



PENGAMANAN FILE DIGITAL MENGGUNAKAN METODE ALGORITMA KRIPTOGRAFI RIJNDAEL

Muhammad Erwanto¹, Sandi Fajar Rodiansyah², Yudha Pradita Putra³

^{1,2,3}Sekolah Tinggi Ilmu Komputer POLTEK Cirebon

Email: ¹ muhammaderwanto@gmail.com, ² Galuh29@Gmail.com,

³Yudha.Pradita.Putra@Hotmail.com

Abstrak

Rijndael termasuk dalam jenis algoritma kriptografi yang sifatnya simetri dan *cipher block*. Dengan demikian algoritma ini mempergunakan kunci yang sama saat *enkripsi* dan *dekripsi* serta masukan dan keluarannya berupa blok dengan jumlah *bit* tertentu. Rijndael mendukung berbagai variasi ukuran blok dan *kunci* yang akan digunakan. Namun Rijndael mempunyai ukuran blok dan *kunci* yang tetap sebesar 128, 192, 256 bit. Pemilihan ukuran blok data dan *kunci* akan menentukan jumlah proses yang harus dilalui untuk proses *enkripsi* dan *dekripsi*. Blok-blok data masukan dan *kunci* dioperasikan dalam bentuk *array*. Setiap anggota *array* sebelum menghasilkan keluaran *ciphertext* dinamakan dengan *state*. Setiap *state* akan mengalami proses yang secara garis besar terdiri dari empat tahap yaitu, *AddRoundKey*, *SubBytes*, *ShiftRows*, dan *MixColumns*

Kata kunci: Advanced Encryption Standard (AES), Hash, Inisialisasi Vektor, Algoritma Rijndael 256, Kriptografi, Algoritma Kunci Simetri.

SECURING DIGITAL FILES USING THE RIJNDAEL CRYPTOGRAPHY ALGORITHM METHOD

Abstract

Rijndael, including the type of cryptographic algorithms that are symmetry and block cipher. Thus these algorithms use the same key when the encryption and decryption as well as inputs and outputs in the form of a block with a certain number of bits. Rijndael supports a wide variety of block sizes and key to be used. However Rijndael block size and the key has fixed at 128, 192, 256 bits. Selection of data block size and the key will determine the number of processes that must be passed to the encryption and decryption process. Blocks of data input and key operated in the form of an array. Each member of the array before generating the output ciphertext is called the state. Each state will undergo a process generally consists of four phases, namely, *AddRoundKey*, *SubBytes*, *ShiftRows*, and *MixColumns*.

Kata kunci: Advanced Encryption Standard (AES), Hash, Initialization Vectors, Rijndael algorithm 256, Cryptography, Key Algorithm Symmetry.



This work is licensed under a [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/)

1. PENDAHULUAN

Memiliki file digital penting atau rahasia tentu membutuhkan perlindungan dan pengamanan yang baik agar data tersebut tidak mudah dibuka dan dilihat isi sebenarnya yang ada di dalamnya, salah satu cara yang digunakan adalah menggunakan teknik Kriptografi yaitu dengan menyandikan isi informasi menjadi kode-kode acak yang tidak dimengerti sehingga apabila disadap maka penyadap akan kesulitan untuk mengetahui isi informasi yang sebenarnya. Teknik penyandian acak tersebut adalah *Enkripsi* dan Deskripsi untuk mengembalikan kode-kode yang teracak tersebut menjadi seperti semula.

Sayembara terbuka yang diadakan oleh NIST (*National Institute of Standards and Technology*) untuk membuat standard algoritma kriptografi yang baru sebagai pengganti *Data Encryption Standard (DES)*. *DES* sudah dianggap tidak aman terutama karena panjang kunci yang relative pendek sehingga mudah dipecahkan menggunakan teknologi saat ini. Metode Algoritma *Rijndael* menjadi pemenang dalam sayembara tersebut yang dalam prosesnya menggunakan substitusi, permutasi, dan sejumlah putaran yang dikenakan pada tiap blok yang akan di*Enkripsi/ Dekripsi*. setiap putarannya, *Rijndael* menggunakan kunci yang berbeda.

