Jurnal KOMITEK
Jurnal Komputer, informasi Dan Teknologi
Penerbit ADM RUMAH PENGETAHUAN

Comparative Analysis of the Blowfish Algorithm and the Des Algorithm in the Document File Encryption and Decryption Process

Analisis Perbandingan Algoritma Blowfish Dan Algoritma Des Dalam Proses Enkripsi Dan Dekripsi File Dokumen

Ronaldo Praja Saputra [1]; Jusuf Wahyudi [2]; Juju Jumadi [3]

[1,2,3] ***Program Studi Informatika, Fakultas Ilmu Komputer, Universitas Dehasenbengkulu***

Email: [1] ronaldops504@gmail.com Horasaryanto@gmail.com rikiternando16@gmail.com

How to Cite :

Saputra, R. P., Wahyudi, J., Jumadi, J. (2022). Comparative Analysis of the Blowfish Algorithm and the Des Algorithm in the Document File Encryption and Decryption Process. Jurnal Komitek, 2 (2). DOI: https://doi.org/10.53697/jkomitek.v2i2

ARTICLE HISTORY

Received [08 November 2022]
Revised [2 Desember 2022]
Accepted [09 Desember 2022]

Keywords :

Algoritma Blowfish, Algoritma DES, File Dokumen, Keamanan

ABSTRAK

Masalah keamanan merupakan salah satu aspek paling penting dalam dunia teknologi informasi, seperti keamanan dokumen. Sebagai besar dokumen-dokumen dibuat melalui paket aplikasi Microsoft Office, karena mudah untuk digunakan. Terdapat beberapa aplikasi yang tersedia di Microsoft Office, yaitu Microsoft Word, Microsoft Excel, Microsoft Access, Microsoft Powerpoint, dan lain-lain yang digunakan untuk mengolah kata dan angka sesuai dengan kebutuhan pengguna. Analisis perbandingan algoritma Blowfish dan algoritma DES dalam proses enkripsi dilakukan berdasarkan 3 aspek perbandingan yaitu waktu proses, ukuran file dan memori yang digunakan. Perbandingan dilakukan dengan 40 data uji yang berupa file dokumen yang masing-masing terdiri dari 10 data uji dengan format extension *.docx, *.xlsx, *.pdf, dan *.pptx, dimana format tersebut familiar dalam pengolahan data menggunakan Microsoft Office. Berdasarkan pengujian yang telah dilakukan tersebut, dapat disimpulkan bahwa Dalam proses enkripsi, Algoritma DES memiliki waktu yang lebih cepat dibandingkan dengan Algoritma Blowfish dengan persentase waktu proses enkripsi Algoritma DES 3,7975%. Dalam proses dekripsi, Algoritma DES memiliki waktu yang lebih cepat dibandingkan dengan Algoritma Blowfish dengan persentase waktu proses enkripsi Algoritma DES 3,595%. Dalam proses enkripsi, ukuran file pada Algoritma DES terjadi penambahan bytes lebih sedikit dibandingkan dengan ukuran file pada Algoritma Blowfish. Dalam proses dekripsi, ukuran file pada Algoritma DES dan Algoritma Blowfish tidak mengalami perubahan, karena ukuran file tersebut kembali seperti ukuran file asli. Dalam proses enkripsi, Algoritma DES menggunakan memory lebih sedikit dibandingkan dengan Algoritma Blowfish dengan persentase memory yang digunakan Algoritma DES 49,655%. Dalam proses dekripsi, Algoritma Blowfish menggunakan memory yang lebih sedikit dibandingkan dengan Algoritma DES dengan persentase memory yang digunakan Algoritma Blowfish 49,5925%

ABSTRACT

Security issues are one of the most important aspects in the world of information technology, such as document security. Most of the documents are created through the Microsoft Office application package, because it is easy to use. There are several applications available in Microsoft Office, namely Microsoft Word, Microsoft Excel, Microsoft Access, Microsoft Powerpoint, and others that are used to process words and numbers according to user needs. Comparative analysis of the Blowfish algorithm and the DES algorithm in the

