National Institute of Standards and Technology (NIST) Amerika Serikat pada tahun 2001. Beberapa poin penting yang harus diketahui ketika menggunakan algoritma AES adalah

a. proses yang bersifat simetris yaitu proses enkripsi dan dekripsi menggunakan kunci yang sama, panjang kunci pada algoritma AES.
b. Menggunakan panjang kunci yang bervariatif yang berpengaruh pada keamanan dan performa dari proses kriptografi.
c. Merupakan algoritma yang telah berstandart internasional yaitu digunakan secara luas oleh banyak pihak.
d. Keamaman yang teruji dari NIST [2].

Poin B pada penjelasan di atas memberikan gambaran terhadap jumlah putaran atau iterasi yang dapat dilakukan oleh algoritma AES. Tabel 1 merupakan tabel yang memperlihatkan keterkaitan penggunaan kunci / key dengan jumlah round / iterasi.

Tabel 1 Jumlah Round pada Algoritma AES

	Key	**Input Block**	**round**
AES-128	128 bits	128 bits	10
AES-192	192 bits	128 bits	12
AES-256	256 bits	128 bits	14

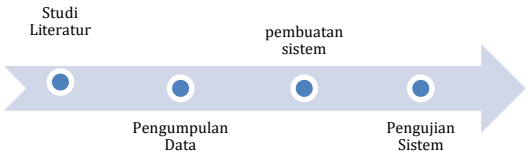
Dari Tabel 1 didapatkan bahwa semakin panjang bit untuk kuncinya maka jumlah putaran yang harus dilalui oleh setiap prosesnya juga bertambah besar. Dengan semakin besarnya proses perulangan tersebut menyebabkan data yang dihasilpan pada proses tersebut akan lebih terjamin keamananya.

II. ANALISA DAN PERANCANGAN SISTEM

Pada penelitian ini terdapat beberapa tahapan, yaitu tahapan yang pertama dimulai dengan mempelajari literatur mengenai

kriptografi, khususnya algoritma AES yang akan menjadi referensi bagi penulis untuk mengatasi permasalahan dalam penelitian ini. Setelah itu analisa data pada suatu instansi dengan mempelajari data apa saja yang akan dilindungi atau diamankan, kemudian membuat sebuah sistem atau aplikasi untuk pengamanan data berbentuk file dokumen digital. Setelah sistem selesai dibuat, akan dilakukan uji coba sistem.

Tahapan ini seperti pada Gambar 1.



Gambar 1. Tahapan penelitian

a. Studi Literatur

Dalam tahapan ini dilakukan tinjauan terhadap suatu jurnal,artikel, atau penelitian terlebih dahulu yang nantinya akan digunakan sebagai bahan referensi bagi penulis dalam mengatasi atau melaksanakan penelitian ini. Literatur yang di pelajari adalah mengenai algoritma AES.

b. Pengumpulan data

Pada metode ini,terdapat beberapa tahapan untuk mengumpulkan suatu informasi,data,dan materi yang berkaitan dengan permasalahan yang ada. Tahapannya yaitu, interview,observasi, analisa dokumen. Berikut penjelasan mengenai kedua metode pengumpulan data tersebut.

a. Interview (Wawancara).

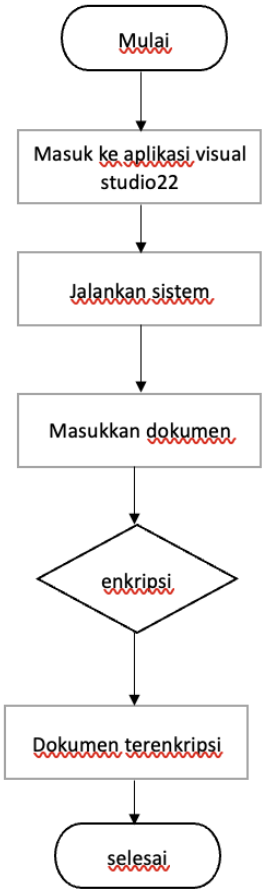
Proses interaksi langsung antara peneliti dan pihak yang terlibat dalam pengembangan suatu aplikasi atau sebuah program melalui wawancara untuk mendapatkan informasi yang mendalam tentang topik tertentu sesuai penelitian yang dilakukan.

b. Observasi.

Metode pengumpulan data dalam penelitian di mana peneliti secara langsung mengamati subjek atau fenomena yang sedang diteliti dalam lingkungan alaminya. Misalnya pengamatan langsung mengenai operasi sistem secara mendalam.

c. Pembuatan Sistem

Sebelum membuat sistem, dilakukan tahapan merancang sistemnya terlebih dahulu. Perancangan sistem didapatkan dengan membuat flowchart yang menjabarkan tahapan perlaksanaan proses enkripsi sebuah dokumen. Gambar 2 merupakan flowchart untuk enkripsi data pada dokumen milik Kantor desa Seren Selimbau. Flowchart sistem digambarkan seperti pada Gambar 2. Dengan adanya flowchart, maka programmer dapat mengembangkan aplikasi dengan menggunakan bahasa pemrograman C#. Bahasa Pemrograman C# dapat dikerjakan dengan menggunakan teks editor berupa Visual Studio22.



