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

Dosen Pembimbing : TEGUH TAMRIN, S.Kom, M.Kom.

Disusun Oleh :

Ahmad Suroyya Mutsaddad

(191240000937)

PROGRAM STUDI TEKNIK INFORMATIKA

FAKULTAS SAINS DAN TEKNOLOGI

UNIVERSITAS ISLAM NAHDLATUL ULAMA JEPARA

2022

PERSETUJUAN PEMBIMBING

DAFTAR ISI

DAFTAR GAMBAR

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. Saat ini, kriptografi modern menghasilkan teknik yang lebih kuat seperti kriptografi kunci publik, kriptografi homomorfik, dan kriptografi kuantum,Kriptografi hanya untuk pengelola data yang bertujuan untuk mengamankan data yang sederhana dan bersifat sementara, tapi setelah terbarukan kriptografi ialah data yang enkripsi serta data dekripsi untuk keamanan [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. Sejarah keamanan kriptografi mencatat beberapa insiden keamanan penting. Salah satu insiden paling terkenal adalah pecahnya mesin Enigma Jerman yang digunakan dalam Perang Dunia II oleh Alan Turing dan timnya. Keberhasilan ini membuka jalan bagi kemenangan Sekutu dalam perang. 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].

Pertukaran informasi adalah salah satu yang sudah dilakukan dalam kehidupan manusia sejak dahulu, yang memungkinkan manusia mendapat informasi dengan manusia lainya. Informasi tersebut dapat dirubah menjadi informasi baru yang berguna untuk manusia sendiri dan untuk orang lain juga. 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 atau ada kebocoran dalam sistem tidak akan mudah mengetahui isi asli dari pesan teks untuk membuka sebuah dokument yang sudah disandikan. Begitu sebaliknya ketika

datat tersebut diterima oleh pengguna asli atau penerima asli dengan mengetahui kunci maka dapat membuka teks sebagai kunci untuk membuka dokument yang diterima[4].

Teknik enkripsi dan dekripsi digunakan untuk mengubah teks menjadi kode-kode tertentu sehingga informasi tersebut tidak dapat dibaca oleh siapapun selain pihak yang berwenang. Metode enkripsi yang umum digunakan adalah algoritma simetris, yang menggunakan kunci yang sama saat melakukan enkripsi dan dekripsi, sehingga informasinya tidak dapat dipahami jika sang pembaca tidak memiliki kunci. Algoritma kriptografi dibagi menjadi algoritma klasik dan algoritma modern. Contoh algoritma klasik adalah cipher pagar kereta api yang saat ini digunakan dalam penelitian ini, sedangkan contoh algoritma modern adalah algoritma Twofish dan Rijndael [5]. Enkripsi adalah proses mengubah informasi (teks) atau data yang akan dikirim menjadi bentuk yang hampir tidak dapat dikenali (acak), sedangkan dekripsi adalah proses mengubah bentuk yang tidak dapat dikenali kembali ke pesan asli (teks)[6].

Tujuan dari kriptografi adalah untuk mendapatkan kerahasiaan dan keaslian dari semua sumber informasi. Kriptografi tidak hanya melindungi data dari pencurian atau mengubah pesan, tetapi juga dapat digunakan untuk mengautentikasi pengguna. Ada beberapa istilah dalam kriptografi, antara lain: kode disebut cipher, informasi atau teks yang disembunyikan disebut plaintext, dan teks yang dikirim setelah mengubah informasi menjadi bentuk rahasia disebut ciphertext. Proses dari plaintext menjadi ciphertext disebut enkripsi, dan proses dari ciphertext menjadi plaintext disebut dekripsi.

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. Untuk melakukan ini, algoritma Base64 membagi setiap blok 3-byte data biner menjadi 4 grup 6 bit, dan kemudian mengubah setiap grup 6 bit menjadi 1 karakter ASCII pesan sehingga pesan pun dapat diacak menggunakan kata-kata yang ada pada pesan tersebut. Semakin banyak kata-kata pada pesan tersebut, maka

hasil ciphertext akan semakin kuat untuk diretas oleh seseorang yang ingin mencuri pesan tersebut. Metode Base64 mengelompokkan setiap blok data biner ke dalam kelompok-kelompok 6 bit. Kemudian, setiap kelompok 6 bit tersebut diubah menjadi 1 karakter ASCII menggunakan tabel karakter Base64 yang telah ditentukan[7]. 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[8].

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.

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

Adapun batasan penelitian dalam pengerjaan penelitian ini adalah sebegai berikut :

a. Metode yang digunakan dalam penelitian adalah metode base64 dan AES (Advanced Encryption Standart).
b. Data yang digunakan dalam enkripsi hanya file berformat pdf.
c. Data diambil dari data file pdf.
d. Penelitian ini tidak menerapkan penyandian dalam aplikasi tertentu.
e. Pengujian / penerapan tidak mempertimbangkan jaringan internet.

1.3 Perumusan Masalah

Berdasarkan latar belakang masalah diatas maka perumusan masalah dalam penelitian ini adalah bagaimana mengamankan pertukaran informasi berupa file memanfaatkan teknik kriptografi untuk menghindari kebocoran terhadap pihdak yang tidak berwenang.