Kunci setiap putaran disebut *round key*. Tetapi tidak seperti *DES* yang berorientasi *Bit*, *Rijndael* beroperasi dalam orientasi *Byte* sehingga memungkinkan untuk implementasi algoritma yang efisien ke dalam *software* dan *hardware*. Ukuran blok untuk algoritma *Rijndael* adalah 128 *Bit* (16 *Byte*). Algoritma *Rijndael* dapat mendukung panjang kunci 128 *Bit* sampai 256 *Bit* dengan step 32 *Bit*. Panjang kunci berpengaruh pada jumlah putaran yang dikenakan pada tiap blok. Misalnya, untuk ukuran blok dan panjang kunci sebesar 128 *Bit* ditentukan 10 putaran, sedangkan untuk ukuran blok 128 *Bit* dan panjang kunci 256 *Bit* jumlah putaran yang ditentukan adalah 14 putaran. Pada permasalahannya adalah Informasi yang bersifat rahasia dan penting tidak cukup aman jika disimpan tanpa adanya perangkat lunak/*software* pengamanan berupa penyandian, penguncian atau penyembunyian *file* informasi tersebut. Penelitian ini bermaksud Untuk memberikan perlindungan File Digital menggunakan aplikasi Pengamanan File Digital Menggunakan Metode Algoritma Kriptografi *Rijndael*.

2. BAHAN DAN METODE

Metode Penelitian Terapan

Penelitian terapan merupakan penelitian yang dikerjakan dengan maksud untuk menerapkan, menguji, dan mengevaluasi kemampuan suatu teori yang diterapkan dalam pemecahan permasalahan praktis. (Moh. Nazir, 2014)

Penelitian terapan merupakan penelitian yang dikerjakan dengan maksud untuk menerapkan, menguji, dan mengevaluasi kemampuan suatu teori yang diterapkan dalam pemecahan permasalahan praktis.

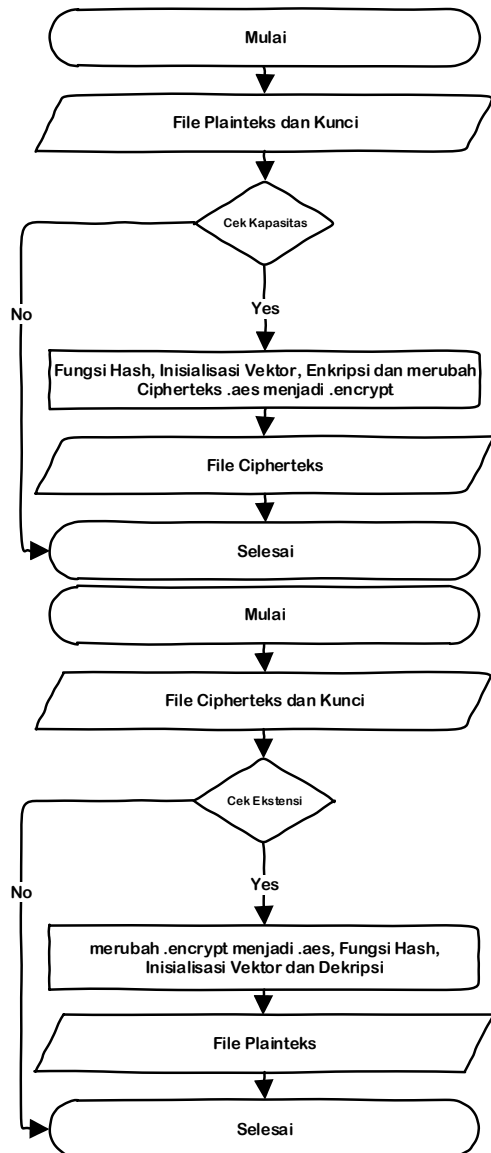
“ Penelitian terapan dapat diartikan sebagai penyelidikan yang hati-hati, sistematis, dan terus menerus terhadap suatu masalah dengan tujuan untuk digunakan dengan segera untuk keperluan tertentu. ” (Moh. Nazir, 2014). langkah-langkah dalam melaksanakan penelitian terapan, yakni:

1. Sesuatu yang sedang diperlukan, dipelajari, diukur, dan diperiksa kelemahannya.
2. Satu dari kelemahan-kelemahan yang diperoleh, dipilih untuk penelitian.
3. Biasanya dilakukan pemecahan dalam laboratorium.
4. Kemudian dilakukan modifikasi sehingga penyelesaian dapat dilakukan untuk diterapkan.
5. Pemecahannya dipertahankan dan menempatkannya dalam suatu kesatuan sehingga ia menjadi bagian yang permanen dari satu sistem.

