JURNAL SINTAKS LOGIKA Vol. 2 No. 2 , Mei- 2022
https://jurnal.umpar.ac.id/index.php/sylog

PENERAPAN KRIPTOGRAFI AES PADA DATABASE

Yuliana[1], Mugaffir yunus[2]
Program Studi Teknik Informatika, Universitas Muhammadiyah Parepare, Indonesia
yuliana.123.iskandar@gmail.com, mugaffir@gmail.com

InformasiArtikel

Riwayat Artikel:

DikirimAuthor:9-01-2022
DiterimaRedaksi :10-01-2022
RevisiReviewer: 12-03-2022
Diterbitkan online: 05-05-2022

Keywords :

AES Cryptography , PHP, MySQL.

ABSTRACT

Information data collection often occurs Several errors, lost files and a buildup of files, so there is a need for a database that can accommodate on a large scale. The purpose of this research is to maintain security on the database so that unauthorized parties cannot understand or read information on the database. The research method used includes collecting data with literature, while the system development method uses the aes key three types namely 128 bit (10 Round), 192 bit (12 round),256 bit (14 round). structured system analysis and design tools are implemented using the PHP and MySQL programming languages as the database. With this system, it is expected to secure data in the database by applying AES cryptography techniques. After doing the decryption prosess, it can return text and image as before they were encrypted as for the duration of the encryption proses, the decryption is affected by the size of the image capacity and the amount of text

Kata kunci :

Kriptografi AES, PHP, MySQL.

ABSTRAK

Pengumpulan data informasi seringkali terjadi beberapa kesalahan penduplikatan berkas, kehilangan berkas dan penumpukan berkas maka perlu adanya database yang mampu menampung dalam skala banyak. Tujuan dalam penelitian ini adalah menjaga keamanan pada database sehingga pihak yang tidak berkepentingan tidak dapat memahami atau membaca informasi pada database. Metode penelitian yang digunakan meliputi pengumpulan data dengan literatur, sedangkan metode pembangunan sistem menggunakan model pengujian Algoritma AES dan panjang kunci AES terdapat tiga jenis yaitu 128 bit (rounde 10), 192 bit (12 rounde), 256 bit (14) . Alat bantu analisis dan perancangan sistem yang terstruktur diimplementasikan menggunakan bahasa pemograman PHP dan MySQL sebagai databasenya. Setelah melakukan proses dekripsi dapat mengembalikan teks dan gambar seperti sebelum dienkripsi adapun durasi proses enkripsi, dekripsi dipenganruhi besarnya kapasitas gambar dan banyaknya teks.

PenulisKorespondensi:

Yuliana,
Program Studi Teknik Informatika,
Universitas Muhammadiyah Parepare,
Jl. Jenderal Ahmad Yani Km.6,
Kota Parepare, Indonesia
Email:
yuliana.123.iskandar@gmail.com

I. PENDAHULUAN

A. Latar belakang

Dalam database ada beberapa data informasi yang tidak semua user dapat membacanya dan perlu kita pahami masih ada beberapa kemungkinan, kesalahan ancaman yang dapat merusak informasi data, jelas sangat merugikan pihak bersangkutan. Menerapkan kriptografi (enkripsi, dekripsi) pada database adalah suatu cara melindungi data informsi dari ancaman, baik dalam bentuk kesengajaan maupun tidak yang bersifat merugikan dan merusak sistem.

Enkripsi yaitu proses mengubah data jelas/asli (plaintext) kedalam bentuk sandi (chiphertext) yang tidak dapat dikenali orang lain tanpa izin dari pihak bersangkutan, chipherteks inilah yang akan terlihat di database sedangkan dekripsi merupakan proses mengembalikan data yang disandikan kembali pada data sebelumnya jelas/asli (plaintext) yang dapat dibaca pihak bersangkutan.

Disini saya akan menerapkan enkripsi, dekripsi pada salasatu algoritma kriptograpi yaitu algoritma AES selain tingkat keamananya memadai, algoritma AES belum ada yang menerapkanya pada database, di Universitas Muhammadiyah Parepare. Berdasarkan masalah diatas, penulis ingin melakukan penelitian dengan judul "Penerapan Kriptografi AES Pada Database".