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 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 pengirim dan penerima 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

BAB I PENDAHULUAN

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

BAB II TINJAUAN PUSTAKA

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 PENELITIAN 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 [9].

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[10].

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[11].

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[12].

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. AES sendiri merupakan algoritma kriptografi dengan menggunakan algoritma caesar chiper yang dapat mengenkripsi dan mendekripsi blok data[13].

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[14].

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, pembaruan perangkat lunak, penggunaan firewall dan penghalang jaringan, keamanan fisik, pemantauan keamanan, kebijakan keamanan dan pelatihan, serta cadangan data[15].

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. Jika ada data-data yang tidak terlalu penting, sehingga apabila publik mengetahui data tersebut, pemilik data tidak terlalu dirugikan untuk sang pemilik. Tetapi apabila Pemilik data adalah pihak militer atau pemerintah, keamanan dalam pertukaran informasi menjadi sangat

penting karena data yang mereka kirim kebanyakan adalah data-data rahasia yang tidak boleh diketahui oleh publik. 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[16].

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. Kemudian, pada abad ke-19, perkembangan mesin kriptografi mekanik seperti Enigma membawa kemajuan yang signifikan. Dalam era komputer pada abad ke-20, kriptografi kunci simetris dan kunci publik menjadi populer. Pada abad ke-21, 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[17]. Pertukaran data melibatkan transfer informasi 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**.**

Teknologi informasi berperan penting sebagai sarana untuk menyajikan informasi dalam bentuk struktur kelembagaan dan nilai-nilai sosial. Informasi dikumpulkan, disimpan, diolah, dan ditukar melalui teknologi ini, termasuk melalui internet. Saat ini,

informasi dapat diakses melalui berbagai media, termasuk media cetak, televisi, radio, dan terutama media elektronik seperti media sosial yang mudah dijangkau melalui perangkat komunikasi seperti smartphone. Media sosial menjadi pilihan utama masyarakat untuk memenuhi kebutuhan informasi. Kelebihan media sosial terletak pada adanya interaksi antara pengguna, yang memungkinkan pertukaran informasi menjadi dua arah. Berbeda dengan media konvensional yang biasanya hanya bersifat satu arah. Media sosial adalah platform online berbasis internet yang dikembangkan dengan menggunakan konsep dan teknologi Web[18].

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.[19].

2.2.5 File

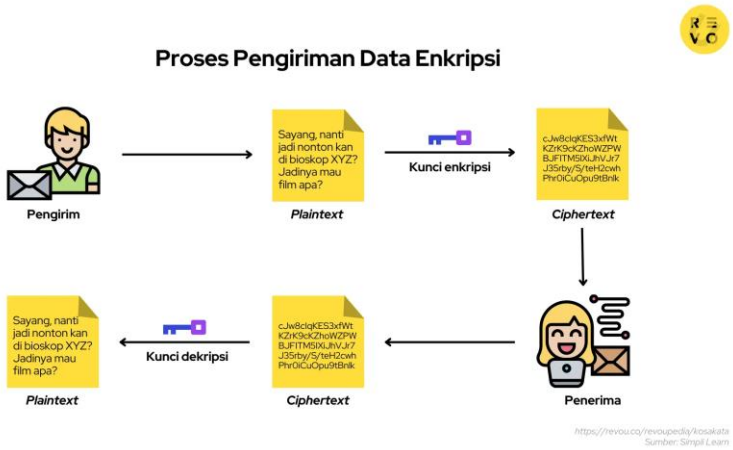
File adalah entitas dari data yang disimpan didalam sistem file yang dapat diakses dan diatur oleh pengguna. Sebuah file memiliki nama yang unik dalam direktori di mana ia berada. Alamat direktori dimana suatu berkas ditempatkan diistilahkan dengan path. sebuah file berisi aliran data (atau data stream) 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.

2.2.5 Kriptografi

Kriptografi memainkan peran penting dalam dunia komputasi karena keberadaan banyak informasi rahasia yang disimpan dan dikirim melalui media komputer. Informasi ini seringkali berupa dokumen penting atau rahasia yang tidak boleh diakses oleh pihak yang tidak berhak. Dalam era komputasi digital, kriptografi memungkinkan penghasilan cipher (teks terenkripsi) yang kompleks dan rumit. Terdapat dua jenis kriptografi, yaitu klasik dan modern. Kriptografi klasik umumnya melibatkan enkripsi karakter per karakter dengan menggunakan alfabet tradisional, sedangkan kriptografi modern beroperasi pada string biner. Lebih dari sekadar memberikan keamanan, baik kriptografi klasik maupun modern juga memiliki implikasi lain dalam dunia digital. Kriptografi merupakan metode untuk mengirim pesan secara rahasia sehingga hanya penerima yang memiliki kemampuan untuk menghapus penyandian dan membaca atau mendekripsi pesan tersebut.[20]. Dalam kriptografi sendiri terdapat beberapa istilah, yaitu: Berikut adalah istilah-istilah yang digunakan dalam bidang kriptografi:

a. Plaintext (M) adalah pesan yang hendak dikirimkan (berisi data asli).
b. Ciphertext (C) adalah pesan ter-enkrip (tersandi) yang merupakan hasil enkripsi.
c. Enkripsi (E) adalah proses pengubahan plaintext menjadi ciphertext.
d. Dekripsi (D) adalah kebalikan dari enkripsi yakni mengubah ciphertext menjadi plaintext, sehingga berupa data awal atau asli.
e. 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)*

2.2.4 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[3].

