Volume 1, Nomor 6 , Juni 2021
p-ISSN ***2774-7018*** ; e-ISSN ***2774-700X***

IMPLEMENTASI ALGORITMA AES DAN RC4 TERHADAP KEAMANAN DATA PRODUK BENIH SAYURAN DI PT. EWINDO

Raja Sari Novica Aswita, Indra Gunawan, Zulaini Masruro Nasution, Sumarno, Heru Satria Tambunan
STIKOM Tunas Bangsa Pematangsiantar
Email : rajasarinovicaaswitaa@gmail.com. indra@amiktunasbangsa.ac.id. zulaini@amiktunasbangsa.ac.id. sumarno@amiktunasbangsa.ac.id. heru@amiktunasbangsa.ac.id.

Diterima:
16 Mei 2021
Direvisi:
31 Mei 2021
Disetujui:
15 juni 2021

ABSTRAK

Penggunaan teknologi komputer dan telekomunikasi yang pesat saat ini telah mengubah cara pandang pada masyarakat dalam segi komunikasi. Salah satu perkembangan yang sangat signifikan adalah penggunaan internet untuk pertukaran informasi. PT. Ewindo adalah perusahaan swasta yang bergerak dalam pembuatan produk benih sayuran yang ada dalam kemasan. Setiap harinya sering terjadi pertukaran data baik yang bersifat eksternal maupun internal. Data hasil produksi merupakan informasi penting didalam perusahaan ini, guna menghindari terjadinya pencurian dan manipulasi data maka perlu diterapkan sistem keamanan data. Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan data. *Advanced Encryption Standart (AES)* dan *Rivest Code 4 (RC4)* adalah salah satu metode yang digunakan dalam pengamanan data/informasi. Algoritma AES juga merupakan algoritma blok *chipertext simetrik* yang dapat mengenkripsi dan dekripsi data. Sedangkan RC4 adalah salah satu jenis *stream chiper*, dimana unit dan input data dapat di proses pada satu saat. Dengan adanya penggabungan algoritma ini maka diharapkan bisa menghasilkan aplikasi untuk pengamanan data di PT. Ewindo.

Kata Kunci : *Data produk, Pengamanan Data, AES-128, RC4, Kriptografi*

Abstract

The rapid use of computer and telecommunications technology today has changed the perspective of society in terms of communication. One very significant development is the use of the internet for the exchange of information. PT. Ewindo is a private company engaged in the manufacture of packaged vegetable seed products. Every day there is frequent exchange of data both external and internal. Production data is important information in this company, in order to avoid theft and data manipulation, it is necessary to apply a data security system. Cryptography is a science that studies mathematical techniques related to aspects of data security. Advanced Encryption Standard (AES) and Rivest Code 4 (RC4) are one of the methods used in securing data/information. The AES algorithm is also a symmetric ciphertext block algorithm that can encrypt and decrypt data. While RC4 is a type of stream cipher, where the

unit and input data can be processed at the same time. By combining this algorithm, it is hoped that it can produce applications for data security at PT. Ewindo.
Keywords: Product data, Data Security, AES-128, RC4, Cryptography

Pendahuluan

Globalisasi tidak dapat dielakkan lagi, pasti akan terjadi dan harus dihadapi oleh masyarakat dunia, tidak terkecuali di Indonesia (Rais, Dien, & Dien, 2018) Di era digital, orang bebas untuk membuat dan mengakses informasi, membuatnya kelebihan beban(Mulyadi, Zulkarnain, & Laugu, 2019). Interaksi merupakan bagian yang tak terpisahkan dalam kehidupan manusia. Salah satu bidang di dalam tehnik komputer adalah bagaimana interaksi antara manusia dan komputer dibentuk (Herdian, 2020).

Kemajuan teknologi ini, generasi modern sangat mudah dalam melahap informasi yang ada. Sehingga dalam belajar pun mereka sudah menggunakan teknologi sebagai media dalam pembelajarannya, misalnya *handphone* dan laptop yang dibantu dengan Sejarah menurut Purnomo, Ratnawati dan Aristin dalam (Lubis, Joebagio, & Pelu, 2019). Periode ini dimulai sekitar tahun 1960-an ketika *mini computer* dan *mainframe* diperkenalkan perusahaan seperti IBM ke dunia industri. Kemampuan menghitung yang sedemikian cepat menyebabkan banyak sekali perusahaan yang memanfaatkannya untuk keperluan pengolahan data (data processing) (Indrajit, 2012). Perkembangan teknologi informasi memberikan kemudahan berkomunikasi tukar informasi sehingga tempat, waktu dan jarak tidak lagi menjadi kendala (yusril, 2019). Multimedia dapat diartikan sebagai teknologi yang menggabungkan berbagai sumber media (teks, grafik dan suara) untuk menyampaikan atau membuat sesuatu sebagai perantara atau suatu bentuk komunikasi (Kirman, 2018).