*encryption process is carried out based on 3 comparison aspects, namely processing time, file size and memory used. Comparisons were made with 40 test data in the form of document files, each consisting of 10 test data with extension formats *.docx, *.xlsx, *.pdf, and *.pptx, where these formats are familiar in data processing using Microsoft Office. Based on the tests that have been carried out, it can be concluded that in the encryption process, the DES Algorithm has a faster time than the Blowfish Algorithm with a percentage of the DES Algorithm's encryption processing time of 3.7975%. In the decryption process, the DES Algorithm has a faster time compared to the Blowfish Algorithm with a percentage of the DES Algorithm's encryption processing time of 3.595%. In the encryption process, the file size in the DES Algorithm increases bytes less than the file size in the Blowfish Algorithm. In the decryption process, the file size in the DES Algorithm and the Blowfish Algorithm does not change, because the file size returns to the original file size. In the encryption process, the DES Algorithm uses less memory compared to the Blowfish Algorithm with the percentage of memory used by the DES Algorithm being 49.655%. In the decryption process, the Blowfish Algorithm uses less memory compared to the DES Algorithm with the percentage of memory used by the Blowfish Algorithm 49.5925%.*

PENDAHULUAN

Dunia teknologi informasi sekarang ini berkembang sangat pesat dan mempengaruhi hampir seluruh aspek kehidupan manusia. Perkembangan tersebut secara langsung maupun tidak langsung mempengaruhi semua sistem yang berhubungan ataupun tidak dengan sistem informasi itu sendiri seperti perdagangan, transaksi, bisnis, perbankan, industri dan pemerintahan.

Masalah keamanan merupakan salah satu aspek paling penting dalam dunia teknologi informasi, seperti keamanan dokumen. Sebagai besar dokumen-dokumen dibuat melalui paket aplikasi Microsoft Office, karena mudah untuk digunakan. Terdapat beberapa aplikasi yang tersedia di Microsoft Office, yaitu Microsoft Word, Microsoft Excel, Microsoft Access, Microsoft Powerpoint, dan lain-lain yang digunakan untuk mengolah kata dan angka sesuai dengan kebutuhan pengguna.

Masalah keamanan dan kerahasiaan sesuatu sangatlah yang penting dalam suatu instansi atau pun perusahaan. Data yang akan digunakan ataupun disimpan agar benar-benar aman secara fisik maupun sistem perlu terlebih dahulu untuk diamankan agar tidak dapat dibaca atau dilacak oleh pihak-pihak yang tidak bertanggung jawab (Yanti, et al., 2018).

Algoritma kriptografi terbagi menjadi 2 yaitu kriptografi klasik dan kriptografi modern. Algoritma kriptografi modern merupakan suatu perbaikan yang mengacu pada kriptografi klasik. Algoritma ini menggunakan pengolahan simbol biner yang dibentuk dari kode ASCII (American Standard Code for Information Interchange) karena berjalan mengikuti operasi komputer digital, sehingga membutuhkan pengetahuan dasar matematika untuk menguasainya. Algoritma kriptografi modern dibagi berdasarkan jenis kunci yang digunakan yaitu simetris, asimetris dan hibrid.

Algoritma kriptografi modern yang menggunakan kunci simetris yaitu algoritma Blowfish, Twofish, DES, AES, IDEA, MD5, RC4, RSA, dan lain-lain. Banyaknya algoritma kriptografi modern yang tersedia, terkadang membuat pengguna bingung dalam memilih algoritma yang tepat untuk mengamankan file dokumen. Oleh karena itu, dalam penelitian ini dilakukan kajian dengan membandingkan performa kinerja dari 2 algoritma kriptografi modern yaitu Algoritma Blowfish dan Algoritma DES. Alasan memilih 2 algoritma ini yaitu sama-sama menggunakan kunci simetris dalam proses enkripsi dan dekripsi serta sama-sama menggunakan blok cipher 64bit yang dibagi 2 bagian 32bit kiri dan 32bit kanan.

