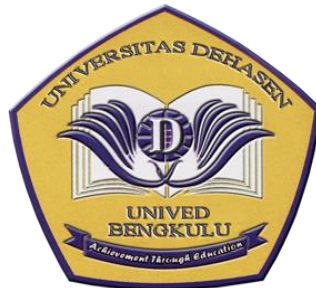


**PENERAPAN ALGORITMA ADVANCED ENCRYPTION STANDARD
(AES) UNTUK PENGAMANAN FILE PADA APLIKASI BERBASIS WEB**

SKRIPSI



Oleh :

FIFMIANTI BIBIOLA
NPM. 18020018

**PROGRAM STUDI REKAYASA SISTEM KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS DEHASEN
BENGKULU
2023**

**PENERAPAN ALGORITMA ADVANCED ENCRYPTION STANDARD
(AES) UNTUK PENGAMANAN FILE PADA APLIKASI BERBASIS WEB**

SKRIPSI

Oleh :

**FIFMIANTI BIBIOLA
NPM. 18020018**

Diajukan Untuk Memenuhi Persyaratan Dalam Menyusun Skripsi
Pada Program Studi Rekayasa Sistem Komputer

**PROGRAM STUDI REKAYASA SISTEM KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS DEHASEN
BENGKULU
2023**

**PENERAPAN ALGORITMA ADVANCED ENCRYPTION STANDARD
(AES) UNTUK PENGAMANAN FILE PADA APLIKASI BERBASIS WEB**

SKRIPSI

Oleh :

FIFMIANTI BIBIOLA
NPM. 18020018

DISETUJUI OLEH :

Dosen Pembimbing Utama



Toibah Umi Kalsum, S.Kom, M.Kom
NIDN. 02.060573.01

Dosen Pembimbing Pendamping



Hendri Alamsyah, S.Kom, M.Kom
NIDN. 02.110391.01

**Mengetahui,
Ketua Program Studi
Rekayasa Sistem Komputer**



Toibah Umi Kalsum, S.Kom, M.Kom
NIDN. 02.060573.01

**PENERAPAN ALGORITMA ADVANCED ENCRYPTION STANDARD
(AES) UNTUK PENGAMANAN FILE PADA APLIKASI
BERBASIS WEB**

SKRIPSI

Disusun Oleh :

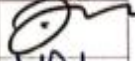



FIFMIANTI BIBIOLA
NPM. 18020018

Telah Dipertahankan Didepan TIM Penguji
Universitas Dehasen Bengkulu Pada :

Hari : Jum'at

Tanggal : 09 Juni 2023

Skripsi ini telah diperiksa dan disetujui oleh TIM Penguji.

Penguji	Nama	NIDN	Tanda Tangan
Ketua	Toibah Umi Kalsum, S.Kom, M.Kom	02.060573.01	
Anggota	Hendri Alamsyah, S.Kom, M.Kom	02.110391.01	
Anggota	Riska, S.Kom, M.Kom	02.240192.01	
Anggota	Yessi Mardiana, S.Kom, M.Kom	02.030288.02	

Mengetahui,

Dekan Fakultas Ilmu Komputer




Siswanto, SE., S.Kom., M.Kom
NIDN. 02.240363.01

SURAT PERNYATAAN ORISINILITAS & PERSETUJUAN PUBLIKASI
AKADEMI SKRIPSI

Yang bertanda tangan dibawah ini :

Nama : Fifmianti Bibiola
NPM : 18020018
Program Study : Rekayasa Sistem Komputer
Fakultas : Ilmu Komputer
Tempat/tanggal lahir : Tanjung Aur, 10 Februari 2000
Alamat : Jln. Pinang mas raya No 57A RT 04 RW 01, Kel. Bentiring.

Dengan ini meyetakan dengan sesungguhnya bahwa SKRIPSI ini berjudul :

**PENERAPAN ALGORITMA ADVANCED ENCRYPTION
STANDARD (AES) UNTUK PENGAMANAN FILE PADA APLIKASI**

1. Adalah benar dibuat oleh saya sendiri untuk memenuhi persyaratan kelulusan akademi.
2. Pada bagian tertentu dalam skripsi yang saya kutip dari hasil karya orang lain telah ditulis sumber secara jelas sesuai dengan norma, kaidah dan etika penulisan ilmiah.
3. Jika dikemudian hari diketahui bukti berdasar bukti-bukti yang kuat ternyata skripsi tersebut oleh dibuat orang lain atau diketahui bahwa skripsi tersebut merupakan plagiat/mencontek/menjiplak hasil karya ilmiah orang lain, maka dengan ini saya bersedia menerima sanksi-sanksi lainnya sesuai dengan peraturan yang berlaku.
4. Dan atas pernyataan orisinilitas tersebut diatas, maka saya menyetujui untuk memberi kepada Universitas Dehasen Bengkulu atas bebas royalti non eksklusif mempublikasikan skripsi saya tanpa perlu meminta izin, selama mencantumkan nama saya sebagai penulis.
5. Saya bersedia menanggung secara pribadi tanpa melibatkan Universitas Dehasen Bengkulu segala bentuk tuntutan hukum yang ditimbulkan atas pelanggaran hak cipta dalam karya ilmiah saya ini.

Demikian surat pernyataan ini dibuat untuk dipergunakan sebagaimana mestinya.

Bengkulu, 25 Mei 2023

Hormat saya



Fifmianti Bibiola
Fifmianti Bibiola
18020018

MOTO DAN PERSEMBAHAN

"You only fail when you stop trying. And don't people your dream, but show them."

"Dan tuhan berfitman, "Berdoalah kepada-Ku, niscaya akan Aku perkenankan bagimu."

(Q.S Gafir:60)

"Dan sungguh, kelak tuhanmu pasti memberikan karunia-Nya kepadamu, sehingga engkau menjadi puas."

(Q.S Ad-duha:5)

Skripsi ini saya persembahkan untuk :

1. Mama Milmayasmil (mil) dan ayah Marsuan yang sangat saya cintai.
2. Wah Fareza Ellyanora, dan Dang Fernandez, selaku kakak kandungku yang spesial sekali dari awal sampai akhir kuliah selalu menjadi garda depan, dalam keadaan apapun. Terima kasih yang luar biasa aku ucapkan.
3. Wahdang Richi, dan donga Windi. Sebagai kakak ipar yang memberi dukuan yang luar biasa.
4. Dodo nova dan adek fhelisyia, sebagai adek dan keponakan kesayangan bunga.
5. Almamater yang saya banggakan.

ABSTRAK

PENERAPAN ALGORITMA ADVANCED ENCRYPTION STANDARD (AES) UNTUK PENGAMANAN FILE PADA APLIKASI BERBASIS WEB

Oleh :

Fifmianti Bibiola¹⁾

Toibah Umi Kalsum, S.Kom, M.Kom²⁾

Hendri Alamsyah, S.Kom., M.Kom²⁾

Tujuan dari penelitian ini yaitu untuk menerapkan algoritma *Advanced Encryption Standard (AES)* dalam mengamankan file sehingga informasi didalamnya menjadi aman dan tidak dapat dipahami oleh sembarang orang. Penerapan Algoritma *Advanced Encryption Standard (AES)* dibuat menggunakan Bahasa Pemrograman PHP dan database MySQL yang dapat diakses melalui link <http://fifmiantiaes.online/>. Dengan adanya Aplikasi pengamanan file menggunakan algoritma *Advanced Encryption Standard (AES)* berbasis web dapat meningkatkan keamanan file dari pihak yang tidak berwenang. Berdasarkan hasil pengujian yang telah dilakukan diperoleh bahwa sistem berhasil melakukan proses enkripsi dan dekripsi menggunakan Algoritma *AES*, dimana file dokumen tersimpan di dalam server dalam bentuk enkripsi, dan waktu proses enkripsi tergantung dari ukuran file dokumen, semakin besar ukuran file, maka semakin lama proses enkripsi yang diperlukan.

Kata Kunci : *Algoritma Advanced Encryption Standard (AES), Pengamanan File, Aplikasi, Berbasis Web*

1) Calon Sarjana

2) Dosen Pembimbing

ABSTRACT

**THE IMPLEMENTATION OF ADVANCED ENCRYPTION STANDARD
(AES) ALGORITHM FOR FILE SECURITY
IN WEB-BASED APPLICATION**

By:

Fifmianti Bibiola¹⁾

Toibah Umi Kalsum²⁾

Hendri Alamsyah²⁾

This study aims to apply the Advanced Encryption Standard (AES) algorithm in securing files therefore the information inside is safe and cannot be understood by just anyone. The application of the Advanced Encryption Standard (AES) Algorithm is made using the PHP Programming Language and MySQL database which can be accessed via the <http://fifmiantiaes.online/> link. With a file security application using the web-based Advanced Encryption Standard (AES) algorithm, it can increase file security from unauthorized parties. Based on the results of the tests that have been carried out, it is found that the system succeeded in carrying out the encryption and decryption process using the AES Algorithm, where the document files are stored on the server in encrypted form, and the encryption process time depends on the size of the document file, the larger the file size, the longer the encryption process required.

Keywords : *AdvancedEncryption Standard (AES) Algorithm, File Security, Application, Web Based*

1) Student

2) Supervisors

JULY 1, 2023



KATA PENGANTAR

Assalamu'alaikum Wr.Wb

Alhamdulillah, penulis ucapkan atas kehadiran Allah SWT yang selalu memberikan rahmat dan karunia-Nya pada penulis, sehingga penulis dapat menyelesaikan Skripsi yang berjudul “**Penerapan Algoritma *Advanced Encryption Standard* (AES) Untuk Pengamanan File Pada Aplikasi Berbasis Web**”. Shalawat serta salam juga penulis panjatkan kepada junjungan Nabi Besar Muhammad SAW. Skripsi ini dibuat untuk memenuhi persyaratan dalam menyelesaikan pendidikan setara satu Pada Program Studi Rekayasa Sistem Komputer Fakultas Ilmu Komputer Universitas Dehasen Bengkulu.

Penulis menyadari dalam menyusun skripsi ini tidak akan selesai tanpa bantuan dari berbagai pihak. Untuk itu, dalam kesempatan ini penulis mengucapkan terima kasih banyak kepada berbagai pihak yang telah membantu penulis, diantaranya :

1. Bapak Siswanto, S.E., S.Kom., M.Kom selaku Dekan Fakultas Ilmu Komputer Universitas Dehasen Bengkulu
2. Ibu Toibah Umi Kalsum, S.Kom., M.Kom selaku Ketua Program Studi Rekayasa Sistem Komputer Fakultas Ilmu Komputer Universitas Dehasen Bengkulu dan selaku Dosen Pembimbing Utama yang telah memberikan kritik dan saran yang membangun dalam penulisan Skripsi ini.

3. Bapak Hendri Alamsyah, S.Kom., M.Kom selaku Dosen Pembimbing Pendamping yang telah memberikan kritik dan saran yang membangun dalam penulisan Proposal Skripsi ini.
4. Kedua orang tua penulis yang tercinta, Bapak Marsuan dan Ibu Milmayasmi, yang telah memberikan kasih sayang, do'a, pengorbanan, dan dukungan dalam bentuk materi dan mental, yang tak terhingga demi masa depan penulis.
5. Kepada saudara-saudara ku yang telah memberikan semangat, serta setia mendampingi penulis baik suka maupun duka.
6. Irma Malini Amir selaku teman seperjuangan yang telah memberikan bantuan dan dukungan yang luar biasa dalam menyelesaikan skripsi ini.

Diharapkan, Skripsi ini bisa bermanfaat untuk semua pihak. Selain itu, kritik dan saran yang membangun sangat penulis harapkan dari pembaca sekalian agar skripsi ini bisa lebih baik lagi.

Wassalamu'alaikum Wr. Wb.

Bengkulu, Februari 2023

Penulis

DAFTAR ISI

	Halaman
HALAMAN JUDUL	i
LEMBAR PENGESAHAN	iii
LEMBAR PERSETUJUAN	iv
RIWAYAT HIDUP	v
MOTTO DAN PERSEMBAHAN.....	vi
ABSTRAK	vii
KATA PENGANTAR.....	viii
DAFTAR ISI.....	x
DAFTAR TABEL.....	xii
DAFTAR GAMBAR.....	xiii
DAFTAR LAMPIRAN	xv
BAB I PENDAHULUAN	1
1.1. Latar Belakang.....	1
1.2. Rumusan Masalah	3
1.3. Batasan Masalah.....	3
1.4. Tujuan Penelitian.....	4
1.5. Manfaat Penelitian.....	4
BAB II LANDASAN TEORI	6
2.1. Kriptografi	6
2.2. Algoritma Kriptografi.....	10
2.3. Enkripsi dan Dekripsi	12
2.4. <i>Advanced Encryption Standard (AES)</i>	13
2.5. <i>Web Server</i>	27
2.6. Keamanan	31
2.7. Aplikasi.....	31
2.8. Hypertext Preprocessor (Php).....	32
2.9. Basis Data (<i>MySQL</i>).....	33
BAB III METODOLOGI PENELITIAN.....	35
3.1. Subyek Penelitian	35

3.1.1. Tempat dan Waktu Penelitian	35
3.1.2. Sejarah Berdirinya Tempat Penelitian	35
3.1.3. Struktur Organisasi	36
3.1.4. Tugas Dan Wewenang	37
3.2. Metode Penelitian	40
3.3. Instrumen Perangkat Lunak dan Perangkat Keras.....	41
3.4. Metode Pengumpulan Data	42
3.5. Metode Perancangan Sistem.....	43
A. Analisis Sistem Aktual.....	43
B. Diagram Blok Global.....	44
C. Desain Sistem	44
D. Prinsip Kerja Sistem	55
E. Rencana Kerja Sistem.....	56
3.6. Metode Pengujian Sistem	57
BAB IV HASIL DAN PEMBAHASAN.....	Error! Bookmark no
4.1. Hasil.....	Error! Bookmark no
4.2. Pembahasan	Error! Bookmark no
4.3. Pengujian Sistem	Error! Bookmark no
BAB V PENUTUP	Error! Bookmark no
5.1. Kesimpulan.....	Error! Bookmark no
5.2. Saran	Error! Bookmark no

DAFTAR PUSTAKA

LAMPIRAN

DAFTAR TABEL

Tabel	Halaman
3.1. Tabel Alur <i>Waterfall</i>	37
3.2. Tabel Pengujian	50

DAFTAR GAMBAR

Gambar	Halaman
2.1. Web Server	25
3.1. Diagram Blok	41
3.2. Use Case Diagram	41
3.3. Activity Diagram User	42
3.4. Activity Diagram Admin	43
3.5. Class Diagram	43
4.6. Sequence Diagram User	44
4.7. Sequence Diagram Admin.....	44
4.8. Deployment Diagram	45
4.9. Tampilan Halaman Login	45
4.10. Tampilan Layar Dashboar	45
4.11. Tampilan Layar Enkripsi	46
4.12. Tampilan File Dekripsi	47
4.13. Tampilan Layar Form Dekripsi	47
4.14. Rencana Kerja Sistem	48

DAFTAR LAMPIRAN

Lampiran

1. Time Schedule
2. Kartu Bimbingan Skripsi
3. Kode Program

BAB I

PENDAHULUAN

1.1. Latar Belakang

Keamanan data merupakan hal yang sangat penting dalam menjaga kerahasiaan informasi terutama yang berisi informasi sensitif yang hanya boleh diketahui isinya oleh pihak yang berhak saja, apalagi jika pengirimannya dilakukan melalui jaringan publik, apabila data tersebut tidak diamankan terlebih dahulu, akan sangat mudah disadap dan diketahui isi informasinya oleh pihak-pihak yang tidak memiliki wewenang.

