INNOVATIVE: Journal Of Social Science Research
Volume 4 Nomor 4 Tahun 2024 Page 1691-1699
E-ISSN 2807-4238 and P-ISSN 2807-4246
Website: https://j-innovative.org/index.php/Innovative

Penerapan Algoritma Kriptografi AES (Advanced Encryption Standard) 128 Pada Aplikasi Manajemen Pengarsipan Dinas Perpustakaan dan Kearsipan Kab. Minahasa Berbasis Web

Parabelem Tinno Dolf Rompas[1], Muhamad Zidan Dailer[2✉], Quido Conferti Kainde[3]
Universitas Negeri Manado
Email: zidan.dailer@gmail.com[2✉]

Abstrak

Penelitian ini mengevaluasi efektivitas penggunaan algoritma Advanced Encryption Standard (AES) 128 dalam mengelola arsip di Dinas Perpustakaan dan Kearsipan Kabupaten Minahasa. Penelitian ini bertujuan untuk mengukur dampak AES-128 terhadap efisiensi dan keamanan dalam mengenkripsi dan mendekripsi arsip berformat PDF. Dengan menganalisis data empiris, penelitian ini menilai peran AES-128 dalam membangun lingkungan digital yang aman untuk manajemen arsip, mengatasi tantangan keamanan data di dalam institusi. Penelitian ini menggunakan metode Siklus Hidup Pengembangan Perangkat Lunak Aman (Secure Software Development Life Cycle/SSDLC) untuk pengembangan perangkat lunak dan pengumpulan data. Teknik-teknik seperti observasi, wawancara, dan studi literatur digunakan. Kriteria evaluasi meliputi waktu enkripsi/dekripsi, tingkat keamanan data, kepatuhan terhadap peraturan hukum, dan efektivitas dalam memastikan integritas dan kerahasiaan arsip. Hasilnya menunjukkan bahwa AES 128 meningkatkan keamanan data secara signifikan, dengan proses enkripsi dan dekripsi yang menunjukkan efisiensi tinggi. Mengenkripsi arsip PDF berukuran 1.146 KB membutuhkan waktu 34 detik, menghasilkan chipertext dengan 9.168 halaman dan 61.160 kata, sedangkan dekripsi membutuhkan waktu 35 detik. AES 128 menunjukkan perlindungan yang kuat terhadap peretasan dan akses yang tidak sah, sehingga mendorong lingkungan digital yang aman.

Kata Kunci: *Advanced Encryption Standard, Dinas Perpustakaan dan Kearsipan Kabupaten Minahasa, Kriptografi, Website*

Abstract

This research evaluates the effectiveness of employing the Advanced Encryption Standard (AES) 128 algorithm in managing archives at the Dinas Perpustakaan dan Kearsipan Kabupaten Minahasa. It aims to gauge AES-128's impact on the efficiency and security of encrypting and decrypting PDF-format archives. By analyzing empirical data, it assesses AES-128's role in establishing a secure digital environment for archive management, addressing data security challenges within the institution. The study utilizes the Secure Software Development Life Cycle (SSDLC) method for software development and data collection. Techniques such as observation, interviews, and literature studies are employed. Criteria for evaluation include encryption/decryption time, data security levels, compliance with legal regulations, and effectiveness in ensuring archive integrity and confidentiality. Results indicate that AES 128 enhances data security significantly, with encryption and decryption processes showing high efficiency. Encrypting a 1,146 KB PDF archive takes 34 seconds, producing a chipertext with 9,168 pages and 61,160 words, while decryption takes 35 seconds. AES 128 demonstrates robust protection against hacking and unauthorized access, fostering a secure digital environment.

Keywords: *Advanced Encryption Standard, Cryptographic, Dinas Perpustakaan dan Kearsipan Kabupaten Minahasa, Web Based*

PENDAHULUAN

Dinas Perpustakaan dan Kearsipan (Disperpusip) Kabupaten Minahasa adalah dinas yang mengurusi urusan pemerintah daerah Kabupaten Minahasa di bidang perpustakaan dan pengarsipan, yang bertugas membantu Bupati melaksanakan urusan di pemerintahan Kabupaten Minahasa dalam hal bidang perpustakaan dan kearsipan. Disperpusip adalah sebuah unit organisasi pemerintahan yang bertanggung jawab dalam mengelola perpustakaan dan arsip di sebuah instansi pemerintah. Arsip adalah salah satu sumber data yang memiliki dampak luar biasa di tempat kerja. Menurut (Suhendri & Syaechurodji, 2022) Menurut penjelasan G.R. Terry yang diacu oleh Yohannes (2008), arsip yang ditempatkan di tempat yang sesuai dengan pedoman yang telah ditentukan sebelumnya, menjamin bahwa setiap arsip yang dibutuhkan dapat ditemukan dengan cepat dan tepat.