Perbandingan antara Algoritma Blowfish dan Algoritma DES menggunakan 10 data uji (file dokumen format extension *.docx, *.xlsx, *.pdf, dan *.pptx) dengan melihat 3 aspek yang dibandingkan yaitu waktu proses enkripsi dan dekripsi, ukuran file sebelum dan sesudah proses

enkripsi, serta memori yang digunakan pada saat proses enkripsi dan dekripsi dilakukan. Untuk membantu proses perbandingan kedua algoritma tersebut, maka dibangun aplikasi menggunakan bahasa pemrograman Visual Basic .Net. Pada aplikasi ini akan menampilkan hasil perbandingan dari ketiga aspek perbandingan antara algoritma Blowfish dan algoritma DES.

LANDASAN TEORI

Kriptografi

Kriptografi adalah suatu cara bagi seseorang agar dapat mengirim pesan rahasia ke pada orang lain atau bisa dibilang si penerima pesannya dengan cara menggunakan sistem kode agar tidak dapat di mengerti oleh orang ketiga atau orang yang berniat tidak baik seperti hacker misalnya walaupun pihak ketiga itu sendiri dapat menginterupsi tranmisi dari sistem mengirim pesan. Alangkah baiknya jika pesan tersebut tidak jatuh kepihak ketiga sebelum terjadinya tranmisi agar bisa dapat dicegah untuk mengira–ngira pesan tersebut, oleh karena itu dibutuhkannya adanya algoritma. Kriptografi pada awalnya dijabarkan sebagai ilmu yang mempelajari bagaimana menyembunyikan pesan (Thahara & Siregar, 2021).

Kriptografi berasal dari bahasa Yunani, crypto dan graphia. Crypto berarti secret (rahasia) dan graphia berarti writing (tulisan). Kriptografi menurut terminologinya adalah sebuah ilmu dan seni untuk menjaga keamanan pesan ketika pesan dikirim dari suatu tempat ke tempat lain. Secara istilah kriptografi didefinisikan sebagai ilmu dan seni untuk menjaga kerahasiaan pesan baik berupa data maupun informasi yang mempunyai arti atau nilai dengan cara menyamarkan (mengacak) menjadi bentuk yang tidak dapat dimengerti dan hanya penerima yang dapat mengubah kode-kode tersebut menjadi pesan asli yang dapat dimengerti (Jamaludin & Romindo, 2020).

Algoritma Blowfish

Blowfish termasuk dalam enkripsi block Chiper 64-bit dengan panjang kunci minimal 32 bit sampai 448-bit. Blowfish alias "OpenPGP.Cipher.4" merupakan enkripsi yang termasuk dalam golongan Symmetric Cryptosystem, metode enkripsinya mirip dengan DES (DES like Cipher) diciptakan oleh seorang Cryptanalyst bernama Bruce Schneier Presiden perusahaan Counterpane Internet Security, Inc (Perusahaan konsultan tentang kriptografi dan keamanan komputer) dan dipublikasikan tahun 1994. Dibuat untuk digunakan pada komputer yang mempunyai mikroprosesor besar (32-bit k eatas dengan cache data yang besar) (Wardoyo, 2016).

Blowfish atau yang disebut juga “OpenPGP.Cipher.4" adalah algoritma kunci simetrik cipher blok yang dirancang pada tahun 1993 oleh Bruce Schneider untuk menggantikan DES (Data Encryption Standard). Algoritma Blowfish dibuat untuk digunakan pada komputer yang mempunyai microposesor besar (32-bit keatas dengan cache data yang besar) (Maradona & Basorudin, 2017).

Algoritma DES

DES, atau juga dikenal sebagai Data Encryption Algorithm (DEA) oleh ANSI dan DEA-1 oleh ISO, merupakan algoritma kriptografi simetris yang paling umum digunakan saat ini. Secara umum, DES termasuk ke dalam sistem kriptografi simetri dan tergolong jenis cipher blok. DES beroperasi pada ukuran blok 64 bit. DES mengenkripsikan 64 bit plainteks menjadi 64 bit cipherteks dengan menggunakan 56 bit kunci internal (internal key) atau lupa-kunci (subkey). Kunci internal dibangkitkan dari kunci eksternal (external key) yang panjangnya 64 bit (Meko, 2018).