Dengan berkembangnya teknologi dibidang jaringan, pengiriman pesan atau data file juga sudah dapat dilakukan menggunakan media jaringan. Maka informasi tersebut harus memerlukan suatu keamanan dan kerahasiaan karena bisa saja informasi tersebut menyimpan hal rahasia atau menjadi dokumen berharga yang harus diawasi kerahasiaannya. Salah satu cara yang dapat dilakukan untuk mengamankan file dokumen tersebut ialah dengan memanfaatkan sistem kriptografi. Kriptografi merupakan suatu teknik yang digunakan untuk mengubah suatu file yang dapat dipahami manusia ke bentuk yang tidak dipahami oleh manusia. Pemakaian kriptografi dalam proses pengiriman file menjadi hal yang wajib belakangan ini. Hal ini ditunjukkan karena pemakaian kriptografi dapat menjadi suatu keamanan tambahan bagi proses pengamanan file tersebut.

Dalam kriptografi terdapat beberapa algoritma yang dapat digunakan untuk melakukan suatu proses kriptografi, salah satunya adalah

algoritma *Advanced Encryption Standard* (AES). *Advanced Encryption Standard* (AES) merupakan algoritma yang menggunakan kunci dan masukan dengan panjang 128 bit. Setiap masukan 128 bit *plaintext* dimasukan ke dalam *state* yang berbentuk bujur sangkar berukuran 4 x 4 *byte*. State ini nantinya akan di- *XOR* dengan *key* dan selanjutnya diolah 10 kali dengan substitusi-transformasi *linear-addkey*.

Penelitian yang telah dilakukan oleh Azhari, dkk (2022), dengan judul implementasi pengamanan data pada dokumen menggunakan algoritma kriptografi *advanced encryption standard* (AES) memperoleh hasil keamanan pada data atau dokumen hasil seleksi para peserta JAMKESMAS sehingga dapat lebih maksimal karena data yang di simpan telah terenkripsi dan hanya bisa dilihat keaslian file tersebut jika file tersebut telah di deskripsi. selain file yang sudah di enkripsi maka akan berubah ekstensi menjadi "AES" dan file yang sudah di dekripsi akan kembali menjadi ekstensi seperti semula tanpa mengubah file keaslian data tersebut. Penelitian lainnya juga sudah dilakukan oleh Azanuddin (2022), dengan judul implementasi keamanan citra menggunakan algoritma AES-128 dengan aplikasi *client-server* dengan hasil proses enkripsi citra digital menggunakan algoritma AES 128 bit memberikan *output cipherimage* yang memiliki tingkat keamanan yang baik.

Dari dua penelitian di atas, akan dilakukan pembuatan aplikasi berbasis web dengan bahasa pemrograman PHP, *database MySQL* dan diakses melalui jaringan *web hosting*, sehingga dapat diakses kapan dan dimana saja, sehingga *user* tidak perlu melakukan proses instalasi pada

komputer yang menggunakan aplikasi pengamanan *file* dengan format *pdf*, *doc*, *txt*.

Berdasarkan dari uraian latar belakang di atas penelitian ini mengambil judul “Penerapan Algoritma *Advanced Encryption Standard* (AES) Untuk Pengaman *File* Pada Aplikasi Berbasis *Web*.”

1.2. Rumusan Masalah

Dari latar belakang diatas, maka rumusan masalah dalam penelitian ini adalah :

1. Bagaimana penerapan algoritma *Advanced Encryption Standard* (AES) untuk pengaman file pada aplikasi berbasis web ?
2. Bagaimana merancang perangkat lunak pengamanan file teks dengan menggunakan metode kriptografi *Advanced Encryption Standard* (AES) ?

1.3. Batasan Masalah

Agar pembahasan dalam penelitian ini tidak meluas, maka penulis memberikan batasan masalah yang akan dibahas pada penelitian ini adalah sebagai berikut :

1. Program Aplikasi yang dibangun berbasis web dengan menyajikan informasi enkripsi dan dekripsi file ini akan diakses berbasis *client server*
2. File yang akan diamankan menggunakan *pdf*, *doc*, *txt*.
3. Bahasa pemrograman yang digunakan adalah PHP
4. *Web server* menggunakan apache dan *database server* menggunakan MySQL *server*

1.4. Tujuan Penelitian

Adapun tujuan penelitian ini, antara lain :

1. Tujuan Umum

Tujuan umum pembuatan skripsi adalah sebagai salah satu syarat akhir dalam penyelesaian studi pada Fakultas Ilmu Komputer Universitas Dehasen Bengkulu

2. Tujuan Khusus

Adapun tujuan khusus dalam penelitian ini berdasarkan latar belakang diatas yaitu :

- a) Untuk menerapkan algoritma *Advanced Encryption Standard (AES)* dalam mengamankan file sehingga informasi didalamnya menjadi aman dan tidak dapat dipahami oleh sembarang orang
- b) Untuk membuat suatu sistem yang dapat mengenkripsi dan mendekripsi isi file dengan menggunakan algoritma *Advanced Encryption Standard (AES)* dalam proses pengamanannya

1.5. Manfaat Penelitian

Adapun manfaat dalam penulisan penelitian ini sebagai berikut :

1. Dapat menerapkan sistem keamanan file berbasis web, dengan Penerapan Algoritma *Advanced Encryption Standard (AES)*
2. Dapat menambah pengetahuan terhadap cara kerja kriptografi *Advanced Encryption Standard (AES)* pada proses enkripsi dan dekripsi isi file dokumen dan sebagai bahan acuan bagi siapapun yang ingin melakukan

penelitian lebih lanjut mengenai penerapan algoritma *AES* dalam pengaman file

BAB II

LANDASAN TEORI

2.1. Kriptografi

Menurut Ilhamsyah (2019:19) Kriptografi (*cryptography*) berasal dari bahasa Yunani dimana *crypto* artinya “*secret*” (rahasia) dan *graphein* artinya “*writing*” (tulisan). Jadi, kata kriptografi adalah “*secret writing*” (tulisan rahasia). Kriptografi ialah ilmu yang berfokus pada cara memproteksi data menggunakan teknik enkripsi, dekripsi dan proses lain yang berhubungan. Matematika merupakan hal yang penting dalam dunia kriptografi, karena hanya dengan pengetahuan matematis dapat dikembangkan prosedur yang dibutuhkan untuk mengenkripsi data secara aman. Hal penting lainnya adalah komputer.

Komputer menjalankan prosedur enkripsi dan dekripsi. Ide utama dari sebuah sistem kriptografi adalah untuk menyamarkan informasi rahasia dengan cara yang tidak dipahami oleh pihak yang tidak berhak. Dua kegunaan umum kriptografi adalah untuk menyimpan data secara aman di komputer dan untuk mengirimkan data melalui saluran yang tidak aman seperti *internet*. Faktanya adalah bahwa pesan yang terenkripsi tidak mencegah pihak lain untuk mengakses pesan tersebut, tetapi dapat dipastikan bahwa pihak lain tidak dapat mengerti apa yang mereka lihat. Setiap orang mempunyai cara-cara yang sangat unik untuk merahasiakan pesan. Cara-cara unik tersebut tentu saja sangat berbeda-beda pada setiap pelaku kriptografi. Setiap cara menulis pesan rahasia, pesan tersebut

mempunyai nilai estetika tersendiri Sehingga kriptografi berkembang menjadi sebuah seni merahasiakan pesan.

Dalam menjaga kerahasiaan data, kriptografi memakai teknik enkripsi dalam mengirimkan data asli (*plaintext*). Setelah melalui proses enkripsi, *plaintext* tersebut berubah ke dalam bentuk data sandi (*ciphertext*) yang tidak dapat dikenali.

Proses untuk mengembalikan *ciphertext* menjadi *plaintext* disebut dengan proses dekripsi. Untuk melakukan proses dekripsi diperlukan adanya suatu kunci rahasia. Dalam kriptografi ini ada 4 tujuan dasar ilmu kriptografi yang merupakan aspek-aspek keamanan informasi sebagai berikut :

- a. Kerahasiaan adalah layanan yang digunakan untuk menjaga isi dari data tersebut agar tidak dapat tidak dapat dibaca oleh siapapun atau pihak-pihak yang tidak berhak.
- b. Integritas Data merupakan layanan yang menjamin data masih asli/utuh selama pengiriman.
- c. Otentikasi Data adalah layanan yang berhubungan dengan identifikasi, baik mengidentifikasi kebenaran pihak-pihak yang berkomunikasi (*user authentication* atau *entity authentication*) maupun mengidentifikasi kebenaran sumber data (*origin authentication*).
- d. Nirpenyangkalan (*Non-repudiation*) adalah merupakan suatu usaha untuk mencegah terjadinya penyangkalan terhadap pengiriman /terciptanya suatu informasi yang telah mengirimkan/ membuat. Di dalam kriptografi

kita akan sering menemukan berbagai istilah atau *terminology* yang penting yang harus diketahui.

Beberapa istilah yang harus diketahui yaitu sebagai berikut :

a. Pesan, *Plaintext* dan *Ciphertext*

Pesan adalah data atau informasi yang dapat dibaca dan dimengerti maknanya. Pesan asli disebut *plaintext*. Agar pesan tidak bisa dimengerti maknanya oleh pihak yang tidak berwenang, maka pesan perlu disandikan ke bentuk lain yang tidak dapat dipahami. Bentuk pesan bersandi adalah *Ciphertext*.

b. Pengirim dan Penerima

Komunikasi data melibatkan pertukaran pesan antara dua entitas. Pengirim (*sender*) adalah entitas yang mengirimkan pesan kepada lainnya. Penerima (*receiver*) adalah entitas yang menerima pesan. Entitas disini dapat berupa orang, mesin (komputer), kartu kredit, kartu atm dan lain-lainnya.

c. Enkripsi dan Dekripsi

Kriptografi mempunyai dua bagian yang penting yaitu, enkripsi dan dekripsi. Enkripsi adalah proses penyandian dari pesan yang asli (*plaintext*) menjadi pesan yang tidak dapat diartikan seperti pesan aslinya (*ciphertext*) dengan menggunakan aturan tertentu. Sedangkan dekripsi merupakan kebalikannya yaitu mengubah pesan yang sedang sudah disandikan menjadi pesan aslinya.

d. Cipher dan Kunci

Algoritma kriptografi disebut juga *cipher* yaitu Aturan *Enchiperling* dan *dechiperling* atau fungsi matematika yang digunakan Untuk enkripsi dan dekripsi. Keamanan algoritma kriptografi sering diukur dari banyaknya kerja (*work*) yang dibutuhkan untuk memecahkan *ciphertext* menjadi *plaintext* tanpa mengetahui kunci yang digunakan. Kunci merupakan parameter yang digunakan untuk transformasi *enciphering* dan *dechiperling*. Kunci biasanya berupa string atau deretan bilangan.

e. Sistem Kriptografi

Kriptografi membentuk sebuah sistem yang dinamakan system kriptografi. Sistem kriptografi (cryptosystem) terdiri dari algoritma kriptografi, semua *plaintext*, *ciphertext*, dan kunci.

f. Penyadap (*eavesdropper*)

Penyadap adalah orang yang mencoba menangkap pesan selama ditransmisikan. Tujuan penyadap adalah untuk memperoleh informasi sebanyak-banyaknya mengenai sistem kriptografi yang digunakan untuk berkomunikasi dengan tujuan memecahkan *ciphertext* menjadi *plaintext*.

g. Kriptanalisis dan kriptologi

Kriptanalisis (*cryptanalysis*) adalah ilmu dan seni untuk memecahkan *ciphertext* menjadi *plaintext* tanpa mengetahui kunci yang digunakan pelaku tersebut adalah kriptanalisis. Jika seorang kriptografi (*cryptographer*) mentransformasikan *plaintext* menjadi *ciphertext* dengan suatu algoritma dan kunci, maka sebaliknya seorang kriptanalisis akan berusaha untuk memecahkan *ciphertext* tersebut untuk menemukan *plaintext* atau kunci. Kriptografi juga memiliki 3 fungsi dasar yaitu :

- a. Enkripsi merupakan hal yang sangat penting dalam kriptografi, merupakan pengamanan data yang dikirim agar terjaga kerahasiannya. Pesan asli disebut *plaintext*, yang diubah menjadi kode-kode yang tidak dimengerti. Enkripsi bisa diartikan *cipher* atau kode dengan menggunakan algoritma yang mengkodekan data yang kita inginkan.
- b. Dekripsi merupakan kebalikan dari proses enkripsi. Pesan yang telah dienkripsi dikembalikan ke bentuk asalnya (teks asli), disebut dengan dekripsi pesan. Algoritma yang digunakan untuk dekripsi tentu berbeda dengan algoritma yang digunakan untuk enkripsi.
- c. Kunci adalah kunci yang dipakai untuk melakukan enkripsi dan dekripsi. Kunci terbagi menjadi dua bagian yaitu, kunci rahasia (*private key*) dan kunci umum (*public key*).

Menurut Pradana dan mayang sari (2021:2) menyatakan kriptografi adalah ilmu dan seni untuk menjaga kerahasiaan pesan dengan cara menyandikannya ke dalam bentuk tidak dapat dipahami lagi maknanya.

2.2. Algoritma Kriptografi

Menurut Ilhamsyah, (2019:24) Algoritma kriptografi atau sering disebut dengan *cipher* adalah suatu fungsi matematis yang digunakan untuk melakukan enkripsi dan dekripsi. Algoritma kriptografi ada dua macam, diantaranya yaitu:

1. Algoritma Simetris

Algoritma simetris atau disebut juga algoritma konvensional adalah algoritma yang menggunakan kunci yang sama pada proses enkripsi dan

dekripsi. Algoritma ini mengharuskan pengirim dan penerima menyetujui satu kunci tertentu sebelum dapat berkomunikasi secara aman. Keamanan algoritma simetri tergantung pada rahasia kunci. Pemecahan kunci berarti memungkinkan setiap orang dapat mengenkripsi dan mendekripsi pesan dengan mudah.

2. Algoritma Asimetris

Algoritma asimetris merupakan algoritma kriptografi yang salah satu kuncinya digunakan untuk proses enkripsi dan satu lagi digunakan untuk proses dekripsi. Semua orang yang mendapatkan kunci *public* dapat menggunakannya untuk mengenkripsi pesan, sedangkan hanya pengirim dan penerima saja yang dapat mendekrip pesan tersebut karena memegang kunci *private*.

Menurut Hulu dan Putri (2021:3) Algoritma kriptografi dapat diklasifikasikan menjadi dua jenis berdasarkan perkembangannya, yaitu kriptografi klasik dan kriptografi modern sebagai berikut :

a. Algoritma Kriptografi Klasik

Algoritma ini digunakan sejak sebelum era komputerisasi dan kebanyakan menggunakan teknik kunci simetris. Cara menyembunyikan pesan adalah dengan menggunakan teknik substitusi atau transposisi atau keduanya. Teknik substitusi adalah mengganti karakter pada plainteks menjadi karakter lain yang hasilnya berupa cipherteks. Sedangkan transposisi adalah teknik mengubah plainteks menjadi cipherteks dengan cara permutasi karakter. Kombinasi kompleks keduanya mendasari pembentukan berbagai algoritma kriptografi modern

b. Algoritma Kriptografi Modern

Algoritma ini memiliki tingkat kesulitan yang lebih kompleks, dan kekuatannya ada di kunci. Algoritma ini menggunakan simbol biner karena mengikuti operasi pemrosesan komputer digital. Sehingga diperlukan suatu bentuk dasar pengetahuan matematika untuk menguasainya .