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.

2.2.5 Dekripsi

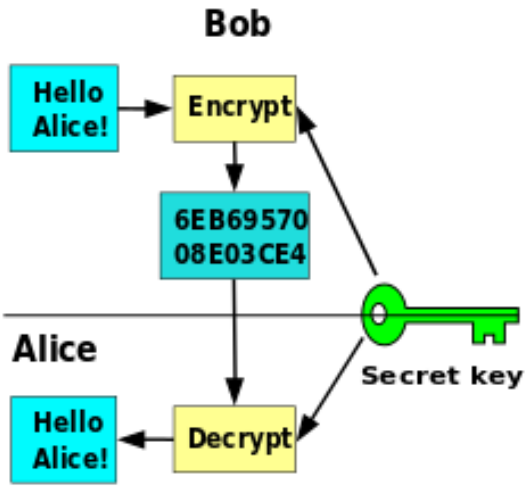
Teknik dekripsi dapat diartikan dalam sebuah pengamanan teks. Dekripsi adalah proses kebalikan dari enkripsi yaitu mengubah pesan yang sudah terenkripsi menjadi pesan asli. Dekripsi disebut dengan proses pengembalian ciphertext menjadi plaintext[21]. Pada

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.

2.2.6 Algoritma Kriptografi

2.2.6.1 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. Pada gambar 2.2 dijelaskan diagram proses enkripsi dan dekripsi algoritma asimetris.



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/)*

Kelebihan algoritma kriptografi simetris adalah:

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

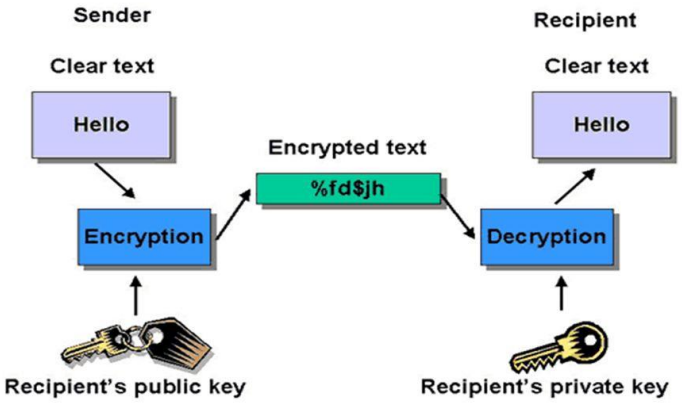
Kekurangan algoritma kriptografi simetris adalah:

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

Contoh algoritma kriptografi simetris Rijndael, Base64, AES

2.2.6.2 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. Pada gambar 2.3 dijelaskan diagram proses enkripsi dan dekripsi algoritma asimetris.



Gambar 2.3. Diagram proses enkripsi dan dekripsi algoritma asimteris

(Sumber : https://slideplayer.info/slide/2423293/)

Kelebihan algoritma kriptografi asimetris :

a. Masalah keamanan pada distribusi kunci dapat lebih baik
b. Masalah manajemen kunci yang lebih baik karena jumlah kunci yang lebih sedikit

Kelemahan algoritma kriptografi asimetris:

a. Kecepatan yang lebih rendah bila dibandingkan dengan algoritma simetris.
b. Untuk tingkat keamanan sama, kunci yang digunakan lebih panjang dibandingkan dengan algoritma simetris.

Contoh algoritma : RSA, ECC, ElGamal.

2.2.7 ASCII

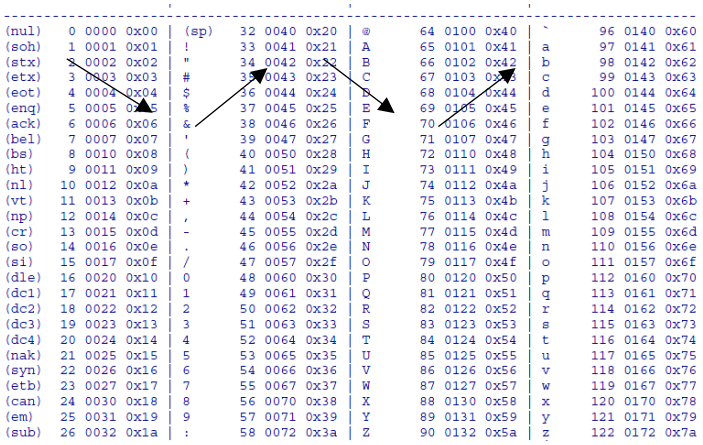
Berdasarkan permasalahan dalam keamanan dalam pertukaran data, proses yang dilakukan oleh metode base64 dan aes (Advanced Encryption Standart) adalah dengan melakukan perubahan nilai terhadap informasi berupa teks rahasia [25]. Penggunaan metode 2 algoritma ini untuk mengamankan data file pada saat pertukaran informasi bisa dikatakan efektif jika hanya penyandian sebuah teks yang menghasilkan output file untuk pengamanan karena sudah diamankan menggunakan algoritma Advanced Standart Encryption sebagai kunci utama.

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).