Pengelolaan file atau dokumen dalam era digital ini merupakan aspek yang sangat krusial bagi setiap instansi atau kelompok. Keamanan data menjadi perhatian utama dalam konteks ini, terutama mengingat perkembangan teknologi dan risiko-risiko yang terkait dengannya. Berdasarkan Peraturan Nomor 43 Tahun 2009 (Indonesia, 2009) tentang Dokumen, yang dimaksud dengan "menjamin kesejahteraan dan keamanan arsip" adalah bahwa arsip, baik yang bersifat fisik maupun data, harus dijaga dengan baik dan aman agar tidak rusak atau hilang".

Dalam pengolahan arsip, risiko keamanan data merupakan salah satu masalah yang sering muncul. Dokumen yang disimpan dalam bentuk fisik menjadi sasaran empuk pencurian atau akses oleh pihak yang tidak berkepentingan. Di sisi lain, dalam lingkungan digital, peretas sering kali dapat meretas sistem dan mengunduh file-file penting, yang pada akhirnya mengancam keamanan data dan informasi rahasia organisasi. Oleh karena itu, melihat permasalahan yang telah diuraikan sebelumnya, Dinas Perpustakaan dan Kearsipan Kabupaten Minahasa, dan instansi sejenis, perlu mempertimbangkan penerapan algoritma AES (Advanced Encryption Standard) - 128 sebagai lapisan proteksi dalam pengelolaan arsip. Penggunaan AES-128 dipilih karena algoritma ini digunakan untuk mengenkripsi arsip digital, mengubahnya menjadi ciphertext atau teks terenkripsi, sehingga membuat file arsip sulit dibaca oleh pihak yang tidak berkepentingan, dan hal ini merupakan langkah penting dalam melindungi keamanan data.

METODE PENELITIAN

Pada sistem penerapan algoritma kriptografi aes (advanced encryption standard) 128 pada aplikasi manajemen pengarsipan dinas perpustakaan dan kearsipan kab. minahasa berbasis web terdapat beberapa tahapan penelitian yang menggunakan metode SSDLC *(Secure Software Development Life Cycle)* yaitu :

Planning & Analisyst

Tahap ini dimulai dengan menentukan kebutuhan pengguna dan kemampuan sistem. Peneliti dan pemangku kepentingan bekerja sama untuk membuat rencana dasar dan mengidentifikasi persyaratan keamanan.

Design

Di tahap ini, peneliti membuat desain keseluruhan sistem dengan memperhatikan keamanan. Keputusan desain dibuat dengan mempertimbangkan persyaratan keamanan yang telah diidentifikasi pada tahap sebelumnya.

Implementation

Tahap ini melibatkan pembuatan kode yang diintegrasikan dengan sistem. Pengembang harus mengikuti standar pengkodean yang baik, dan melakukan pengujian keamanan selama pengembangan kode.

Testing

Tahap pengujian penting untuk memastikan bahwa sistem aman dan sesuai dengan persyaratan keamanan. Tes yang dilakukan mencakup pengujian fungsional, pengujian keamanan, dan pengujian performa.

Deployment

Tahap ini melibatkan instalasi sistem di lingkungan produksi. Pada tahap ini, pengembang harus memastikan bahwa sistem aman dan sesuai dengan persyaratan keamanan, serta memastikan bahwa lingkungan produksi juga aman.

Maintenance

Tahap akhir melibatkan pemeliharaan sistem. Hal ini termasuk memperbaiki bug dan kerentanan, memastikan bahwa sistem selalu up-to-date dengan patch keamanan terbaru, serta mengelola perubahan yang diperlukan dalam sistem.

HASIL DAN PEMBAHASAN

Hasil riset menjelaskan bahwa implementasi algoritma Advanced Encryption Standard (AES) 128 pada aplikasi pengelolaan arsip Dinas Perpustakaan dan Kearsipan Kabupaten Minahasa memberikan hasil yang cukup besar dalam meningkatkan keamanan dan integritas arsip digital. Penggunaan algoritma AES-128 mampu mengenkripsi dan mendekripsi dokumen dengan efisiensi yang tinggi, dengan waktu yang cukup singkat dan tingkat keberhasilan yang tinggi. Dalam pengujian, sebuah dokumen berformat PDF dengan ukuran 1.146 KB dapat dienkripsi dalam waktu 34 detik, menghasilkan chipertext dengan jumlah halaman 9.168 dan jumlah kata 61.160. Proses dekripsi membutuhkan waktu 35 detik, dan dokumen berhasil dikembalikan ke bentuk aslinya tanpa kehilangan informasi.