2.3. Enkripsi dan Dekripsi

Menurut Ilhamsyah (2019:25). Enkripsi merupakan sebuah metode penyandian sebuah pesan atau informasi menjadi sebuah teks yang tidak dapat dibaca. Enkripsi berkaitan erat dengan kriptografi, yang merupakan sebuah metode untuk mengamankan sebuah pesan hingga tidak dapat dibaca oleh pihak ketiga. Enkripsi dapat dibagi menjadi dua proses enkripsi yang berbeda yaitu *Block Cipher* dan *Stream Cipher*. Dekripsi yaitu kebalikan dari proses enkripsi yaitu proses konversi data yang sudah dienkripsi (*ciphertext*) kembali menjadi data aslinya (*Original Plaintext*) sehingga dapat dibaca atau dimengerti kembali. Pesan yang akan dienkripsi disebut *plaintext* yang dimisalkan *plaintext*, proses enkripsi dimisalkan enkripsi, proses dekripsi dimisalkan dekripsi, dan pesan yang sudah dienkripsi disebut *ciphertext* yang dimisalkan *ciphertext*.

Menurut Awinda (2019:25) Enkripsi merupakan proses yang dilakukan untuk menyandikan *plaintext* menjadi *ciphertext* dengan tujuan pesan tersebut tidak dapat dibaca oleh pihak yang tidak berwenang. Deskripsi merupakan proses yang dilakukan untuk memperoleh kembali *Plaintext* dari *ciphertext*.

2.4. *Advanced Encryption Standard (AES)*

Menurut Ilhamsyah (2019:28), Algoritma *rijndael* disebut juga dengan *advanced encryption standard (AES)*. Algoritma AES menggunakan substitusi dan permutasi, dan sejumlah putaran (*cipher* berulang), setiap putaran menggunakan kunci internal yang berbeda (kunci setiap putaran disebut *round key*). Panjang kunci yang digunakan adalah 128 bit sampai 256 bit dengan langkah 32 bit, *rijndael* beroperasi dalam orientasi *byte* (untuk mengkasuskan implementasi algoritma kedalam *software* dan *hardware*). Algoritma AES mempunyai 3 parameter, sebagai berikut :

1. Plaintext : array yang berukuran 16-byte, yang berisi data masuka.
2. Ciphertext : array yang berukuran 16-byte, yang berisi hasil enkripsi.
3. Key : array yang berukuran 16-byte, yang berisi kunci ciphering (disebut juga cipher key).

Algoritma AES dengan 16-byte, maka baik blok data dan kunci yang berukuran 128-bit dapat disimpan didalam ketiga array tersebut (128= 16 x 8). Selama kalkulasi plainteks menjadi ciphertext, status sekarang dari data disimpan didalam array of bytes dua dimensi, *state*, yang berukuran $NROWS \times NCOLS$. Untuk blok data 128-bit, ukuran *state* adalah 4 x 4. Elemen *array* diacu sebagai $S[r,c]$, dengan $0 \leq r < Nb$ (Nb adalah panjang blok dibagi 32. Pada *AES-128 bit*, $Nb = 128/32=4$). *Advanced Encryption Standard (AES)* Pada tahun 1997 kontes pemilihan suatu standar algoritma kriptografi baru. baru pengganti DES dimulai dan diikuti oleh 21 peserta dari seluruh dunia. Setelah melewati tahap seleksi yang ketat, pada tahun 1999 hanya tinggal 5 calon yaitu algoritma *Serpent* (Ross Anderson-

University of Cambridge, Eli Biham-Technion, Lars Knudsen-University of California San Diego), MARS (IBM Amerika), Twofish (Bruce Schneier, John Kelsey, dan Niels Ferguson-Counterpane Internet Security Inc, DougWhiting-Hi/fn Inc, David Wagner-University of California Berkeley, Chris Hall-Princeton University), Rijndael (Dr. Vincent Rijmen-Katholieke Universiteit Leuven dan Dr. Joan Daemen-Proton World International), dan RC6.

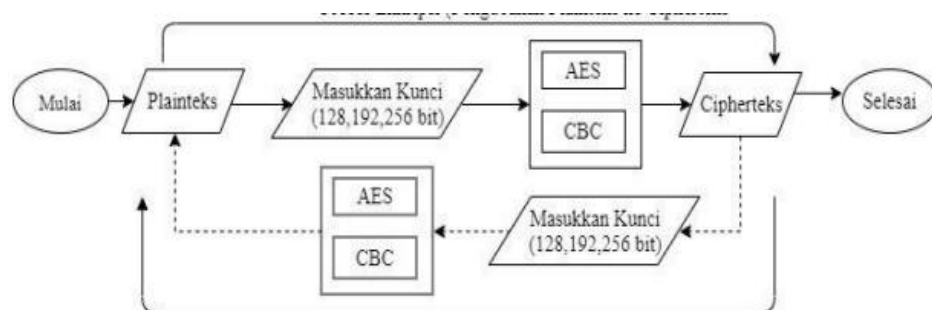
Menurut Pramana dan Nurnanengsi (2018:3) *Advanced Encryption Standard (AES)* merupakan algoritma *cryptographic* yang dapat digunakan untuk mengamankan data. Algoritma AES adalah blok *chiphertext* simetrik yang dapat mengenkripsi (*encipher*) dan dekripsi (*decipher*) informasi. Enkripsi merubah data yang tidak dapat lagi dibaca disebut *ciphertext*; sebaliknya dekripsi adalah merubah *ciphertext* data menjadi bentuk semula yang kita kenal sebagai *plaintext*. Algoritma AES menggunakan kunci kriptografi 128, 192, dan 256 bits untuk mengenkrip dan dekripsi data. Secara umum metode yang digunakan dalam pemrosesan terbagi dua, yaitu

1. Enkripsi Enkripsi adalah proses penyandian *plaintext* menjadi *ciphertext*, atau perubahan data menjadi bentuk rahasia. Proses enkripsi algoritma AES terdiri dari 4 jenis transformasi *bytes*, yaitu *SubBytes*, *ShiftRows*, *Mixcolumns*, dan *AddRoundKey*. Pada awal proses enkripsi, input yang telah dicopykan ke dalam state akan mengalami transformasi *byte AddRoundKey*. Setelah itu, state akan mengalami transformasi *SubBytes*, *ShiftRows*, *MixColumns*, dan *AddRoundKey* secara berulang-ulang sebanyak *Nr*. Proses ini dalam algoritma AES disebut sebagai *round function*. Round yang

terakhir agak berbeda dengan round-round sebelumnya dimana pada round terakhir, state tidak mengalami transformasi *MixColumns*. Dekripsi Dekripsi adalah proses memperoleh kembali *plaintext* menjadi *ciphertext*, atau proses perubahan kembali data yang berbentuk rahasia menjadi semula. *Transformasi byte* yang digunakan pada *invers cipher* adalah *InvShiftRows*, *InvSubBytes*, *InvMixColumns*, dan *AddRoundKe*.

Menurut Hasibuan (2020) Hitungan Manual Untuk Proses Enkripsi Dan Dekripsi Dokument Menggunakan *Advanced Encryption Standard (Aes)*. Berikut ini merupakan hasil dari analisis algoritma perhitungan metode AES, dimulai dari ekspansi kunci, enkripsi dan dekripsi.

memanfaatkan modifikasi AES menggunakan rantai proses yang dipengaruhi tiap proses enkripsi maupun dekripsi sebelumnya. Penggambaran alur kerja penelitian tertera pada Gambar dibawah:

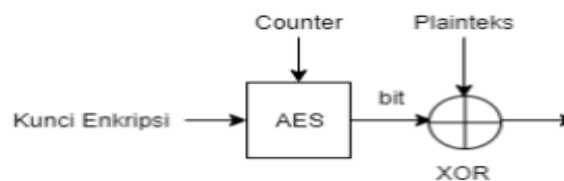


Gambar 1. Alur Kerja Enkripsi dan Dekripsi AES CBC

proses enkripsi dilakukan dengan memasukkan plaintext kemudian penggunaan kunci dengan penyesuaian bit. Proses pengamanan informasi menggunakan AES dan CBC kemudian jika sudah diproses akan muncul ciphertext. Sedangkan proses dekripsi maka akan mengembalikan pesan ciphertext ke dalam bentuk pesan informasi semula. AES merupakan pengganti dari kriptografi algoritma Data Encryption Standard (DES),

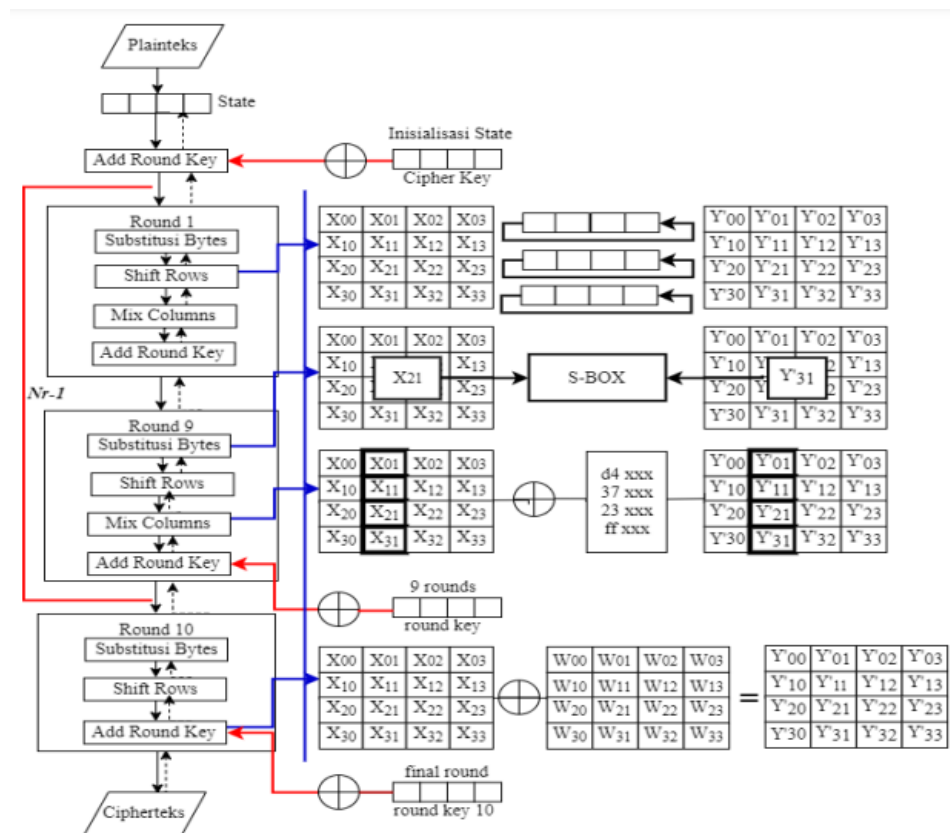
karena algoritma ini memakai blok 56 bit yang dianggap sudah tidak aman [22][28]. Algoritma AES termasuk pada algoritma kriptografi kunci simetri dengan single key yang menggunakan kunci yang sama ketika proses enkripsi dan dekripsi. Sehingga mampu meningkatkan pengoperasian sistem secara real time dan cukup cepat. Kini AES mendukung beberapa ukuran blok kunci dalam menentukan proses komputasi ketika enkripsi dan dekripsi, perbandingan tersedia pada Tabel

Bit Blok	Nb (Number of bit)	Nk (Number of key)		Nr (Number of rounds)
		Row	Column	
128	4	16	4	10
192	4	24	6	12
256	4	32	8	14



proses enkripsi pada AES menerima teks sehingga diproses pada algoritma menyesuaikan dengan bit yang digunakan, kemudian hasil tiap enkripsi pada plaintext melakukan XOR antar state sehingga di menghasilkan pesan baru tak bermakna. Secara umum proses algoritma AES tertera pada Gambar 3. Penggambaran algoritma AES pada Gambar 3. Sebagai berikut : 1) Add Round Key : initialization state dengan melakukan XOR, dengan mengoperasikan array dengan row 16 dan column 4, dimana hasil operasi ini menghasilkan cipher key. 2) Round 1 dan Round 9 : Putaran dengan perhitungan Number of Round (Nr)-1 kali, dimana tiap putaran tersebut memproses 4 tahapan pada AES, yaitu : a. Tahap Sub Bytes substitution dengan tabel (S-Box). b. Tahap Shift Rows

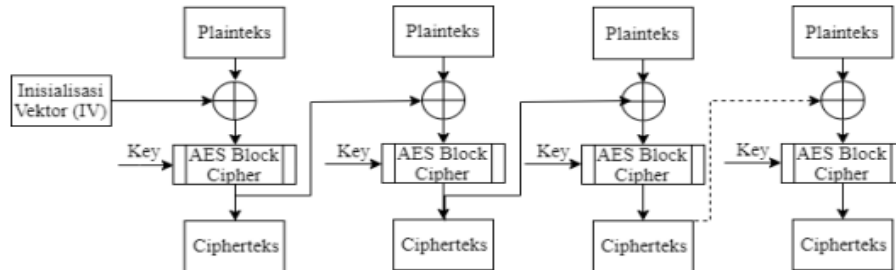
melakukan pergeseran pada baris array, menyesuaikan dengan nilai baris.
 c. Tahap Mix Columns melakukan perkalian dengan kolom tiap array state.
 d. Tahap Add Round Key akan melakukan XOR antara state yang paling terbaru sampai mencapai akhir. 3) Hingga pada tahap Final Round kembali ke proses Substitution Bytes, Shift Rows dan Add Round Key terakhir tanpa melakukan Mix Column hingga mencapai putaran ke -10.



Gambar 3. Algoritma Metode AES pada 128 bit

Modifikasi Advance Encryption Standard (AES) mode Cipher Block Cipher (CBC), Kriptografi AES mode CBC menjadi algoritma yang melibatkan nilai Inisialisasi Vektor (IV) pada blok cipher [30]. IV berdasarkan ukuran pada setiap blok masukan plaintext-nya. Pada rangkaian bit pada plaintext akan dibagi menjadi blok yang sama hingga memiliki

ukuran yang serupa. kemudian diadopsi dengan mode block chaining dalam menghasilkan ciphertext.



menjelaskan jika cara kerja dari modifikasi AES dengan CBC bekerja secara sekuensial, dimana blok data pertama mempengaruhi hasil blok yang kedua dan seterusnya. Awal pengoperasian peneliti memanfaatkan nilai pada data IV di blok dengan awal hasil AES Blok Cipher. Kinerja dari blok tersebut memanfaatkan AES dengan 128 bit yaitu dengan penggunaan kunci 16 karakter, 192 bit untuk kunci 24 karakter dan 256 bit menggunakan kunci 32 karakter. Fungsi matematis persamaan sebagai berikut: $C_0 = EK(P_0 \oplus IV)$ (1) $C_i = EK_i(P_i \oplus C_{i-1})$ (2) $C_{i+1} = EK_{i+1}(P_{i+1} \oplus C_i)$ (3) $C_n = EK_n(P_n \oplus C_{n-1})$ (4) Dimana, pengoperasian enkripsi pada fungsi persamaan (1)(2)(3)(4) nilai EK_x nilai x, y mewakili indek dari plaintext dari nilai 1 sampai n di nilai EK_x . Nilai pada IV di inisiasi sesuai bit blok yang digunakan. Sedangkan untuk fungsi matematis persamaan proses dekripsi AES CBC modifikasi sebagai berikut : $P_0 = DK(C_0 \oplus IV)$ (5) $P_i = DK_i(C_i \oplus C_{i-1})$ (6) $P_{i+1} = DK_{i+1}(C_{i+1} \oplus C_i)$ (7) $P_n = DK_n(C_n \oplus C_{n-1})$ (8) Pengoperasian pengembalian ciphertext ke plaintext atau proses dekripsi pada rumus persamaan (5)(6)(7)(8) nilai DK_x nilai x, y mewakili indek dari enkripsi dari nilai 1 sampai n di nilai DK_x .