Berikut adalah beberapa contoh kode ASCII untuk karakter-karakter umum:

- Huruf-huruf 'A': 65.
- Huruf-huruf 'a': 97.
- Angka-angka '0': 48.
- Tanda baca titik ("."): 46.
- Karakter baris baru: 10.
- Karakter spasi: 32.

Tabel ASCII dari algoritma base64.



(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 2.4. Tabel ASCII

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

Dalam komputasi, ASCII digunakan sebagai representasi internal untuk karakter-karakter dalam berbagai operasi seperti pemrosesan teks, pemrosesan file, komunikasi jaringan, dan lain-lain. ASCII memungkinkan komputer untuk menyimpan, memproses, dan menampilkan teks dalam format yang dapat dipahami oleh manusia.

2.2.8 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.

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

Contoh proses enkripsi :

a. Teks yang akan dienkripsi adalah “Hello” sebagai plaintext.
b. Untuk mendapatkan hasil enkripsi, konversi plainteks diatas kedalam bentuk biner menggunakan kode ASCII dari “Hello”.

c. Selanjutnya dari hasil konversi ASCII dirubah menjadi dalam bentuk biner 8bit yang menghasilkan 'H' = 01001000, 'e' = 01100101, 'l' = 01101100, 'l' = 01101100, 'o' = 01101111.
d. Gabungkan biner menjadi satu urutan 01001000 01100101 01101100 01101100 01101111.
e. Bagi menjadi grup dengan panjang 6 bit 010010 000110 010110 001100 011011 110.
f. Konversi grup ke dalam bentuk desimal 18 6 22 12 27 62.
g. Konversi desimal ke dalam bentuk karakter Base64 SGVsbG8=.

Contoh proses dekripsi :

h. Teks yang akan didekripsi adalah “Hello” sebagai chipertext.

i. 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.
j. 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.
k. Bagi menjadi grup dengan panjang 6 bit 01001000 01100101 01101100 01101100 01101111.
l. Konversi grup ke dalam bentuk sesuai dengan tabel ASCII 01001000 = 'H', 01100101 = 'e', 01101100 = 'l', 01101100 = 'l', 01101111 = 'o'.
m. Konversi dan gabungkan ke dalam bentuk karakter Base64 Hello.

2.2.9 AES (*Advanced Encryption Standart*)

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.

Pada tahun 1997, NIST (National Institute of Standards and Technology) Amerika Serikat mengadakan kompetisi untuk mencari algoritma enkripsi baru yang lebih aman daripada DES. Setelah melalui peninjauan dan evaluasi yang intensif, algoritma Rijndael, yang dikembangkan oleh Joan Daemen dan Vincent Rijmen dari Belgia, terpilih sebagai pemenang pada tahun 2001.

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 AESSebagai 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. AES menggunakan 4 jenis transformasi yaitu:

2.2.9.1 SubBytes

SubBytes adalah langkah penting dalam algoritma enkripsi dan dekripsi AES (Advanced Encryption Standard). Pada langkah SubBytes, setiap byte dalam blok data diganti dengan byte baru menggunakan tabel substitusi yang disebut S-box (kotak substitusi). Prosedur SubBytes dilakukan secara independen untuk setiap byte dalam blok data. Setiap byte diganti dengan byte baru yang sesuai dengan posisinya di S-box. S-box

bertindak sebagai tabel substitusi yang telah ditentukan sebelumnya yang menghubungkan setiap nilai byte dengan nilai byte baru yang sesuai. Langkah SubBytes di AES memberikan non-linearitas ke algoritme karena setiap byte diganti dengan byte baru secara non-linear.Hal ini berkontribusi pada keamanan algoritme AES karena memperburuk risiko perubahan data selama enkripsi dan dekripsi. . Misalnya, jika kita memiliki blok data berukuran 4x4, setiap byte dalam blok tersebut akan digantikan oleh byte baru yang diambil dari S-box. Proses ini menghasilkan blok data

2.2.9.2 ShiftRows

ShiftRows adalah tahap yang penting dalam algoritma enkripsi dan dekripsi AES (Advanced Encryption Standard) yang melibatkan pergeseran baris dalam blok data. Pada tahap ShiftRows, setiap baris dalam blok data bergeser secara siklik ke kiri. Baris pertama tidak mengalami perubahan, baris kedua digeser satu posisi ke kiri, baris ketiga digeser dua posisi ke kiri, dan baris keempat digeser tiga posisi ke kiri. Proses ini menghasilkan perubahan posisi byte dalam setiap baris, menciptakan pengacakan data yang lebih lanjut dan meningkatkan kompleksitas algoritma. Tujuan dari tahap ShiftRows adalah untuk mencampur byte-byte dalam blok data, memberikan diffusi yang lebih baik dan meningkatkan keamanan algoritma AES.Sebagai contoh, jika kita memiliki blok data 4x4, setiap baris dalam blok tersebut akan mengalami pergeseran ke kiri sesuai dengan jumlah posisi yang ditentukan. Pergeseran ini akan mengubah urutan byte dalam blok data.Setelah tahap ShiftRows selesai, blok data akan melanjutkan ke tahap-tahap berikutnya dalam algoritma AES, seperti MixColumns dan AddRoundKey, untuk membentuk alur enkripsi atau dekripsi yang lengkap dan lebih aman.Dengan menggabungkan tahap-tahap seperti SubBytes, ShiftRows, dan tahap-tahap lainnya, algoritma AES mampu menciptakan difusi yang kuat dan meningkatkan keamanan data yang dienkripsi dan didekripsi.

