PENERAPAN KEAMANAN FILE MENGGUNAKAN ALGORITMA BASE64 DAN AES (ADVANCED STANDART ENCRYPTION)

Dosen Pembimbing : Teguh Tamrin, S.Kom, M.Kom.

Disusun Oleh :

Ahmad Suroyya mutsaddad

(19240000937)

PROGAM STUDI TEKNIK INFORMATIKA

FAKULTAS SAINS DAN TEKNOLOGI

UNIVERSITAS ISLAM NADHALATUL ULAMA JEPARA

2023

PERSETUJUAN PEMBIMBING

Assalamualaikum Wr.Wb.

Setelah Kami Meneliti dan mengadakan perbaikan seperlunya , bersama ini saya kirim Naskah ProposalSkripsi Saudara :

Nama	:	Ahmad Suroyya Mutsaddad
Nim	:	191240000937
Progam Studi	:	Teknik Informatika
Judul	:	Penerepan Keamanan File Menggunakan Algoritma Base64 dan AES (Advanced Standart Encryption)

Proposal skripsi ini telah disetujui pembimbing dan siap untuk dipertahankan dihadapan Dewan Penguji Progam Sarjana Strata 1 (S.1) Fakultas Sains dan Teknologi Universitas Islam Nadhalatul Ulama Jepara.

Demikian harap menjadikan maklum.

Wassalamualikum Wr.Wb.

Jepara,15 Juni 2023

Pembimbing 1	**Pembimbing 2**
Teguh Tamrin, S.Kom, M.Kom.	**R. Hadapiningradja Kusumodestoni,S.Kom, M.Kom**
NIDN. 0620127603	**NIDN. 0625056505**

Mengetahui.

Ketua Progam Studi Teknik Informatika

Gentur Wahyu Nyipto Wibowo , M.Kom.

NIDN. 0623117902

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I

PENDAHULUAN

1.1 Latar Belakang

Di zaman teknologi yang semakin berkembang dan maju, orang-orang telah melakukan banyak pengembangan dalam bidang teknologi digital dalam hal pengamanan data secara digital dan pengamanan dokumen secara digital. Keamanan kriptografi bermula dari kebutuhan untuk melindungi pesan rahasia dari orang-orang yang tidak berwenang. Sejarah kriptografi bisa dilacak kembali hingga ribuan tahun yang lalu, ketika orang menggunakan teknik-teknik sederhana seperti penggantian karakter atau penjumlahan numerik untuk menyandikan pesan rahasia. Namun, dengan berkembangnya teknologi komunikasi, metode kriptografi sederhana ini menjadi mudah dibobol oleh orang yang tidak berhak. Oleh karena itu, kriptografi modern menggunakan algoritma matematika yang rumit untuk menyandikan pesan dan melindungi data pribadi. Teknologi tumbuh dalam kecanggihan seiiringnya waktu dan serangan dunia maya yang canggih kriptografi dapat terus berkembang untuk mengatasi ancaman baru[1].

Keamanan dalam kriptografi merupakan isu penting karena informasi sensitif dan pribadi seringkali disimpan dan dikirimkan dalam bentuk digital. Tanpa tindakan pengamanan yang memadai, informasi ini dapat dicuri, dimanipulasi, atau diakses oleh pihak yang tidak berwenang. Salah satu untuk mengatasi cara dalam menjaga isi pesan tersebut dengan dilakukanya sebuah pengubahan pesan dari suatu text maupun file menjadi sandi yang hanya diketahui oleh pengirim dan penerima pesan. Meskipun kriptografi terus berkembang, tantangan keamanan tetap ada. Salah satu tantangan utamanya adalah serangan siber yang dapat menembus sistem keamanan dan mengakses informasi sensitif. Serangan dunia maya dapat dilakukan dengan berbagai cara, seperti serangan brute force, serangan phishing, atau serangan man-in-the-middle[2].

Pada zaman sekarang berbagi informasi tidak hanya secara langsung maupun melalui surat dengan berkembangnya zaman berbagi informasi

dapat dilakukan menggunakan aplikasi seperti whatsaap, telegram maupun facebook. Bukan berarti hal tersebut tidak memiliki kekurangan semua sistem digital pasti memliki kekuranganya masing-masing. Informasi pada aplikasi tersebut dapat dengan mudah dilihat oleh orang lain, baik penyedia maupun orang yang berniat dalam melakukan pencurian data maupun informasi yang biasa disebut hacker. Hal ini dapat dicegah melalui pihak ketiga dalam pengiriman sebuah file maupun bisa menggunakan kunci untuk membuka informasi yang diterima untuk guna menghindari orang berniat buruk dalam mengetahui informasi untuk keperluan sendiri atau diperjual belikan[3].

Pengubahan teks informasi dilakukan dengan cara teknik yang biasa disebut enkripsi dimana teks asli yang disebut dengan (plaintext) diacak menggunakan suatu kunci yang menghasilkan teks acak yang disebut (chipertext). Dalam kasus enkripsi ada beberapa istilah yaitu enkripsi simteris dengan melakukan pengacakan menggunakan kunci atau key yang sama atau tidak berubah teknik ini dapat mendapat teks asli dengan menggunakan teknik yang sama, enkripsi asimteris dengan melakukan teknik pengacakan dengan pengamanan key atau kunci yang berbeda untuk membukanya dalam kasus penggunaan teknik asimteris kemungkinan kecil dalam pencurian data dengan menggunakan bruteforce.Enkripsi dan dekripsi teks maupun dokumen akan disandikan dengan metode tertentu sehingga kebocoran data infromasi kepada tangan yang tidak berwewenang[4].

Algoritma base64 sangat baik untuk digunakan dalam mengacak teks. Karakter-karakter pada plaintext akan ditransposisikan ke tempat lain sehingga plaintext tersebut tidak dapat difahami oleh orang lain. Dengan menerapkan algoritma ini, data akan terjamin kerahasiaannya. Metode ini sangat cepat dalam operasinya. Semakin banyak kata-kata pada pesan tersebut, maka hasil ciphertext akan semakin kuat untuk diretas oleh seseorang yang ingin mencuri pesan tersebut. Advanced Encryption Standard (AES) sebuah algoritma kriptografi simetris yang digunakan untuk mengenkripsi dan mendekripsi data. Algoritma AES dikenal juga dengan

nama Rijndael, yang diusulkan oleh dua ahli kriptografi Belgia, Vincent Rijmen dan Joan Daemen. AES menggunakan sebuah kunci rahasia yang sama untuk mengenkripsi dan mendekripsi data.

Dengan adanya permasalahan kemanan pada melakukan pertukaran data dan informasi berbasis sebuah file solusi dalam menangani tersebut dengan adanya kombinasi dalam sebuah penerapan algoritma untuk melakukan enkripsi sehingga kemungkinan dalam terjadinya kebocoran data menggunakan kombinasi antara base64 dan AES (Advanced Encryption Standart) kemungkinan kecil terjadinya kebocoran sebuah sebuah informasi. Dikarenakan metode ini dalam tahap proses penulisan kita perlu mengubah sebuah kedalam format ASCII dengan hasil chipertext base64 tadi di enkrip lagi menggunakan Algoritma AES dengan kunci yang sudah ditentukan sehingga menambah kerumitan dalam melakukan enkripsi dan dekripsi[5].

Berdasarkan permasalahan diatas bertujuan bagaimana dalam melakukan suatu pengamanan suatu file untuk berbagi informasi ke pihak penerima untuk menghindari bocornya suatu informasi ke pihak yang tidak berwenang maupun pihak yang tidak seharusnya menerima pesan itu, oleh karena itu adanya pengamanan dimana perlu menggunakan kunci untuk membuka suatu informasi yang berupa file yang sudah dienkripsi menggunakan 2 algoritma yaitu base64 dan AES(Advanced Standart Encryption).

1.2 Batasan Penelitian

Batasan yang dimaksud yaitu untuk membatasi ruang lingkup kerja dengan tujuan memperkecil masalah yang ada pada bagian umum. Adapun batasan penelitian yang akan dibahas meliputi :

1. Metode yang digunakan dalam penelitian adalah metode base64 dan AES (Advanced Encryption Standart).
2. Data yang digunakan dalam enkripsi hanya file berformat pdf.
3. Penelitian menggunakan data public tidak terikat instansi tertentu.
4. Pengujian / penerapan tidak mempertimbangkan jaringan internet.

5. Penelitian ini tidak menerapkan penyandian dalam aplikasi tertentu.

1.3 Perumusan Masalah

Berdasarkan latar belakang masalah diatas maka perumusan masalah dalam penelitian ini adalah bagaimana mengamankan pertukaran informasi berupa file dengan memanfaatkan teknik kriptografi enkripsi dan dekripsi.

1.4 Tujuan Penelitian

Berdasarkan perumusan masalah diatas maka tujuan penelitian dalam penelitian ini adalah menerapkan metode base64 dan AES(Advanced Encryption Standart) untuk mengamankan pertukaran informasi dengan menggunakan data file sebagai keamanan dari pihak tidak berwenang.

1.5 Manfaat Penelitian

Dari penelitian diatas diharapkan dapat memberikan manfaat sebagai berikut :

a. Manfaat bagi peneliti

   Adapun manfaat bagi peneliti yaitu menambah ilmu pengetahuan khususnya pada keamanan dalam menggunakan algortima kriptografi.

b. Manfaat bagi penerima dan pengirim pesan

   Pengirim dan penerima pesan dapat menyandi file agar lebih aman saat berkomunikasi.

c. Manfaat bagi Pembaca

   Dapat menambah wawasan bagi pembaca dan dapat dipergunakan sebagai referensi untuk penelitian selanjutnya.

d. Manfaat bagi keamanan informasi

   Dapat menjaga keamanan dalam bertukar informasi dengan menerapkan metode lebih 1 algoritma base64 dan AES (Advanced Encryption Standart).

1.6 Sistematika Penulisan

Sistematika penulisan ini disusun untuk memberikan gambaran secara umum mengenai penyusunan penelitian yang akan dilakukan. Pokok pembahasan laporan peneletian dibagi menjadi beberapa bab. Sistematikapenulisannya adalah sebagai berikut :

BAB I PENDAHULUAN

Pada bab ini membahas tentang latar belakang, rumusan masalah, batasan penelitian, tujuan penelitian, manfaat penelitian, serta sistematika penulisan.

BAB II TINJAUAN PUSTAKAN

Pada bab ini berisi mengenai tinjauan studi, tinjuan pustaka, dan kerangka pemikiran.

BAB III METODOLOGI PENELITIAN

Pada bab ini mejelaskan tentang kerangka penelitian, pengumpulan data, metode pengembangan sistem, dan pengujian metode.

BAB IV HASIL DAN PEMBAHASAN

Pada bab ini mejelaskan tentang penerapan algoritma ke aplikasi tersebut.

BAB V KESIMPULAN DAN SARAN

Pada bab ini mejelaskan tentang kesimpulan dan saran yang diharapkan dapat bermanfaat untuk mengembangkan pembuatan program aplikasi selanjutnya.