Dewasa ini kebutuhan informasi menjadi sangat penting untuk semua aspek kehidupan. Informasi yang dibutuhkan harus cepat, terkini serta dapat dipercaya (Ardi,2013), bahkan Teknologi juga digunakan untuk pembelajaran dan terus mengalami perkembangan seiring dengan perkembangan zaman (Marryono Jamun, 2018). Kemajuan teknologi dalam tiga dasawarsa ini telah menampakkan pengaruhnya yang begitu besar pada setiap dan semua kehidupan individu, masyarakat dan negara (Fatah, 2017). Perubahan Sosial dewasa ini disebabkan karena adanya perkembangan kemajuan teknologi yang mengarah kepada kehidupan modern (Maharidiawan Putra, 2018). Lalu lintas internet diartikan sebagai kepadatan data atau informasi yang ada diInternet atau dalam bahasa lain yang dapat kita katakan sebagai aliran data diinternet (Namdev, Agrawal, & Silkari, 2015).

Penggunaan teknologi komputer serta telekomunikasi pada era sekarang telah mengubah cara msyarakat dalam melakukan komunikasi. Salah satu perkembangan yang sangat signifikan adalah penggunaan internet untuk pertukaran informasi. Namun demikian perlu diperhatikan tingkat keamanan informasi tersebut, karena penggunaan jaringan internet merupakan infrastruktur telekomunikasi yang dapat dipergunakan oleh banyak orang. Penyadapan informasi serta manipulasi data merupakan hal yang sangat merugikan bagi pengguna jaringan komunikasi saat ini. Dengan adanya kemungkinan penyadapan dan manipulasi data tersebut, maka keamanan data menjadi sangat penting.

Hal ini akan membuat para pengguna merasa aman dan nyaman.

PT. Ewindo adalah perusahaan swasta yang bergerak dalam pembuatan produk benih sayuran yang ada dalam kemasan. Setiap harinya sering terjadi pertukaran data baik yang bersifat eksternal maupun internal. Dari pengamatan penulis, perusahaan ini memiliki data hasil produksi serta data penjualan benih sayuran yang kemungkinan kapan saja bisa diretas/dimanipulasi oleh pihak yang tidak bertanggungjawab seiring persaingan bisnis yang sangat sengit dibidang ini. Oleh karena itu pengamanan data di perusahaan ini sangat diperlukan.