2.2.9.3 MixColumns

MixColumns adalah tahap penting dalam algoritma enkripsi dan dekripsi AES (Advanced Encryption Standard) yang melibatkan operasi matriks pada blok data.Pada tahap MixColumns, setiap kolom dalam blok data mengalami transformasi menggunakan matriks MixColumns. Transformasi ini melibatkan perkalian dan penjumlahan byte dalam

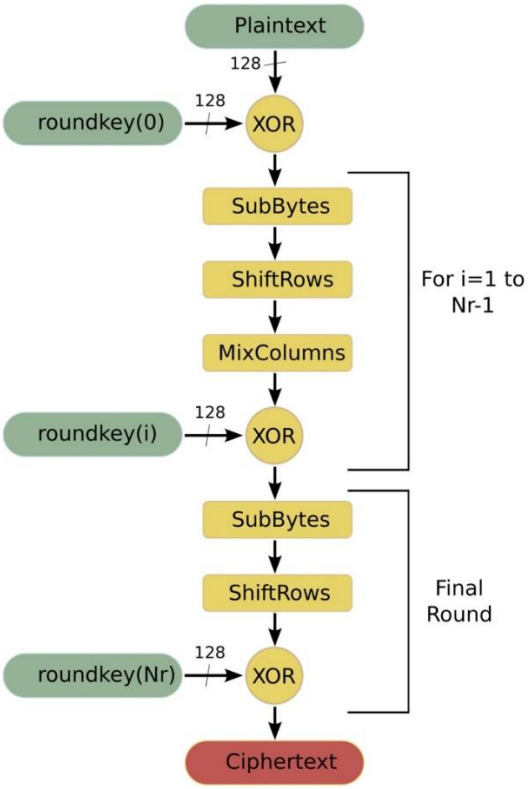
kolom tersebut.Setiap kolom dianggap sebagai polinomial byte, dan perkalian dalam matriks MixColumns dilakukan dengan menggunakan operasi perkalian polinomial dalam Galois Field. Byte-byte dalam kolom akan dikalikan dengan konstanta polinomial tertentu dan hasil perkalian akan dijumlahkan dengan byte-byte lainnya untuk menghasilkan byte baru.Proses MixColumns bertujuan untuk menyebarkan informasi dalam kolom dan menciptakan efek difusi yang lebih baik. Hal ini meningkatkan keamanan dan kompleksitas algoritma AES, karena mengubah pola data yang ada dalam kolom-kolom blok data.Sebagai contoh, jika kita memiliki blok data 4x4, setiap kolom dalam blok tersebut akan mengalami transformasi menggunakan matriks MixColumns. Hasil transformasi ini akan menghasilkan blok data baru dengan byte-byte yang berbeda.Setelah tahap MixColumns selesai, blok data akan melanjutkan ke tahap-tahap berikutnya dalam algoritma AES, seperti AddRoundKey, untuk membentuk alur enkripsi atau dekripsi yang lengkap dan lebih aman.Dengan menggabungkan tahap-tahap seperti SubBytes, ShiftRows, MixColumns, dan tahap-tahap lainnya, algoritma AES mencapai tingkat difusi yang kuat dan memastikan keamanan dan keandalan dalam enkripsi dan dekripsi data.

2.2.9.4 AddRoundKey

Tahap AddRoundKey merupakan langkah penting dalam algoritma AES (Advanced Encryption Standard) yang melibatkan kombinasi eksklusif (XOR) antara blok data dengan kunci ronde yang sesuai. Pada tahap ini, setiap byte dalam blok data di-XOR dengan byte yang sesuai dari kunci ronde yang telah dihasilkan sebelumnya. Kunci ronde tersebut telah dihasilkan melalui tahap ekspansi kunci, di mana kunci enkripsi awal diperluas menjadi serangkaian kunci ronde. Proses XOR antara blok data dan kunci ronde bertujuan untuk mengintegrasikan informasi kunci dengan blok data, sehingga menciptakan transformasi yang kompleks dan meningkatkan keamanan data. Dengan melakukan operasi XOR, setiap bit dalam blok data akan berubah sesuai dengan nilai bit pada kunci ronde yang relevan. Contohnya, jika kita memiliki blok data 4x4 dan kunci ronde yang sesuai, setiap byte dalam blok data akan di-XOR dengan byte yang sesuai dari kunci ronde. Hasil XOR ini akan mengubah nilai byte dalam blok data. Tahap AddRoundKey dilakukan pada setiap ronde enkripsi dan dekripsi, sehingga memberikan kontribusi yang signifikan dalam proses difusi data dan memastikan keamanan algoritma

AES. Melalui penggabungan tahap-tahap seperti SubBytes, ShiftRows, MixColumns, dan AddRoundKey, algoritma AES mencapai tingkat difusi yang kuat dan memastikan keamanan dan keandalan dalam proses enkripsi dan dekripsi data.