B. Tinjauan literatur singkat

Melihat dari sejumlah judul dan tema yang berkaitan dengan penelitian yang dilakukan, diperoleh persamaan dan perbedaan dari penelitian yang akan dilakukan.Tujuannya membuktikan bahwa penulisan tugas akhir ini asli dan bukan duplikasi dari tugas akhir penelitian lain, seperti berikut ini :

Angga aditya Permana dan Desi nurnaningsih (2018) "Rancangan Aplikasi Pengamanan data dengan algoritma *Advanced Encyption standard (aes)* ". Pada penelitian ini penelitian merancang suatu sistem untuk melindungi data file agar kerahasian informasi terjaga. Adapun metode yang diterapkan yaitu algoritma AES.

Ahmad rifai dan hery sunandar (2016) "Aplikasi Kriptografi Database *MySQL* Menggunakan Metode Markel Helman". Pada penelitian ini dirancang suatu sistem dengan tujuan melindungi akses data dari pihak-pihak yang tidak diharapkan maka sangat diperlukan enkripsi dan dekripsi .sehingga dibutuhkan metode markel helman untuk enkripsi dan dekripsi.

Santoso dan Wahyu Priyoatmoko (2016), "Pengamanan Data *MySQL* Pada *E-Commerce* Dengan Algoritma *AES* 256". Pada penelitian ini bertujuan mengamankan data pengguna dari pihak pihak tertentu seperti hacher atau pesaing bisnis lainya maka diperlukan adanya enkripsi dekripsi data Mysql pada E-comerce

Dari ketiga penelitian diatas memiliki perbedaan dalam penelitian ini, yaitu letak tampat penelitian, fitur aplikasi, dan tahun pembuatan penelitian.

C. Alasan diadakan penelitian

Berdasarkan latar belakang, maka identifikasi masalah dari tugas akhir yaitu bagaimana cara membuat aplikasi dalam menerapkan algoritma Kriptografi AES pada database MySQL dengan tepat sehingga mencapai tujuan yang ditetapkan

D. Tujuan penelitian

Berdasarkan pengamatan dan penelitian, penulis bermaksud bagaimana cara menjaga keamanan pada database sehingga pihak yang tidak berkepentingan tidak dapat memahami atau membaca informasi pada database. Adapun tujuan penelitian ini adalah mengamankan data pada database dengan menerapkan teknik *Cryptography AES*.

II. METODE PENELITIAN

Jenis penelitian yang digunakan yaitu :

a. Penelitian lapangan adalah penelitian yang dilakukan secara langsung terhadap objek yang akan diteliti. Dalam penelitian lapangan, yang dilakukan penulis yakni melakukan pengumpulan data Mahasiswa(i) UM Parepare.
b. Penelitian pustaka adalah penelitian yang dilakukan dengan menggunakan beberapa buku sebagai referensi penulis untuk pembuatan aplikasi Kriptografi AES.

III. HASIL DAN PEMBAHASAN

Analisis aliran data bertujuan mengetahui aliran proses informasi. Dalam analisis sistem ini, penulis menggunakan pengembangan orientasi objek sehingga menggunakan *Use Case* Diagram, *Activity* Diagram dan *Sequence* Diagram

a. *Use Case* Diagram

a) Aktor Pengguna

Use Case Diag11ram pada penerapan kriptografi AES pada database. *Use Case* Diagram sebagai berikut:

Gambar 1. Use Case *Diagram Pengguna*

b. *Perancangan* Database

Racangan *database* untuk membuat sebuah sistem dengan Penerapan Kriptografi AES Pada Datavase dan juga tabel-tabelnya.

Tabel 10. Mahasiswa

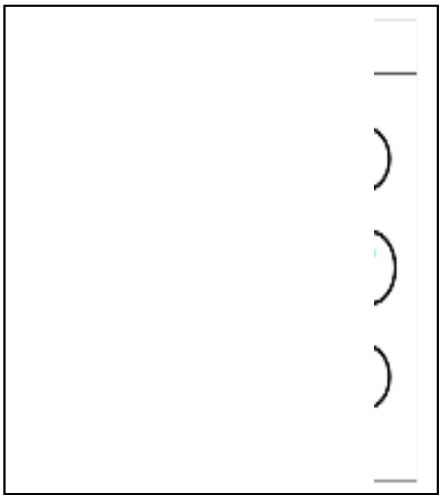
No	Nama	Jenis	Ukuran	Ket
1	Idmahasiswa	*Int*	11	*AUTO_INCREMENT*
2	Namamahasiswa	*varchar*	500	