Selain itu, penerapan SSDLC dalam pengembangan perangkat lunak enkripsi menunjukkan bahwa metode ini efektif dalam memastikan keamanan dari awal hingga akhir siklus pengembangan perangkat lunak. Tahap analisis dan perencanaan, desain, implementasi, pengujian, penyebaran, dan pemeliharaan dilakukan dengan cermat untuk memastikan perangkat lunak yang dihasilkan memiliki tingkat keamanan yang tinggi dan berfungsi dengan baik.

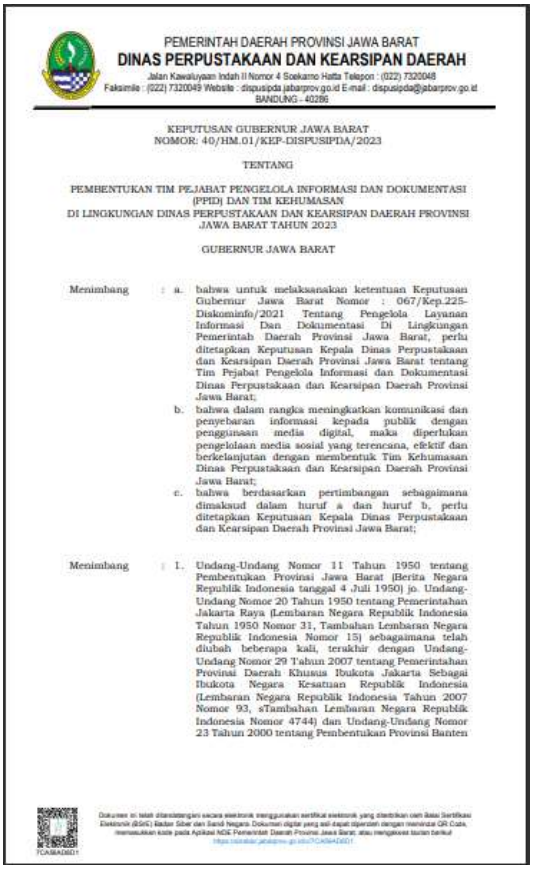
Total keseluruhan, hasil riset menunjukkan bahwa implementasi algoritma AES-128 dan metode SSDLC dapat menjadi solusi yang efektif dalam meningkatkan keamanan dan integritas dokumen digital di lingkungan Dinas Perpustakaan dan Kearsipan Kabupaten Minahasa. Langkah ini penting dilakukan untuk melindungi informasi yang bersifat sensitif

dan memastikan bahwa dokumen tidak mudah diakses atau dimanipulasi oleh pihak-pihak yang tidak berkepentingan.

Tabel 1 Hasil Pengujian Arsip Yang Telah Diupload & Enkripsi

No	Nama	Kode Arsip	Kategori	Password	Ukuran File	Waktu Upload & Enkripsi
1.	B1498 Undangan FGD DAK 2024	B.1498 /2/PRC.05/II.2024	Arsip Umum	asd123	212.649 bytes	08.33 Detik
2.	Edaran Pakaian Dinas 2024	1057/BM-XII-2023	Arsip Dinamis	zxc345	2.714.677 bytes	01:30.15 Detik
3.	Pojok Pajak Penyampaian SPT Tahunan dan Validasi NIK bagi ASN di Lingkungan Pemkab Minahasa	S-86/KPP.1606/2024	Arsip Dinamis	qwe123	239.431 bytes	09.02 Detik
4.	SURAT DISPENSASI KPU MIN	51/PP.04.1-SD/7102/4/2024	Arsip Dinamis	cvb456	237.879 bytes	08.05 Detik
5.	Undangan Kerja Bakti Benteng Moraya Jumat	005/027/seks-Disbudpar	Arsip Dinamis	fgh678	276.835 bytes	06.88 Detik

Di bawah ini merupakan dokumen asli arsip yang akan diuji, atau dokumen yang belum terenkripsi. Dokumen tersebut berformat pdf dan mempunyai jumlah 10 halaman dan 2.063 kata.