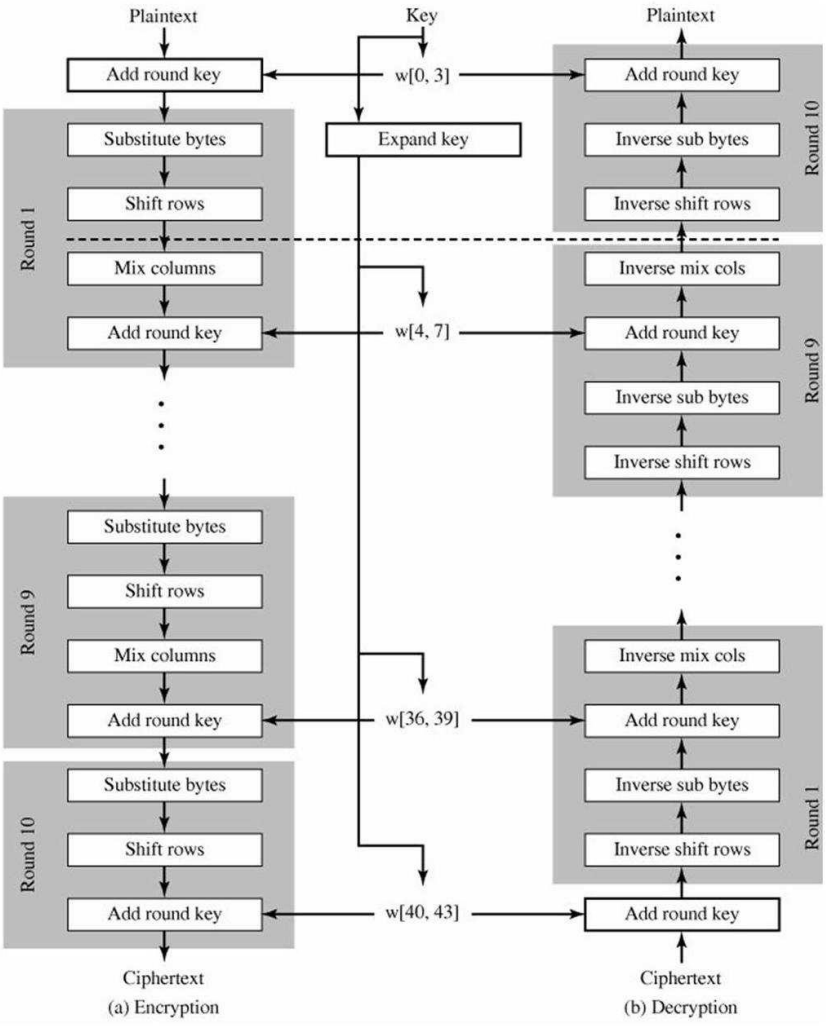
Pada ronde terakhir yaitu ronde ke-Nr dilakukan tranformasi serupa dengan ronde lain namun tanpa tranformasi serupa dengan ronde lain namun tanpa mixColumns.



2.5 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.



2.6. 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 128 bit atau 4 kata, maka akan menghasilkan sebuah array yang terdiri

dari 44 kata yang akan menjadi kunci. Berikut adalah langkah-langkah untuk melakukan ekspansi kunci:

1. Pertama kunci AES 128 bit di organisir menjadi 4 word dan disalin ke word keluaran (W) pada 4 elemen pertama (W [0], W[1], W[2], W[3]).
2. Untuk elemen keluaran selanjutnya W[i] dengan i = {4,…,43} dihitung sebagai berikut:
    a. Salin W [i-1] pada word t.
    b. Jika i mod 4 = 0 (I habis dibagi 4) maka lakukan W[i]= f (t,i) ⊕ W[i-4] ,dengan fungsi f(t,i) adalah sebagai berikut:
    f(t,i) = Subword (rotword(t)) ⊕RC[i/4].
    c. Jika i mod 4 = 0 (I habis dibagi 4) maka lakukan W[i]= f (t,i) ⊕ W[i-4] ,dengan fungsi f(t,i) adalah sebagai berikut:f(t,i) = Subword (rotword(t)) ⊕RC[i/4].

Adapun penyelesaian metode AES dalam penelitian ini yaitu dengan melakukan pengenkripsian Transaksi Data Member pada Toko Sweet Amirah. Adapun contoh yang akan di enkripsi yaitu dengan Plaintext: Mentari dan Key: TOKOSWEETAMIRAHH. Adapun proses penyelesaian enkripsi dan dekripsi dari contoh data yang akan di amankan adalah sebagai berikut:

1. Perhitungan Enkripsi
   Plaintext: Mentari (16 ASCII characters)
   Plaintext dalam Hexadecimal (128 bits): 4D 45 4E 54 41 52 49 14 14 14 14 14 14 14 14 14 Key: TOKOSWEETAMIRAHH (16 ASCII characters)
   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 2.7 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 2.8 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