Algoritma Data Encryption Standard (DES) merupakan algoritma enkripsi yang paling banyak digunakan di dunia yang diadopsi oleh NIST (National Institue of Standards and Technology) sebagai standar pengolah informasi Federal AS. Plain dienkrip dalam blok-blok 64 bit menjadi 64 bit data ciphertext menggunakan kunci 56 bit kunci internal (internal key). DES mentransformasikan input 64 bit dalam beberapa tahap enkripsi ke dalam output 64 bit. Dengan demikian, DES termasuk block cipher. Berdasarkan tahapan dan kunci yang sama, DES digunakan untuk membalik

enkripsi. Kunci internal pada algoritma DES dibangkitkan dari kunci eksternal (external key) 64 bit4]. DES beroperasi pada ukuran blok 64 bit dan termasuk ke dalam sistem kriptografi simetri dan tergolong jenis cipher block. DES mengenkripsikan 64 bit plainteks menjadi 64 bit cipherteks dengan menggunakan 56 bit kunci internal (internal key) atau up-kunci (subkey). Kunci internal dibangkitkan dari kunci eksternal (external key) yang panjangnya 64 bit (Yanti, et al., 2018).

Visual Studio 2010

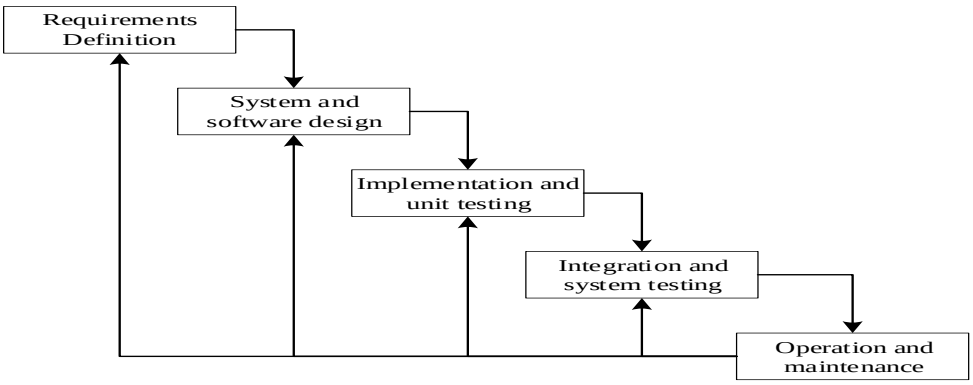
Microsoft Visual Studio adalah sebuah lingkungan pengembangan terpadu (IDE) dari Microsoft. Hal ini digunakan untuk mengembangkan program komputer untuk sistem operasi Microsoft Windows superfamili, serta situs web, aplikasi web dan layanan web. Visual studio menggunakan Microsoft Platform dalam pengembangan perangkat lunak seperti API Windows, Windows Forms, Windows Presentation Foundation, Windows Store dan Microsoft Silverlight (Blazing, 2018).

Microsoft Visual Basic .Net adalah sebuah alat untuk mengembangkan dan membangun aplikasi yang bergerak di atas sistem .Net Framework, dengan menggunakan bahasa basic. Dengan menggunakan alat ini, para programmer dapat membangun aplikasi windows form, aplikasi web berbasis ASP.Net dan juga aplikasi command-line. Bahasa Visual Basic .Net sendiri menganut paradigma bahasa pemrograman berorientasi objek yang dapat dilihat sebagai evolusi dari Microsoft Visual Basic versi sebelumnya yang diimplementasikan di atas .Net Framework (Blazing, 2018).

METODE PENELITIAN

Metode Penelitian.