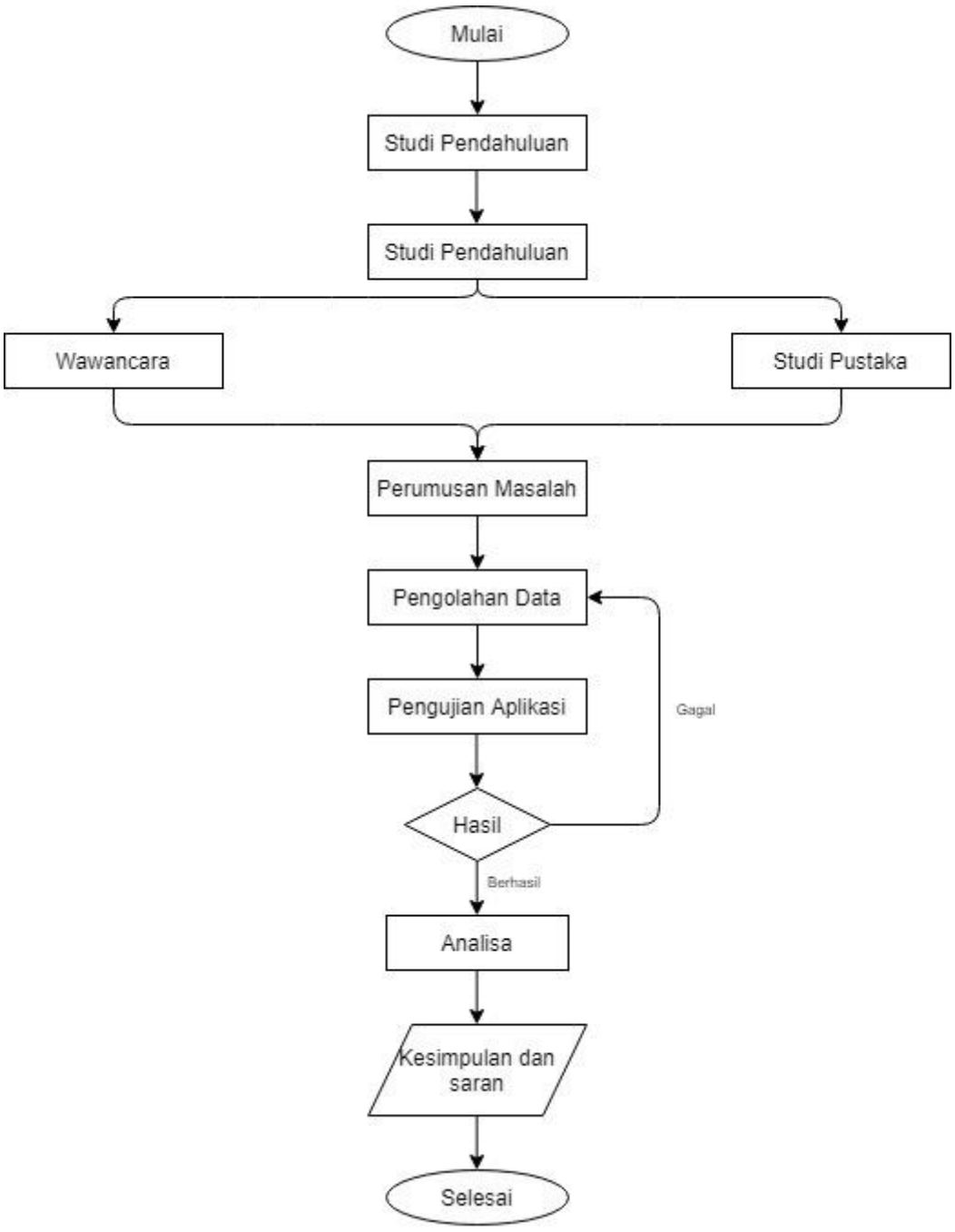
Penelitian ini akan dilakukan pengamanan berupa data hasil produksi yang berbentuk file document, excel dan pdf dengan mengimplementasikan metode kriptografi yaitu algoritma *Advanced Encryption Standart (AES)* dan *RC4 (Rivest Code4)*. Hasil penelitian yaitu membuat aplikasi untuk pengaman data hasil produksi benih sayuran di PT. Ewindo.

Penelitian ini relevan dengan penelitian yang dilakukan oleh (Pramudito & Kusumaningsih, 2018) dengan judul Implementasi ”Algoritma Aes 128 Dan Rc4 Untuk Pengamanan E-mail pada PT. Dinamika Hydro Engineering” yang mana pada penelitian tersebut menerangkan tentang bagaimana cara Implementasi Algoritma AES dan RC4 Untuk pengamanan Email. Bedanya dengan yang penulis lakukan adalah penelitian ini menerangkan tentang Implementasi Algoritma Aes Dan Rc4 Terhadap Keamanan Data Produk Benih Sayuran.

Tujuan dilakukan penelitian ini adalah menghasilkan sebuah aplikasi yang dapat melakukan enkripsi dan dekripsi data menggunakan metode algoritma AES dan RC4 yang akan digunakan untuk mengamankan data-data produk benih sayuran di PT. EWINDO.

Metode Penelitian

Dalam aplikasi kriptografi algoritma AES-128 bit dan RC4 ini membutuhkan beberapa tahap perancangan, tahapan ini dimaksudkan agar perancangan mudah dipahami berdasarkan urutan langkah dari awal hingga akhir proses.



Gambar 3.1. Flowchart penelitian
(Sumber : Penulis, 2020)

Penjelasan flowchart penelitian yang dibuat penulis seperti pada gambar 3.1 sebagai berikut :

1. Studi Pendahuluan

Studi pendahuluan dilaksanakan untuk memperoleh masukan mengenai data

yang akan diteliti. Melalui studi ini, diharapkan dapat memperoleh informasi mengenai permasalahan yang diangkat dalam penelitian dan variable-variabel yang terkait dengan masalah tersebut.