BAB II

LANDASAN TEORI

2.1 Tinjauan Studi

Penelitian ini merujuk pada beberapa referensi yang telah dilakuka oleh peneliti peneliti sebelumnya untuk dijadikan refererensi sekaligus sebagai sumber bertukar informasi diantaranya:

Penelitian yang dilakukan oleh Tio Lovian, Iskandar Fitri.Pada tahun 2022,dengan judul "Implementasi Algoritma Base64 Sebagai Tingkat Keamanan Data Pada Website Sistem Informasi Pencatat Barang",dalam penelitian ini permasalahan yang dikhawatirkan terjadi pencurian data pada aplikasi pencatat yang dimana aplikasi menyimpan data email password dan data tranksaksi sehingga diterapkanya pengamanan enkripsi pada data guna menghindari kebocoran data yang bersifat penting, pada hasil akhir penelitian ini mendapatkan hasil percobaan dengan 300 data dengan 20 percobaan metode dekripsi yang dimana dihasilkan hanya perlu menggunakan 1 algoritma utma yaitu algoritma base64 untuk mendapatkan nilai yang benar atau valid[6].

Penelitian yang dilakukan Harry Witriyono dan Sandhy Fernandez. Pada tahun 20212, dengan judul "Implementasi Enkripsi Base64, Hashing SHA1 dan MD5 pada QR Code Presensi Kuliah", Dalam penelitian ini terdapatnya kecurangan sistem yang dilakukan mahasiswa dalam absen dengan diterapkanya proses absen menggunakan QR ini dapat meminimalisir kecurangan dalam proses absensi untuk penerapan absensi pada sistem parameter yang dikirim dan terdapat beberapa algoritma yang diterapkan khususnya base64 untuk upaya pengamanan data SQL dan data parameter URL supaya pada pengmanan tersebut tetap terjaga tidak dapat mengetahui nilai asli jika terjadi kebocoran suatu data[7].

Pada artikel yang telah dibuat Muhammad Azhari1, Dadang Iskandar Mulyana2, Faizal Joko Perwitosari danFirhan Ali. Pada tahun 2022 dengan judul "Implementasi Pengamanan Data pada Dokumen Menggunakan Algoritma Kriptografi Advanced Encryption Standard (AES)", peneliti merancang sebuah aplikasi sistem informasi yang hanya mengandalkan sistem

backup dan kurang efektif dan pegawai dapat langsung mengubah data tanpa perlu ada perlindungan keamanan data, sehingga dikhawatirkan data akan bocor ke pihak yang tidak bertanggung jawab, maka keamanan file data diterapkan disini. Disini pada pengamnan datat diterapkan menggunakan algoritma AES yang sudah menjadi standart enkripsi pengamanan data nasional maka akan terjaminya data untuk tidak akan bocor jika tidak dibuka menggunakan kunci tertentu[8].

Penelitian yang ditulis oleh Maya Sari, Hindriyanto Dwi Purnomo, dan Irwan Sembiring 2022 dengan judul "Algoritma Kriptografi Sistem Keamanan SMS di Android", dalam penelitian ini membahas tentang penggunaan smartphone yang luas dimasyarakat. Namun, meskipun teknologi smartphone ini memiliki banyak fitur, penggunanya tetap memiliki pertimbangan khusus untuk email SMS (Short Message Service). Tetapi SMS ini memiliki keterbatasan, hanya dalam keamanan pertukaran informasi rahasia, sistem ini diperlukan untuk memberikan keamanan pertukaran informasi melalui SMS berbasis Android. Oleh karena itu diperlukan pengamanannya dengan menggunakan metode kriptografi dan diperlukan tingkat keamanan yang tinggi. Pada penelitian ini akan membandingkan tiga algoritma kriptografi yaitu Advanced Encryption Standard (AES), Rivest Shamir Adleman, dan Tiny Encryption Algorithm yang dilakukan dengan cara membandingkan karakteristik algoritma enkripsi yang hasilnya akan digunakan untuk sistem keamanan SMS berbasis Android dengan keamanan yang lebih tinggi[9].

Permasalahan dalam penelitian yang dibuat oleh R M. Abu Jihad Plaza, dan Hartono, R. Pada tahun 2021, "Penerapan Kriptografi Caesar Chiper Pada Aplikasi Chatting Berbasis Local Area Network", dalam penelitian ini masalah yang diangkat adalah pengguna jaringan komputer sering dihadapkan pada masalah komunikasi antar pengguna. Peneliti membuat sebuah Aplikasi chat digunakan sebagai media komunikasi antar sesama pengguna komputer yang terhubung dalam suatu jaringan, baik melalui teks, gambar, maupun suara yang diimplementasikan ke dalam algoritma Advanced Encryption Standard (AES) yang digunakan sebagai algoritma kriptografi standar Caesar Chiper.

Penelitian selanjutnya yang diteliti oleh Ripto Sudiyarno pada tahun "Modifikasi Metode Base64 Menggunakan Caesar Cipher Dan Kunci Rahasia", masalah pada penelitian ini ketidakseimbangan antara setiap perkembangan suatu teknologi yang tidak diiringi dengan perkembangan pada sistem keamanannya itu sendiri, maka dari itu peneliti melakukan melakukan proteksi terhadap pengamanan teks yang sebelumnya dapat dicrack ini dikombinasikan menggunakan algoritma Caesar sebagai kunci untuk membuka data teks dengan diterapkanya dua algoritma ini dapat meminimilisir isi dari keaslian data tersebut[10].

2.2 Tinjauan Pustaka

2.2.1 Keamanan Data

Keamanan data melibatkan upaya untuk melindungi integritas, kerahasiaan, dan ketersediaan data dari ancaman dan risiko yang dapat mengakibatkan akses tidak sah, perubahan yang tidak diinginkan, pencurian, atau kehilangan data. Beberapa aspek penting yang perlu dipertimbangkan untuk menjaga keamanan data meliputi enkripsi data, pengelolaan akses, penyimpanan data yang aman, pemantauan keamanan, kebijakan keamanan dan pelatihan, serta cadangan data[11].Dengan adanya kemungkinan penyadapan data, maka keamanan dalam penyampaian data menjadi sangat penting karena suatu penyampaian data jarak jauh belum tentu memiliki jalur yang aman dari penyadapan atau pembobolan yang tidak sah. Masalah keamanan merupakan salah satu aspek terpenting dari suatu sistem informasi. Maka dari itu dibutuhkan keamanan informasi menggunakan kriptografi. Algoritma base64 dalam perubahan data file dan AES (Advanced Encryption Standart) sebagai keamanan menggunakan kunci diimplementasikan untuk melakukan enkripsi dan dekripsi data sebuah file[12].

2.2.2 Pertukaran Data

Pertukaran data dalam kriptografi memiliki sejarah panjang yang dimulai sejak zaman kuno. Pada masa-masa awal, teknik pengacakan dan substitusi karakter digunakan untuk menjaga kerahasiaan pesan. Selama Abad Pertengahan, teknik kriptografi menjadi lebih rumit dengan penggunaan sandi

seperti Vigenère. dengan meningkatnya penggunaan internet dan komunikasi digital, perlindungan data melalui kriptografi menjadi semakin penting. Protokol seperti SSL/TLS digunakan untuk melindungi pertukaran data saat browsing web dan transfer file. Selain itu, teknologi blockchain dan kriptokurensi seperti Bitcoin juga mengandalkan kriptografi. Seiring perkembangan teknologi, kriptografi terus mengalami perkembangan untuk menjawab tantangan keamanan data dalam era digital saat ini[13].

Pertukaran data melibatkan transfer informasi berupa text atau file dari satu pihak ke pihak lain melalui berbagai saluran komunikasi. Untuk menjaga keamanan dan kerahasiaan data selama pertukaran, langkah-langkah seperti enkripsi data, pengamanan jaringan, autentikasi dan otorisasi yang tepat, penggunaan protokol aman, penghapusan data yang aman, auditing dan pemantauan, serta kebijakan dan pelatihan yang baik perlu diperhatikan. Dengan memperhatikan hal-hal tersebut, pertukaran data dapat dilakukan dengan keamanan yang lebih baik.

2.2.3 Ancaman Kebocoran Data

Ancaman kebocoran data terhadap keamanan sistem sering terjadi di dunia digital. Serangan ini dilakukan oleh sekelompok individu atau berkelompok yang berusaha untuk menembus lapisan keamanan suatu sistem. Tujuan mereka adalah mencari, mendapatkan, mengubah, bahkan menghapus informasi yang ada dalam sistem tersebut jika dianggap perlu. Tidak semua upaya peretasan dilakukan secara tersembunyi atau hanya berfokus pada eksploitasi perangkat keras, karena perkembangan keamanan komputer membuatnya semakin sulit untuk ditembus. Teknik ini sering digunakan untuk menyebarkan virus malware atau mencuri informasi penting, seperti identitas seseorang, dan sebagainya. Istilah "social engineering" digunakan untuk berbagai tindakan kejahatan yang dilakukan dengan memanipulasi interaksi manusia. Teknik ini menggunakan manipulasi untuk menipu korban agar melakukan kesalahan keamanan dan memberikan informasi sensitif. Social engineering sering digunakan oleh peretas karena mereka menyadari bahwa manusia adalah sasaran lemah dalam sistem keamanan jaringan. Meskipun sistem keamanan yang baik telah dibangun oleh para pengembang, namun jika

dioperasikan oleh pengguna yang tidak kompeten, sistem masih bisa mudah diserang oleh peretas[14].

2.2.4 File

File adalah entitas dari data yang disimpan didalam sistem file yang dapat diakses dan diatur oleh pengguna. Sebuah file memiliki nama yang unik dalam direktori di mana ia berada. Alamat direktori dimana suatu berkas ditempatkan diistilahkan dengan path. sebuah file berisi aliran data (atau data stream) yang berisi sekumpulan data yang saling berkaitan serta atribut berkas yang disebut dengan properties yang berisi informasi mengenai file yang bersangkutan seperti informasi mengenai kapan sebuah berkas dibuat[15].

2.2.5 Hypertext Preprocessor (PHP)

PHP adalah singkatan dari Hypertext Preprocessor, sebuah scripting yang dijalankan di server. PHP memungkinkan penggunaan kode scripting dalam dokumen HTML, sehingga menghasilkan konten dinamis berdasarkan permintaan. Kelebihan PHP meliputi kesederhanaan bahasa dan mesin scripting, serta kemudahan dalam pengembangan melalui modul dan komponen yang dapat digunakan kembali. PHP juga mendukung konektivitas dengan berbagai jenis server basis data dan merupakan platform open source. Sebagai bahasa pemrograman server-side scripting, PHP digunakan untuk membuat halaman web dinamis. MySQL merupakan sistem manajemen database yang umumnya digunakan dengan PHP, tetapi PHP juga mendukung berbagai sistem database lainnya seperti PostgreSQL, d-base, Oracle, Interbase, Microsoft Access, dan sebagainya[16].

2.2.6 XAMPP

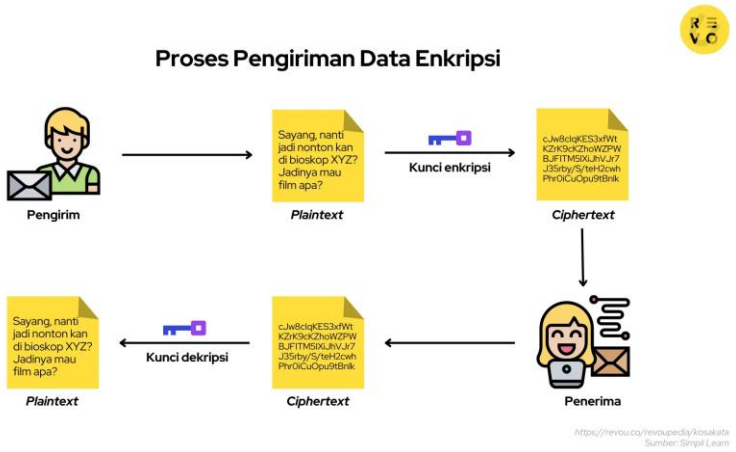
XAMPP adalah sebuah paket perangkat lunak yang menggabungkan beberapa komponen penting untuk pengembangan web dalam satu instalasi yang mudah digunakan. Singkatan XAMPP sendiri terdiri dari nama-nama komponen utamanya, yaitu Cross-platform (X), Apache (A), MySQL (M), PHP (P), dan Perl (P). Dengan XAMPP, pengembang dapat dengan mudah mengatur dan menjalankan server web Apache, server basis data MySQL, serta menggunakan interpreter PHP dan Perl di lingkungan pengembangan web

lokal. Hal ini memungkinkan pengembang untuk menguji dan mengembangkan aplikasi web secara offline sebelum mempublikasikannya ke server yang sebenarnya. XAMPP tersedia untuk berbagai platform seperti Windows, Linux, dan macOS, dan banyak digunakan oleh pengembang web sebagai solusi all-in-one untuk kebutuhan pengembangan web mereka[17].