Metode penelitian yang diterapkan pada penelitian ini adalah dengan pengembangan metode *waterfall*. Metode *waterfall* merupakan model pengembangan sistem informasi yang sistematik dan sekuensial. Metode *waterfall* memiliki tahapan-tahapan seperti Gambar 1.



Gambar 1. Metode Waterfall

Keterangan :

1. *Requirements analysis and definition.* Layanan sistem, kendala, dan tujuan ditetapkan oleh hasil konsultasi dengan pengguna yang kemudian didefinisikan secara rinci dan berfungsi sebagai spesifikasi sistem.
2. *System and software design.* Tahapan perancangan sistem mengalokasikan kebutuhan-kebutuhan sistem baik perangkat keras maupun perangkat lunak dengan membentuk arsitektur sistem secara keseluruhan. Perancangan perangkat lunak melibatkan identifikasi dan penggambaran abstraksi sistem dasar perangkat lunak dan hubungannya.

3. *Implementation and unit testing.* Pada tahap ini, perancangan perangkat lunak direalisasikan sebagai serangkaian program atau unit program. Pengujian melibatkan verifikasi bahwa setiap unit memenuhi spesifikasinya.
4. *Integration and system testing.* Unit-unit individu program atau program digabung dan diuji sebagai sebuah sistem lengkap untuk memastikan apakah sesuai dengan kebutuhan perangkat lunak atau tidak. Setelah pengujian, perangkat lunak dapat dikirimkan ke *customer*
5. *Operation and maintenance.* Biasanya (walaupun tidak selalu), tahapan ini merupakan tahapan yang paling panjang. Sistem dipasang dan digunakan secara nyata. *Maintenance* melibatkan pembetulan kesalahan yang tidak ditemukan pada tahapan-tahapan sebelumnya, meningkatkan implementasi dari unit sistem, dan meningkatkan layanan sistem sebagai kebutuhan baru.

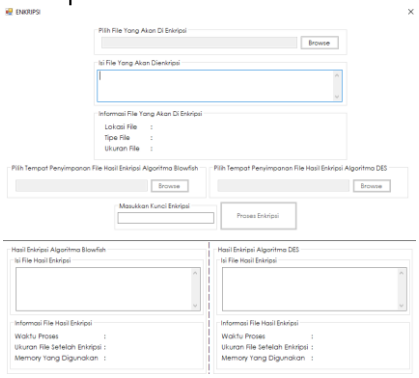
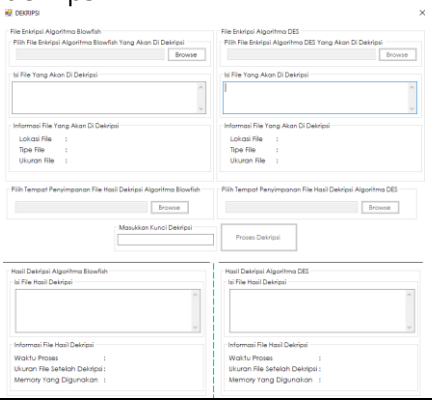
HASIL DAN PEMBAHASAN