Gambar 2. Flowchart sistem

Kegiatan enkripsi dokumen yang dilakukan pada Gambar 2 dimulai dengan masuk pada penu tampilan pada Visual Studio22 kemudian memasukkan dokumen yang ingin dienkripsi dan hasil akhir berupa dookumen yang telah

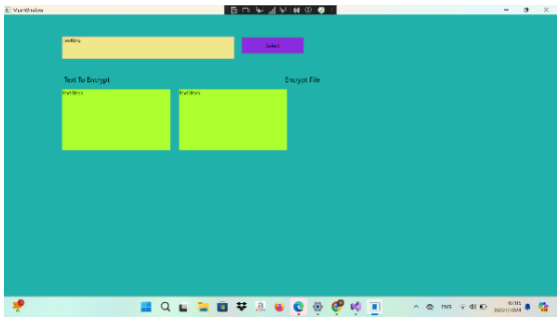
pISSN: 2252-486X
eISSN: 2548-4710

terenkripsi sehingga susah untuk dipahami oleh orang lain.

III. IMPLEMENTASI DAN PEMBAHASAN

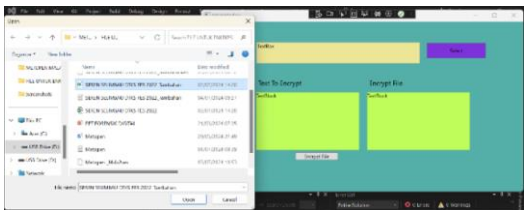
Gambar 3. Tampilan Masuk ke Visual Basic22

Gambar 3 menunjukan langkah awal sebelum menjalankan sistem, masuk ke aplikasi Visual Studio22 untuk memulai. Setelah itu, pengguna diminta untuk menjalankan sistem melalui Visual Studio.



Gambar 4. Tampilan Sistem

Gambar 4 menunjukan tampilan awal dari sistem. Setelah sistem run, akan muncul tampilan seperti Gambar 5

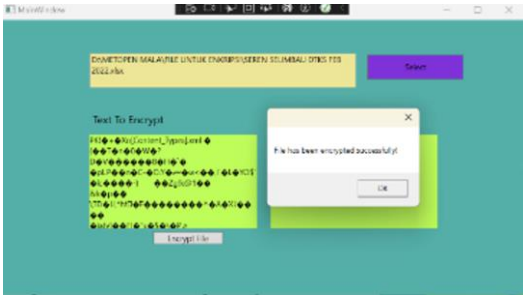


Gambar 5. Tampilan Masukan Dokumen

Gambar 5 menampilkan proses pengambilan dokumen/file yang akan dienkripsi. Setalh itu dokumen akan mulai melakukan enkripsi data. Proses enkripsi data terlihat pada Gambar 6.

Gambar 6. Tampilan Proses enkripsi

Proses enkripsi dokumen dapat dilihat pada Gamabr 6. Setelah pengguna memasukkan dokumen, dokumen tersebut akan diproses untuk dienkripsi.



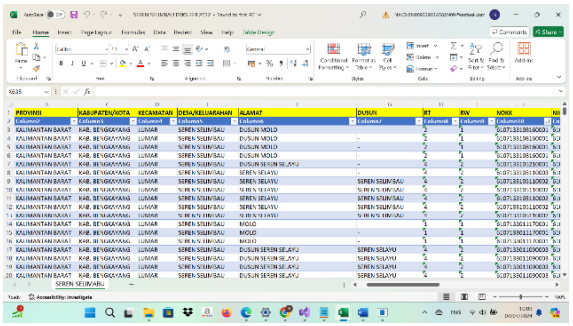
Gambar 7. Tampilan Proses enkripsi berhasil

Untuk melihat proses enkripsi berhasil dapat dilihat pada Gambar 7. Ketika proses enkripsi berhasil, akan muncul notif bahwa proses enkripsi telah berhasil.