2.2.7 Kriptografi

Kriptografi memiliki peran penting dalam dunia komputasi karena adanya banyak informasi rahasia yang disimpan dan dikirim melalui media komputer. Tujuan kriptografi adalah melindungi dokumen penting atau rahasia agar tidak dapat diakses oleh pihak yang tidak berhak. Dalam komputasi digital, kriptografi memungkinkan pembuatan teks terenkripsi yang kompleks dan rumit, yang disebut cipher. Terdapat dua jenis kriptografi, yaitu kriptografi klasik dan modern. Kriptografi klasik melibatkan enkripsi karakter per karakter menggunakan alfabet tradisional, sedangkan kriptografi modern beroperasi pada string biner. Selain memberikan keamanan, kriptografi juga memiliki implikasi lain dalam dunia digital. Melalui kriptografi, pesan dapat dikirim secara rahasia, di mana hanya penerima yang memiliki kemampuan untuk menghapus penyandian dan membaca atau mendekripsi pesan tersebut[18].Dalam kriptografi sendiri terdapat beberapa istilah, yaitu: Berikut adalah istilah-istilah yang digunakan dalam bidang kriptografi:

1. Plaintext (M) adalah pesan yang hendak dikirimkan (berisi data asli).
2. Ciphertext (C) adalah pesan ter-enkrip (tersandi) yang merupakan hasil enkripsi.
3. Enkripsi (E) adalah proses pengubahan plaintext menjadi ciphertext.
4. Dekripsi (D) adalah kebalikan dari enkripsi yakni mengubah ciphertext menjadi plaintext, sehingga berupa data awal atau asli.
5. Kunci adalah suatu bilangan yang dirahasiakan yang digunakan dalam proses enkripsi dan dekripsi.



Gambar 2. 1 Diagram Alur Kriptografi(Sumber:https://revou.co/kosakata/enkripsi)

2.2.8 Enkripsi

Pada kriptografi terdapat teknik yang digunakan untuk mengamankan suatu pengaman data yaitu teknik enkripsi. Enkripsi adalah proses mengubah teks asli menjadi berbentuk teks yang susah dipahami oleh manusia yang dimana susah dimengerti jika tidak memiliki dasar pengetahuan kriptografi[19].Enkripsi, yang juga dikenal sebagai proses mengubah teks biasa menjadi teks terenkripsi, melibatkan penggunaan rumus atau algoritma tertentu. Rumus-rumus ini digunakan untuk melakukan transformasi teks sesuai dengan algoritma yang digunakan. Contoh, jika menggunakan algoritma metode yang umum digunakan untuk mengubah data biner menjadi teks ASCII. Proses enkripsi ini melibatkan langkah-langkah seperti mengambil data biner, membaginya menjadi kelompok tiga byte, mengkonversikannya menjadi nilai desimal, dan mengubah nilai desimal menjadi karakter ASCII menggunakan tabel konversi Base64. Karakter-karakter ASCII yang dihasilkan digabungkan menjadi satu string. Jika panjang data tidak habis dibagi tiga, padding menggunakan karakter "=" ditambahkan.

2.2.9 Dekripsi

Teknik dekripsi dapat diartikan dalam sebuah pengamanan teks. Dekripsi adalah proses kebalikan dari enkripsi yaitu mengubah pesan yang sudah terenkripsi menjadi pesan asli. Dekripsi disebut dengan proses pengembalian ciphertext menjadi plaintext[]. Pada proses dekripsi ini proses pengubahan teks yang susah dibaca menjadi teks yang bisa dibaca lagi dengan

cara membuka teks enkripsi dengan kunci yang sudah ditentukan. Contoh, jika yang akan didekripsi menggunakan Algoritma base64 Dalam proses dekripsi Base64, langkah-langkah tertentu diperlukan untuk mengembalikan teks terenkripsi dalam format Base64 menjadi bentuk aslinya. Pertama, periksa apakah ada karakter padding pada akhir teks terenkripsi dan hapus karakter padding jika ada. Kemudian, konversikan teks terenkripsi kembali menjadi nilai desimal menggunakan tabel konversi Base64. Selanjutnya, nilai desimal dikonversikan menjadi kelompok tiga byte data biner. Gabungkan kelompok-kelompok tiga byte data biner yang dihasilkan menjadi satu data biner. Jika ada padding yang ditambahkan selama enkripsi, hapus padding dari data biner. Data biner yang dihasilkan adalah teks terdekripsi dalam bentuk aslinya. Penting untuk dicatat bahwa proses dekripsi Base64 tidak melibatkan penggunaan kunci enkripsi dan bertujuan untuk mengembalikan data biner menjadi teks ASCII asli[20].

2.2.10 Algoritma Kriptografi Simetris

Algoritma simetris adalah juga dikenal sebagai kriptografi kunci-sesama, adalah jenis algoritma kriptografi yang menggunakan kunci yang sama untuk proses enkripsi dan dekripsi. Dalam algoritma ini, pesan yang akan dienkripsi diubah menjadi bentuk terenkripsi dengan menggunakan kunci yang sama, dan kemudian pesan terenkripsi dapat didekripsi kembali menjadi bentuk aslinya menggunakan kunci yang sama[21].

Adapun kelebihan dan kekurangan dalam penggunaan algoritma simteris yaitu:

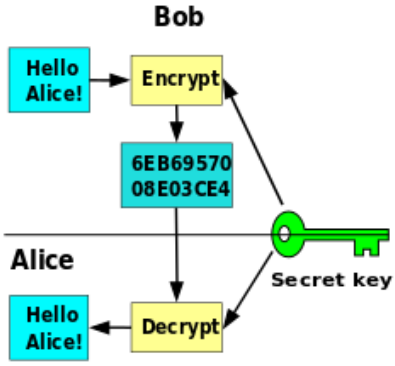
Kelebihan :

1. Kecepatan operasi lebih tinggi bila dibandingkan dengan algoritma asimetrik.
2. Karena kecepatannya yang cukup tinggi, maka dapat digunakan pada sistem real-time.

Kekurangan :

1. Untuk tiap pengiriman pesan dengan pengguna yang berbeda dibutuhkan kunci yang berbeda juga, sehingga akan terjadi kesulitan dalam manajemen kunci tersebut

Berikut contoh diagram dari algoritma simetris :



Gambar 2. 2 Diagram proses enkripsi dan dekripsi algoritma simteris

(sumber : https://p3mpbc.uma.ac.id/2023/01/07/perbedaan-simetris-dan-asimetris-pada-kriptografi/)

2.2.11 Algoritma Kriptografi Asimetris

juga dikenal sebagai kriptografi kunci publik, adalah jenis algoritma kriptografi yang menggunakan sepasang kunci yang berbeda untuk proses enkripsi dan dekripsi. Dalam algoritma ini, terdapat kunci publik yang digunakan untuk enkripsi pesan, sedangkan kunci privat digunakan untuk dekripsi pesan[22]. Pada gambar 2.3 dijelaskan diagram proses enkripsi dan dekripsi algoritma asimetris.

Adapun kelebihan dan kekurangan dalam penggunaan algoritma simteris yaitu:

Kelebihan :

1. Masalah keamanan pada distribusi kunci dapat lebih baik.
2. Masalah manajemen kunci yang lebih baik karena jumlah kunci yang lebih sedikit.

Kekurangan :

1. Kecepatan yang lebih rendah bila dibandingkan dengan algoritma simetris.

2. Untuk tingkat keamanan sama, kunci yang digunakan lebih panjang dibandingkan dengan algoritma simetris

2.2.12 ASCII

ASCII (American Standard Code for Information Interchange) adalah standar pengodean karakter yang digunakan dalam komputasi dan komunikasi data. ASCII mengonversi karakter-karakter ke dalam representasi numerik antara 0 hingga 127. Hal ini memungkinkan komputer untuk memproses dan menyimpan teks dalam bentuk biner. ASCII telah menjadi standar dalam pertukaran data teks di antara sistem komputer yang berbeda. Terdapat variasi ASCII yang diperluas, seperti Extended ASCII, yang memungkinkan representasi karakter tambahan dalam berbagai bahasa dan simbol-simbol tambahan. Standar ASCII mencakup total 128 karakter yang terdiri dari 7 bit, dengan rentang nilai 0 hingga 127. Karakter-karakter ini meliputi huruf-huruf besar dan kecil (A-Z, a-z), angka-angka (0-9), tanda-tanda baca umum, karakter-karakter khusus (seperti karakter baris baru dan tab), dan karakter-karakter kontrol (seperti karakter nol dan bel)[23].

Berikut contoh tabel dari ASCII :

(nul)	0	0000	0x00	(sp)	32	0040	0x20	@	64	0100	0x40	`	96	0140	0x60
(soh)	1	0001	0x01	!	33	0041	0x21	A	65	0101	0x41	a	97	0141	0x61
(stx)	2	0002	0x02	"	34	0042	0x22	B	66	0102	0x42	b	98	0142	0x62
(etx)	3	0003	0x03	#	35	0043	0x23	C	67	0103	0x43	c	99	0143	0x63
(eot)	4	0004	0x04	$	36	0044	0x24	D	68	0104	0x44	d	100	0144	0x64
(enq)	5	0005	0x05	%	37	0045	0x25	E	69	0105	0x45	e	101	0145	0x65
(ack)	6	0006	0x06	&	38	0046	0x26	F	70	0106	0x46	f	102	0146	0x66
(bel)	7	0007	0x07	'	39	0047	0x27	G	71	0107	0x47	g	103	0147	0x67
(bs)	8	0010	0x08	(	40	0050	0x28	H	72	0110	0x48	h	104	0150	0x68
(ht)	9	0011	0x09	)	41	0051	0x29	I	73	0111	0x49	i	105	0151	0x69
(nl)	10	0012	0x0a	*	42	0052	0x2a	J	74	0112	0x4a	j	106	0152	0x6a
(vt)	11	0013	0x0b	+	43	0053	0x2b	K	75	0113	0x4b	k	107	0153	0x6b
(np)	12	0014	0x0c	,	44	0054	0x2c	L	76	0114	0x4c	l	108	0154	0x6c
(cr)	13	0015	0x0d	-	45	0055	0x2d	M	77	0115	0x4d	m	109	0155	0x6d
(so)	14	0016	0x0e	.	46	0056	0x2e	N	78	0116	0x4e	n	110	0156	0x6e
(si)	15	0017	0x0f	/	47	0057	0x2f	O	79	0117	0x4f	o	111	0157	0x6f
(dle)	16	0020	0x10	0	48	0060	0x30	P	80	0120	0x50	p	112	0160	0x70
(dc1)	17	0021	0x11	1	49	0061	0x31	Q	81	0121	0x51	q	113	0161	0x71
(dc2)	18	0022	0x12	2	50	0062	0x32	R	82	0122	0x52	r	114	0162	0x72
(dc3)	19	0023	0x13	3	51	0063	0x33	S	83	0123	0x53	s	115	0163	0x73
(dc4)	20	0024	0x14	4	52	0064	0x34	T	84	0124	0x54	t	116	0164	0x74
(nak)	21	0025	0x15	5	53	0065	0x35	U	85	0125	0x55	u	117	0165	0x75
(syn)	22	0026	0x16	6	54	0066	0x36	V	86	0126	0x56	v	118	0166	0x76
(etb)	23	0027	0x17	7	55	0067	0x37	W	87	0127	0x57	w	119	0167	0x77
(can)	24	0030	0x18	8	56	0070	0x38	X	88	0130	0x58	x	120	0170	0x78
(em)	25	0031	0x19	9	57	0071	0x39	Y	89	0131	0x59	y	121	0171	0x79
(sub)	26	0032	0x1a	:	58	0072	0x3a	Z	90	0132	0x5a	z	122	0172	0x7a