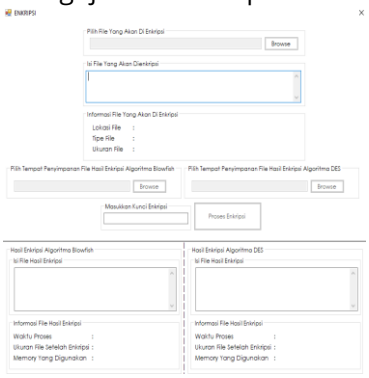
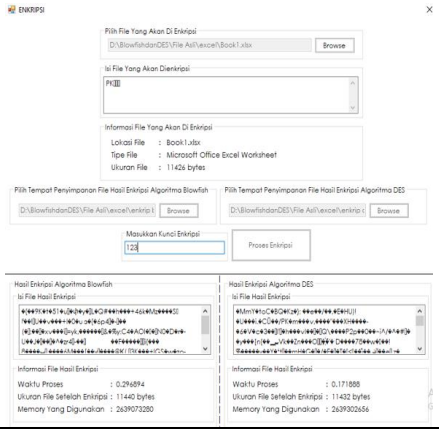
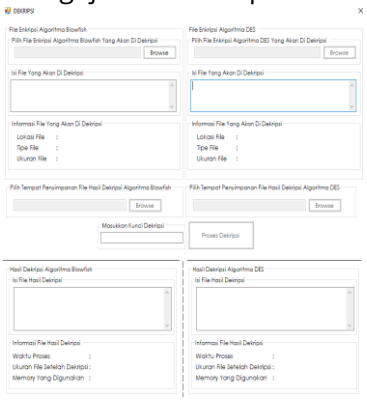
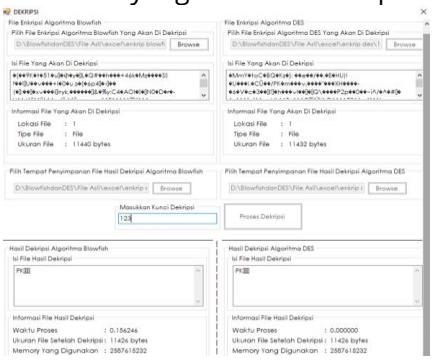
Hasil Penelitian

Pengujian Sistem

Pengujian sistem pada aplikasi kriptografi Blowfish dan DES menggunakan metode black box. Adapun hasil pengujian tersebut, seperti Tabel 1.

Tabel 1 Hasil Pengujian Metode Black Box

No	Komponen Pengujian	Skenario Pengujian	Hasil Pengujian
1	Menguji Form Menu Utama 	Memilih sub menu Enkripsi	Sistem berhasil menampilkan form enkripsi 
		Memilih sub menu Dekripsi	Sistem berhasil menampilkan form dekripsi 

2	Menguji Form Enkripsi 	Melakukan proses enkripsi pada file dokumen	Sistem berhasil mengenkripsi file dokumen tersebut 
3	Menguji Form Dekripsi 	Melakukan proses dekripsi pada file dokumen yang sudah terenkripsi	Sistem berhasil mendekripsikan file dokumen yang sudah terenkripsi 

Berdasarkan pengujian yang telah dilakukan tersebut, dapat disimpulkan bahwa aplikasi kripografi Blowfish dan DES mampu melakukan proses enkripsi dan dekripsi file dokumen dan fungsional dari aplikasi telah berjalan sesuai harapan.

KESIMPULAN DAN SARAN

Kesimpulan

1. Analisis perbandingan algoritma Blowfish dan algoritma DES dalam proses enkripsi dilakukan berdasarkan 3 aspek perbandingan yaitu waktu proses, ukuran file dan memori yang digunakan. Untuk membantu proses analisis tersebut, telah dibangun aplikasi kriptografi menggunakan bahasa pemrograman Visual Basic .Net dimana pada aplikasi tersebut telah diterapkan 2 algoritma tersebut yaitu algoritma Blowfish dan algoritma DES.
2. Berdasarkan pengujian yang telah dilakukan tersebut, dapat disimpulkan bahwa aplikasi kripografi Blowfish dan DES mampu melakukan proses enkripsi dan dekripsi file dokumen dan fungsional dari aplikasi telah berjalan sesuai harapan.
3. Berdasarkan pengujian yang telah dilakukan sebanyak 40 data uji yang berupa file dokumen yang masing-masing terdiri dari 10 data uji dengan format extension *.docx, *.xlsx, *.pdf, dan *.pptx, diperoleh hasil :
   a) Waktu proses