Contoh : Penelitian terapan, antara lain yaitu peningkatan kualitas belajar mengajar siswa, pengaruh pemupukan terhadap tanaman, pengaruh implementasi kurikulum MBS terhadap mutu pendidikan dan sebagainya.

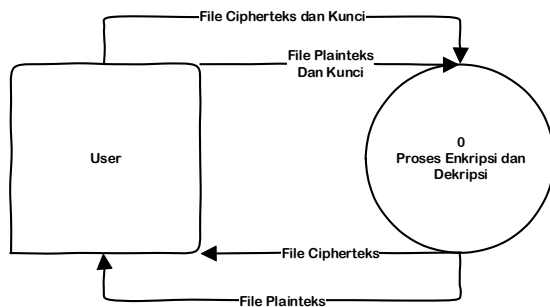
DIAGRAM ALIR DATA (DAD)

1. Flowchart Proses *Enkripsi* dan *Dekripsi*



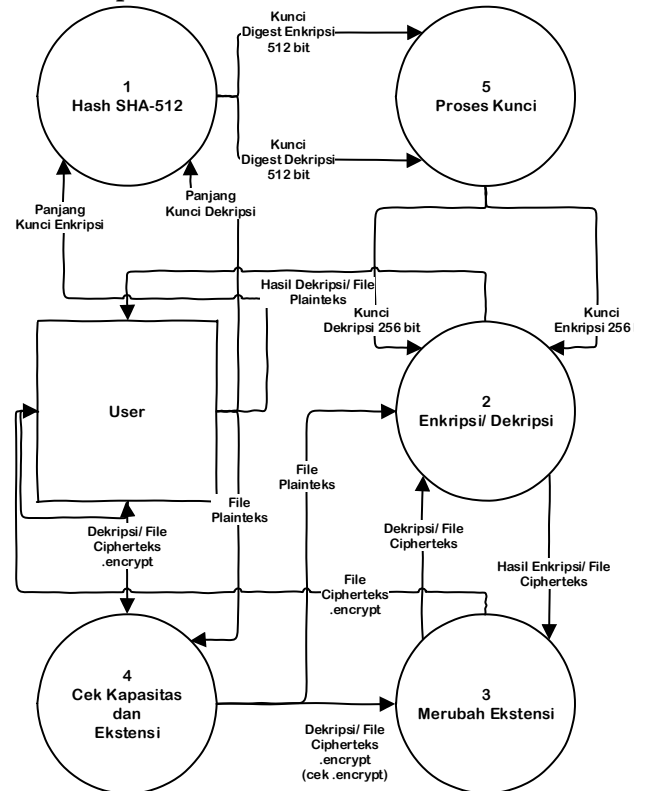
Gambar 1 - Proses Enkripsi dan Dekripsi

2. DAD Level 0 / Sistem Enkripsi dan Dekripsi



Gambar 2 - DAD / Level 0 (Sistem Enkripsi dan Dekripsi)

3. DAD Level 1 / Proses Enkripsi dan Dekripsi

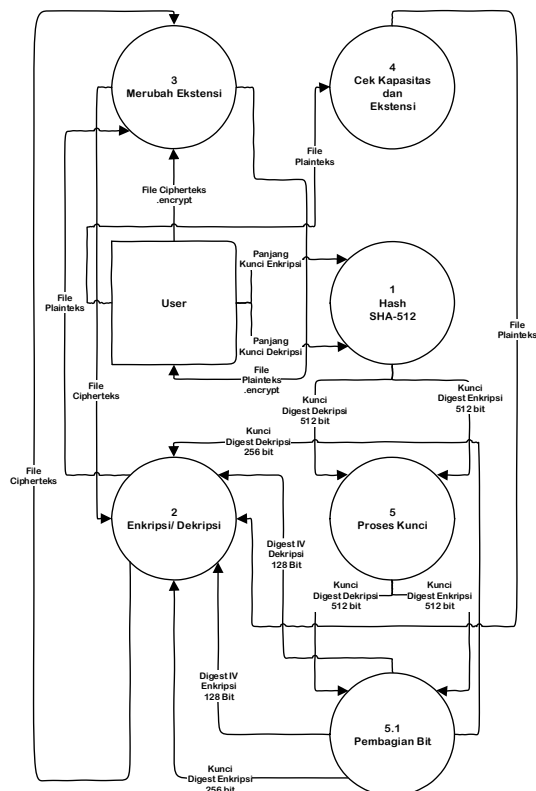


Gambar 3 - DAD / Level 1 (Proses Enkripsi dan Dekripsi)