Gambar 2. 3 Tabel ASCII

(sumber : https://komputerbusuk.blogspot.com/2016/11/kode-ascii-dan-tabel.html)

2.2.13 Algoritma Base64

Algoritma Base64 merupakan algoritma kriptografi kunci simetri yang menggunakan pengkodean yang digunakan untuk mengubah data biner menjadi format teks ASCII. Prosesnya melibatkan pembagian data biner menjadi grup dengan panjang tetap, biasanya 3 byte. Setiap grup data kemudian dikonversi menjadi nilai numerik dalam rentang 0 hingga 63. Nilai-nilai numerik ini kemudian diubah menjadi karakter-karakter ASCII menggunakan tabel karakter Base64 yang khusus. Hasilnya adalah teks terenkripsi Base64, yang dapat terdiri dari huruf besar, huruf kecil, angka, dan karakter padding (=) jika diperlukan. Proses dekode Base64 melibatkan langkah-langkah sebaliknya, yaitu mengubah karakter-karakter Base64 kembali menjadi nilai numerik dan mengembalikannya ke bentuk data biner aslinya. Penting untuk dicatat bahwa algoritma Base64 tidak digunakan untuk enkripsi data, tetapi hanya untuk mengubah representasi data biner menjadi format teks yang dapat dibaca[24].

Contoh langkah – langkah yang perlu dilakukan untuk mengenkripsi teks dalam algoritma base64 adalah sebagai berikut:

Contoh proses enkripsi :

a. (M) Plaintext yaitu Hello.
b. Rubah Hello kedalam bentuk binner 'H' = 01001000, 'e' = 01100101, 'l' = 01101100, 'l' = 01101100, 'o' = 01101111.
c. Gabungkan biner menjadi satu urutan 01001000 01100101 01101100 01101100 01101111.
d. Bagi menjadi grup dengan panjang 6 bit 010010 000110 010110 001100 011011 110.
e. Konversi grup ke dalam bentuk desimal 18 6 22 12 27 62.
f. Konversi desimal ke dalam bentuk karakter Base64 SGVsbG8=.

Contoh proses dekripsi :

a. (C) Chipertext yaitu SGVsbG8=.
b. Untuk mendapatkan hasil dekripsi, konversi chipertext diatas kedalam bentuk nilai desimal dari “SGVsbG8=” S = 18, G = 6, V = 21, s = 47, b = 1, G = 6, 8 = 42.

c. Selanjutnya dari hasil konversi desimal dirubah menjadi dalam bentuk biner 8bit yang menghasilkan 18 = 010010, 6 = 000110, 21 = 010101, 47 = 101111, 1 = 000001, 6 = 000110, 42 = 101010.
d. Bagi menjadi grup dengan panjang 6 bit 01001000 01100101 01101100 01101100 01101111.
e. Konversi grup ke dalam bentuk sesuai dengan tabel ASCII 01001000 = 'H', 01100101 = 'e', 01101100 = 'l', 01101100 = 'l', 01101111 = 'o'.
f. Konversi dan gabungkan ke dalam bentuk karakter Base64 Hello.

2.2.14 Algoritma AES (Advanced Standart Encryption)

AES (Advanced Encryption Standard) adalah sebuah algoritma kriptografi yang secara luas digunakan untuk mengamankan data melalui proses enkripsi dan dekripsi. AES menggantikan algoritma sebelumnya, yaitu DES (Data Encryption Standard), karena memberikan tingkat keamanan yang lebih tinggi dan efisiensi yang baik. Kelebihan AES terletak pada tingkat keamanan yang tinggi dan performa yang baik. AES memiliki beberapa varian kunci dengan panjang 128 bit,192 bit, dan 256 bit. Dengan menggunakan pengulangan blok enkripsi dan teknik substitusi dan permutasi yang kompleks, AES mencapai tingkat keamanan yang kuat. Algoritma ini telah diadopsi sebagai standar enkripsi oleh banyak lembaga pemerintah dan industri di seluruh dunia[].Penggunaan luas dan penerimaan yang tinggi dalam berbagai aplikasi, seperti keamanan komunikasi jaringan, enkripsi data pada perangkat penyimpanan, dan pengamanan transaksi keuangan, menunjukkan keandalan dan keamanan AES Sebagai salah satu algoritma enkripsi teraman dan paling banyak digunakan di dunia, AES menjadi landasan dalam menjaga kerahasiaan dan keamanan data dalam konteks komputasi modern. Pada Proses enkripsi awalnya teks asli dibentuk sebagai sebuah state. Kemudian sebelum ronde 1 dimulai blok teks asli dicampur dengan kunci ronde ke-0 (transformasi ini disebut AddRoundKey). Setelah itu, ronde ke-1 sampai dengan ronde ke-(Nr-1) dengan Nr adalah jumlah ronde[25].

AES menggunakan 4 jenis transformasi yaitu:

1. SubBytes

SubBytes adalah langkah yang melibatkan penggantian byte dalam blok data dengan byte baru menggunakan tabel substitusi yang disebut S-box. Setiap byte dalam blok data diganti secara independen sesuai dengan posisinya di S-box. Langkah SubBytes memberikan non-linearitas ke algoritma AES, meningkatkan keamanan dengan memperburuk risiko perubahan data selama enkripsi dan dekripsi. Misalnya, dalam blok data 4x4, setiap byte digantikan oleh byte baru dari S-box, menghasilkan blok data yang telah diubah.

2. ShiftRows

ShiftRows adalah tahap p yang melibatkan pergeseran baris dalam blok data. Pada tahap ini, setiap baris dalam blok data bergeser ke kiri secara siklik. Tujuannya adalah mencampur byte-byte dalam blok data, meningkatkan kompleksitas algoritma, dan memberikan diffusi yang lebih baik. Setelah pergeseran selesai, blok data akan melanjutkan ke tahap-tahap berikutnya seperti MixColumns dan AddRoundKey. Dengan menggabungkan tahap-tahap ini, algoritma AES mencapai tingkat difusi yang kuat dan meningkatkan keamanan data yang dienkripsi dan didekripsi.

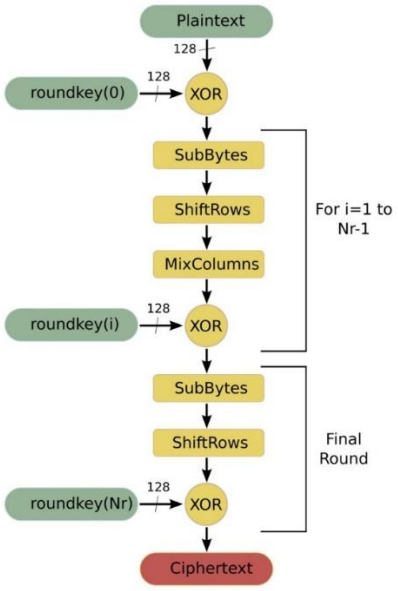
3. MixColums

MixColumns merupakan tahap yang melibatkan operasi matriks pada blok data. Pada tahap ini, setiap kolom dalam blok data diubah menggunakan matriks MixColumns. Transformasi ini melibatkan perkalian dan penjumlahan byte dalam kolom tersebut, dengan menggunakan operasi perkalian polinomial dalam Galois Field. Proses ini bertujuan untuk menyebarkan informasi dalam kolom, menciptakan efek difusi, dan meningkatkan keamanan algoritma AES. Setelah tahap MixColumns selesai, blok data akan melanjutkan ke tahap-tahap berikutnya dalam algoritma AES untuk membentuk enkripsi atau dekripsi yang aman. Dengan menggabungkan tahap-tahap seperti SubBytes, ShiftRows, MixColumns, dan tahap-tahap lainnya, algoritma AES mencapai tingkat difusi yang kuat dan memastikan keamanan dalam enkripsi dan dekripsi data.

4. AddRoundKey

Tahap AddRoundKey dalam AES merupakan langkah penting yang melibatkan XOR antara blok data dengan kunci ronde. Pada tahap ini, setiap byte dalam blok data di-XOR dengan byte yang sesuai dari kunci ronde yang telah dihasilkan sebelumnya. Hal ini mengintegrasikan informasi kunci ke dalam blok data, menciptakan transformasi kompleks yang meningkatkan keamanan. Tahap AddRoundKey dilakukan pada setiap ronde enkripsi dan dekripsi, memastikan difusi data yang kuat dan keamanan algoritma AES. Dengan menggabungkan tahap-tahap seperti SubBytes, ShiftRows, MixColumns, dan AddRoundKey, algoritma AES mencapai tingkat difusi yang kuat dan keandalan dalam enkripsi dan dekripsi data.

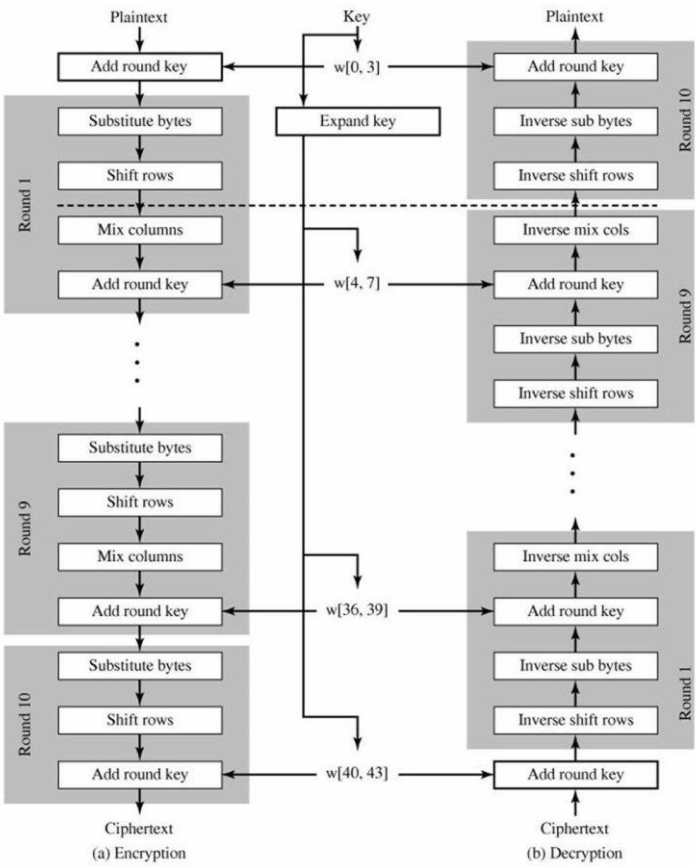
Pada ronde terakhir yaitu ronde ke-Nr dilakukan tranformasi serupa dengan ronde lain namun tanpa tranformasi serupa dengan ronde lain namun tanpa mixColumns.