2. Pengamatan di Lapangan

Pada tahap ini penulis melakukan Interview kepada karyawan PT. EWINDO tentang permasalahan-permasalahan yang dihadapi, setelah ditemukannya permasalahan yang dihadapi, kemudian mencari dan mempelajari berbagai referensi yang mengacu dari berbagai sumber, baik dari buku maupun dari jurnal yang dijadikan referensi untuk memperoleh data dan teori yang dibutuhkaan untuk mendukung penulis dalam melakukan penelitian.

3. Perumusan Masalah

Pada langkah ini dilakukan penentuan permasalahan yang dihadapi Pt. EWINDO serta melakukan usaha atau solusi perbaikan terhadap permasalahan tersebut.

4. Pengolahan Data

Pada langkah ini data-data yang sudah didapat dari studi pendahuluan dan pengamatan di lapangan yang kemudian diolah untuk menyelesaikan permasalahan yang ditemukan.

5. Pembuatan Aplikasi

Setelah data yang sudah diolah atau ditentukan langkah selanjutnya adalah merancang aplikasi yang dapat menyelesaikan permasalahn yang dialami.

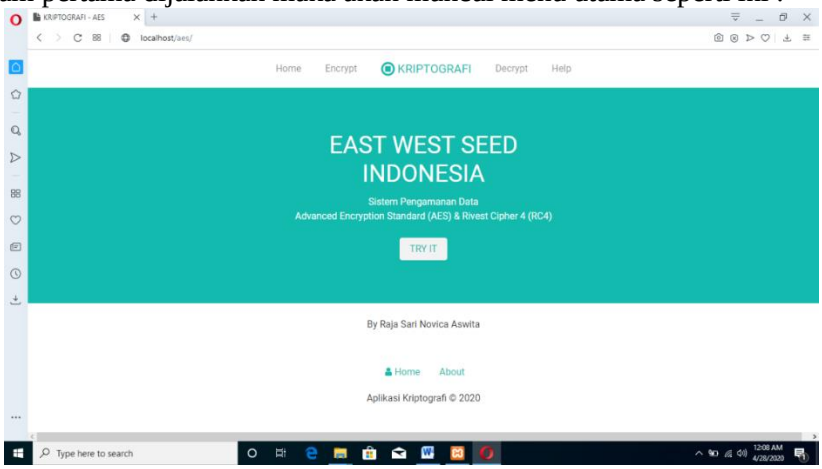
6. Pengujian Aplikasi

Setelah pembuatan aplikasi yang sudah jadi, kemudian langkah pengujian aplikasi yang sudah dirancang untuk memperoleh hasil akhir, apakah aplikasi yang dirancang sesuai yang diharapkan untuk menyelesaikan masalah yang sudah didapat.

Hasil dan Pembahasan

1. Hasil

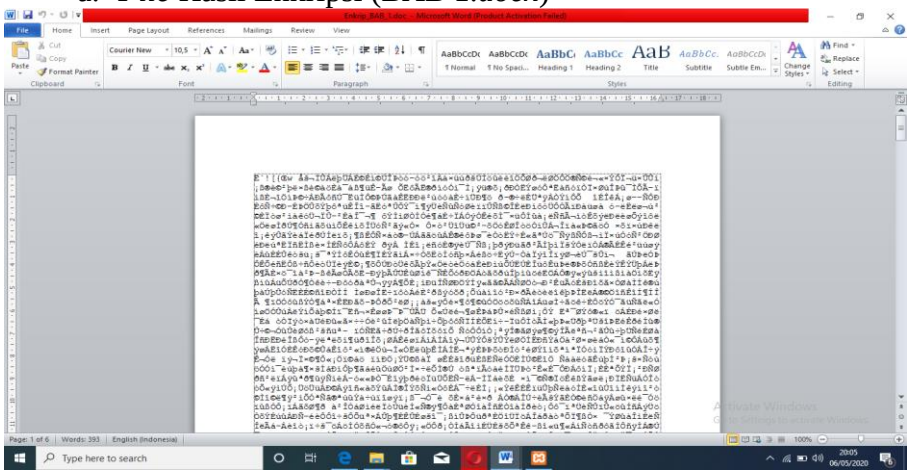
Berikut adalah tahapan proses penggunaan aplikasi pengamanan data produk benih sayuran berbasis web yang mengimplementasikan algoritma AES dsn RC4. Pada saat program pertama dijalankan maka akan muncul menu utama seperti ini :