1) Dalam proses enkripsi, Algoritma DES memiliki waktu yang lebih cepat dibandingkan dengan Algoritma Blowfish dengan persentase waktu proses enkripsi Algoritma DES 3,7975%
2) Dalam proses dekripsi, Algoritma DES memiliki waktu yang lebih cepat dibandingkan dengan Algoritma Blowfish dengan persentase waktu proses enkripsi Algoritma DES 3,595%

b) Ukuran File
1) Dalam proses enkripsi, ukuran file pada Algoritma DES terjadi penambahan bytes lebih sedikit dibandingkan dengan ukuran file pada Algoritma Blowfish
2) Dalam proses dekripsi, ukuran file pada Algoritma DES dan Algoritma Blowfish tidak mengalami perubahan, karena ukuran file tersebut kembali seperti ukuran file asli

c) Memory Yang Digunakan
1) Dalam proses enkripsi, Algoritma DES menggunakan memory lebih sedikit dibandingkan dengan Algoritma Blowfish dengan persentase memory yang digunakan Algoritma DES 49,655%
2) Dalam proses dekripsi, Algoritma Blowfish menggunakan memory yang lebih sedikit dibandingkan dengan Algoritma DES dengan persentase memory yang digunakan Algoritma Blowfish 49,5925%

Saran

1. Agar memilih algoritma DES dibandingkan dengan algoritma Blowfish, dikarenakan waktu proses algoritma DES lebih cepat, ukuran file mengalami penambahan bytes lebih sedikit, memori yang digunakan lebih sedikit.
2. Diperlukan penelitian selanjutnya dengan menguji jenis file lain seperti audio, gambar, dan video.
3. Diperlukan kombinasi kriptografi dengan steganografi agar file lebih aman.

DAFTAR PUSTAKA

Adhar, D., 2019. Implementasi Algoritma DES (Data Encryption Standard) Pada Enkripsi dan Dekripsi SMS Berbasis Android. *Jurnal Teknik Informatika Kaputama (JTIK),* Volume Vol.3 No.2 P-ISSN.2548-9704.

Blazing, A., 2018. *Pemrograman Windows Dengan Visual Basic .Net : Praktikum Pemrograman VB.Net.* s.l.:Google Book.

Jamaludin & Romindo, 2020. *Kriptografi Teknik Hybrid Cryptosystem Menggunakan Kombinasi Vigenere Cipher dan RSA.* Medan: Yayasan Kita Menulis.

Maradona, H. & Basorudin, 2017. Analisis Algoritma Blowfish Pada Proses Enkripsi dan Dekripsi File. *Riau Journal of Computer Science,* Volume Vol.3 No.2 .

Meko, D. A., 2018. Perbandingan Algoritma DES, AES, IDEA dan Blowfish Dalam Enkripsi dan Dekripsi Data. *Jurnal Teknologi Terpadu,* Volume Vol.4 No.1 e-ISSN:2460-7908.

Rosa & Shalahuddin, 2016. *Rekayasa Perangkat Lunak Terstuktur dan Berorientasi Objek.* Bandung: Penerbit Informatika.

Santoso & Nurmalina, R., 2017. Perencanaan dan Pengembangan Aplikasi Absensi Mahasiswa Menggunakan Smart Card Guna Pengembangan Kampus Cerdas (Studi Kasus Politeknik Negeri Tanah Laut). *Jurnal Integrasi,* Volume Vol.9 No.1 April 2017 e-ISSN : 2548-9828.

Sumandri, 2017. *Studi Model Algoritma Kriptografi Klasik dan Modern.* Yogyakarta, Seminar Matematika dan Pendidikan Matematika ISBN.978-602-73403-2-9.

Thahara, A. & Siregar, I. T., 2021. Implementasi Kriptografi Untuk Keamanan Data dan Jaringan Menggunakan Algoritma DES. *JURTI,* Volume Vol.5 No.1 ISSN:2579-8790.

Wardoyo, S., 2016. Enkripsi dan Dekripsi File Dengan Algoritma Blowfish Pada Perangkat Mobile Berbasis Android. *Jurnal Paper Aes ,* Volume Vol. 5 No.1 ISSN 2302-2949.

Yanti, N. R., Alimah & Ritonga, D. A., 2018. Implementasi Algoritma Data Encryption Standard Pada Penyandian Record Database. *Jurnal Sains Komputer dan Informatika (J-Sakti),* Volume Vol.2 No.1 e-ISSN:2549-7200.