PEMERINTAH DAERAH PROVINSI JAWA BARAT
DINAS PERPUSTAKAAN DAN KEARSIPAN DAERAH
Jalan Kawaluyaan Indah II Nomor 4 Soekarno Hatta Telepon : (022) 7320048
Faksimile : (022) 7320049 Website : dispusipda.jabarprov.go.id E-mail : dispusipda@jabarprov.go.id
BANDUNG - 40286

KEPUTUSAN GUBERNUR JAWA BARAT
NOMOR: 40/HM.01/KEP-DISPUSIPDA/2023

TENTANG

PEMBENTUKAN TIM PEJABAT PENGELOLA INFORMASI DAN DOKUMENTASI (PPID) DAN TIM KEHUMASAN
DI LINGKUNGAN DINAS PERPUSTAKAAN DAN KEARSIPAN DAERAH PROVINSI JAWA BARAT TAHUN 2023

GUBERNUR JAWA BARAT

Menimbang : a. bahwa untuk melaksanakan ketentuan Keputusan Gubernur Jawa Barat Nomor : 067/Kep.225-Diskominfo/2021 Tentang Pengelola Layanan Informasi Dan Dokumentasi Di Lingkungan Pemerintah Daerah Provinsi Jawa Barat, perlu ditetapkan Keputusan Kepala Dinas Perpustakaan dan Kearsipan Daerah Provinsi Jawa Barat tentang Tim Pejabat Pengelola Informasi dan Dokumentasi Dinas Perpustakaan dan Kearsipan Daerah Provinsi Jawa Barat;

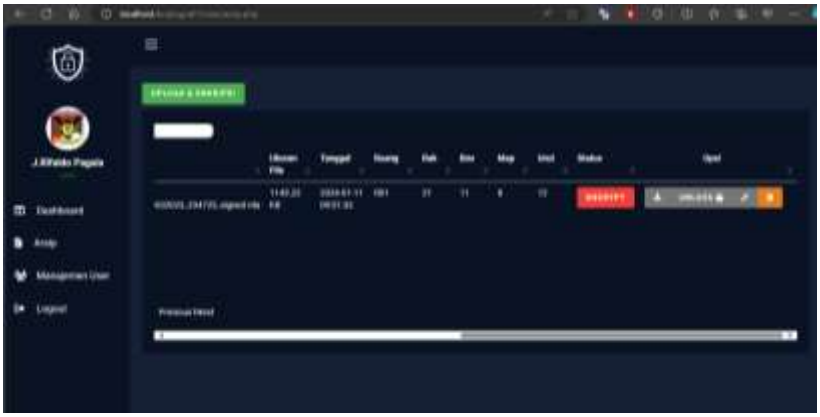
b. bahwa dalam rangka meningkatkan komunikasi dan penyebaran informasi kepada publik dengan penggunaan media digital, maka diperlukan pengelolaan media sosial yang terencana, efektif dan berkelanjutan dengan membentuk Tim Kehumasan Dinas Perpustakaan dan Kearsipan Daerah Provinsi Jawa Barat;

c. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a dan huruf b, perlu ditetapkan Keputusan Kepala Dinas Perpustakaan dan Kearsipan Daerah Provinsi Jawa Barat;

Menimbang : 1. Undang-Undang Nomor 11 Tahun 1950 tentang Pembentukan Provinsi Jawa Barat (Berita Negara Republik Indonesia tanggal 4 Juli 1950) jo. Undang-Undang Nomor 20 Tahun 1950 tentang Pemerintahan Jakarta Raya (Lembaran Negara Republik Indonesia Tahun 1950 Nomor 31, Tambahan Lembaran Negara Republik Indonesia Nomor 15) sebagaimana telah diubah beberapa kali, terakhir dengan Undang-Undang Nomor 29 Tahun 2007 tentang Pemerintahan Provinsi Daerah Khusus Ibukota Jakarta Sebagai Ibukota Negara Kesatuan Republik Indonesia (Lembaran Negara Republik Indonesia Tahun 2007 Nomor 93, sTambahan Lembaran Negara Republik Indonesia Nomor 4744) dan Undang-Undang Nomor 23 Tahun 2000 tentang Pembentukan Provinsi Banten