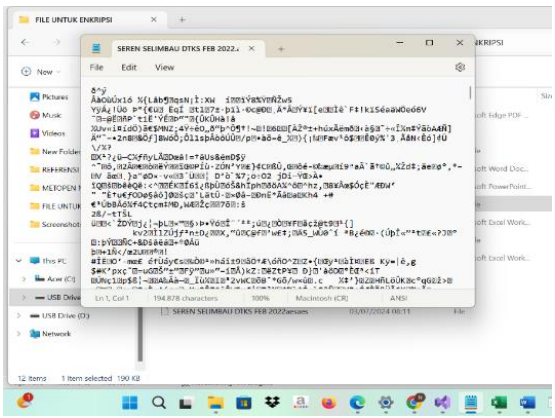
Gambar 7 menunjukkan keadaan file sebelum enkripsi, file tersebut berisi bebera padata yang diperlukan pengguna. Hasil dari proses enkripsi dapat dilihat pada Gambar 7, dimana isi diubah dari plaintext yang dapat dibaca menjadi ciphertext yang tidak dapat dibaca dan tidak mengandung informasi.

IV. PENGUJIAN

Pengujian yang dilakukan pada penelitian ini adalah pengujian yang bersifat *black box*. Dimana tester akan menguji sistem yang telah dikembangkan dari fungsi sistem yang berjalan. Pengujian ini yang dilakukan terlihat pada Gambar 8 yaitu file dokumen yang belum dienkripsi. Dapat dilihat bahwa dokumen tersebut masih berbentuk tulisan dan dapat di baca.



Gambar 8. Dokumen sebelum dienkripsi



Gambar 9. Sesudah enkripsi

Sesudah dilakukan enkripsi, dokumen yang tadinya masih bisa di baca,sekarang berubah menjadi tulisan yang sulit dibaca.

V. KESIMPULAN

Dari hasil penelitian yang telah dilakukan pada implementasi menggunakan algoritma enkripsi AES dalam mengamankan dokumen dapat disimpulkan bahwa penerapan metode algoritma AES dapat diterapkan dslam keamanan dokumen. Hasil dari implementasi ini menunjukkan bahwa AES mampu mengenkripsi dokumen dengan cepat tanpa mengorbankan keamanan data. Metode keamanan enkripsi dapat digunakan oleh suatu instansi untuk membantu menjaga keamanan informasi terkait instansi tersebut. Pada tahap ini, saran-saran disusun yang berguna untuk meningkatkan kualitas dan efisiensi dari implementasi tersebut, serta untuk memperbaiki sistem agar lebih baik.

REFERENSI

[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] W. Putra, M. R. Fahlevi, and A. T. Hidayat, "Implementasi Algoritma Advanced Encryption Standard Untuk Kemanan Dokumen," *J. Ilmu Komputer, Teknol. Dan Inf.*, vol. 1, no. 2, pp. 76–83, 2023, doi: 10.62866/jurikti.v1i2.55.

[3] V. Lusiana, "Implementasi Kriptografi Pada File Dokumen Menggunakan Algoritma Aes-128," *J. Din. Inform.*, vol. 3, no. 2, pp. 79–83, 2011.

[4] 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.

[5] C. Irawan and E. H. Rachmawanto, "Keamanan Data Menggunakan Gabungan Kriptografi AES dan RSA," *Proceeding SENDIU*, vol. l, no. 2, pp. 978–979, 2021.

[6] F. A. Nurbi and U. Budiyanto, "Penerapan Algoritme Rivest Code 4 Untuk Pengamanan Dokumen Di CV. Bintang Pratama Mandiri," *Semin. Nas. Mhs. ...*, no. September, pp. 182–191, 2022, [Online]. Available: http://senafti.budiluhur.ac.id/index.php/senafti/article/view/176%0Ahttps://senafti.budiluhur.ac.id/index.php/senafti/article/download/176/60

[7] G. Rassia Raudha and S. Amini, "Implementasi Algoritma Rivest Code 4 (Rc4) Untuk Pengamanan Dokumen Pada Pt. Tri Tunggal Multikreasi," *Semin. Nas. Mhs. Fak. Teknol. Inf. Jakarta-Indonesia*, vol. 4, no. September, pp. 310–318, 2022, [Online]. Available: https://senafti.budiluhur.ac.id/index.php/senafti/index

[8] 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.

pISSN: 2252-486X
eISSN: 2548-4710

[9] H. Saputra Djong and S. Siswanto, "Implementasi Kriptografi Dengan Menggunakan Metode Rc4 Dan Aes-256 Untuk Mengamankan File Dokumen Pada Pt Varnion Technology Semesta," *Semin. Nas. Mhs. Fak. Teknol. Inf. Jakarta-*

[10] H. Fiji Ardiansyah and N. Juliasari, "Implementasi Pengamanan Dokumen Menggunakan Kriptografi Dengan Advanced Encryption Standard 256 pada Celebes Kontruksindo PT.," *SENAFTI (Seminar Nas. Mhs. Fak. Teknol. Informasi)*, vol. 2, no. 2, pp. 260–268, 2023, [Online]. Available: https://senafti.budiluhur.ac.id/index.php/senafti/index