3	Nimmahasiswa	*varchar*	500	
4	Jkmahasiswa	*varchar*	500	
5	Fakultasmahasiswa	*varchar*	500	
6	Jurusanmahasiswa	*varchar*	500	
7	Emailmahasiswa	*varchar*	500	
8	Alamatmahasiswa	*longtext*		
9	Nohpmahasiswa	*Varchar*	500	
10	Foto	*Varchar*	200	
11	Kunci	*varchar*	50	
12	Tanggalbuat	*Timestamp*		

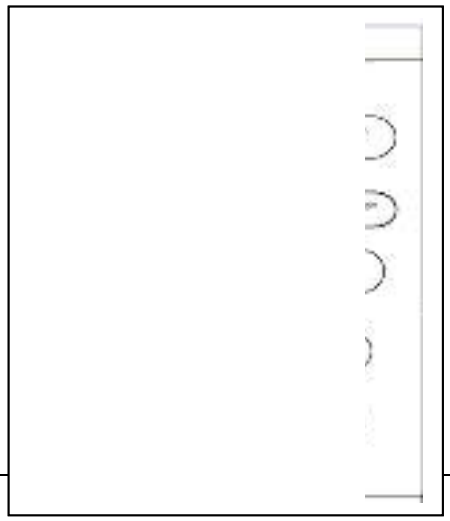
c. *Activity Diagram*

Aktivity Diagram ini menjelaskan tentang aktivitas-aktivitas yang terjadi dalam sebuah aliran proses pada sistem

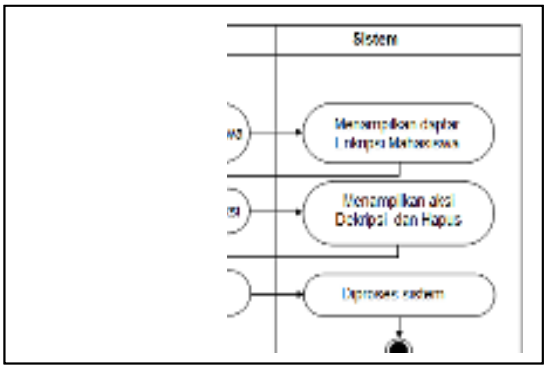
a) Diagram *Aktivity* Data Mahasiswa



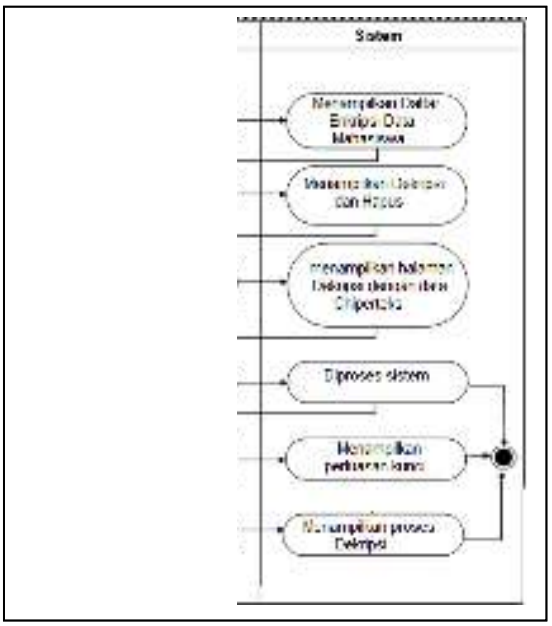
b) Diagram *Aktivity* Enkripsi 1



c) Diagram *Aktivity* Hapus Data Enkripsi Mahasiswa



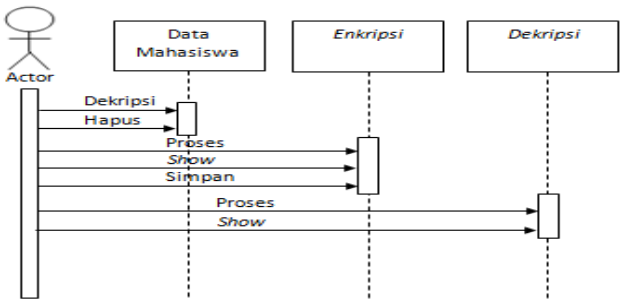
d) Diagram *Aktivity* Dekripsi



d. *Sequence* Diagram

Sequence Diagram merupakan aliran antara objek yang membentuk proses, berikut adalah diagram sequencenya pada Penerapan Kriptografi AES Pada Database.

Diagram Sequence Pengguna



e. Rancangan Input/Output

1. Halaman Data Mahasiswa

Merupakan tampilan halaman daftar *enkripsi* data mahasiswa, yang digunakan pengguna untuk mengelola data dan melihat data yang terlah terenkripsi juga digunakan untuk mengdekripsi data.