1. Enkripsi

Pada tahapan ini *plaintext* yang akan di enkripsikan “PUSKOPKARTIK BB”. Proses enkripsi dari plantetks sebagai berikut:

Plantetks : PUSKOPKARTIK BB

Dikonverensi kedalam bilangan heksadisimal :

50 55 53 4B 4F 50 4B 41 52 54 49 4B 41 20 42 42

Urutkan baris kolom menjadi 4 *state*

$$\begin{array}{|c|c|c|c|} \hline 50 & 4F & 52 & 41 \\ \hline 55 & 50 & 54 & 20 \\ \hline 53 & 4B & 49 & 42 \\ \hline 4B & 41 & 4B & 42 \\ \hline \end{array} \oplus \begin{array}{|c|c|c|c|} \hline 44 & 53 & 41 & 4E \\ \hline 41 & 49 & 4E & 4A \\ \hline 54 & 4D & 50 & 41 \\ \hline 41 & 50 & 49 & 4D \\ \hline \end{array} = \begin{array}{|c|c|c|c|} \hline 14 & 1C & 13 & 0F \\ \hline 14 & 19 & 1A & 6A \\ \hline 07 & 06 & 19 & 03 \\ \hline 0A & 11 & 02 & 0F \\ \hline \end{array}$$

Hasil dari *AddRoundKey* diatas akan menjadi masukan untuk ronde ke-1 yang akan diproses dengan 4 transformasi, yaitu *SubByte*, *MixColumns*, dan *AddRoundkey*.

Pada transformasi *SubByte*, setiap *byte* akan ditukar dengan tabel *S-Box*.

		y															
		0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
x	0	63	7c	77	7b	f2	6b	6f	c5	30	01	57	2b	fe	d7	ab	76
	1	ca	82	e9	7d	fa	59	47	f0	ad	d4	12	af	9c	a4	72	e0
	2	b7	fd	93	26	36	3f	f7	cc	34	a5	55	f1	71	d8	31	15
	3	04	c7	23	c3	18	96	05	9a	07	72	70	e2	eb	27	b2	75
	4	89	83	2c	1a	1b	68	3a	a0	52	75	d6	b3	29	e3	2f	84
	5	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
	6	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
	7	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
	8	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
	9	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
	a	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
	b	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
	c	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
	d	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
	e	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
	f	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

14	1C	13	0F
14	19	1A	6A
07	06	19	03
0A	11	02	0F

 $\xrightarrow{\text{SubBytes}}$

FA	9C	7D	76
FA	D4	A2	02
C5	6F	D4	7B
67	82	77	76

Dilanjutkan dengan melakukan proses *ShiftRows*, yaitu menggeser setiap baris pada *state*.

FA	9C	7D	76
FA	D4	A2	02
C5	6F	D4	7B
67	82	77	76

 $=$

FA	9C	7D	76
D4	A2	02	FA
D4	7B	C5	6F
76	67	82	77

Proses selanjutnya *MixColumns*. Pada proses ini, dilakukan proses perkalian antara suatu polinomial tetap dengan *state* hasil *ShiftRows*.

$$\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \times \begin{bmatrix} FA & 9C & 7D & 76 \\ D4 & A2 & 02 & FA \\ D4 & 7B & C5 & 6F \\ 76 & 67 & 82 & 77 \end{bmatrix} = \begin{bmatrix} 2A & C2 & BB & E1 \\ 58 & 29 & AF & 5F \\ FA & 61 & 73 & CB \\ F9 & A8 & 5F & E1 \end{bmatrix}$$

Pada proses perhitungan untuk mencari baris pertama menggunakan operator polinomial GF (2^8) dimana jika dikali 01 maka hasilnya tetap, jika dikali 02 maka dileftshit 1 dan jika hasil leftshift 3 byte di Xor dengan 11B dan jika dikali 03 maka dilakukan operasi dikali 02 dan Xor dengan bilangan itu sendiri, *Byte* baris 1 kolom 1 (S^0_0)

$$02 \times FA = (10) \times (111110101) \quad 03 \times DA = (11) \times (11010100)$$

$$= 11110100$$

$$= F4$$

$$01 \times D4 = (1) \times (11010100)$$

$$= 11010100$$

$$= D4$$

$$= 01111100$$

$$= 7C$$

$$01 \times 76 = (1) \times (01110110)$$

$$= 01110110$$

$$= 76$$

Untuk mendapatkan S^{-1} , semua hasil dari proses perkalian diatas di *Xor* kan. $S^{-1} = F4 \oplus 7C \oplus D4 \oplus 76 = 2A$

Setelah hasil dari proses *MixColumns* diperoleh, langkah terakhir dari ronde ke-1 yaitu *AddRoundKey* ini sama dengan sebelumnya, namun *state* hasil dari proses *MixColumns* di-*Xor*-kan dengan kunci ronde ke-1.

2A	C2	BB	E1
58	29	AF	5F
07	61	73	CB
F9	A8	5F	E1

93	CO	81	CF
C2	8B	C5	BF
B7	FA	AA	EB
6E	3E	77	3A

B9	02	3A	2E
9A	A2	6A	E0
B0	9B	D9	20
97	96	28	DB

Hasil proses enkripsi dari ronde ke-1 akan menjadi masukan untuk ronde ke-10. Hasil dari transformasi proses enkripsi untuk ronde ke-2 sampai ke-10.

Round 2

<i>Text</i>	<i>SubBytes</i>	<i>ShiftRows</i>	<i>MixColumns</i>	<i>RoundKey 2</i>	<i>AddRoundKey</i>
[B9 02 3A 2E]	[56 77 80 31]	[56 77 80 31]	[6E D7 FC 91]	[E2 22 A3 6C]	[8C F5 5F FD]
[9A A2 6A E0]	[B8 3A 02 70]	[3A 02 70 B8]	[C4 39 C2 52]	[2B A0 65 EA]	[EF 99 A7 B8]
[B0 9B D9 20]	[E7 14 35 B7]	[35 B7 E7 14]	[D6 83 8E FD]	[37 CD 67 8C]	[E1 4E E9 71]
[97 96 28 DB]	[88 90 34 B9]	[B9 88 90 34]	[9C 27 37 97]	[E4 DA AD 97]	[78 FD 9A 00]

Round 3

<i>Text</i>	<i>SubBytes</i>	<i>ShiftRows</i>	<i>MixColumns</i>	<i>RoundKey 3</i>	<i>AddRoundKey</i>
[8C F5 5F FD]	[64 E6 CF 54]	[64 E6 CF 54]	[9C 2C 9D 45]	[61 43 E0 8C]	[FD 2C 7D C9]
[EF 99 A7 B8]	[DF EE 5C 6C]	[EE 5C 6C DF]	[E2 1C 50 38]	[4F EF 8A 60]	[AD F3 DA 58]
[E1 4E E9 71]	[F8 2F 1E A3]	[1E A3 F8 2F]	[13 38 B4 06]	[BF 72 15 99]	[AC 4A A1 9F]
[78 FD 9A 00]	[BC 54 B8 63]	[63 BC 54 B8]	[9A AD 76 67]	[B4 6E C3 54]	[2E C3 B5 33]

Round 4

<i>Text</i>	<i>SubBytes</i>	<i>ShiftRows</i>	<i>MixColumns</i>	<i>RoundKey 4</i>	<i>AddRoundKey</i>
[FD 2C 7D C9]	[54 A8 FF DD]	[54 A8 FF DD]	[4E 58 E4 06]	[B9 FA 1A 96]	[F7 A2 FE 90]
[AD F3 DA 58]	[95 0D 57 6A]	[0D 57 6A 95]	[DB 41 AD 58]	[A1 4E C4 A4]	[7A 0F 69 FC]
[AC 4A A1 9F]	[91 D6 32 D8]	[32 D8 91 D6]	[63 01 DE 9B]	[9F ED F8 61]	[FC EC 26 FA]
[2E C3 B5 33]	[31 2E D5 C3]	[C3 31 2E D5]	[5E 0D BD 8E]	[D0 BE 7D 29]	[8E B3 C0 A7]

Round 5

Text	SubBytes	ShiftRows	MixColumns	RoundKey 5	AddRoundKey
[F7 A2 FE 90]	[68 3A BB 60]	[68 3A BB 60]	[E1 50 7B C1]	[E0 1A 00 96]	[01 4A 7B 57]
[7A 0F 69 FC]	[DA 76 F9 B0]	[76 F9 B0 DA]	[DA BD 66 3C]	[4E 00 C4 60]	[94 BD A2 5C]
[FC EC 26 FA]	[B0 CE F7 2D]	[F7 2D B0 CE]	[0F B2 C7 E8]	[3A D7 2F 4E]	[35 65 E8 A6]
[8E B3 C0 A7]	[19 6D BA 5C]	[5C 19 6D BA]	[81 A8 0C DB]	[40 FE 83 AA]	[C1 56 8F 71]

Round 6

Text	SubBytes	ShiftRows	MixColumns	RoundKey 6	AddRoundKey
[01 4A 7B 57]	[7C D6 21 5B]	[7C D6 21 5B]	[4E A5 BB EE]	[10 0A 0A 9C]	[5E A1 B1 72]
[94 BD A2 5C]	[22 7A 3A 4A]	[7A 3A 4A 22]	[9D B6 A5 BB]	[61 61 A5 C5]	[FC D7 00 7E]
[35 65 E8 A6]	[96 4D 9B 24]	[9B 24 96 4D]	[D5 2C 94 76]	[96 41 6E 20]	[43 6D FA 56]
[C1 56 8F 71]	[78 B1 73 A3]	[A3 78 B1 73]	[38 8F C6 64]	[D0 2E AD 07]	[E8 A1 6B 63]

Round 7

Text	SubBytes	ShiftRows	MixColumns	RoundKey 7	AddRoundKey
[5E A1 B1 72]	[58 79 C8 40]	[58 79 C8 40]	[74 7D AD 08]	[F6 FC F6 6A]	[82 81 5B 62]
[FC D7 00 7E]	[B0 0E 63 F3]	[0E 63 F3 B0]	[C8 EC 29 00]	[D6 B7 12 D7]	[1E 5B 3B D7]
[43 6D FA 56]	[1A 3C 2D B1]	[2D B1 1A 3C]	[1A D5 59 09]	[53 12 7C 5C]	[49 C7 25 55]
[E8 A1 6B 63]	[9B 32 7F FB]	[FB 9B 32 7F]	[26 74 C3 B2]	[0E 20 8D 8A]	[28 54 4E 38]

Round 8

Text	SubBytes	ShiftRows	MixColumns	RoundKey 8	AddRoundKey
[82 81 5B 62]	[13 0C 39 AA]	[13 0C 39 AA]	[55 ED 7B 05]	[78 84 72 18]	[2D 69 09 1D]
[1E 5B 3B D7]	[72 39 E2 0E]	[39 E2 0E 72]	[27 F8 48 05]	[9C 2B 39 EE]	[BB D3 71 EB]
[49 C7 25 55]	[3B C6 3F FC]	[3F FC 3B C6]	[5D 51 21 61]	[2D 3F 43 1F]	[70 6E 62 7E]
[28 54 4E 38]	[34 20 1A 07]	[07 34 20 1A]	[3D 62 3E 65]	[0C 2C A1 2B]	[31 5C 9F 4E]

Round 9

Text	SubBytes	ShiftRows	MixColumns	RoundKey 9	AddRoundKey
[2D 69 09 1D]	[D8 F9 01 A4]	[D8 F9 01 A4]	[84 23 5C 32]	[4B CF BD A5]	[CF EC E1 97]
[BB D3 71 EB]	[EA 66 A3 E9]	[66 A3 E9 EA]	[DE 6D 14 0A]	[5C 77 4E A0]	[82 1A 5A 00]
[70 6E 62 7E]	[51 9F AA F3]	[AA F3 51 9F]	[80 F5 3B 1D]	[DC E3 A0 BF]	[5C 16 9B A2]
[31 5C 9F 4E]	[C7 2F DB 2F]	[2F C7 2F DB]	[E1 D5 E5 2F]	[A1 8D 2C 07]	[40 58 C9 28]

Round 10

Text	SubBytes	ShiftRows	RoundKey 10	AddRoundKey	CipherText
[CF EC E1 97]	[8A CE F8 88]	[8A CE F8 88]	[97 58 E5 40]	[1D 96 1D C8]	[1D 96 1D C8]
[82 1A 5A 00]	[13 A2 BE 63]	[A2 BE 63 13]	[54 23 6D CD]	[F6 9D C1 DE]	[F6 9D C1 DE]
[5C 16 9B A2]	[4A 47 14 3A]	[14 3A 4A 47]	[19 FA 5A E5]	[0D C0 10 A2]	[0D C0 10 A2]
[40 58 C9 28]	[09 6A DD 34]	[34 09 6A DD]	[A7 2A 06 01]	[93 23 6C DC]	[93 23 6C DC]

Hasil dari proses *AddRoundKey* pada ronde ke-10 merupakan hasil akhir proses enkripsi

Hasil :

ivmYctL19mp55ItmCV6uzTVDP0oPLe8jolvIbeap7xUJwuiLHt
 J8EJQgItTIP64/PF1sJGYWlw17dZg4KaeAzVBMVIC/YPcFBlc
 HEOerGyBT0j15K0f7M9pJuzGN6jErI3LibkhL5mIdG1PWzoLtd
 FtixIBYS2HmXfstfKEPiK9NMbIZT/D1sM/xqbeS3SheCTPmq
 W3IbD3q8OwI8HlzbksDjMbEJ3lcpdkJ6S/8IWOkTLHDD/1Bza
 KXQwJX+WpFT+PfhQcvbCjdK4eBgEOqTX/

2. Dekripsi

Proses transformasi pada dekripsi dalam metode *Advanced Encryption Standard (AES)* yaitu *InvSubByte*, *InvShiftRows*, *InvMixColimns*, dan *AddRoundKey*. *AddRoundKey* merupakan transformasi yng bersifat *selfinvers*. Kunci yang digunakan sama dengan yang digunakan pada proses enkripsi.

Round 1

Lakukan proses *AddRoundKey* antara *ciphertext* yang telah diperoleh dari proses enkripsi dengan *roundKey* ke-10

1D	96	1D	C8	97	58	E5	40	8A	CE	F8	88
F6	9D	C1	DE	54	23	6D	CD	A2	BE	63	13
0D	C0	10	A2	19	FA	5A	E5	14	3A	4A	47
93	23	6C	DC	A7	2A	06	01	34	09	6A	DD

Pada proses ke-1 dalam proses dekripsi, tidak dilakukan *InvMixColimns*. Maka proses selanjutnya adalah melakukan transformasi *InvShiftRows*.

8A	CE	F8	88	8A	CE	F8	88
A2	BE	63	13	13	A2	BE	63
14	3A	4A	47	4A	47	14	3A
34	09	6A	DD	09	6A	DD	34

Setelah proses *InvShiftRows* selesai, selanjutnya adalah melakukan proses transformasi *SubByte*

8A	CE	F8	88	CF	EC	E1	97
13	A2	BE	63	82	1A	5A	00
4A	47	14	3A	5C	16	9B	A2
09	6A	DD	34	40	58	C9	28

Setelah proses *InvSubByte* kemudin melakukan operasi *Xor* antara hasil *InvSubByte* dengan Round ke 9 untuk melakukan transformasi ke-2

CF	EC	E1	97	⊕	4B	CF	BD	A5	=	84	23	5C	32
82	1A	5A	00		5C	77	4E	A0		DE	6D	14	0A
5C	16	9B	A2		DC	E3	A0	BF		80	F5	3B	1D
40	58	C9	28		A1	8D	2C	07		E1	D5	E5	2F

Hasil InvSubByte
Round Key 9
Hasil AddRound Key

Kemudian hasil *AddRoundKey* tersebut akan melakukan proses transformasi *InvMixColumns* dengan aturan *irreducible polynomial*.