Gambar 4.1. Tampilan Menu Utama
(*Sumber : Penulis, 2020*)

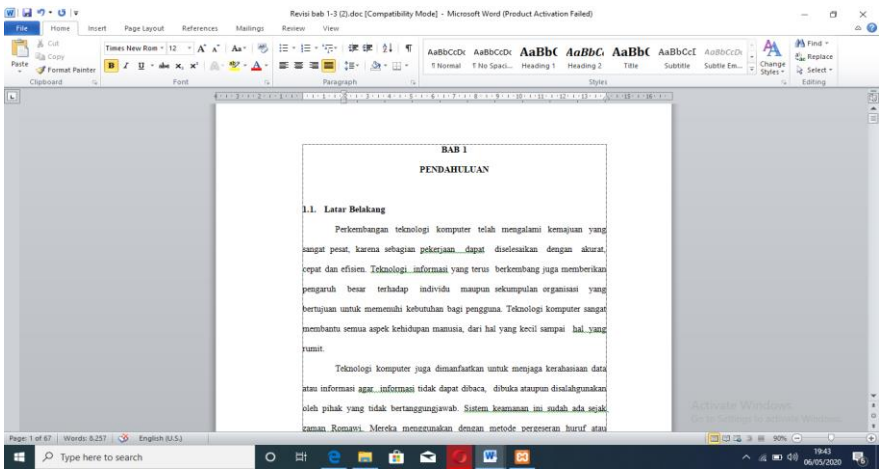
Dapat dilihat dari tampilan menu utama terdapat empat pilihan yaitu home, encrypt, decrypt, dan help yang berisi panduan dalam menggunakan aplikasi.

a. *File* Hasil Enkripsi (BAB 1.*docx*)



Gambar 4.17. *File* BAB 1.*doc*
(*Sumber : Penulis, 2020)*

b. *File* Hasil Dekripsi (BAB 1.*docx*)



Gambar 4.18. *File* Hasil Decryp BAB 1.*doc*
(*Sumber : Penulis, 2020*)

2. Pembahasan

Spesifikasi Kebutuhan Sistem
Perangkat keras merupakan salah satu faktor penting dalam pembuatan sebuah

aplikasi. Semakin tinggi spesifikasi perangkat keras yang digunakan maka akan semakin mempermudah pembuatan aplikasinya. Perangkat keras yang digunakan pada pembangunan aplikasi kriptografi ini yaitu seperti pada tabel 4.1. berikut.

Tabel 4.1. Spesifikasi Perangkat Keras

No	Nama Perangkat	Spesifikasi
1	Processor	Intel Core i3 2.40 GHz
2	Monitor	1 4 inch (1366x768)
3	Ram	4GB

Analisis kebutuhan perangkat lunak

Perangkat lunak yang digunakan dalam pembuatan aplikasi ini adalah seperti pada table 4.2 berikut :

Tabel 4.2. Spesifikasi Perangkat Lunak

No	Nama Perangkat
1	Operating System Windows 10 Ultimate 64-bit
2	Visual Studio Code
3	Web Server Apache

Analisis Waktu Enkripsi dan Dekripsi

Dalam proses enkripsi dan dekripsi maka aplikasi membutuhkan waktu untuk menyelesaikan proses tersebut. Berikut ini perbandingan antara waktu proses enkripsi dan dekripsi dengan bentuk file dan ukuran file.

Tabel 4.3. Hubungan antara Waktu Proses Enkripsi dan Dekripsi dengan Ukuran File

No	Nama File	Ukuran File Awal	Password AES	Password RC4	Ukuran File setelah di encrypt (Bytes)	Waktu Enkripsi (ms)	Waktu Dekripsi (ms)	Ukuran File setelah di decryp (Bytes)
1	BAB1.docx	24kb	12345678	12345678	17.747070 3125 Kb	1.133790 0161	1.140057086 9	18 Kb
2	Data benih Sayuran.xlsx	18kb	12345678	12345678	13.209960 9375 Kb	0.884047 9850	0.852046966 5	14 Kb
3	SERVOF1.pdf	578kb	12345678	12345678	433.20605 46875 Kb	48.19704 1988	49.48092603	434 Kb

Dari tabel 4.3 di atas menunjukkan bahwa semakin besar ukuran File maka akan semakin lama pula waktu yang dibutuhkan untuk melakukan proses enkripsi dan dekripsi.