Gambar 2. 4 Diagram Algoritma AES (sumber: https://www.researchgate.net/figure/Flowchart-of-the-AES-algorithm-Encryption-process_fig4_233828516)

Algoritma AES dapat didekripsikan seperti gambar 2.4 Algoritma dekripsi AES menggunakan transformasi invers dari semua transformasi dasar yang digunakan dalam algoritma enkripsi AES. Transformasi dasar tersebut meliputi

InvSubBytes, InvShiftRows, dan InvMixColumns. Selain itu, transformasi AddRoundKey juga bersifat self-invers, tetapi dengan syarat bahwa kunci yang digunakan sama dengan kunci enkripsi.



Gambar 2. 5 Proses Enkripsi dan Dekripsi *(Sumber: http://studyinformatics.blogspot.com/2012/07/aes-advanced-encryption-standard.html)*

Gambar 2.4 menggambarkan proses enkripsi dan dekripsi menggunakan AES. Untuk melakukan penyandian AES, diperlukan kunci ronde yang digunakan dalam setiap putaran transformasi. Kunci ronde ini dihasilkan melalui proses ekspansi dari kunci AES. Bagian ini menjelaskan bagaimana kunci ronde dihasilkan dari kunci AES. Jika kunci AES memiliki panjang 128ibit atau 4 kata, maka akan menghasilkan sebuah array yang terdiri dari 44 kata yang akan menjadi kunci

Contoh Enkripsi :

M (Plaintext) = Mentari

K (Key) = TOKOSWEETAMIRAHH

1. Perhitungan Enkripsi

   Plaintext dalam Hexadecimal (128 bits): 4D 45 4E 54 41 52 49 14 14 14 14 14 14 14 14 14

   Key dalam Hexadecimal (128 bits): 54 4F 4B 4F 53 57 45 45 54 41 4D 49 52 41 48 48

   a) Key Schedule

	x0	x1	x2	x3	x4	x5	x6	x7	x8	x9	xa	xb	xc	xd	xe	xf
0x	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
1x	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
2x	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
3x	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
4x	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
5x	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
6x	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
7x	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
8x	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
9x	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
ax	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
bx	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
cx	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
dx	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
ex	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
fx	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

Gambar 2. 6 Nilai S-Box

01	02	04	08	10	20	40	80	1b	36
00	00	00	00	00	00	00	00	00	00
00	00	00	00	00	00	00	00	00	00
00	00	00	00	00	00	00	00	00	00

Gambar 2. 7 Nilai Rcon

Dengan Menggunakan

Wi-1 Wi Wi-2 Wi Wi-10 Wi

54	53	54	52													
4F	57	41	41													
4B	45	4D	48													
4F	45	49	48													

Mencari Nilai Wi – 1 Wi :

41		83
48		52
48		52
52		0

41		83		01		D6
48		52		00	=	1D
48		52		00		19
52		00		00		4F

Adapun cara perhitungan manualnya :

54 Hex = 01010100
83 Hex = 10000011
01 Hex = 00000001
Hasil = 11010110 (Bin) = D6 (Hex)

Wi-1 Wi Wi-2 Wi Wi-10 Wi

54	53	54	52	D6												
4F	57	41	41	1D												
4B	45	4D	48	19												
4F	45	49	48	4F												

53		D6		85
57		1D	=	4A
45		19		5C
45		4F		A

Adapun Cara Perhitungan manualnya :

53 Hex = 01010011
D6Hex = 11010110
Hasil = 10000101 (Bin) = 85 (Hex)

Dengan dilakukan perhitungan seperti jalan di atas, maka didapatkan hasil untuk Key Schedule sebagai berikut:

Wi-1 Wi Wi-2 Wi Wi-10 Wi

54	53	54	52	D6	85	D1	83	02	87	56	D5		52	31	4F	31
4F	57	41	41	1D	4A	0B	4A	D6	9C	97	DD		94	40	B1	5B
4B	45	4D	48	19	5C	11	59	32	6E	7F	26		8C	14	EE	A1
4F	45	49	48	4F	0A	43	0B	A3	A9	EA	E1		20	A4	2D	66

Round 1 Round 2 Round 10

b) SubBytes

4D	41	14	14		54	53	54	52		19	12	40	46
45	52	14	14		4F	57	41	41	=	0A	5	55	55
4E	49	14	14		4B	45	4D	48		5	0C	59	5C
54	14	14	14		4F	45	49	48		1B	51	5D	5C

19	12	40	46								D4	C9	9	5A
0A	5	55	55	Konversi Menggunakan S- Box							67	6B	FC	FC
5	0C	59	5C								6B	FE	CB	4A
1B	51	5D	5C								AF	D1	4C	4A

c) ShiftRows

D4	C9	9	5A						
67	6B	FC	FC		Rotate Byte 1 <--				
6B	FE	CB	4A		Rotate Byte 2 <--				
AF	D1	4C	4A		Rotate Byte 3 <--				

Hasil

D4	C9	9	5A
6B	FC	FC	67
CB	4A	6B	FC
4A	AF	D1	4C

d) MixColumns

D4	C9	9	5A		2	3	1	1		D4
6B	FC	FC	67		1	2	3	1		6B
CB	4A	6B	FC		1	1	2	3		CB
4A	AF	D1	4C		3	1	1	2		4A

Karena hasil untuk kolom pertama sudah didapatkan, maka dilakukan perhitungan untuk kolom berikutnya sehingga didapatkan hasil akhir dari MixColumn sebagai berikut:

D4	C9	9	5A		2	3	1	1		D4		8F
6B	FC	FC	67		1	2	3	1		6B	=	0E
CB	4A	6B	FC		1	1	2	3		CB		EC
4A	AF	D1	4C		3	1	1	2		4A		53

Hasil MixColums

8F	73	B7	AF
0E	5B	86	C1
EC	4B	4B	0E
53	B3	35	EF

e) AddRoundKey

Adapun Pencarian AddRoundKey 1 adalah sebagai berikut:

8F	73	B7	AF		D6	85	D1	83		59	F6	66	2C
0E	5B	86	C1		1D	4A	0B	4A	=	13	11	8D	8B
EC	4B	4B	0E		19	5C	11	59		F5	17	5A	57
53	B3	35	EF		4F	0A	43	0B		1C	B9	76	E4

MixColums RoundKey 1 AddRoundKey

Untuk cara perhitungannya dengan melakukan Xor terhadap kolom MixColumn dengan RoundKey, dengan contoh sebagai berikut:

8F		D6	=	59
0E		1D		
EC		19		
53		4F		

8F Hex = 1000 1111
D6 Hex = 1101 0110
Hasil Xor = 0101 1001 (Bin) = 59 (Hex)

Dengan cara yang sama, sehingga dihasilkan untuk AddRoundKey 1 sebagai berikut:

59	F6	66	2C
13	11	8D	8B
F5	17	5A	57
1C	B9	76	E4

Untuk mendapatkan hasil akhir dari Enkripsi Metode AES, lakukan 4 tahapan proses transformasi tersebut dilakukan sembilan kali lagi (dengan total sepuluh kali transformasi). Namun, untuk transformasi MixColumns tidak dilakukan pada transformasi terkahir (ke-10).

After SubBytes

Round 2

CB	42	33	71
7D	82	5D	3D
E6	F0	BE	5B
9C	56	38	69

Round 3

A6	26	C6	BC
37	59	56	4D
5C	BC	4A	EE
2B	D6	E8	73

After Shiftrow

Round 2

CB	42	33	71
82	5D	3D	7D
BE	5B	E6	F0
69	9C	56	38

Round 3

A6	26	C6	BC
59	56	4D	37
4A	EE	5C	BC
73	2B	D6	E8

After MixColums

Round 2

C7	A4	91	AD
64	89	2E	B8
95	16	23	BF
A8	E3	22	6E

Round 3

85	73	CA	6E
B9	88	6E	E5
FE	CA	52	CB
04	84	F7	9F

Round Key

Round 2

02	87	56	D5
D6	9C	97	DD
32	6E	7F	26
A3	A9	EA	E1

Round 3

C7	40	16	C3
21	BD	2A	F7
CA	A4	DB	FD
A0	09	E3	02

=

=

After Round Key

Round 2

C5	23	C7	78
B2	15	B9	65
A7	78	5C	99
0B	4A	C8	8F

Round 3

42	33	DC	AD
98	35	44	12
34	6E	89	36
A4	8D	14	9D

Sampai hasil AddRoundKey ke-10

E5	6C	99	B4		E5	6C	99	B4		52	31	4F	31		B7	5D	D6	85
21	E1	33	6E	□	E1	33	6E	21	□	94	40	B1	5B	=	75	73	DF	7A
2E	72	BE	E5		BE	E5	2E	72		8C	14	EE	A1		32	F1	C0	D3
DD	9D	2B	57		57	DD	9D	2B		20	A4	2D	66		77	79	B0	4D

Dari hasil perhitungan di atas, maka didapatkan hasil Enkripsi dengan bilangan Hexadecimal: B7 75 32 77 5D 73 F1 79 D6 DF C0 B0 85 7A D3 4D. Untuk penjabaran hasil dari Enkripsinya adalah sebagai berikut:

Tabel 2. 1 Hasil enkripsi

No.	Round	Kode ASCII	Karakter
1	B7	183	.
2	75	117	u
3	32	50	2
4	77	119	w
5	5D	93	]
6	73	115	s
7	F1	241	ñ
8	79	121	y
9	D6	214	Ö
10	DF	223	ß
11	C0	192	À
12	B0	176	o
13	85	133	...
14	7A	122	z
15	D3	211	Ó
16	4D	77	m

2. Perhitungan Dekripsi

Untuk melakukan dekripsi data dari hasil Enkripsi sebelumnya yaitu dengan menggunakan kunci yang sama pada proses Enkripsi. Berikut adalah proses dekripsi dari hasil Ciphertext yang telah diperoleh dari proses Enkripsi.

B7	75	32	77	5D	73	F1	79	D6	DF	C0	B0	85	7A	D3	4D

Kemudian susun 16 byte pertama dari Ciphertext yang telah diubah ke bentuk Hexadecimal ke dalam state 4x4:

B7	5D	D6	85
75	73	DF	7A
32	F1	C0	D3
77	79	B0	4D

Lakukan XOR antara Ciphertext dengan RoundKey Ke-10. Proses ini dinamakan AddInvRoundKey.

B7	5D	D6	85		52	31	4F	31		E5	6C	99	B4
75	73	DF	7A	□	94	40	B1	5B	=	E1	33	6E	21
32	F1	C0	D3		8C	14	EE	A1		BE	E5	2E	72
77	79	B0	4D		20	A4	2D	66		57	DD	9D	2B

Proses AddInvRoundKey di atas masih dalam initial-round, dan akan menjadi masukan untuk ronde ke -1 yang akan diproses dengan 4 transformasi yaitu InvShiftRows, InvShiftRows, AddInvRoundKey dan InvMixColumns.

a. InvShiftRows, lakukan tahapan ini pada hasil initial-round dari AddInvRoundKey yang dieksekusi lewat pergeseran siklik secara memutar. Baris ke dua digeser secara siklik ke kiri tiga kali, baris ke tiga dua kali dan baris ke empat sekali.