84	23	5C	32	⊕	0E	0B	0D	09	=	6F	F9	01	A4
DE	6D	14	0A		09	0E	0B	0D		66	A3	E9	EA
80	F5	3B	1D		0D	09	0E	0B		AA	F5	51	9F
E1	D5	E5	2F		0B	0D	09	0E		2F	C7	2F	DB

Hasil AddRound Key
Nilai Matriks InvMixColumns
Hasil Matriks InvMixColumns

Berikut uraian perhitungan perhitungan transformasi *InvMixColumns* yang sesuai dengan perhitungan diatas.

$$\begin{aligned}
 S_{0,0} &= (S_{0,0} * 0E) \oplus (S_{1,0} * 0B) \oplus (S_{2,0} * 0D) \oplus (S_{3,0} * 09) \\
 &= 84 * 0E \oplus DE * 0B \oplus 80 * 0D \oplus E1 * 09 \\
 &= 79 \oplus D3 \oplus 6D \oplus A8 \\
 &= 6F
 \end{aligned}$$

Proses uraian perhitungan di atas dapat dirincikan dengan mengubah bilangan heksadesimal ke bilangan biner, kemudian di aplikasikan dengan *irreducible polynomial* sebagai berikut :

- a. Representasi dari $S_{0,0}$ yaitu 84 (10000100) dalam *polynomial* ($x^7 x^2$) dan bilangan 0E (00001110) dalam *polynomial* ($x^3 + x^2 + x$).

$$S_{0,0} = 84 * 0E$$

$$\begin{aligned}
&= (10000100) * (00001110) \\
&= (x^7 + x^2) * (x^3 + x^2 + x) \\
&= (x^{10} + x^9 + x^8 + x^5 + x^4 + x^3) \\
&= ((x^2 \cdot x^8) + x^9 + x^8 + x^5 + x^4 + x^3) \\
&= ((x^2 (x^4 + x^3 + x + 1)) + x^9 + x^8 + x^5 + x^4 + x^3) \\
&\equiv ((x^6 + x^5 + x^3 + x^2)) x^9 + x^8 + x^5 + x^4 + x^3) \\
&= (x^9 + x^8 + x^6 + x^4 + x^2) \\
&= ((x (x^4 + x^3 + x + 1)) + x^8 + x^6 + x^4 + x^2) \\
&\equiv ((x^5 + x^4 + x^2 + x) + x^8 + x^6 + x^4 + x^2) \\
&= (x^8 + x^6 + x^5 + x) \\
&= ((1 (x^4 + x^3 + x + 1)) + x^6 + x^5 + x) \\
&= ((x^4 + x^3 + x + 1) + x^6 + x^5 + x) \\
&= x^6 + x^5 + x^4 + x^3 + 1 \\
&= 01111001 \\
&= 79
\end{aligned}$$

Untuk proses *round* selanjutnya hanya akan ditampilkan hasil dari masing-masing transformasi yang dapat dilihat dibawah ini.

Round 2

Text	Round Key 9	AddRoundKey	InvMixColumns	InvShiftRows	InvSubBytes
[CF EC E1 97]	[4B CF BD A5]	[84 23 5C 32]	[D8 F9 01 A4]	[D8 F9 01 A4]	[2D 69 09 1D]
[82 1A 5A 00]	[5C 77 4E A0]	[DE 6D 14 0A]	[66 A3 E9 EA]	[EA 66 A3 E9]	[BB D3 71 EB]
[5C 16 9B A2]	[DC E3 A0 BF]	[80 F5 3B 1D]	[AA F3 51 9F]	[51 9F AA F3]	[70 6E 62 7E]
[40 58 C9 28]	[A1 8D 2C 07]	[E1 D5 E5 2F]	[2F C7 2F DB]	[C7 2F DB 2F]	[31 5C 9F 4E]

Round 3

Text	Round Key 8	AddRoundKey	InvMixColumns	InvShiftRows	InvSubBytes
[2D 69 09 1D]	[78 84 72 18]	[55 ED 7B 05]	[13 0C 39 AA]	[13 0C 39 AA]	[82 81 5B 62]
[BB D3 71 EB]	[9C 2B 39 EE]	[27 F8 48 05]	[39 E2 0E 72]	[72 39 E2 0E]	[1E 5B 3B D7]
[70 6E 62 7E]	[2D 3F 43 1F]	[5D 51 21 61]	[3F FC 3B C6]	[3B C6 3F FC]	[49 C7 25 55]
[31 5C 9F 4E]	[0C 2C A1 2B]	[3D 62 3E 65]	[07 34 20 1A]	[34 20 1A 07]	[28 54 4E 38]

Round 4

<i>Text</i>	<i>Round Key 7</i>	<i>AddRoundKey</i>	<i>InvMixColumns</i>	<i>InvShiftRows</i>	<i>InvSubBytes</i>
[82 81 5B 62]	[F6 FC F6 6A]	[74 7D AD 08]	[58 79 C8 40]	[58 79 C8 40]	[5E A1 B1 72]
[1E 5B 3B D7]	[D6 B7 12 D7]	[C8 EC 29 00]	[0E 63 F3 B0]	[B0 0E 63 F3]	[FC D7 00 7E]
[49 C7 25 55]	[53 12 7C 5C]	[1A D5 59 09]	[2D B1 1A 3C]	[1A 3C 2D B1]	[43 6D FA 56]
[28 54 4E 38]	[0E 20 8D 8A]	[26 74 C3 B2]	[FB 9B 32 7F]	[9B 32 7F FB]	[E8 A1 6B 63]

Round 5

<i>Text</i>	<i>Round Key 6</i>	<i>AddRoundKey</i>	<i>InvMixColumns</i>	<i>InvShiftRows</i>	<i>InvSubBytes</i>
[5E A1 B1 72]	[10 0A 0A 9C]	[4E A5 BB EE]	[7C D6 21 5B]	[7C D6 21 5B]	[01 4A 7B 57]
[FC D7 00 7E]	[61 61 A5 C5]	[9D B6 A5 BB]	[7A 3A 4A 22]	[22 7A 3A 4A]	[94 BD A2 5C]
[43 6D FA 56]	[96 41 6E 20]	[D5 2C 94 76]	[9B 24 96 4D]	[96 4D 9B 24]	[35 65 E8 A6]
[E8 A1 6B 63]	[D0 2E AD 07]	[38 8F C6 64]	[A3 78 B1 73]	[78 B1 73 A3]	[C1 56 8F 71]

Round 6

<i>Text</i>	<i>Round Key 5</i>	<i>AddRoundKey</i>	<i>InvMixColumns</i>	<i>InvShiftRows</i>	<i>InvSubBytes</i>
[01 4A 7B 57]	[E0 1A 00 96]	[E1 50 7B C1]	[68 3A BB 60]	[68 3A BB 60]	[F7 A2 FE 90]
[94 BD A2 5C]	[4E 00 C4 60]	[DA BD 66 3C]	[76 F9 B0 DA]	[DA 76 F9 B0]	[7A 0F 69 FC]
[35 65 E8 A6]	[3A D7 2F 4E]	[0F B2 C7 E8]	[F7 2D B0 CE]	[B0 CE F7 2D]	[FC EC 26 FA]
[C1 56 8F 71]	[40 FE 83 AA]	[81 A8 0C DB]	[5C 19 6D BA]	[19 6D BA 5C]	[8E B3 C0 A7]

Round 7

<i>Text</i>	<i>Round Key 4</i>	<i>AddRoundKey</i>	<i>InvMixColumns</i>	<i>InvShiftRows</i>	<i>InvSubBytes</i>
[F7 A2 FE 90]	[B9 FA 1A 96]	[4E 58 E4 06]	[54 A8 FF DD]	[54 A8 FF DD]	[FD 2C 7D C9]
[7A 0F 69 FC]	[A1 4E C4 A4]	[DB 41 AD 58]	[0D 57 6A 95]	[95 0D 57 6A]	[AD F3 DA 58]
[FC EC 26 FA]	[9F ED F8 61]	[63 01 DE 9B]	[32 D8 91 D6]	[91 D6 32 D8]	[AC 4A A1 9F]
[8E B3 C0 A7]	[D0 BE 7D 29]	[5E 0D BD 8E]	[C3 31 2E D5]	[31 2E D5 C3]	[2E C3 B5 33]

Round 8

<i>Text</i>	<i>Round Key 3</i>	<i>AddRoundKey</i>	<i>InvMixColumns</i>	<i>InvShiftRows</i>	<i>InvSubBytes</i>
[FD 2C 7D C9]	[61 43 E0 8C]	[9C 2C 9D 45]	[64 E6 CF 54]	[64 E6 CF 54]	[8C F5 5F FD]
[AD F3 DA 58]	[4F EF 8A 60]	[E2 1C 50 38]	[EE 5C 6C DF]	[DF EE 5C 6C]	[EF 99 A7 B8]
[AC 4A A1 9F]	[BF 72 15 99]	[13 38 B4 06]	[1E A3 F8 2F]	[F8 2F 1E A3]	[E1 4E E9 71]
[2E C3 B5 33]	[B4 6E C3 54]	[9A AD 76 67]	[63 BC 54 B8]	[BC 54 B8 63]	[78 FD 9A 00]

Round 9

Text	Round Key 2	AddRoundKey	InvMixColumns	InvShiftRows	InvSubBytes
[8C F5 5F FD]	[E2 22 A3 6C]	[6E D7 FC 91]	[56 77 80 31]	[56 77 80 31]	[B9 02 3A 2E]
[EF 99 A7 B8]	[2B A0 65 EA]	[C4 39 C2 52]	[3A 02 70 B8]	[B8 3A 02 70]	[9A A2 6A E0]
[E1 4E E9 71]	[37 CD 67 8C]	[D6 83 8E FD]	[35 B7 E7 14]	[E7 14 35 B7]	[B0 9B D9 20]
[78 FD 9A 00]	[E4 DA AD 97]	[9C 27 37 97]	[B9 88 90 34]	[88 90 34 B9]	[97 96 28 DB]

Round 10

Text	Round Key 1	AddRoundKey	InvMixColumns	InvShiftRows	InvSubBytes
[B9 02 3A 2E]	[93 C0 81 CF]	[2A C2 BB E1]	[FA 9C 7D 76]	[FA 9C 7D 76]	[14 1C 13 0F]
[9A A2 6A E0]	[C2 8B C5 BF]	[58 29 AF 5F]	[D4 A2 02 FA]	[FA D4 A2 02]	[14 19 1A 6A]
[B0 9B D9 20]	[B7 FA AA EB]	[07 61 73 CB]	[D4 7B C5 6F]	[C5 6F D4 7B]	[07 06 19 03]
[97 96 28 DB]	[6E 3E 77 3A]	[F9 A8 5F E1]	[76 67 82 77]	[67 82 77 76]	[0A 11 02 0F]

Setelah proses ronde ke-10 selesai, hasil dari *InvSubBytes* ronde ke-10 di-*XOR*-kan dengan *cipherkey* atau kunci ronde ke-0.

14	1C	13	0F	44	53	41	4E	50	4F	52	41
14	19	1A	6A	41	49	4E	4A	55	50	54	20
07	06	19	05	54	4D	50	41	53	4B	49	42
0A	11	02	0F	41	50	49	4D	4B	41	4B	42

Langkah selanjutnya adalah mengubah hasil dari *InvSubBytes* ronde ke-10 di-*XOR*-kan dengan *cipherkey* ke dalam bentuk bilangan desimal kemudian diubah lagi ke dalam bentuk text berdasarkan kode ASCII.

Dalam bilangan heksadesimal :

50 55 53 4B 4F 50 4B 41 52 54 49 4B 41 20 42 42

Plainteks :

PUSKOPKARTIKA BB

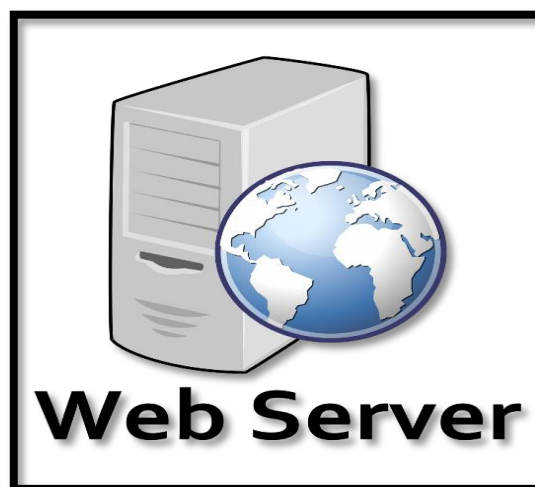
2.5. Web Server

Menurut Roihan (2018:91), Web Server adalah layanan server yang berfungsi menerima permintaan HTTP atau HTTPS dari klien dengan menggunakan web browser dan mengirimkan kembali hasilnya dalam

bentuk halaman-halaman web yang umumnya berbentuk dokumen HTML dan format dokumen web lainnya.

Menurut Kosasih (2015:14), *Web Server* merupakan sebuah perangkat lunak dalam *server* yang berfungsi menerima permintaan berupa halaman *web* melalui HTTP atau HTTPS dari klien yang dikenal dengan *browser web* dan mengirimkan kembali hasilnya dalam bentuk halaman-halaman *web* yang umumnya berbentuk dokumen HTML.

Berdasarkan pengertian diatas dapat disimpulkan bahwa Web Server adalah sebuah *Software* (perangkat lunak) yang memberikan layanan berupa data. Berfungsi untuk menerima permintaan HTTP atau HTTPS dari klien atau kita kenal dengan web browser (*Chrom, Firefox*).



Gambar 2.2 Web Server.

Web Server berfungsi menerima permintaan HTTP atau HTTPS dari klien atau kita kenal dengan web browser (*Chrom, Firefox*). Ia juga akan mengirimkan respon atas permintaan kepada *client* dalam bentuk halaman web yang umumnya HTML. Web Server berfungsi menerima permintaan HTTP atau HTTPS dari klien atau kita kenal dengan web browser

(*Chrom, Firefox*). Ia juga akan mengirimkan respon atas permintaan kepada *client* dalam bentuk halaman web yang umumnya HTML. Jenis-jenis dari web server adalah sebagai berikut

1. Web Server Apache

Web server yang populer dan paling banyak digunakan kebanyakan orang, yaitu jenis Apache. Pada awalnya Apache didesain guna mendukung penuh sistem operasi UNIX. Selain cukup mudah dalam implementasinya, Apache juga memiliki beberapa program pendukung sehingga memberikan layanan yang lengkap, seperti PHP, SSI dan control akses. Berikut detailnya:

a. PHP (*Personal Home Page* atau *PHP Hypertext Processor*)

Program semacam CGI, berfungsi memproses teks yang bekerja di server. Apache sangat mendukung PHP dengan menempatkannya sebagai salah satu modulnya (*mod php*). Hal tersebut membuat PHP bekerja lebih baik.

b. SSI (*Server Side Include*)

Perintah yang bisa disertakan dalam bekas HTML. Kemudian ia dapat diproses oleh web server ketika pengguna mengaksesnya.

c. Access Control

Kontrol Akses dapat dijalankan berdasarkan nama *host* atau nomor IP CGI (*Common Gateway Interface*). Lalu yang paling umum untuk digunakan adalah perl (*Practical Extraction and Report Language*), disupport oleh Apache dengan menempatkannya sebagai modul (*mod perl*).