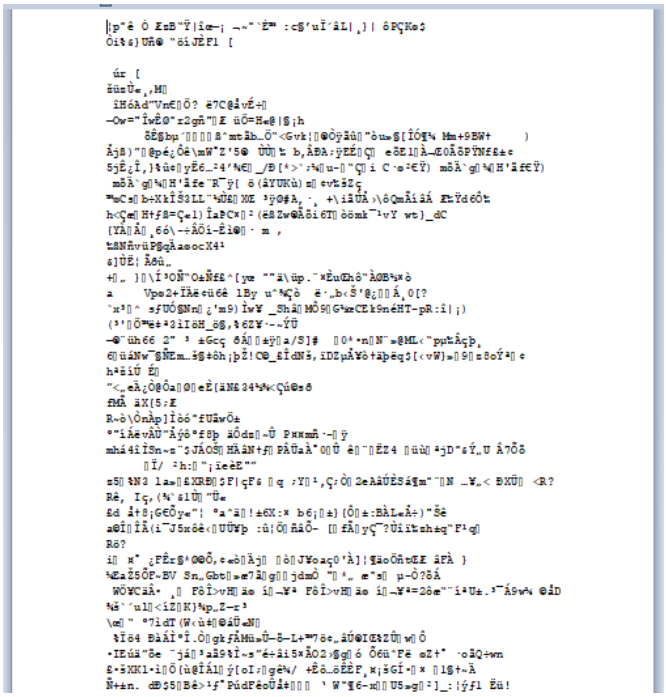
Gambar 1 Tampilan Arsip sebelum dienkripsi

Gambar 1 merupakan pengujian arsip yang akan dienkripsi. Dokumen tersebut merupakan contoh Surat Keputusan Gubernur Jawa Barat, dengan kode cdnk909, nama a, kategori surat keputusan, yang disimpan pada ruangan R05, rak 33, box 33, map 33, urutan ke 30, dengan menggunakan password “secret257”, dan keterangannya. Pada pengujian enkripsi arsip, saat user menekan tombol biru yang bertuliskan “ENKRIPSI FILE”, maka proses pengenkripsian akan dijalankan oleh algoritma AES-128. Dengan ukuran file 1.146 KB, proses pengenkripsian membutuhkan waktu 34 Detik.



Gambar 2 Status Arsip Setelah dienkripsi

Gambar 2 merupakan tampilan pada halaman arsip yang telah berhasil di upload, dengan status “Encrypt”. Pada saat kita mengunduh file tersebut, maka isinya akan ter-enkripsi dengan jumlah halaman 9.168 dan jumlah kata 61.160 seperti pada gambar di bawah.



Gambar 3 Arsip yang telah dienkripsi

SIMPULAN

Hasil implementasi algoritma AES–128 pada aplikasi manajemen arsip Dinas Perpustakaan dan Kearsipan Kabupaten Minahasa menunjukkan bahwa arsip berformat PDF dengan ukuran 1.146 KB, yang dienkripsi, memerlukan waktu 34 detik untuk menghasilkan chipertext dengan jumlah 9.168 halaman dan jumlah kata sebanyak 61.160. Proses dekripsi arsip tersebut, mengembalikannya ke bentuk aslinya dalam format PDF dengan ukuran 1.146 KB, memerlukan waktu 35 detik. Sejumlah arsip dari dinas telah diuji dan berhasil dienkripsi.

Penerapan AES–128 memungkinkan proses enkripsi yang cepat, memberikan tingkat keamanan tinggi terhadap ancaman peretasan atau akses tidak sah. Ini berhasil mengatasi masalah keamanan arsip. Implementasi sistem keamanan dinas, yang menggunakan algoritma enkripsi yang kuat, menjadi langkah strategis untuk memperkuat keamanan secara menyeluruh, melindungi integritas dan kerahasiaan arsip. Selain itu, algoritma AES–128 membantu memenuhi kewajiban hukum terkait keselamatan dan keamanan arsip, memberikan jaminan bahwa arsip tetap terlindungi.

DAFTAR PUSTAKA

Anwar, B., & Santoso, I. (2018). Aplikasi Kriptografi Keamanan Dokumen Dinas Perhubungan Provinsi Sumatera Utara Dengan Algoritma AES (Advanced Encryption Standard) Berbasis Web. *Jurnal Cyber Tech*, *1*(2), 1–8. https://ojs.trigunadharma.ac.id/index.php/jct/article/view/654

Ayumida, S., Tabrani, M., Natalia, F., & Abdurrahman Hariri, K. (2021). Aplikasi Propas (Program Pengarsipan Surat) Pada Kantor Desa Cihambulu-Subang. *Jurnal Interkom: Jurnal Publikasi Ilmiah Bidang Teknologi Informasi Dan Komunikasi*, *14*(3), 4–11. https://doi.org/10.35969/interkom.v14i3.72