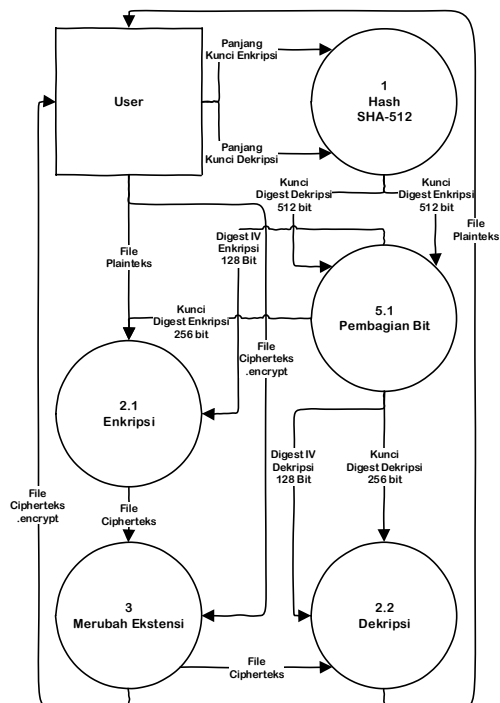
4. DAD Level 2 / Proses Pembagian Kunci dan Proses Algoritma Rijndael

Proses Pembagian Kunci / DAD Level 2

•



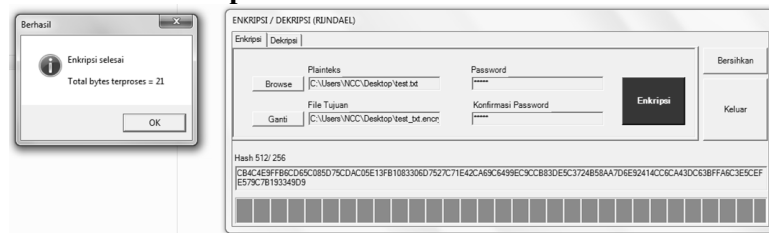
Gambar 4 - DAD / Level 2 (Proses Pembagian Kunci)
Proses Rijndael 256 - Enkripsi dan Dekripsi / DAD Level 2



Gambar 5 - DAD / Level 2 Proses Rijndael 256/ Enkripsi dan Dekripsi

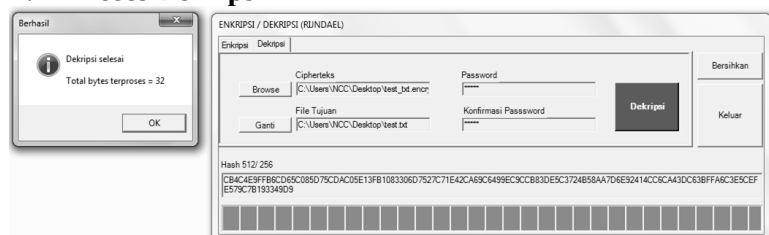
3. HASIL DAN BAHASAN

1. Proses Enkripsi



Gambar 6 - Proses Enkripsi file test.txt.

2. Proses Dekripsi



Gambar 7 - Dekripsi Ciphertexts asli.

3. Hasil Kapasitas

Pembahasan kapasitas ini bertujuan untuk mengetahui berapa besar kapasitas file yang telah diproses *Enkripsi* menggunakan Metode Algoritma *Rijndael* menggunakan kunci 256. File yang akan digunakan dalam menentukan besaran kapasitas file *Enkripsi* adalah PDF, Foto dan Musik.

Berikut adalah rincian dari *Enkripsi* file *Plainteks* menjadi *Ciphertexts* pada file berjenis PDF, Gambar (JPEG) dan Musik (MP3) untuk mengetahui berapa kapasitas yang berubah jika sudah menjadi *Ciphertexts* adalah sebagai berikut.

• Kapasitas *Enkripsi* PDF

	(Bill Sheldon, Billy Hollis, Kent Sharkey, Jonathan Marbutt, Rob Windsor, Gastón C. Hilla...	Date modified: 04/11/2015 6:51 Size: 32,6 MB
	(Evangelos Petroustos) Mastering Microsoft Visual Basic NET, 2010	Date modified: 04/11/2015 6:39 Size: 7,29 MB
	(Louis Hendri Sullivan) Dataflow Diagrams	Date modified: 02/07/2015 7:25 Size: 427 KB
	(Roger S. Pressman) Software Engineering A Practitioner's Approach 7th edition	Date modified: 03/11/2015 13:18 Size: 20,0 MB
	(Sentot K) Teori dan Aplikasi Kriptografi	Date modified: 08/09/2015 21:09 Size: 2,28 MB

Gambar 8 - PDF/ Plainteks dan Ciphertexts.