Apache sangat aman dan nyaman untuk digunakan karena memiliki beberapa keuntungan seperti proses instalasi yang mudah, freeware, dan sistem konfigurasi yang masih tergolong mudah. Selain itu ia juga mampu bekerja pada sistem operasi *open* atau *closed source*.

2. Web Server Nginx

Salah satu pesaing unggul Apache yaitu Nginx. Nginx dikenal mampu melayani segala macam permintaan, seperti request pada dengan tingkat kepadatan lalu lintas atau traffic yang sangat padat. Nginx memang lebih unggul dari segi kualitas, kecepatan dan dalam hal performannya. Nginx memiliki banyak kelebihan dalam hal fitur, diantaranya *URL rewriting*, *virtual host*, *file serving*, *reverse proxying*, *access control*, dan masih banyak lagi.

3. Web Server IIS

Web Server IIS (*Internet Information Services*) adalah web server yang bekerja pada jenis protokol seperti DNS, TCP/IP, atau beragam *software* lainnya yang berguna untuk merangkai sebuah situs.

4. Web Server Lighttpd

Programmer asal Jerman telah menciptakan web server berbasis *open source* guna mendukung sistem *Linux* dan *Unix*. Bila dilihat dari segi keunggulan, web server yang satu ini memiliki beberapa keunggulan berdasarkan fitur tambahan yang tersedia. Seperti *FastCGI*, *Output-Compression*, *FastCGI*, dan *URL writing*. Jika kamu menggunakan web server Lighttpd, kamu akan merasakan performa yang lebih cepat dan efektif.

2.6. Keamanan

Menurut Noviansyah dan Salya (2021:38) Keamanan jaringan adalah salah satu aspek penting dalam dunia internet suatu jaringan internet perusahaan membutuhkan keamanan khusus yang dapat menjaga data dimana berfungsi sebagai keamanan jaringan.

Menurut Wijaya dan Pratama (2020:97) keamanan jaringan komputer sebagai bagian dari sebuah system informasi adalah sangat penting untuk menjaga validitasi dan integritas data serta menjamin ketersediaan layanan bagi penggunanya. Sistem harus dilindungi dari segala macam serangan dan usaha-usaha penyusupan oleh pihak yang tidak berhak.

Sedangkan keamanan sendiri adalah sistem dari semua itu yang berarti sesuatu yang membuat kita menjadi aman. Biasanya istilah ini biasa digunakan dengan hubungan dengan kejahatan dan segala bentuk kecelakaan. Keamanan sendiri adalah suatu yang sangat penting karena ini sangat menjaga kestabilan contohnya keamanan nasional yang mencegah dari kriminalitas tingkat tinggi seperti terorisme, cracker atau hacker dan keamanan terhadap ekonomi nasional. Tujuan utama dengan adanya keamanan adalah untuk membatasi akses informasi dan sumber hanya untuk pemakai yang memiliki hak akses.

2.7. Aplikasi

Menurut Widarma Dan Rahayu (2017:2) Aplikasi adalah program siap pakai yang dapat digunakan untuk menjalankan perintah-perintah dari pengguna aplikasi tersebut dengan tujuan mendapat hasil yang lebih akurat

sesuai dengan tujuan pembuatan aplikasi tersebut, aplikasi mempunyai arti yaitu pemecahan masalah yang menggunakan salah satu teknik pemrosesan data aplikasi yang biasanya berpacu pada sebuah komputasi yang diinginkan atau diharapkan. Pengertian aplikasi secara umum adalah alat terapan yang difungsikan secara khusus dan terpadu sesuai kemampuan yang dimilikinya, aplikasi merupakan suatu perangkat komputer yang siap pakai bagi *user*.

Regita (2022:3) aplikasi adalah koleksi *windows* dan objek-objek yang menyediakan fungsi untuk aktifitas *user*, seperti pemasukan data, proses dan pelaporan. Aplikasi bisa berisi. Seperti antar lain: menu, window dan control, dimana user berinteraksi langsung dengan aplikasi. Proses logika aplikasi: kejadian dan fungsi skrip yang dibuat sebagai logika aplikasi, validasi dan proses lainnya.

2.8. Hypertext Preprocessor (Php)

Menurut Halawa, dkk, (2022:3) Php adalah bahasa pemrograman yang digunakan untuk membuat sebuah website yang dinamis dan statis. Website dinamis adalah website yang kontennya dapat berubah. Contohnya seperti toko online. Website statis adalah website yang kontennya tidak dapat berubah-ubah. Contohnya *Company Profile*. Bahasa pemrograman php mudah digunakan dan dipelajari, memiliki banyak framework, serta memiliki komunitas yang besar. PHP merupakan kepanjangan dari *PHP Hypertext Preprocessor* yang merupakan suatu bahasa pemrograman yang berjalan pada sisi server (*server side scripting*), jadi dapat disimpulkan PHP membutuhkan web server untuk dapat menjalankannya. PHP menyatu dengan kode HTML.

Menurut Agustiansyah dan Solikin (2021:2) PHP adalah bahasa server-side scripting yang menyatu dengan HTML untuk membuat halaman web yang dinamis. Maksud dari server-side scripting adalah sintaks dan perintah-perintah yang diberikan akan sepenuhnya akan dijalankan di server tetapi disertakan pada dokumen HTML. Pembuatan web ini merupakan kombinasi antara php sendiri sebagai bahasa pemrograman dan HTML sebagai pembangun halaman web, PHP sebenarnya juga dapat digunakan untuk membuat aplikasi command line dan GUI. Cara kerja PHP adalah dengan menyelipkannya di antara kode HTML (Hyper text Markup Language). PHP singkatan dari Personal Hypertext Preprocessor yang digunakan sebagai bahasa script server-side dalam pengembangan Web yang disisipkan pada dokumen HTML. Pengembangan PHP memungkinkan Web dapat dibuat dinamis sehingga maintenance situs Web tersebut menjadi lebih mudah dan efisien.

2.9. Basis Data (*MySQL*)

Menurut Lubis (2016:5) Basis data merupakan gabungan File data yang dibentuk dengan hubungan/relasi yang logis dan dapat diungkapkan dengan catatan serta bersifat independen. Adapun basis data adalah tempat berkumpulnya data yang saling berhubungan dalam suatu wadah (organisasi/perusahaan) bertujuan agar dapat mempermudah dan mempercepat untuk pemanggilan atau pemanfaatan kembali data tersebut.

Menurut Pamungkas (2017:46) Sistem basis data merupakan sekumpulan basis data dengan para pemakai yang menggunakan basis data

secara bersama-sama, personil yang merancang dan mengelola basis data, teknik-teknik untuk merancang dan mengelola basis data, serta sistem komputer yang mendukungnya. Komponen utama penyusun sistem basis data adalah perangkat keras, sistem operasi, basis data, sistem pengelola basis data (DBMS), pemakai (Programmer, User mahir, user umum, user khusus).

BAB III

METODOLOGI PENELITIAN

3.1. Subyek Penelitian

3.1.1. Tempat dan Waktu Penelitian

1. Tempat Penelitian

Penelitian dilaksanakan di Laboratorium Jaringan Komputer UPT. Puskom Universitas Dehasen Bengkulu yang beralamatkan di Jl. Meranti Raya No. 32 Sawah Lebar Bengkulu.

2. Waktu Penelitian

Penelitian ini dilakukan dengan dua tahap yaitu:

a) Pra – Penelitian

Pra - penelitian ini dilakukan dari bulan Januari 2022 sampai dengan bulan Mei 2022.

b) Penelitian

Penelitian ini dilakukan dari bulan November 2022 sampai dengan bulan Desember 2022.

3.1.2. Sejarah Berdirinya Tempat Penelitian

Unit Pelaksana Teknis Pusat Komputer (UPT. PUSKOM) terbentuk semenjak Universitas Dehasen Bengkulu berdiri yaitu, tanggal 17 maret 2008. UPT. PUSKOM merupakan unit pelaksana perkuliahan komputer. Tujuan didirikan antara lain adalah : Memberikan pelayanan dalam pengolahan pelaksanaan

perkuliahan dan praktikum komputer, memberikan pelayanan terhadap jaringan komputer dan memberikan pelayanan terhadap teknologi informasi.

UPT. Puskom UNIVED memiliki 7 ruangan lab komputer yang terdiri dari : Lab Prodi Teknik Informatika (Lab. Pemrograman dan Internet), Lab Prodi Sistem Informasi, Lab Manajemen Informatika, Lab Prodi Sistem Komputer Dan Teknik Komputer (Lab. Hardware), Lab Aplikasi Komputer, Lab Multimedia, Dan Lab Bahasa.

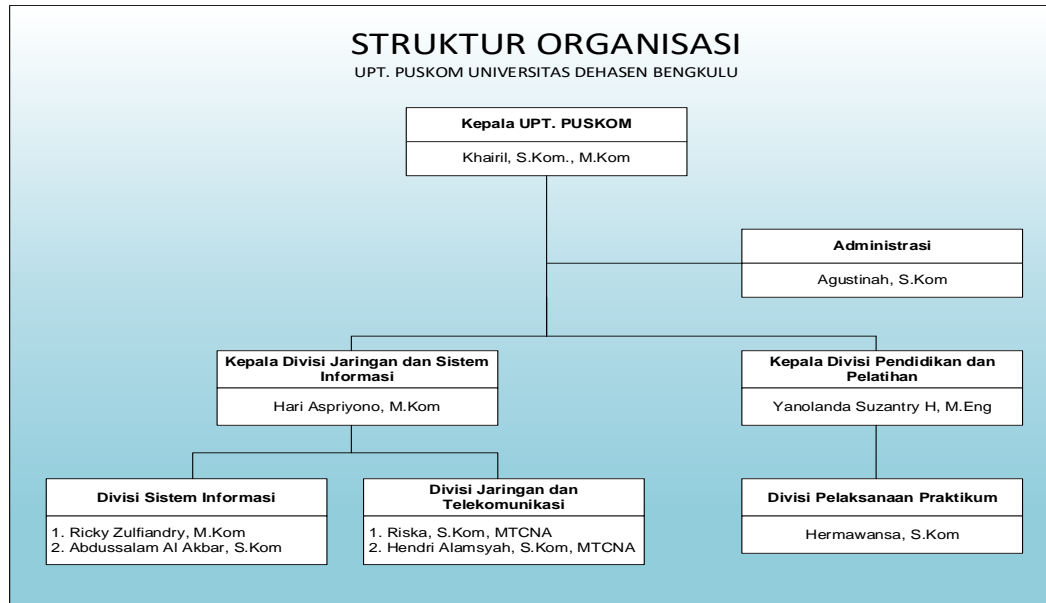
Semua ruangan pada lab dengan dinding kaca agar terlihat transparan yang berukuran rata-rata, jumlah computer setiap lab terdiri dari 55 unit komputer client dan 1 unit komputer server yang sudah terkoneksi dengan jaringan komputer (LAN). Masing-masing lab sudah dilengkapi dengan LCD Proyektor dan AC untuk pendingin ruangan supaya suasana belajar lebih nyaman

3.1.3. Struktur Organisasi

Struktur Organisasi merupakan kerangka kerja dimana didalamnya menggambarkan hubungan dan tanggung jawab setiap tingkat yang berada dalam Organisasi tersebut untuk melaksanakan demi tercapainya tujuan yang telah ditetapkan. Dengan demikian orang-orang tersebut mempunyai tugas, wewenang, dan tanggung jawab sesuai tugas masing-masing.

Struktur Organisasi sangatlah penting dalam suatu perusahaan atau instansi pemerintah. Karena dengan adanya struktur organisasi akan memperlihatkan dengan jelas kedudukan seseorang, sehingga setiap karyawan atau pegawai perusahaan atau instansi yang bersangkutan dapat mengetahui aktifitas dari perusahaan atau instansi dan dapat bekerja secara baik dari segi pembagian

tugas maupun hal pelimpahan wewenang yang telah ditetapkan dalam struktur. Adapun struktur organisasi UPT. Puskom Universitas Dehasen Bengkulu ditunjukkan pada gambar 3.1



3.1.4. Tugas Dan Wewenang

A. Kepala Pusat Komputer (Puskom)

- a. Menyusun Rencana Induk Teknologi Informasi Unived.
- b. Menyelenggarakan perkuliahan dan praktikum komputer.
- c. Melakukan perencanaan standar peralatan Teknologi Informasi , pengoperasian, pendayagunaan, dan pemeliharaan jaringan dilingkungan Unived.
- d. Memasyarakatkan layanan Teknologi Informasi kepada pengguna dan calon pengguna.
- e. Melakukan pengendalian keamanan dan keandalan kinerja jaringan baik dari sisi hardware maupun software sesuai dengan kemajuan teknologi.

- f. Melaksanakan pengelolaan layanan Teknologi Informasi yang antisipatif terhadap kebutuhan Universitas dan responsif terhadap keluhan pengguna.
- g. Menetapkan kualifikasi dan memberikan pertimbangan dalam rekrutmen dan penerimaan teknisi Teknologi Informasi pada semua unit di lingkungan Unived.
- h. Melakukan koordinasi dan memberikan konsultasi teknis jaringan secara berkala kepada para teknisi Teknologi Informasi di lingkungan Unived.
- i. Mengelola dan menjamin kelancaran akses Informasi ke jaringan lokal Universitas dan jaringan global bagi semua pengguna.
- j. Membuat laporan secara periodik kepada pimpinan Unived.

B. Administrasi

- a. Membantu menyusun RKAT Pusat Komputer.
- b. Mewakili tugas Kepala Pusat Komputer.
- c. Melaksanakan urusan keuangan.
- d. Melakukan tatalaksana dan kepegawaian.
- e. Melaksanakan urusan rumah tangga.
- f. Melaksanakan sosialisasi layanan Puskom.
- g. Melaksanakan administrasi layanan Puskom.
- h. Membina kelompok tenaga ahli.
- i. Membuat laporan pelaksanaan kegiatan Puskom.
- j. Melaksanakan tugas lain yang diberikan oleh pimpinan.

C. Divisi Pendidikan dan Pelatihan

- a. Menyusun rencana dan program kerja.

- b. Mengkoordinasikan penyusunan Rencana Kerja dan Anggaran.
- c. Mengkoordinasikan pelaksanaan praktikum.
- d. Melaksanakan kebijakan umum dan teknis pendidikan dan pelatihan bagi dosen dan mahasiswa.
- e. Menyampaikan saran dan pertimbangan kepada kepala UPT. Puskom guna kelancaran pelaksanaan kegiatan.

D. Divisi Pelaksana Praktikum

- a. Mengkoordinasikan hardware dan software praktikum dengan dosen pengasuh.
- b. Mengkoordinasikan jadwal praktikum dengan administrasi.
- c. Menyiapkan fasilitas perkuliahan dan/atau praktikum komputer.

E. Divisi Jaringan Telekomunikasi

- a. Menyusun RKAT di lingkungan seksi Layanan Jaringan Komputer.
- b. Memelihara hardware, software, dan sistem operasi komputer;
- c. Cabling dan switching.
- d. Routing, Bandwidth management, dan firewall.
- e. Penataan/pemetaan (topologi) jaringan.
- f. Melakukan pelatihan pengoperasian jaringan di lingkungan Unived.