*Gambar **1**.* Halaman Data Mahasiswa

Merupakan tampilan halaman *enkripsi* yang digunakan pengguna untuk memasukkan data dan melakukan proses enkripsi.

Gambar 2. Halaman Enkripsi

2. Halaman *Dekripsi*

Merupakan tampilan halaman *dekripsi* yang digunakan pengguna untuk melakukan proses *dekripsi*

Gambar 3. Halaman Dekripsi

f. Implementasi

Implementasi sistem merupakan tahap penerapan dari suatu teknologi yang didesain untuk siap dioperasikan. Tahap ini merupakan terjemahan perancangan dari bab hasil analisis sebelumnya dalam suatu bahasa pemrograman. Bahasa pemrograman yang digunakan untuk membangun sebuah sistem Penerapan Kriptograpi *AES* Pada Database adalah bahasa pemrograman *PHP*.

a. Kebutuhan perangkat keras

Spesifikasi minimum perangkat keras sebagai berikut :

Tabel 4.3. Kebutuhan Perangkat keras

Jenis	Spesifikasi
Notebook/Komputer	*ASUS*-9101CFRU
Processor	Intel Celeron n400,up to 6.ghz
Memory	2GB RAM
Harddisk	500GB

b. Kebutuhan perangkat lunak

Spesifikasi minimum perangkat lunak sebagai berikut :

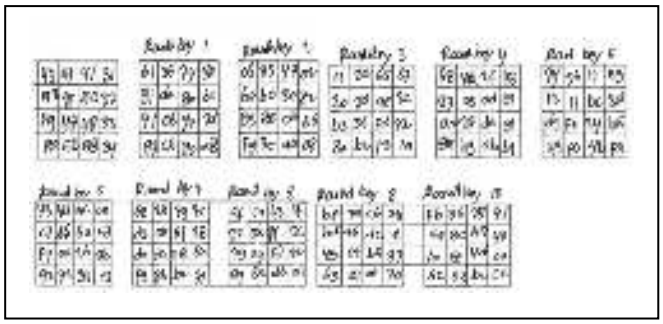
Tabel 4.4. Kebutuhan Perangkat Lunak

Jenis	Spesifikasi
Sistem Operasi	*Windows 7 x64bit*

g. Pengujian Sistem dan Pengujian Menual

Pengujian Kriptografi *AES* dengan kunci (CRYPTOGRAPY12345) dengan teks (YULIANA) .

Adapun perbandingan perluasan kunci dapat dilakukan secara menual maupun dengan aplikasi sebagai berikut:

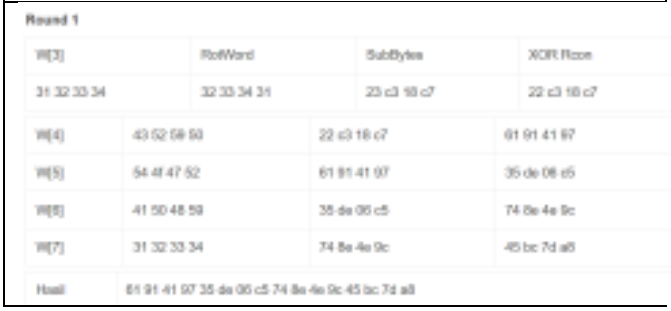


Gambar 4.10. Perluasan Kunci CRYPTOGRAPY12345

Tabel 4.5.perluasan kunci 1

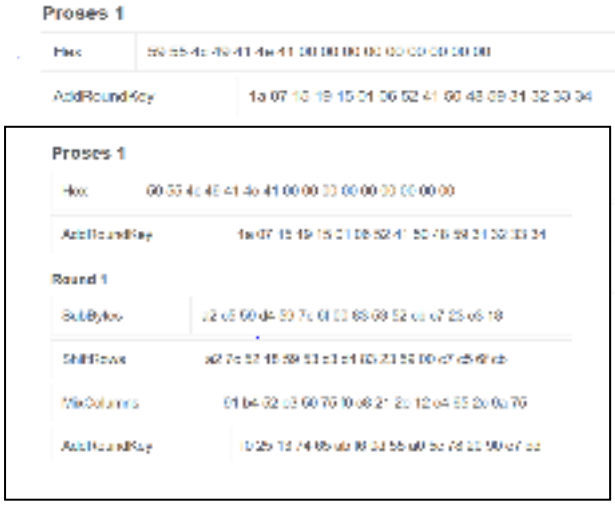
Menual

Aplikasi



Round 1			
W[3]	RotWord	SubBytes	XOR Rcon
31 32 33 34	32 33 34 31	23 c3 18 c7	22 c3 18 c7
W[4]	43 02 59 50	22 c3 18 c7	61 91 41 97
W[5]	54 47 47 52	61 91 41 97	35 de 06 c5
W[6]	41 50 48 59	35 de 06 c5	74 8e 4e 9c
W[7]	31 32 33 34	74 8e 4e 9c	45 bc 7d a8
Hasil	61 91 41 97 35 de 06 c5 74 8e 4e 9c 45 bc 7d a8		

Dari tabel diatas perbandihan perluasan kunci secara menual dan pada aplikasi. Untuk mendapatkan kunci round berikutnya dilakukan cara yang sama. Setelah melakunan perluasan kunci kemudian lanjut pada proses enkripsi. Adapun proses enkripsi d a a P



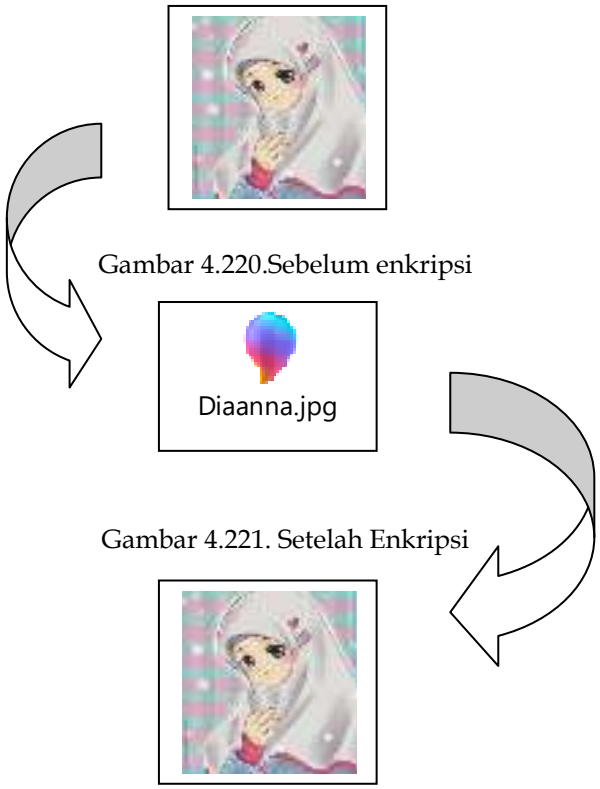
Gambar 4.47.Proses enkripsi pada aplikasi

Proses menual:

Gambar 4.11. Pengujian 1, Round 1a

*Gambar 4.13. Pengjian 1,*round *1c*

Gambar 4.11. Pengujian 1, Round 1a



Gambar 4.220.Sebelum enkripsi

Gambar 4.221. Setelah Enkripsi

Gambar 4.222.Setelah Dekripsi

Dari proses enkripsi AES aplikasi maupun menual transformasi *round* 1 sampai *round* 10 saling bersinambungan adapun proses transpormasi yaitu *SubBytes,Shifrows,Mixcolums,Addroundkey* kecuali *round* 10 tidak dilakukan *Mixcolums*

h. Pengujian Validitas Dan Durasi Enkripsi, Dekripsi

Tabel 4.9.Durasi enkripsi pada gambar

No	Nama	Kapasistas gambar		Durasi waktu	
		Sebelum enkripsi	Setelah dekripsi	Proses enkripsi	Proses dekripsi
1	Fadiyah.jpg	5.15 kb	5.15 kb	00 detik	00 detik
2	Daerah.jpg	28 kb	28 kb	00 detik	01 detik
3	Ciara.jpg	38.2 kb	38.2 kb	01 detik	01 detik
4	Nahdarafanda.jpg	48.5 kb	48.5 kb	01 detik	01 detik
5	Diaanna.jpg	163 KB	163 KB	02 detik	03 detik

Tabel 4.10.Durasi enkripsi pada teks

NO	Teks			Durasi waktu	
	Sebelum enkripsi	Setelah enkripsi	Setelah dekripsi	Proses enkripsi	Proses dekripsi
	Kabupaten Enrekang,	d1c06b62ac5a66f9527a5c9947f1ea62842b184615bbf8a4db78997d8d2eb39a	Kabupaten Enrekang,	25 detik	25 detik
	Kabupaten Enrekang, kecamatan Baraka	d1c06b62ac5a66f9527a5c9947f1ea62fd8400b454	Kabupaten Enrekang, kecamatan Baraka	26 detik	26 detik