Dari gambar tersebut dapat disimpulkan bahwa file PDF yang di *Enkripsi* menggunakan Algoritma *Rijndael*, kapasitas *Ciphertexts* tersebut sama dengan kapasitas *Plainteks*.

• Kapasitas *Enkripsi Gambar*

	Desert	Type: JPG File Dimensions: 1024 x 768	Date taken: 14/03/2008 13:59 Size: 826 KB
	Hydrangeas	Type: JPG File Dimensions: 1024 x 768	Date taken: 24/03/2008 16:41 Size: 581 KB
	Jellyfish	Type: JPG File Dimensions: 1024 x 768	Date taken: 11/02/2008 11:02 Size: 757 KB
	Penguins	Type: JPG File Dimensions: 1024 x 768	Date taken: 18/02/2008 5:07 Size: 759 KB
	Tulips	Type: JPG File Dimensions: 1024 x 768	Date taken: 07/02/2008 11:33 Size: 606 KB

	Desert.jpg.encrypt	Type: ENCRYPT File	Date modified: 24/11/2015 Size: 826 KB
	Hydrangeas.jpg.encrypt	Type: ENCRYPT File	Date modified: 24/11/2015 Size: 581 KB
	Jellyfish.jpg.encrypt	Type: ENCRYPT File	Date modified: 24/11/2015 Size: 757 KB
	Penguins.jpg.encrypt	Type: ENCRYPT File	Date modified: 24/11/2015 Size: 759 KB
	Tulips.jpg.encrypt	Type: ENCRYPT File	Date modified: 24/11/2015 Size: 606 KB

Gambar 9 - JPG/ Plainteks dan Cipherteks. Sama halnya dengan PDF, gambar Cipherteks berformat JPG tersebut sama dengan Plainteks, tidak ada perubahan dalam kapasitas

• Kapasitas *Enkripsi Musik*

	01 whitney houston - i will always love you_mp3.encrypt	Type: ENCRYPT File	Date modified: 24/11/2015 12:54 Size: 4,11 MB
	02 celine dion - my heart will go on_mp3.encrypt	Type: ENCRYPT File	Date modified: 24/11/2015 12:54 Size: 4,29 MB
	03 josh groban - you raise me up_mp3.encrypt	Type: ENCRYPT File	Date modified: 24/11/2015 12:54 Size: 4,45 MB
	04 mariah carey - hero_mp3.encrypt	Type: ENCRYPT File	Date modified: 24/11/2015 12:55 Size: 4,00 MB
	05 madonna - take a bow_mp3.encrypt	Type: ENCRYPT File	Date modified: 24/11/2015 12:55 Size: 4,16 MB

	(Bill Sheldon, Billy Hollis, Kent Sharkey, Jonathan Marbutt, Rob Windsor, Gastón C., Hill...)	Type: ENCRYPT File	Date modified: 24/11/2015 13:00 Size: 32,6 MB
	(Evangelos Petroustos) Mastering Microsoft Visual Basic NET, 2010_pdf.encrypt	Type: ENCRYPT File	Date modified: 24/11/2015 13:00 Size: 7,29 MB
	(Louis Hendri Sullivan) Dataflow Diagrams_pdf.encrypt	Type: ENCRYPT File	Date modified: 24/11/2015 13:01 Size: 427 KB
	(Roger S., Pressman) Software Engineering A Practitioner's Approach 7th edition_pdf...	Type: ENCRYPT File	Date modified: 24/11/2015 13:01 Size: 20,0 MB
	(Sentot K) Teori dan Aplikasi Kriptografi_pdf.encrypt	Type: ENCRYPT File	Date modified: 24/11/2015 13:01 Size: 2,28 MB

	01 whitney houston - i will always love you
	02 celine dion - my heart will go on
	03 josh groban - you raise me up
	04 mariah carey - hero
	05 madonna - take a bow

Gambar 10 - MP3/ Plainteks dan Cipherteks.