E5	6C	99	B4
E1	33	6E	21
BE	E5	2E	72
57	DD	9D	2B

E5	6C	99	B4
21	E1	33	6E
2E	72	BE	E5
DD	9D	2B	57

b. Dari hasil InvShiftRows disubtitusikan dengan nilai pada tabel Inves S-Box, yang dapat dilihat pada gambar berikut:

x \ y	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	52	09	6a	d5	30	36	a5	38	bf	40	a3	9e	81	f3	d7	fb
1	7c	e3	39	82	9b	2f	ff	87	34	8e	43	44	c4	de	e9	cb
2	54	7b	94	32	a6	c2	23	3d	ee	4c	95	0b	42	fa	c3	4e
3	08	2e	a1	66	28	d9	24	b2	76	5b	a2	49	6d	8b	d1	25
4	72	f8	f6	64	86	68	98	16	d4	a4	5c	cc	5d	65	b6	92
5	6c	70	48	50	fd	ed	b9	da	5e	15	46	57	a7	8d	9d	84
6	90	d8	ab	00	8c	bc	d3	0a	f7	e4	58	05	b8	b3	45	06
7	d0	2c	1e	8f	ca	3f	0f	02	c1	af	bd	03	01	13	8a	6b
8	3a	91	11	41	4f	67	dc	ea	97	f2	cf	ce	f0	b4	e6	73
9	96	ac	74	22	e7	ad	35	85	e2	f9	37	e8	1c	75	df	6e
a	47	f1	1a	71	1d	29	c5	89	6f	b7	62	0e	aa	18	be	1b
b	fc	56	3e	4b	c6	d2	79	20	9a	db	c0	fe	78	cd	5a	f4
c	1f	dd	a8	33	88	07	c7	31	b1	12	10	59	27	80	ec	5f
d	60	51	7f	a9	19	b5	4a	0d	2d	e5	7a	9f	93	c9	9c	ef
e	a0	e0	3b	4d	ae	2a	f5	b0	c8	eb	bb	3c	83	53	99	61
f	17	2b	04	7e	ba	77	d6	26	e1	69	14	63	55	21	0c	7d

Gambar 2. 8 Inves S-Box

E5	6C	99	B4
21	E1	33	6E
2E	72	BE	E5
DD	9D	2B	57

=

2A	B8	F9	C6
7B	E0	66	45
C3	1E	5A	2A
C9	75	0B	DA

c. XOR hasil dari InvSubBytes dengan RoundKey ke-9. Proses ini disebut AddInvRoundKey.

2A	B8	F9	C6
7B	E0	66	45
C3	1E	5A	2A
C9	75	0B	DA

E3	63	7E	7E
10	D4	F1	EA
3F	98	FA	4F
D3	84	89	4B

C9	DB	87	B8
6B	34	97	AF
FC	86	A0	65
1A	F1	82	91

d. Hasil dari AddInvRoundKey ditransformasikan oleh InvMixColumns dengan mengoperasikan state kolom demi kolom. Operasi ini dilakukan pada state kolom, dengan mengkoversikan setiap kolom sebagai polinominal.

0E	0B	0D	09
09	0E	0B	0D
0D	09	0E	0B
0B	0D	09	0E

x

$S_{0.1}$
$S_{1.1}$
$S_{2.1}$
$S_{3.1}$

=

$S^{1}_{0.1}$
$S^{1}_{1.1}$
$S^{1}_{2.1}$
$S^{1}_{3.1}$

$s^{0.1}$ = ([0E]. $S_{0.1}$)Xor ([0B]. $S_{1.1}$)Xor([0D]. $S_{2.1}$)Xor([09]. $S_{3.1}$)
= ([0E]. $S_{0.1}$) = (0E). (C9)
= ([0E]. $S_{0.1}$) = (1110). (1100 1001)
= ([0E]. $S_{0.1}$) = $(x^3 + x^2 + x)(x^7 + x^6 + x^3 + 1)$
= ([0E]. $S_{0.1}$) = $x^{10} + x^9 + x^9 + x^8 + x^5 + x^8 + x^7 + x^4 + x + 1$
= ([0E]. $S_{0.1}$) = $x(x^5 + x^4 + x + 1)x^7 + x^5 + x^4 + x + 1$
= ([0E]. $S_{0.1}$) = $x^6 + x^5 + x^2 + x + x^7 + x^5 + x^4 + x + 1$
= ([0E]. $S_{0.1}$) = $x^7 + x^6 + x^4 + x^2 + 1$
= ([0E]. $S_{0.1}$) = **1101 0101**
= ([0B]. $S_{1.1}$) = (0B). (6B)
= ([0B]. $S_{1.1}$) = (1011). (0110 1011)
= ([0B]. $S_{1.1}$) = $(x^3 + x + 1)(x^6 + x^5 + x^3 + x + 1)$
= ([0B]. $S_{1.1}$) = $x^9 + x^8 + x^6 + x^4 + x^3 + x^7 + x^5 + x^4 + x^2 + 1$
= ([0B]. $S_{1.1}$) = $x^9 + x^6 + x^5 + x^2 + 1$
= ([0B]. $S_{1.1}$) = $x(x^4 + x^3 + x + 1) + x^6 + x^5 + x^2 + 1$
= ([0B]. $S_{1.1}$) =x5+x4+x2= ([0B]. $S_{1.1}$) = $x^5 + x^4 + x^2 + x + x^6 + x^5 + x^2 + 1$
= ([0B]. $S_{1.1}$) = $x^6 + x^4 + x + 1$
= ([0B]. $S_{1.1}$) = **0101 0011**
= ([0D]. $S_{2.1}$) = (0D). (FC)
= ([0D]. $S_{2.1}$) = (1101). (0110 1101)
= ([0D]. $S_{2.1}$) = $(x^3 + x^2 + 1)(x^6 + x^5 + x^3 + x^2 + 1)$

= ([0D]. $S_{2.1}$) = $x^9 + x^8 + x^6 + x^5 + x^7 + x^5 + x^8 + x^7 + x^5 + x^4 + 1$
= ([0D]. $S_{2.1}$) = $x^9 + x^6 + x^5 + x^4 + 1$
= ([0D]. $S_{2.1}$) = $x(x^4 + x^3 + x + 1) + x^6 + x^5 + x^4 + 1$
= ([0D]. $S_{2.1}$) = $x^5 + x^4 + x^2 + x) + x^6 + x^5 + x^4 + 1$
= ([0D]. $S_{2.1}$) = $x^6 + x^5 + x^2 + x + 1$
= ([0D]. $S_{2.1}$) = **0110 0111**
= ([09]. $S_{3.1}$) = (09). (1A)
= ([09]. $S_{3.1}$) = (1001). (1111 1001)
= ([09]. $S_{3.1}$) = $(x^3 + 1)(x^7 + x^6 + x^5 + x^4 + x^3 + 1)$
= ([09]. $S_{3.1}$) = $x^{10} + x^9 + x^8 + x^7 + x^6 + 1$
= ([09]. $S_{3.1}$) = $x(x^5 + x^4 + x + 1) + x(x^4 + x^3 + x + 1) + (x^4 + x^3 + x + 1) + x^7 + x^6 + 1$
= ([09]. $S_{3.1}$) = $(x^6 + x^5 + x^2 + x) + (x^5 + x^4 + x^2 + x) + (x^4 + x^3 + x + 1) + x^7 + x^6 + 1$
= ([09]. $S_{3.1}$) = $x^7 + x^3 + x$
= ([09]. $S_{3.1}$)
= **1000 1000** $s^{0.1}$
= 0001 0000 = 10
$s^{1.1}$ = ([0E]. $S_{0.1}$)Xor ([0B]. $S_{1.1}$)Xor([0D]. $S_{2.1}$)Xor([09]. $S_{3.1}$) $s^{1.1}$ = 1101 0011 = D3
$s^{1.2}$ = ([0E]. $S_{0.2}$)Xor([0B]. $S_{1.2}$)Xor([0D]. $S_{2.2}$)Xor([09]. $S_{3.2}$) $s^{1.2}$ = 1010 1101 = AD
$s^{1.3}$ = ([0E]. $S_{0.3}$)Xor([0B]. $S_{1.3}$)Xor([0D]. $S_{2.3}$)Xor([09]. $S_{3.3}$) $s^{1.3}$ = 0010 1010 = 2A

Lakukan perulangan seperti yang di atas, hingga didapatkan hasil InvMixColumns seperti berikut:

C9	DB	87	B8
6B	34	97	AF
FC	86	A0	65
1A	F1	82	91

→

10	45	82	75
D3	46	14	62
AD	33	C1	75
2A	A8	65	81

Proses di atas diulang sampai 10 kali putaran (round). Berikut adalah hasil dari Dekripsi hingga round ke 10:

2B	E8	0C	3F
6E	6D	BD	80
C7	98	7A	D3
DF	E3	EB	57

91	15	9B	38
D0	B8	33	1
B0	94	2E	CD
9C	F3	8D	42

4F	77	92	28
AC	48	67	38
12	5F	FE	7D
70	9E	DD	F2

DA	FC	42	97
78	47	8D	95
C0	FA	F2	26
1E	DB	1E	51

00	FC	12	9E
B7	B3	7A	59
0D	9	98	E3
F9	D2	FA	92

85	73	CA	6E
B9	88	6E	E5
FE	CA	52	CB
04	84	F7	9F

C7	A4	91	AD
64	89	2E	B8
95	16	23	BF
A8	E3	22	6E

8F	73	B7	AF
0E	5B	86	C1
EC	4B	4B	0E
53	B3	35	EF

4D	41	14	14
45	52	14	14
4E	49	14	14
54	14	14	14

Untuk round ke-10 transformasi InvMixColumns tidak dilakukan, hanya transformasi InvShiftRow, InvSubBytes dan AddInvRoundKey[]. Berdasarkan proses yang dilakukan maka akan didapatkan hasil dalam bentuk karakter pada tabel ASCII sebagai berikut:

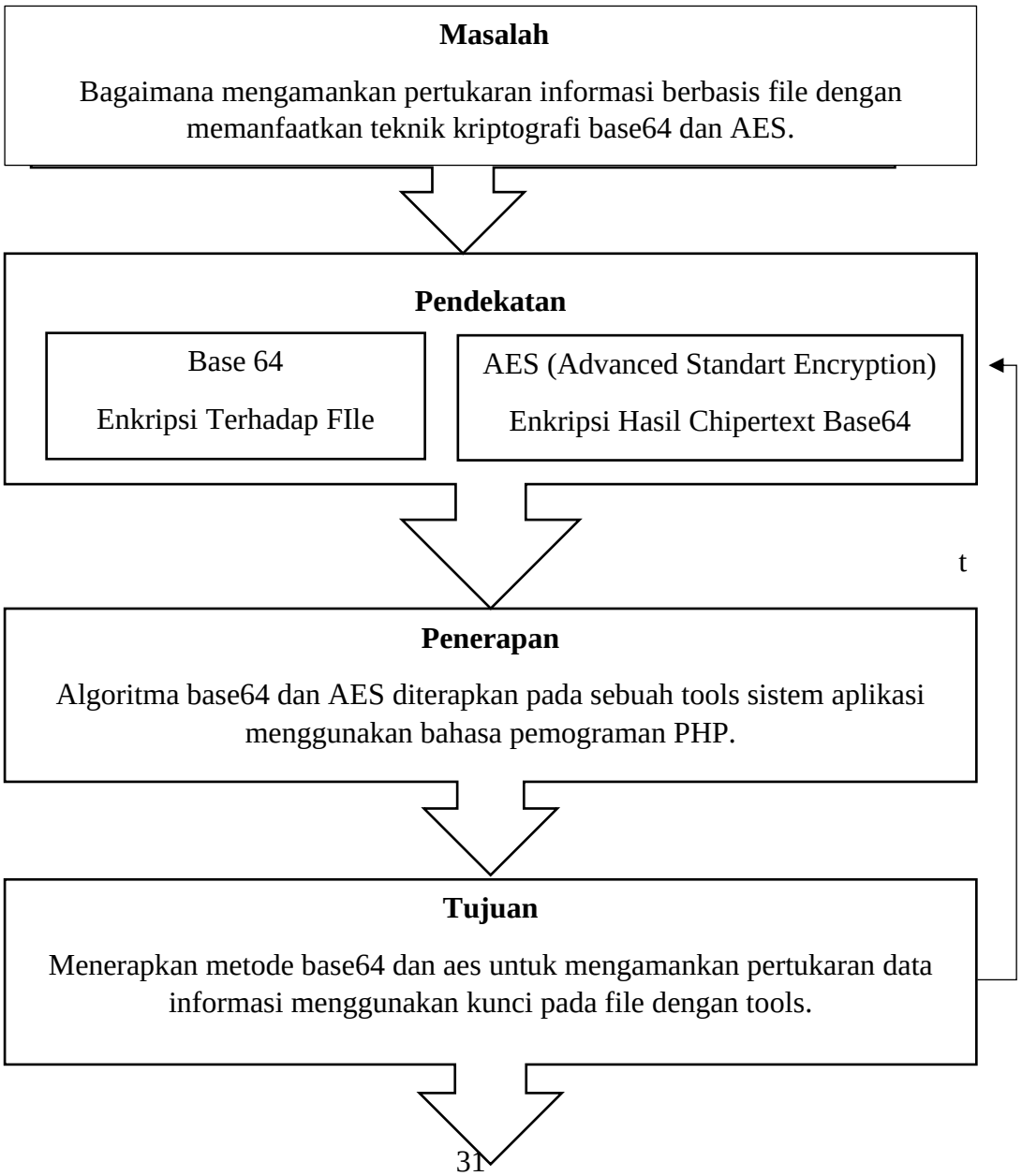
Tabel 2. 2 Hasil dekripsi

No.	Round	Kode ASCII	Karakter
1	4D	77	M
2	45	69	e
3	4E	78	n
4	54	84	t
5	41	65	a
6	52	82	r
7	49	73	i
8	14	20	
9	14	20	
10	14	20	
11	14	20	
12	14	20	
13	14	20	
14	14	20	
15	14	20	
16	14	20	

2.2.15 Verifikasi dan validasi

Verifikasi dan validasi adalah proses penting dalam pengembangan perangkat lunak untuk memastikan bahwa perangkat lunak sesuai dengan spesifikasinya dan memenuhi kebutuhan pelanggan. Verifikasi berfokus pada memeriksa kesesuaian perangkat lunak dengan spesifikasi yang telah ditetapkan, sedangkan validasi melibatkan penilaian keseluruhan terhadap perangkat lunak untuk memastikan bahwa itu memenuhi harapan pengguna atau pelanggan. Melalui verifikasi dan validasi yang komprehensif, perangkat lunak dapat dipastikan berfungsi dengan benar dan memenuhi kebutuhan yang ada.

2.3 Kerangka Pemikiran



Hasil

Hasil berupa alat simulasi enkripsi dan dekripsi untuk penyandian informasi menggunakan kunci kedalam file.

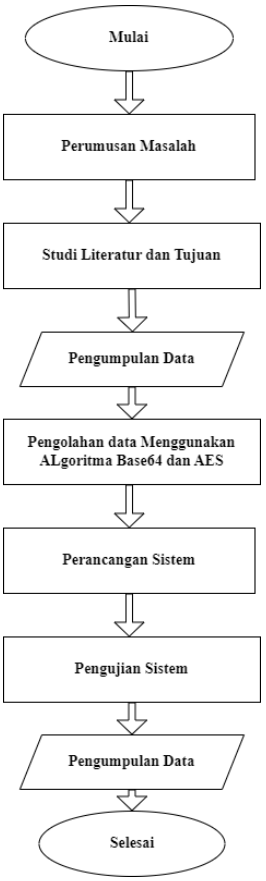
BAB III

METODOLOGI PENELITIAN

3.1 Studi Literatur

Pada tahap ini diteliti beberapa alat dan konsep yang akan digunakan untuk membuat tugas akhir ini. Penelitian dilakukan terhadap beberapa tools yang akan digunakan untuk membangun sistem pada tugas akhir ini.Penelitian juga dilakukan dengan mempelajari berbagai buku teks, petunjuk perkuliahan, jurnal, karya ilmiah, tugas akhir dan disertasi yang berkaitan dengan pokok bahasan yang akan dibahas yaitu kriptografi khususnya metode base64 dan AES (Advanced Standart Encryption), sehingga penulis memperoleh referensi yang kuat ketika menentukan metode yang tepat untuk memecahkan masalah penelitian.

3.1.1 Skema Penelitian



Gambar 3. 1 Skema penelitian

3.2 Pengumpulan Data

Saat mengumpulkan sumber data, peneliti mengumpulkan sumber data dari public berupa data file. sumber data penelitian yang diperoleh secara tidak langsung (diperoleh atau direkam oleh pihak lain) oleh seorang peneliti melalui perantara. Data ini berupa pesan file. Para peneliti memperoleh data dengan mencari data file secara online di kumpulan data, yang tersedia secara gratis untuk umum.

3.3 Analisa Data

Analisis data merupakan bagian dari proses penyelesaian masalah keamanan, yang melibatkan tahap analisis data. Dalam analisis data, dilakukan langkah-langkah sebagai berikut:

1. Pengumpulan data yang berfungsi untuk memperoleh data yang diperlukan dalam pengujian program.
2. Pengelompokan data sesuai dengan jenis dan fungsinya.
3. Mencari data dalam berjenis File (pdf) yang akan dienkripsi dalam penelitian.

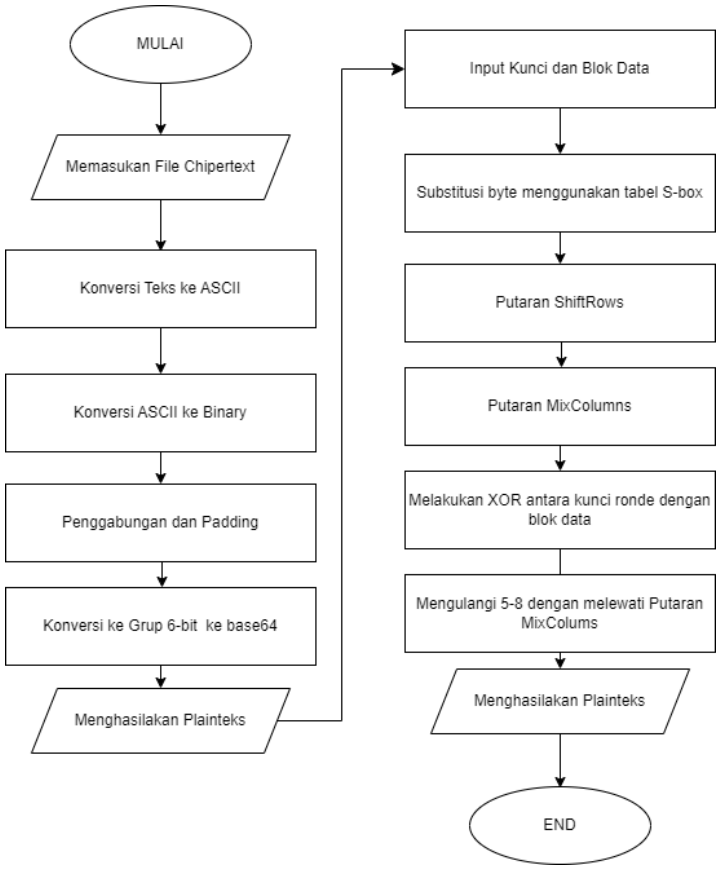
3.4 Gambaran Umum Penerapan Algoritma

Penerapan algoritma dalam keamanan file digunakan untuk melindungi kerahasiaan, integritas, dan otentikasi informasi yang dikirim melalui media elektronik seperti email, pesan teks, dll. Salah satu algoritme yang sering digunakan adalah algoritme kriptografi, yang tujuannya adalah untuk mengubah suatu pesan yang akan dikirim menjadi bentuk yang tidak dapat dibaca oleh pihak yang tidak berwenang. Saat menerapkan algoritma enkripsi, ada beberapa hal yang perlu diperhatikan agar pesan yang dikirim tetap aman. Pertama, gunakan kunci yang kuat dan kompleks agar tidak mudah ditebak oleh pihak yang tidak berwenang. Kedua, serangan brute-force dicegah dengan membatasi jumlah upaya oleh pihak yang mencoba membuka pesan terenkripsi. Ketiga, cegah serangan lain, seperti serangan man-in-the-middle, serangan replay, dll., dengan menggunakan protokol keamanan yang benar.

Penerapan metode yang digunakan adalah metode base64 dan algoritma Advanced Standart Encryption teks yang semula encoding dari penggunaan base64 file dan dienkripsi menggunakan kunci AES. Metode ini diterapkan pada sebuah aplikasi kriptografi yang dapat mengenkripsi sebuah pesan file dan meneruskan hasilnya sebagai file pesan ke aplikasi pengiriman pesan seperti aplikasi Whatsapp, Email, dan sejenisnya.

3.5 Flowchart Enkripsi

Flowchart sistem mennggambarkan urutan proses secara mendetail dan hubungan antara satu proses dengan proses lainnya. Flowchart sistem untuk enkripsi data dapat dilihat pada Gambar.

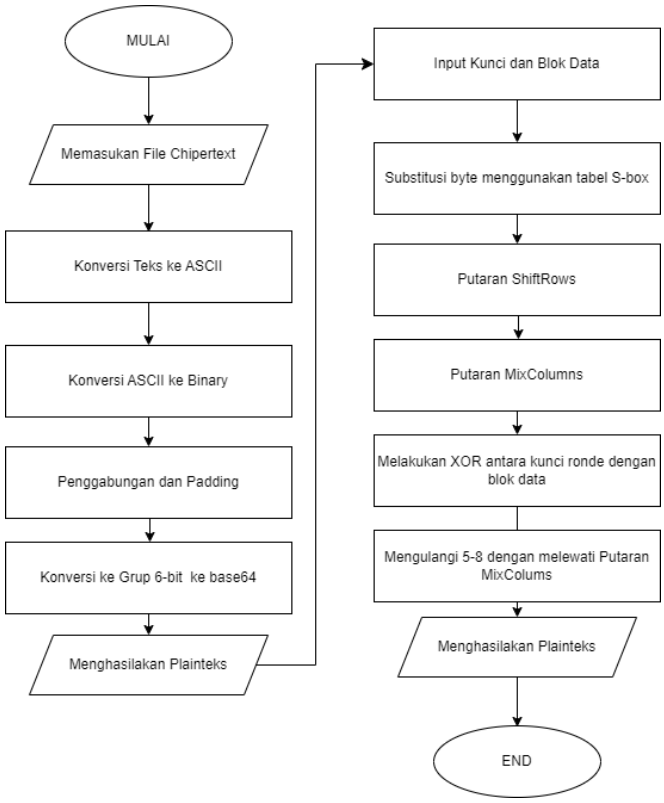


Gambar 3. 2 Flowchart enkripsi

Berdasarkan gambar 3.1, Penjabaran dari flowchart enkripsi adalah teks string sebagai plaintext berupa teks biasa yang terdiri dari abjad A-Z. Proses enkripsinya adalah teks string dienkripsi dengan cara mengubah teks biasa yang

semulanya bisa dibaca menjadi teks yang tidak bisa dibaca dan dimengerti menggunakan algoritma base64 dan AES sehingga keluaran dari teks yang terenkripsi menjadi ciphertext.