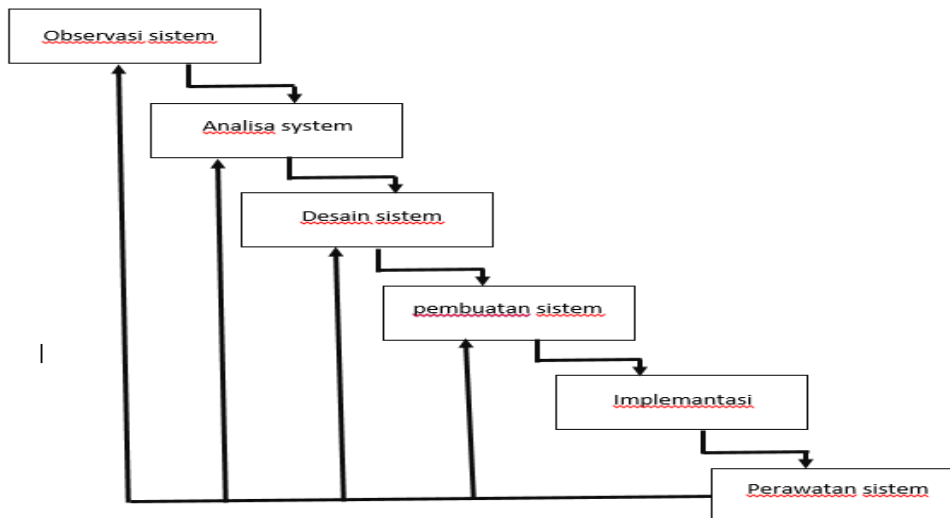
F. Divisi Sistem Informasi

- a. Menyusun RKAT di lingkungan Seksi Layanan Teknologi Informasi .
- b. Layanan e-mail dan web server.
- c. Layanan aplikasi teknologi Informasi .
- d. Bantuan teknis operasional sistem Informasi manajemen.

- e. Sistem pencadangan data (backup sistem).
- f. Layanan instalasi software aplikasi.
- g. Mengembangkan software teknologi Informasi .
- h. Melaksanakan pelatihan operasional software manajemen Informasi di lingkungan Unived.

3.2. Metode Penelitian

Dalam proses pembuatan program ini, penulis menggunakan metode *waterfall* yang meliputi beberapa proses, antara lain :



Gambar 3.1 Tabel alur *waterfall*

Berikut di bawah ini merupakan penjelasan dari alur *waterfall* pada gambar diatas :

1) Observasi Sistem

Tahapan pertama dari pembuatan program ini yaitu penulis mengobservasi terhadap yang sudah menggunakan algoritma *Advanced Encryption Standard (AES)* dalam teknologi pengamanan file. Penulis mengobservasi mengenai tampilan, cara kerja

program tersebut dan juga bagaimana mereka memproses data menggunakan algoritma *Advanced Encryption Standard (AES)*.

2) Analisis sistem

Tahapan kedua yang perlu dilakukan yaitu menganalisis sistem dari yang sudah ada. Penulis menganalisis cara kerja, alur proses dan tampilan.

3) Desain sistem

Setelah penulis mengobservasi dan menganalisa, penulis mendesain sistem enkripsi dan dekripsi algoritma *Advanced Encryption Standard (AES)* dengan menggunakan bahasa pemrograman PHP.

4) Pembuatan Sistem

Langkah selanjutnya adalah pembuatan sistem, pada tahapan ini penulis membuat sistem dengan menggunakan bahasa pemrograman PHP.

5) Implementasi

Langkah selanjutnya adalah implementasi sistem, dimana melakukan perancangan aplikasi telah dibuat.

6) Perawatan Sistem.

Menganalisa kesalahan atau *error* yang muncul pada program serta melakukan perbaikan.

3.3. Instrumen Perangkat Lunak dan Perangkat Keras

Dalam melakukan penelitian ini, alat dan bahan yang digunakan meliputi perangkat lunak dan perangkat keras :

a. Perangkat Lunak (Software)

Adapun perangkat lunak (software) yang digunakan sebagai berikut :

- a. Sistem linux Ubuntu server 20.04
- b. PHP
- c. PHP My Admin
- d. Apache
- e. MySQL
- f. Server web hosting

b. Perangkat Keras (Hardware)

Adapun perangkat Keras (hardware) yang digunakan dalam penelitian ini yaitu :

No	Kebutuhan	Perangkat	Spesifikasi
1.	2 unit Laptop	Lenovo G40	Intel(R) Core i7-5500V
			4 GB DDR3
			1 TB HDD
			DVDRW, Bluetooth, Wifi, NIC
			VGA AMD Radeon R5-M2302GB
			Camera, 14 WXGA
		HP Notebook 14-G008AUR	AMD E1-2100 APU with Radeon(TM) HD Grafik
			1.00 GHz
			Installed RAM 2.00 GB
			64-bit operating system, x64-based processor

3.4. Metode Pengumpulan Data

Untuk memperoleh data yang diperlukan dalam penyusunan skripsi nanti penulis menggunakan beberapa metode dalam pengumpulan data

a. Observasi

Merupakan metode pengumpulan data yang digunakan dengan cara melakukan pengamatan langsung pada jaringan yang ada di Lab Hardware Universitas Dehasen Bengkulu.

b. Studi Pustaka

Merupakan metode pengumpulan data yang dilakukan dengan cara membaca buku-buku di perpustakaan kampus maupun perpustakaan daerah dan artikel di *internet* yang ada hubungannya dengan masalah yang dibahas dalam penelitian ini

3.5. Metode Perancangan Sistem

Dalam proses pembuatan program ini, adapun metode perancangan yang dilakukan sebagai berikut :

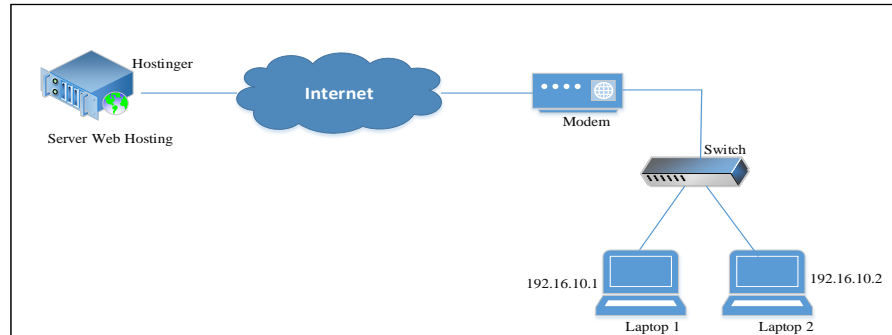
A. Analisis Sistem Aktual

Keamanan data, file atau informasi adalah hal yang sangat penting bagi pengguna jaringan saat ini, kasus penyadapan akan file merupakan salah satu hal yang sangat merugikan, dengan adanya kemungkinan terjadinya kejahatan ini, maka perlunya peningkatan dalam hal keamanan file. Saat ini, keamanan file perlu mendapatkan perhatian khusus, maka penelitian ini membuat suatu penerapan kriptografi algoritma AES-128 untuk enkripsi dan dekripsi data yang berupa file dokumen format (pdf, docx, txt). Algoritma Advanced Encryption Standard dipilih karena memiliki suatu tingkatan keamanan yang baik, dan pada penelitian ini akan diuji file dokumen dengan format

tertentu dan untuk melihat kecepatan waktu yang dibutuhkan selama proses enkripsi dan dekripsi.

B. Diagram Blok Global

Adapun diagram blok global pada rangkaian ini sebagai berikut :



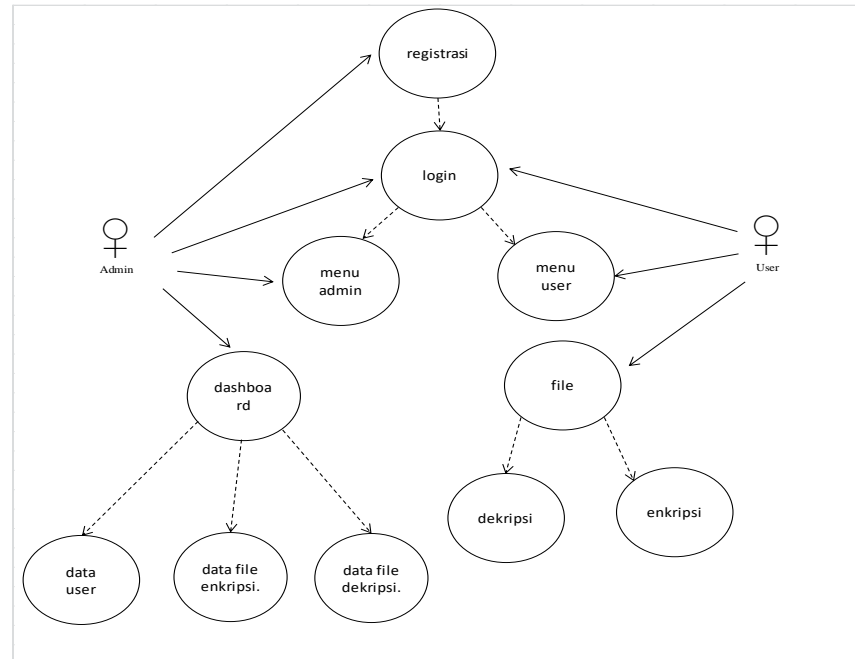
Gambar 3.3 Diagram blok global

Pada rangkaian perancangan penelitian ini dibangun aplikasi keamanan file berbasis web, yang dapat diakses melalui jaringan internet, dengan pengujian menggunakan 2 unit laptop. Laptop satu digunakan sebagai user dan laptop 2 digunakan sebagai admin

C. Desain Sistem

a. Use case

Berikut dibawah ini desain sistem dengan *Use case* :

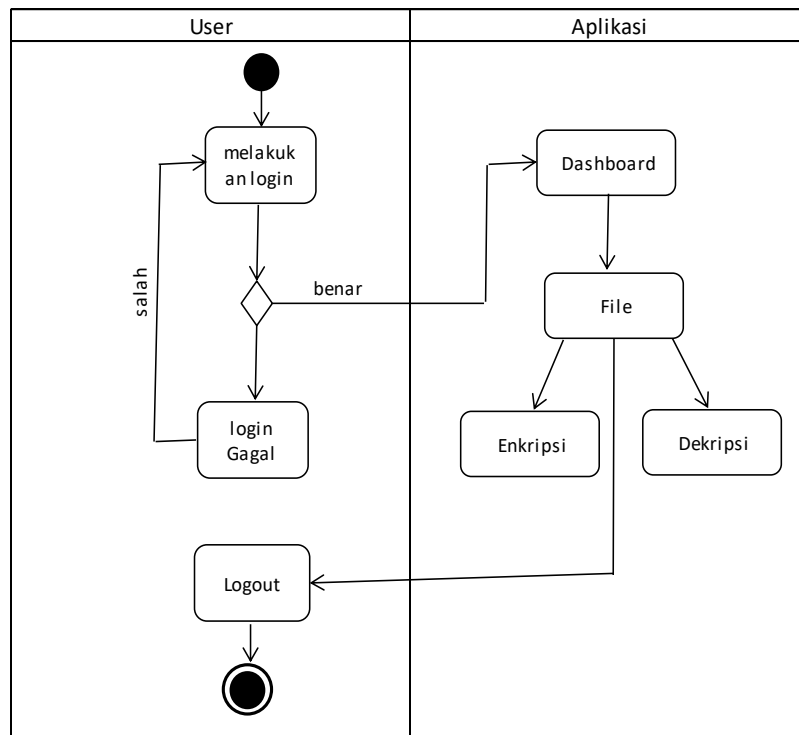


Gambar 3.4 Use Case Diagram

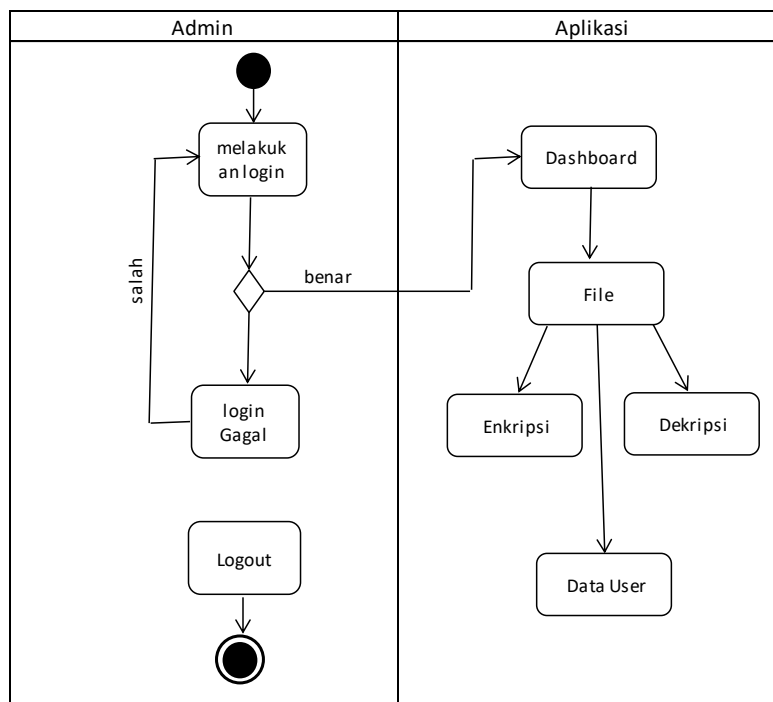
Pada gambar 3.4 tersebut terdapat 2 aktor yang akan mengakses aplikasi yaitu admin dan user. Setiap user akan melakukan login pada aplikasi terlebih dahulu. Jika login sebagai admin maka, admin data mengelola data user dan data file. Jika login sebagai user dapat menginput file yang akan dienkripsi dan dekripsikan.

b. Activity diagram

Activity diagram menggambarkan aktivitas user terhadap terhadap aplikasi yang melibatkan user, admin dan aplikasi. Adapun activity diagram pada gambar 3.5 dan 3.6 sebagai berikut:



Gambar 3.5 Activity Diagram user



Gambar 3.6 Activity Diagram Admin

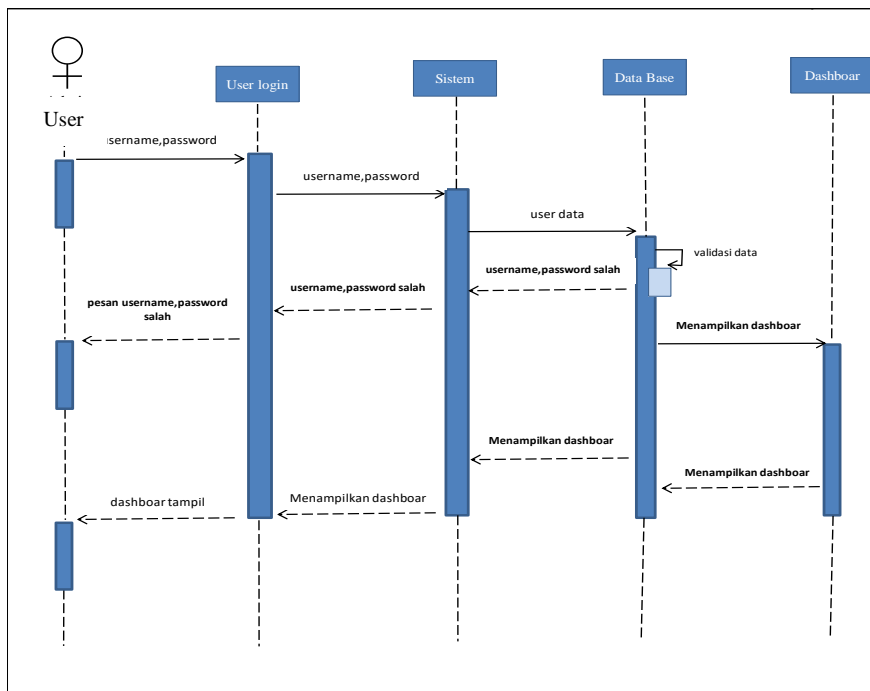
c. Class Diagram



Gambar 3.7 Class Diagram

d. Sequence Diagram

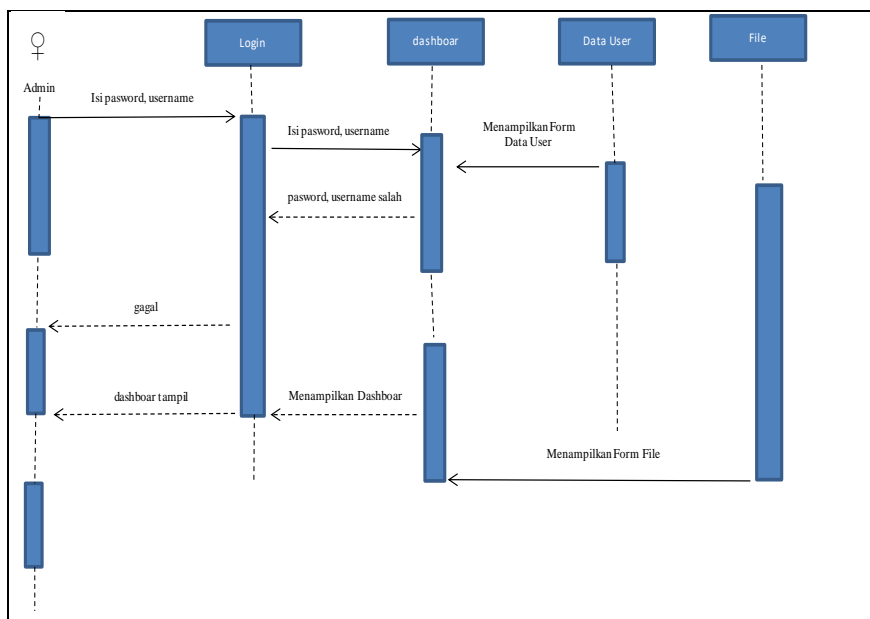
Sequence Diagram menggambarkan keterhubungan antara user terhadap objek aplikasi seperti gambar 3.8 dan 3.9