Kesimpulan

Setelah dilakukan perancangan, implementasi serta evaluasi terhadap aplikasi enkripsi dan dekripsi data menggunakan metode algoritma *AES* dan *RC4* maka dapat ditarik kesimpulan sebagai berikut :

1. Data di dalam komputer yang dianggap penting dapat terjaga kerahasiannya dari

pihak yang tidak bertanggungjawab dan tidak berkepentingan.

2. Dengan menggunakan algoritma *Advanced Encrytion Standart (AES)* dan *Rivest Code4 (RC4),* data yang sudah dienkripsi dapat dikembalikan menjadi lampiran asli tanpa ada perubahan.

Bibliography

Ardi, Bagus Kusuma. (2013). *Pengaruh Kemajuan Teknologi Informasi Terhadap Perkembangan Sistem Informasi Akuntansi. Dharma Ekonomi*, *20*(38), 1–12. Retrieved from http://www.ejurnal.stiedharmaputra-smg.ac.id/index.php/DE/article/view/30/30

Fatah, Raden. (2017). *Integritas Pendidikan Agama Islam Terhadap Ilmu Pengetahuan Dan Teknologi*. *Tadrib: Jurnal Pendidikan Agama Islam*, *2*(1), 27–40.

Herdian, Caca Arif. (2020). *Augmented Reality sebagai Metafora Baru dalam Teknologi Interaksi Manusia dan Komputer*. *1*(2), 60–64. https://doi.org/10.31219/osf.io/79fy2

Indrajit, Richardus Eko. (2012). *Evolusi Perkembangan Teknologi*. *Blogspot.Com*, 1–5. Retrieved from https://bit.ly/2HWDlmF

Kirman, Kirman. (2018). *Implementasi Algoritma Rc4 Untuk Proteksi File Mp3. Pseudocode*, *5*(1), 80–86. https://doi.org/10.33369/pseudocode.5.1.80-86

Lubis, Muhammad Novriansyah, Joebagio, Hermanu, & Pelu, Musa. (2019). *Dalihan Na Tolu Sebagai Kontrol Sosial Dalam Kemajuan Teknologi*. *Sejarah Dan Budaya Jurnal Sejarah Budaya Dan Pengajarannya*, *13*(1), 25–33. https://doi.org/10.17977/um020v13i12019p025

Maharidiawan Putra. (2018). *Hukum Dan Perubahan Sosial* (Tinjauan Terhadap Modernisasi Dari Aspek Kemajuan Teknologi) . *Morality : Jurnal Ilmu Hukum*, *4*(1).

Marryono Jamun, Yohannes. (2018). *Dampak Teknologi Terhadap Pendidikan*. (10), 48–52.

Mulyadi, Mulyadi, Zulkarnain, Iskandar, & Laugu, Nurdin. (2019). *Adaptasi pustakawan dalam menghadapi kemajuan teknologi*. *Berkala Ilmu Perpustakaan Dan Informasi*, *15*(2), 163. https://doi.org/10.22146/bip.39843

Namdev, Neeraj, Agrawal, Shikha, & Silkari, Sanjay. (2015). *Recent advancement in machine learning based internet traffic classification. Procedia Computer Science*, *60*(1), 784–791. https://doi.org/10.1016/j.procs.2015.08.238

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. Retrieved from http://jom.fti.budiluhur.ac.id/index.php/SKANIKA/article/view/2499

Rais, Nurlaila Suci Rahayu, Dien, M. Maik Jovial, & Dien, Albert Y. (2018). *Kemajuan Teknologi Informasi Berdampak Pada Generalisasi Unsur Sosial Budaya Bagi Generasi Milenial*. *Jurnal Mozaik, X*, 61–71.

4(1), 62. https://doi.org/10.31289/simbollika.v4i1.1474

Subandi Subandi, Basuki Hari Prasetyo, Dian Anubhakti. (2019). *Aplikasi Pengamanan File Dengan Metode Kriptografi AES 192, RC4 Dan Metode Kompresi Huffman. Jurnal Bit, 16(2), 47–53.*

yusril, farhania putri. (2019). *Pemanfaatan Teknologi Informasi Dalam Bidang Pendidikan (E-Education)*. *2*(1). https://doi.org/10.31219/osf.io/ycfa2