Azhari, M., Mulyana, D. I., Perwitosari, F. J., & Ali, F. (2022). Implementasi Pengamanan Data pada Dokumen Menggunakan Algoritma Kriptografi Advanced Encryption Standard (AES). *Jurnal Pendidikan Sains Dan Komputer*, *2*(01), 163–171. https://doi.org/10.47709/jpsk.v2i01.1390

Efdiningsih, E., Saputri, G. J., & Yudertha, A. (2023). Perancangan Sistem Informasi Arsip Kontrak Vendor Berbasis Web Menggunakan Boostrap di PT Perkebunan Nusantara VI. *Journal on Education*, *05*(04), 11397–11405. https://jonedu.org/index.php/joe/article/view/2082%0Ahttp://jonedu.org/index.php/joe/article/download/2082/1723

Ignasius, A., & Shaka Yudha Sakti, D. V. (2022). Penerapan Algoritma Aes (Advance Encryption Standart) 128 Untuk Enkripsi Dokumen Di Pt. Gunung Geulis Elok Abadi. *Skanika*, *5*(1), 1–10. https://doi.org/10.36080/skanika.v5i1.2118

Jayana, M. A., Rafael, D., & Rahman, A. A. (2022). Implementasi Pengamanan Data Pengarsipan Dengan Metode Algoritma Kriptografi Aes Studi Kasus Pada Bank Bjb Kcp Pasteur Bandung. *Prosiding Seminar Sosial Politik, Bisnis, Akuntansi Dan Teknik*, *4*, 184. https://doi.org/10.32897/sobat.2022.4.0.1922

Khatiningsih, R. F., Anwar, N., Widodo, A. M., & Karsono Juman, K. (2022). Rancang Bangun Aplikasi Pengelolaan E-Arsip Berbasis Laman di PT. XYZ. *Ikraith-Informatika*, *7*(2), 58–65. https://doi.org/10.37817/ikraith-informatika.v7i2.2251

Munir, R. (2004). *Advanced Encryption Standard (AES) Departemen Teknik Informatika Institut Teknologi Bandung 13 . Advanced Encryption Standard (AES)*.

Munir, R. (2021). *01 - Pengantar Kriptografi*.

Nasution, Z. H., Lubis, A., Hariyanto, E., Pembangunan, U., & Budi, P. (2023). *Rancang bangun sistem e-arsip berbasis web menggunakan metode design thinking web-based e-archive system design using the design thinking method*. *6*, 60–65.

Pratama, A. M. R. (2019). *Aji Mukti Rizkio Pratama - 122410101085*.

Sari, I. P., Batubara, I. H., Al-Khowarizmi, A.-K., & Hariani, P. P. (2022). Perancangan Sistem Informasi Pengelolaan Arsip Digital Berbasis Web untuk Mengatur Sistem Kearsipan di SMK Tri Karya. *Wahana Jurnal Pengabdian Kepada Masyarakat*, *1*(1), 18–24. https://doi.org/10.56211/wahana.v1i1.101

Suhendri, B., & Syaechurodji, S. (2022). Perancangan Aplikasi Arsip Digital Di Koni Kota Serang. *Jurnal Sistem Informasi Dan Informatika (Simika)*, *5*(2), 182–192. https://doi.org/10.47080/simika.v5i2.2098

Sujjada, A., & Juniar, E. (2021). *IMPLEMENTASI ALGORITMA HILL CIPHER UNTUK PROSES ENKRIPSI DATA MENGGUNAKAN MEDIA*. *3*(1), 1–17.

Tanjung, T. (2023). Perancangan Sistem Informasi Pemberkasan Arsip Dinamis Berbasis Web (Studi Kasus: PT. Griya Indah Persada). *OKTAL: Jurnal Ilmu Komputer Dan Sains*, *2*(2), 600–610. https://journal.mediapublikasi.id/index.php/oktal/article/view/830%0Ahttps://journal.mediapublikasi.id/index.php/oktal/article/download/830/961

Tipton, H. F., & Krause, M. (2020). Secure Development Life Cycle. *Information Security Management Handbook*, 2494–2501. https://doi.org/10.1201/9781439833032-197

Togas, P. V., Naharia, O., Manggopa, H., Rompas, P. D. ., & Oroh, R. (2021). Development of Web-Based Digital System Learning Media. *Asia Pacific Journal of Management and Education*, *4*(3), 22–34. https://doi.org/10.32535/apjme.v4i3.1263.