Dari kelima .MP3 tersebut tidak ada perubahan kapasitas antara Plainteks MP3 dan Ciphertek MP3, semuanya memiliki kapasitas yang sama

4. KESIMPULAN

Berdasarkan dari hasil penelitian yang sudah dilakukan dengan berbagai file yang sudah diuji untuk melakukan pemrosesan *Enkripsi*, *Dekripsi*, hasing dengan menggunakan Metode Algoritma *Rijndael* 256, maka dapat disimpulkan bahwa Teknik Algoritma *Rijndael* 256 dapat diimplementasikan menggunakan Bahasa Pemrograman Visual Basic dan dapat berjalan dengan baik dan hingga saat ini Algoritma Kriptografi *Rijndael* belum diketahui celah untuk dipecahkan rancangannya.

Cipherteks yang dihasilkan dapat di*Dekripsikan* kembali menjadi *Plainteks* tanpa membuat informasi yang terdapat didalamnya berubah atau sama dengan aslinya dan isi dari *Cipherteks* tersebut tidak dapat dikenali atau tidak sama dengan *Plainteks*, dalam hal ini proses *Enkripsi* dan *Dekripsi* berhasil. Sedangkan kapasitas dari *Cipherteks* yang

dihasilkan dari *Plainteks* tidak terdapat perubahan baik penambahan kapasitas ataupun pengurangan kapasitas.

Saran dari penulis mengenai hasil penelitian ini adalah dimaksud agar untuk selanjutnya akan ada yang bisa mengembangkan penelitian ini dengan lebih baik, berikut ini adalah saran dari penulis :

1. Informasi yang bersifat rahasia yang sudah dilindungi dengan pengamanan kriptografi *Rijndael* tersebut masih dapat dihapus/ *delete*. Tentu jika bersifat rahasia tidak hanya dilindungi dengan kriptografi tapi dengan pengamanan penyembunyian atau tidak dapat dihapus/ *undelete*
2. Cipherteks yang dihasilkan berupa file dengan kapasitas yang sama dengan plaintek, di era digital dengan perkembangan internet yang pesat, kapasitas menjadi sangat penting karena mempengaruhi biaya dan kecepatan dalam bertukar data. Penulis berharap kedepannya adalah dapat dilakukan

penelitian hasil *Cipherteks* dengan adanya kompresi file.

menggunakan algoritma Rijndael berbasis Java SE.

3. Pada saat proses *Enkripsi*, file *Plainteks* asli tersebut hilang dan diganti dengan file *Cipherteks*, hal tersebut bisa menjadi keunggulan atau kelemahan dan saran dari penulis adalah adanya pilihan untuk merubah *Cipherteks* tanpa menghilangkan file *Plainteks* atau sebaliknya.

5. DAFTAR PUSTAKA

- Ahmad Rosyadi, R., Rizal Isnanto, R., & Kodrat. (2012). Implementasi algoritma kriptografi AES untuk enkripsi dan dekripsi email.
- Basuki Rakhmat. (2010). Steganografi menggunakan metode least significant bit dengan kombinasi algoritma kriptografi Vigenère dan RC4. *Jurnal Dinamika Informatika*.
- David Kahn. (2012). *The codebreakers*. House of Mittler & Sohn.
- Evangelos Petroustos. (2010). *Mastering Microsoft Visual Basic .NET*. Wiley Publishing, Inc.
- Febriyansyah. (2012). Program studi teknik informatika, Fakultas Teknik Komputer, Universitas Bina Darma.
- Muhammad Fairuzabadi. (2010). Implementasi kriptografi klasik menggunakan Borland Delphi. *Jurnal Dinamika Informatika*.
- Muhammad Raudy Nurdinta. (2013). Analisis dan simulasi perbandingan algoritma DES dan Baker Map pada kriptografi untuk citra digital. *Jurnal Dinamika Informatika*.
- Indrajani, S.Kom., MM. (2015). *Database design*. Elex Media Komputindo.
- Pazaini. (2012). Smart messaging pada mobile Android dengan Advanced Encryption Standard (AES) dan kompresi Huffman.
- Roger S. Pressman. (2010). *Rekayasa perangkat lunak*. McGraw Hill.
- Sentot K. (2010). *Teori dan aplikasi kriptografi*.
- Tata Sutabri. (2012). Analisa sistem informasi.
- William Stallings. (2011). *Cryptography and network security: Principles and practice* (5th ed.). Prentice Hall.
- Yoga Aprianto. (2014). Rancang bangun aplikasi enkripsi dan dekripsi citra digital