		1709a92c1cf4163d969a19726e15d544d66adfcc42edc571ab0e1a			
	Kabupaten Enrekang, kecamatan Baraka,Desa kading	d1c06b62ac5a66f9527a5c9947f1ea62fd8400b4541709a92c1cf4163d969a19242622f8c45f61f505ed4c5649bcd98f42c9d27b20d723e7e39057fd062504e9	Kabupaten Enrekang, kecamatan Baraka,Desa kading	27 detik	27 detik
	Kabupaten Enrekang, kecamatan Baraka,Desa kading,Dusun matawai	d1c06b62ac5a66f9527a5c9947f1ea62fd8400b4541709a92c1cf4163d969a19242622f8c45f61f505ed4c5649bcd98f3e5d715fc599531a3892c2e04fe48d07	Kabupaten Enrekang, kecamatan Baraka,Desa kading,Dusun matawai	28 detik	28 detik
	Kabupaten Enrekang, kecamatan Baraka,Desa kading,Dusun matawai,Dusun matawai	d1c06b62ac5a66f9527a5c9947f1ea62fd8400b4541709a92c1cf4163d969a19242622f8c45f61f505ed4c5649bcd98f7da9e588a5449d99b352a004ea8fabe5fc34bfea7ee6af64dc1e7f1a6f9e8e8c	Kabupaten Enrekang, kecamatan Baraka,Desa kading,Dusun matawai, Dusun matawai	29 detik	29 detik

IV. KESIMPULAN

Berdasarkan hasil dari pengujian sistem yang dilakukan penulis maka disimpulkan bahwa:
Aplikasi kriptografi dibuat menggunakan bahasa pemograman php dan algoritma kriptografi AES. Terdiri dari plainteks berupa teks asli dienkripsi sehingga menghasilkan chiperteks (teks disandikan) kemudian tersimpan di database. Chiperteks yang tersimpan di database didekripsi sehingga kembali teks asli, AES memiliki panjang kunci 128 bit (10 round), 198 bit (12), 156 bit (14). Penyandian AES menggunakan proses yang berulang sehingga AES sangat baik untuk menjaga keamanan data Pada aplikasi terdiri dari from input data mahasiswa berupa (Nama mahasiswa, Nim, Jenis kelamin, Fakultas, Jurusan, Email, Alamat, No.telpon dan Foto) dan memiliki fitur show proses untuk menampilkan proses enkripsi dan dekripsi dari tiap tiap teks. Dari pengujian validasi pada gambar dan teks dapat disimpulkan setelah melakukan proses dekripsi dapat mengembalikan teks dan gambar seperti sebelum dienkripsi adapun durasi proses enkripsi, dekripsi dipengaruhi besarnya kapasitas gambar dan banyaknya teks, semakin besar kapasitas gambar dan semakin banyanyak teks maka semakin lama proses enkripsi dekripsinya.

REFERENSI

[1] Aditya, Angga dan Nurmaningsi Desi. 2018. *Rancangan Aplikasi Pengamanan data Dengan Algororitma*

Advanced Encytion Standar (AES). Tanggerang: Universitas Muhammadiah Tangerang.

[2] Andree , Dimas. 2016. *Materi Pembahasan Algoritma Simetris*.Fromhttps://dimasandree.wordpress.com/2013/11/13/kriptografi-simetri-dan-asimetri. (2 Juli 2020).

[3] Arifianto,Rahmad.2014.*MateriFlowchart*.From https://rahmatarifianto.wordpress.com/2014/11/20/pengertian-flowchart-dan-jenis-jenisnya.html. (2 Juli 2020).

[4] Kadir, Abdul. 2011. From Zero to A Pro CSS. Yogyakarta : Andi.

[5] Kadir, Abdul. 2013. From Zero to A Pro HTML 5. Yogyakarta : Andi.

[6] Komputer, Wahana. 2016. Seri Panduan Lengkap Menguasai Pemrograman Web. Yogyakarta : Andi.

[7] Komputer, wahana. 2012. Paling Dicari! JavaScript Source Code. Yogyakarta : Andi.

[8] Madiun, Madcoms. 2008. Teknik Mudah Membangun Website dengan HTML, PHP, dan MySQL. Yogyakarta : Andi.