3.6 Flowchart Dekripsi



Gambar 3. 3 Flowchart dekripsi

Berdasarkan Gambar 3.2, Penjabaran dari flowchart dekripsi adalah teks yang terenkripsi (ciphertext) akan didekripsi menggunakan proses metode algoritma base64 dan AES, yang mana ciphertext akan dirubah menjadi plaintext kembali. Hasil keluaran dari dekripsi merupakan teks yang bisa dibaca secara normal.

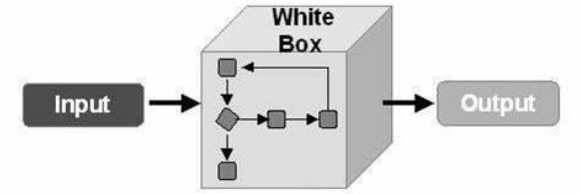
3.7 Pengujian Metode Algoritma

Teknik pengujian dilakukan dengan menggunakan whitebox dan menggunakan file berbeda-beda. Dan dilakukan untuk proses enkripsi dan dekripsi teks, dimana aplikasi yang digunakan untuk menguji penerapan algoritma ini adalah berbasis web. Dalam pengujian white box, penguji biasanya menggunakan teknik seperti analisis jalur dan analisis titik putus untuk menemukan kelemahan dalam kode program. Analisis jalur melibatkan

pelacakan semua kemungkinan jalur yang dapat diambil oleh program saat menjalankan fungsi tertentu, sementara analisis titik putus melibatkan identifikasi titik di mana program dapat berhenti atau terganggu.

Setelah kesalahan kode progam ditemukan bisa menggunakan metode debuging untuk melihat suatu kesalahan dalam penulisan kode progam, penguji biasanya memiliki akses penuh ke kode program dan lingkungan pengembangan perangkat lunak. Oleh karena itu, pengujian white-box dapat memberikan hasil yang akurat dan terperinci tentang keamanan algoritme dan kendala program. Namun, pengujian white-box bisa lebih memakan waktu dan sumber daya intensif daripada metode pengujian lainnya.

Beberapa teknik yang dapat digunakan dalam white box testing antara lain branch coverage, statement coverage, path coverage, dan condition coverage. Setiap teknik memiliki kelebihan dan kekurangan masing-masing, sehingga sebaiknya teknik yang digunakan disesuaikan dengan kebutuhan dan kondisi sistem yang diuji.



Gambar 3. 4 Skema Whitebox

3.8 White Box Testing

Pengujian white box merupakan cara pengujian dengan melihat ke bagian modul guna meneliti kode-kode program yang ada, serta menganalisis apakah terdapat kesalahan atau tidak. Jika ada modul yang menghasilkan output yang tidak sesuai dengan proses program yang dilakukan, maka baris-baris kode program, variable, serta parameter yang terlibat pada unit tersebut akan dicek satu persatu dan diperbaiki. Berikut adalah pengujian dari kode program kriptografi rail fence cipher.

Table 3. 1 Skenario Pengujian

Skenario	**Hasil Skenario**	**Menampilkan hasil chipertext**	**validasi**
Input Paintext dengan key	Menampilkan hasil chipertex	Menampilkan hasil chipertex	
Input Plaintext tanpa key	Menampilkan error	Menampilkan error	
Input ciphertext dengan key	Menampilkan hasil plaintext	Menampilkan hasil plaintext	
Input ciphertext tanpa key	Menampilkan error	Menampilkan error	

Table 3. 2 Kriteria Pengujian

Keterangan	
Valid	V
Invalid	I

DAFTAR PUSTAKA

[1] A. Hermawan and H. I. E. Ujianto, "InfoTekJar : Jurnal Nasional Informatika dan Teknologi Jaringan Implementasi Enkripsi Data Menggunakan Kombinasi AES dan RSA," *J. Nas. Inform. dan Teknol.*, vol. 2, no. 1, 2021.

[2] M. Azwar, M. Qulub, and F. Fatimatuzzahra, "Kombinasi Metode Kriptografi Subsitusi Dalam Pengaman Pesan dan Informasi," *ICIT J.*, vol. 8, no. 2, pp. 172–180, 2022, doi: 10.33050/icit.v8i2.2407.

[3] Imam Riadi, Abdul Fadlil, and Fahmi Auliya Tsani, "Pengamanan Citra Digital Berbasis Kriptografi Menggunakan Algoritma Vigenere Cipher," *JISKA (Jurnal Inform. Sunan Kalijaga)*, vol. 7, no. 1, pp. 33–45, 2022, doi: 10.14421/jiska.2022.7.1.33-45.

[4] E. Yoppi and Z. Situmorang, "Aplikasi Tanda Tangan Digital Dengan Algoritma Gost Untuk Keamanan Pengiriman File Dokumen," *KAKIFIKOM (Kumpulan Artik. Karya Ilm. Fak. Ilmu Komputer)*, vol. 03, no. 01, pp. 13–21, 2021, [Online]. Available: http://dx.doi.org/10.54367/kakifikom.v3i1.1196%0Ahttp://ejournal.ust.ac.id/index.php/KAKIFIKOM/article/download/1196/pdf1.

[5] F. Efendi, J. Informatika, U. A. Yogyakarta, and C. Catur, "Implementasi Kriptografi dalam Sistem Keamanan Anjungan Tunai Mandiri," vol. 5, no. 1, pp. 51–54, 2019.

[6] T. Lovian and I. Fitri, "Implementasi Algoritma Base64 Sebagai Tingkat Keamanan Data Pada Website Sistem Informasi Pencatat Barang," vol. 6, pp. 692–700, 2022, doi: 10.30865/mib.v6i1.3513.

[7] Harry Witriyono and Sandhy Fernandez, "Implementasi Enkripsi Base64, Hashing SHA1 dan MD5 pada QR Code Presensi Kuliah," *SATIN - Sains dan Teknol. Inf.*, vol. 7, no. 2, pp. 73–81, 2021, doi: 10.33372/stn.v7i2.724.

[8] M. Azhari, D. I. Mulyana, F. J. Perwitosari, and F. Ali, "Implementasi Pengamanan Data pada Dokumen Menggunakan Algoritma Kriptografi Advanced Encryption Standard (AES)," *J. Pendidik. Sains dan Komput.*, vol. 2, no. 01, pp. 163–171, 2022, doi: 10.47709/jpsk.v2i01.1390.

[9] M. Sari, H. D. Purnomo, and I. Sembiring, "Review : Algoritma Kriptografi Sistem Keamanan SMS di Android," *J. Inf. Technol.*, vol. 2, no. 1, pp. 11–15, 2022, doi: 10.46229/jifotech.v2i1.292.

[10] R. Sudiyarno, "Modifikasi Metode Base64 Menggunakan Caesar Cipher dan Kunci Rahasia," *J. Rekayasa Teknol. Inf.*, vol. 5, no. 1, p. 1, 2021, doi: 10.30872/jurti.v5i1.4271.

[11] R. Ocanitra and M. Ryansyah, "Implementasi Sistem Keamanan Jaringan Menggunakan Firewall Security Port pada Vitaa Multi Oxygen," vol. 7, no. 1, pp. 52–59, 2019.

[12] R. Nuari and N. Ratama, "Implementasi Algoritma Kriptografi AES

(Advanced Encryption Standard) 128 Bit Untuk Pengamanan Dokumen Shipping," *J. Artif. Intell. Innov. Appl.*, vol. 1, no. 2, pp. 2716–1501, 2020, [Online]. Available: http://openjournal.unpam.ac.id/index.php/JOAIIA.

[13] M. P. Sipahutar, "Berbagai Kasus Penyerangan Terhadap Kriptografi," 2019, [Online]. Available: https://informatika.stei.itb.ac.id/.

[14] E. M. Safitri, Z. Ameilindra, and R. Yulianti, "Analisis Teknik Social Engineering Sebagai Ancaman Dalam Keamanan Sistem Informasi: Studi Literatur," *J. Ilm. Teknol. Inf. dan Robot.*, vol. 2, pp. 21–26, 2020.

[15] S. M. Intani and F. Salsabila, "Implementasi Kriptografi AES pada File Word," no. December, 2019, [Online]. Available: https://www.researchgate.net/publication/338192815.

[16] Suparyanto dan Rosad (2015, "Aplikasi Penilaian Kinerja Guru Berdasarkan Buku Pedoman Pelaksanaan Penilaian Kinerja Guru," *Suparyanto dan Rosad (2015*, vol. 5, no. 3, pp. 248–253, 2020.

[17] Nirsal, Rusmala, and Syafriadi, "Desain Dan Implementasi Sistem Pembelajaran Berbasis E-Learning Pada Sekolah Menengah Pertama Negeri 1 Pakue Tengah," *J. Ilm. d'Computare*, vol. 10, pp. 30–37, 2020, [Online]. Available: http://www.elsevier.com/locate/scp.

[18] T. S. Alasi, R. Wanto, and V. H. Sitanggang, "Implementasi Kriptografi Algoritma Idea Pada Keamanan Data Teks Berbasis Android," *J. Inf. Komput. Log.*, vol. 2, no. 1, pp. 1–4, 2021.

[19] M. Ziaurrahman, E. Utami, and F. W. Wibowo, "Modifikasi Kriptografi Klasik Vigenere Cipher Menggunakan One Time Pad Dengan Enkripsi Berlanjut," *J. Inform. dan Teknol. Inf.*, vol. 4, no. 1, pp. 63–68, 2019.

[20] C. Saefudin, G. Abdillah, and A. Maspupah, "Pengamanan Source Code Program Menggunakan Algoritma Advanced Encryption Standard Dan Algoritma Base64," *Semin. Nas. Apl. Teknol. Inf.*, p. 2019, 2019.

[21] T. H. Saputro *et al.*, "Survei tentang algoritma kriptografi asimetris," pp. 67–72, 2019.

[22] J. Pseudocode, R. Efendi, and B. Susilo, "Vigenere Cipher Dalam Aplikasi," vol. III, pp. 69–82, 2016.

[23] N. P. S. Winarno and T. A. Cahyanto, "Penggunaan Karakter Kontrol ASCII Untuk Integrasi Data Pada Hasil Enkripsi Algoritma Caesar Cipher," *INFORMAL Informatics J.*, vol. 6, no. 3, p. 197, 2021, doi: 10.19184/isj.v6i3.21091.

[24] S. Supiyandi, H. Hermansyah, and K. A. P. Sembiring, "Implementasi dan Penggunaan Algoritma Base64 dalam Pengamanan File Video," *J. Media Inform. Budidarma*, vol. 4, no. 2, p. 340, 2020, doi: 10.30865/mib.v4i2.2042.

[25] A. Rachmayanti and W. Wirawan, "Implementasi Algoritma Advanced Encryption Standard (AES) pada Jaringan Internet of Things (IoT) untuk Mendukung Smart Healthcare," *J. Tek. ITS*, vol. 11, no. 3, 2022, doi:

10.12962/j23373539.v11i3.97042.