Gambar 3.10

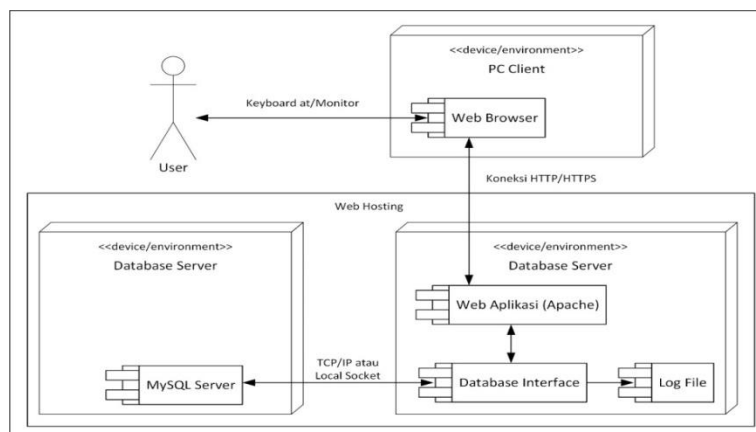
Sequence Diagram User

Adapun gambar 3.11 dibawah ini merupakan Sequence Diagram admin sebagai berikut :



Gambar 3.11 Sequence Diagram admin

e. *Deployment Diagram*



Gambar 3.12 Sequence Diagram Admin

e. Rancangan program

1. Tampilan halaman login

Login

Silahkan isi username dan password anda dengan benar !!

Username

Password

Apakah anda belum memiliki akun di aplikasi ?

Silahkan lakukan registrasi terlebih dahulu dengan klik tombol di bawah ini :

Gambar 3.13 Tampilan halaman login

2. Tampilan Registrasi User

Registrasi	
Nama Lengkap	<input type="text"/>
Alamat	<input type="text"/>
Username	<input type="text"/>
Password	<input type="text"/>
<input type="button" value="Registrasi"/>	

Gambar 3.14. Halaman Registrasi User

3. Administrator

a) Halaman Menu Utama Administrator

Header	
Selamat Datang Di halaman Menu Utama Administrator	
Main Menu	
Dashboard	
User	
Daftar File Enkripsi	
Logout	

Gambar 3.15. Halaman Menu Utama Administrator

b) Halaman User

Data User				
Nama Lengkap	Alamat	Username	Status	Aksi
XXXX	XXXX	XXXXXX	XXXXXX	Aktif Tidak Aktif Hapus
XXXX	XXXX	XXXXXX	XXXXXX	Aktif Tidak Aktif Hapus
XXXX	XXXX	XXXXXX	XXXXXX	Aktif Tidak Aktif Hapus
XXXX	XXXX	XXXXXX	XXXXXX	Aktif Tidak Aktif Hapus
XXXX	XXXX	XXXXXX	XXXXXX	Aktif Tidak Aktif Hapus

Gambar 3.16. Halaman User

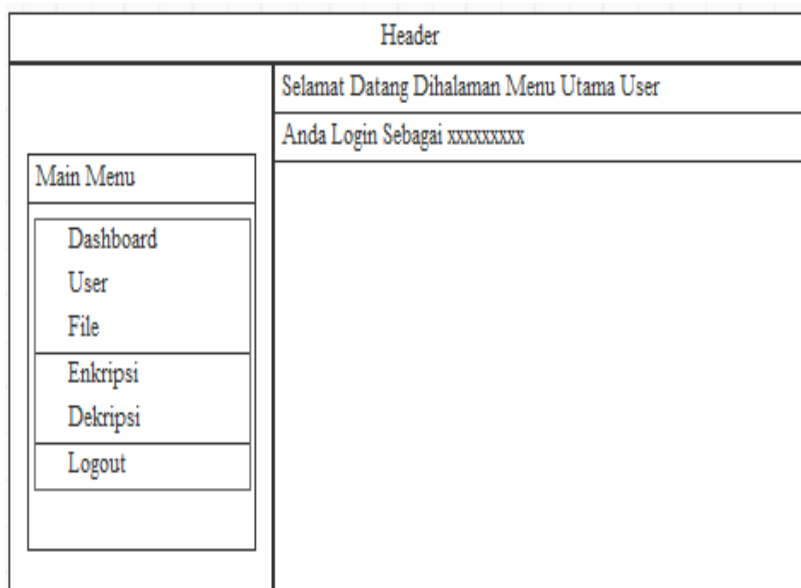
c) Halaman Daftar File Enkripsi

Daftar File Enkripsi					
Tanggal	Username	Nama File	Ukuran File	Keterangan File	Aksi
d/M/y	XXXXXX	XXXXXXXX	XXXXXX	XXXXXXXX	Download Hapus
d/M/y	XXXXXX	XXXXXXXX	XXXXXX	XXXXXXXX	Download Hapus
d/M/y	XXXXXX	XXXXXXXX	XXXXXX	XXXXXXXX	Download Hapus
d/M/y	XXXXXX	XXXXXXXX	XXXXXX	XXXXXXXX	Download Hapus
d/M/y	XXXXXX	XXXXXXXX	XXXXXX	XXXXXXXX	Download Hapus

Gambar 3.17. Halaman Daftar File Enkripsi

4. User

a) Halaman Menu Utama User



Gambar 3.18. Halaman Menu Utama User

b) Halaman User

Biodata User	
Nama Lengkap	: xxxxxxxxxxxxxxxxxxxxxxxxxxx
Alamat	: xxxxxxxxxxxxxxxxxxxxxxxxxxx
Username	: xxxxxxxxxxxxxxxxxxxxxxxxxxx

Gambar 3.19. Halaman User

c) Halaman File Enkripsi

Form Enkripsi

Tanggal

File

Password

Keterangan File

Tanggal	Nama File	Ukuran File	Keterangan File	Aksi
d/M/y	xxxxxx	xxxxxxxx	xxxxxx	xxxxxxxx Download Hapus
d/M/y	xxxxxx	xxxxxxxx	xxxxxx	xxxxxxxx Download Hapus
d/M/y	xxxxxx	xxxxxxxx	xxxxxx	xxxxxxxx Download Hapus
d/M/y	xxxxxx	xxxxxxxx	xxxxxx	xxxxxxxx Download Hapus
d/M/y	xxxxxx	xxxxxxxx	xxxxxx	xxxxxxxx Download Hapus

Gambar 3.20. Halaman File Enkripsi (1)

Informasi Enkripsi

Nama File Enkripsi : xxxxxxxxxxxxxxxxxxxxxxxxxxxx

Ukuran File Enkripsi : xxxxxxxxxxxxxxxxxxxxxxxxxxxx

Tanggal Enkripsi : xxxxxxxxxxxxxxxxxxxxxxxxxxxx

Keterangan File Enkripsi : xxxxxxxxxxxxxxxxxxxxxxxxxxxx

Waktu proses enkripsi yang terjadi selama : xxxxxxxxxxxxxxxxxxxxxxxxxxxx

Gambar 3.20. Halaman File Enkripsi (2)

d) Halaman File Dekripsi

Form Dekripsi

Tanggal	Nama File Enkripsi	Ukuran File Enkripsi	Keterangan File Enkripsi	Aksi
d/M/y	xxxxxxx	xxxxxx	xxxxxxx	Download File Enkripsi Dekripsi
d/M/y	xxxxxxx	xxxxxx	xxxxxxx	Download File Enkripsi Dekripsi
d/M/y	xxxxxxx	xxxxxx	xxxxxxx	Download File Enkripsi Dekripsi
d/M/y	xxxxxxx	xxxxxx	xxxxxxx	Download File Enkripsi Dekripsi
d/M/y	xxxxxxx	xxxxxx	xxxxxxx	Download File Enkripsi Dekripsi
d/M/y	xxxxxxx	xxxxxx	xxxxxxx	Download File Enkripsi Dekripsi

Gambar 3.21. Halaman File Dekripsi (1)

Form Dekripsi

Nama File Enkripsi : xx

Ukuran File Enkripsi : xx

Tanggal Enkripsi : xx

Keterangan File Enkripsi : xx

Masukkan Password Untuk Mendekripsi

Gambar 3.22. Halaman File Dekripsi (2)

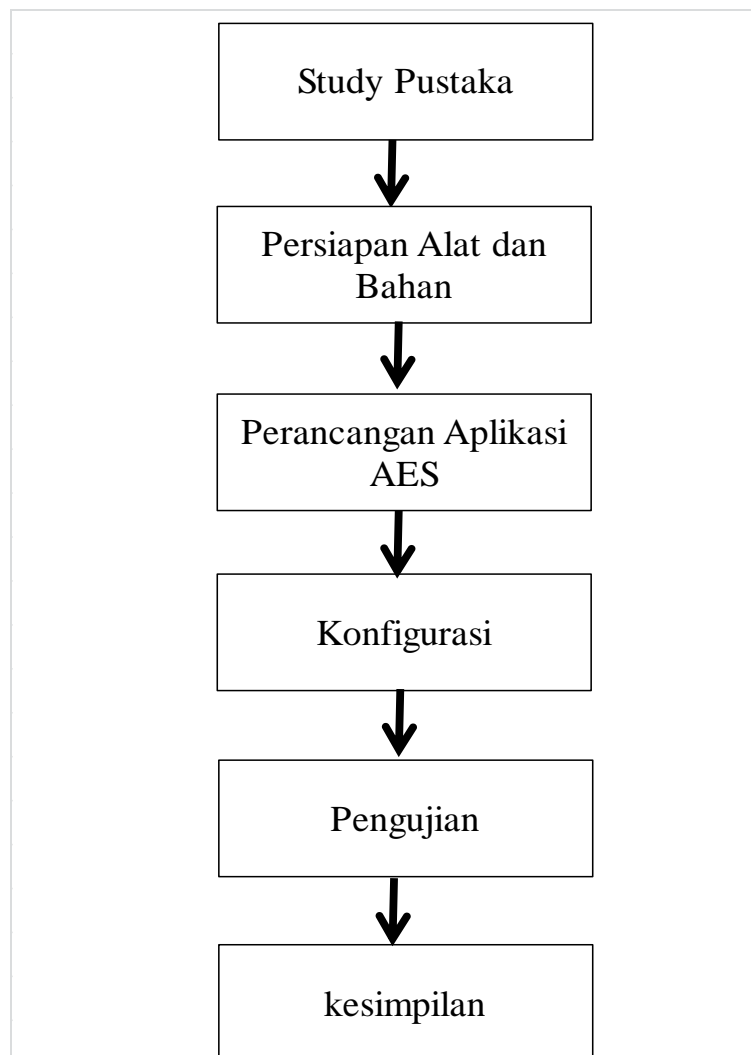
D. Prinsip Kerja Sistem

Prinsip kerja sistem algoritma *Advanced Encryption Standard (AES)*, diterapkan pada pengaman file, Sistem pembuatan pengamanan file ini menggunakan bahasa pemrograman PHP, menyajikan file berupa karakter huruf, dan angka dari file dokumen dengan format (*pdf*, *docx*, *doc*). Yang nantinya menggunakan metode

perancangan sistem *waterfall*. *Advanced Encryption Standard (AES)* sendiri merupakan sebuah algoritma kriptografi yang berkeja sebagai mengenkripsikan dan mngedekripsikan sebuah file yang akan nanti diujikan.

E. Rencana Kerja Sistem

Rencana kerja dari Penerapan *Advanced Enkryption Standard (AES)* Untuk Pengamanan File Pada Aplikasi Berbasis Web adalah sebagai berikut.



Gamabar 3.18 Tampilan rencana kerja sistem

Berikut ini merupakan penjelasan dari gambar diatas :

1. Studi Pustaka

2. Studi pustaka dilakukan dengan cara membaca buku-buku di perpustakaan kampus maupun perpustakaan daerah dan artikel di *internet* yang ada hubungannya dengan masalah yang dibahas dalam penelitian ini.

3. Persiapan Alat dan Bahan

4. Adapun alat dan bahan yang harus disiapkan, sebagai berikut :

- a. 2 Unit Laptop sebagai *user* dan admin
- b. Modem

5. Perancangan aplikasi AES

Perancangan aplikasi AES akan dilakukan pembuatan aplikasi berbasis web dengan bahasa pemrograman PHP dan data base *MySQL* yang dapat diakses melalui jaringan.

6. Konfigurasi.

Konfigurasi dapat dilakukan sehingga antara sistem operasi *server* dan *client* dapat saling berkomunikasi.

7. Pengujian

Tahapan ini dilakukan untuk menguji sistem yang di implementasikan pada jaringan. Apakah berjalan dengan baik ataupun sebaliknya.

8. Kesimpulan

Pada tahapan ini adalah tahapan untuk menyimpulkan hasil dari penelitian hasil dari penelitian yang telah dilakukan.

3.6. Metode Pengujian Sistem

Pengujian ini dilakukan dengan metode *blackbox*, yaitu sebuah metode yang digunakan untuk menentukan kesalahan dan Mendemonstrasikan fungsional sistem saat dioperasikan, apakah *input* diterima dengan benar dan *output* yang dihasilkan telah sesuai dengan yang diharapkan membuktikan kebenarannya. Adapun rancangan pengujian dapat dilihat seperti pada tabel 3.1 berikut ini :

Tabel 3.1 Pengujian dan Analisa.

No	Jenis Pengujian	Kriteria	Hasil	Ket
1.	Pengujian Enkripsi	Melakukan enkripsi file dengan format <i>pdf, docx, doc</i> Pada aplikasi berbasis web		
2.	Pengujian Dekripsi	Melakukan dekripsi file pada aplikasi berbasis web		
3.	Pengujian Keamanan File	Melakukan <i>sniffing</i> menggunakan aplikasi wireshark		
4.	Pengujian waktu yang dibutuhkan dalam Proses Enkripsi	Waktu proses enkripsi		