41	83	
48	52	
48	52	SubBytes
52	00	

54		83		01		D6
4F	□	52	□	00	=	1D
4B		52		00		19
4F		00		00		4F

Adapun perhitungan secara manualnya seperti berikut:
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 perhitungan secara manualnya seperti berikut:
53 (Hex) =
01010011 D6 (Hex)
= 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
Key				Round 1				Round 2				Round 10			

b. SubBytes

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

□

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

=

19	12	40	46
0A	05	55	55
05	0C	59	5C
1B	51	5D	5C

19	12	40	46
0A	05	55	55
05	0C	59	5C
1B	51	5D	5C

Konversi dengan menggunakan S-Box =

D4	C9	09	5A
67	6B	FC	FC
6B	FE	CB	4A
AF	D1	4C	4A

c. ShiftRows

D4	C9	09	5A
67	6B	FC	FC
6B	FE	CB	4A
AF	D1	4C	4A

<----Rotate over 1 byte

D4	C9	09	5A
6B	FC	FC	67
6B	FE	CB	4A
AF	D1	4C	4A

D4	C9	09	5A
6B	FC	FC	67
CB	4A	6B	FC
AF	D1	4C	4A

<----Rotate over 2 byte

D4	C9	09	5A
6B	FC	FC	67
CB	4A	6B	FC
AF	D1	4C	4A

D4	C9	09	5A
6B	FC	FC	67
CB	4A	6B	FC
4A	AF	D1	4C

<----Rotate over 3 byte

D4	C9	09	5A
6B	FC	FC	67
CB	4A	6B	FC
4A	AF	D1	4C

d. MixColumns

D4	C9	09	5A
6B	FC	FC	67
CB	4A	6B	FC
4A	AF	D1	4C

$$\begin{vmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{vmatrix} \cdot \begin{vmatrix} D4 \\ 6B \\ CB \\ 4A \end{vmatrix}$$

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

D4	C9	09	5A
6B	FC	FC	67
CB	4A	6B	FE
4A	AF	D1	4C

$$\begin{vmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{vmatrix} \cdot \begin{vmatrix} D4 \\ 6B \\ CB \\ 4A \end{vmatrix} = \begin{vmatrix} 8F \\ 0E \\ EC \\ 53 \end{vmatrix}$$

Hasil MixColumnnya adalah sebagai berikut:

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
0E	5B	86	C1
EC	4B	4B	0E
53	B3	35	EF

MixColumn

□

D6	85	D1	83
1D	4A	0B	4A
19	5C	11	59
4F	0A	43	0B

RoundKey 1

=

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

AddRoundKey

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

8F		D6		59	------>	8F (Hex) = 1000 1111 (Bin)
0E		1D	=			D6 (Hex) = 1101 0110 (Bin)
EC		19				Hasil Xor = 0101 1001 (Bin) = 59 (Hex)
53		4F				

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).

	Round 2				Round 3			
After SubBytes	CB	42	33	71	A6	26	C6	BC
	7D	82	5D	3D	37	59	56	4D
	E6	F0	BE	5B	5C	BC	4A	EE
	9C	56	38	69	2B	D6	E8	73
After ShiftRows	CB	42	33	71	A6	26	C6	BC
	82	5D	3D	7D	59	56	4D	37
	BE	5B	E6	F0	4A	EE	5C	BC
	69	9C	56	38	73	2B	D6	E8
After MixColumns	C7	A4	91	AD	85	73	CA	6E
	64	89	2E	B8	B9	88	6E	E5
	95	16	23	BF	FE	CA	52	CB
	A8	E3	22	6E	04	84	F7	9F
Round Key								
After AddRoundKey	02	87	56	D5	C7	40	16	C3
	D6	9C	97	DD	21	BD	2A	F7
	32	6E	7F	26	CA	A4	DB	FD
	A3	A9	EA	E1	A0	09	E3	02
	=				=			
	C5	23	C7	78	42	33	DC	AD
	B2	15	B9	65	98	35	44	12
	A7	78	5C	99	34	6E	89	36
	0B	4A	C8	8F	A4	8D	14	9D

Sampai hasil AddRoundKey ke-10 sebagai berikut:

Round 10

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

□

52	31	4F	31
94	40	B1	5B
8C	14	EE	A1
20	A4	2D	66

=

B7	5D	D6	85
75	73	DF	7A
32	F1	C0	D3
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 3.1 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 2.9 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

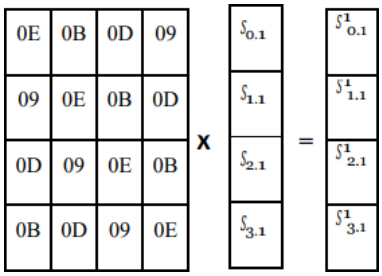
c. XOR hasil dari InvSubBytes dengan RoundKey ke-9. Proses ini disebut AddInvRoundKey

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.



$s^{0.1}$ = ([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:

Round 1

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

Round 2

91	15	9B	38
D0	B8	33	01
B0	94	2E	CD
9C	F3	8D	42

Round 3

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

Round 4

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

Round 5

00	FC	12	9E
B7	B3	7A	59
0D	09	98	E3
F9	D2	FA	92

Round 6

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

Round 7

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

Round 8

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

Round 9

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[22]. Berdasarkan proses yang dilakukan maka akan didapatkan hasil dalam bentuk karakter pada tabel ASCII sebagai berikut:

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	

2.2.10 Verifikasi dan Validasi

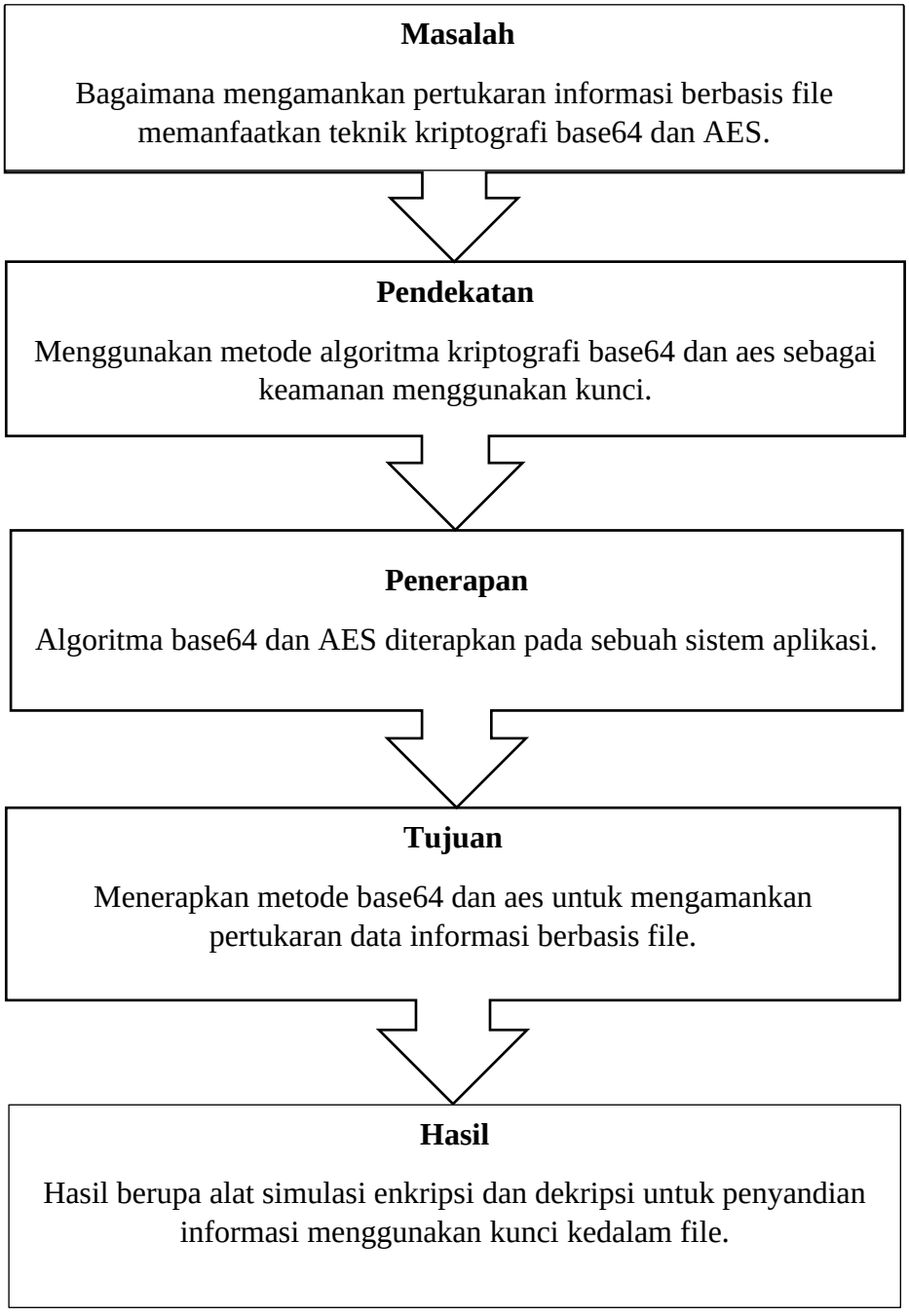
Verifikasi dan validasi adalah istilah yang digunakan untuk menggambarkan proses pemeriksaan dan analisis yang memastikan bahwa perangkat lunak sesuai dengan spesifikasinya dan memenuhi kebutuhan pelanggan yang membayar untuk perangkat lunak tersebut. Verifikasi dan validasi perlu dilakukan pada setiap tahap dalam proses pengembangan perangkat lunak. Tujuan dari kegiatan ini adalah untuk memeriksa apakah hasil dari proses tersebut sesuai dengan spesifikasi yang telah ditetapkan.

Meskipun verifikasi dan validasi seringkali digunakan secara bersamaan, keduanya memiliki peran yang berbeda. Verifikasi melibatkan pemeriksaan yang bertujuan untuk memastikan bahwa perangkat lunak sesuai dengan spesifikasi yang telah ditetapkan. Sistem harus memenuhi persyaratan fungsional dan non-fungsional yang telah disepakati.

Di sisi lain, validasi merupakan proses yang lebih umum yang bertujuan untuk memastikan bahwa perangkat lunak memenuhi harapan dari klien atau pelanggan. Hal ini melibatkan penilaian secara keseluruhan terhadap perangkat lunak dan memverifikasi bahwa perangkat lunak tersebut memenuhi kebutuhan bisnis atau pengguna yang diharapkan.

Dengan melakukan verifikasi dan validasi secara komprehensif, perangkat lunak dapat dikonfirmasi bahwa ia berfungsi dengan benar sesuai dengan spesifikasi dan dapat memenuhi harapan dan kebutuhan pengguna atau pelanggan yang ada.

2.3.Kerangka Pemikiran



BAB III

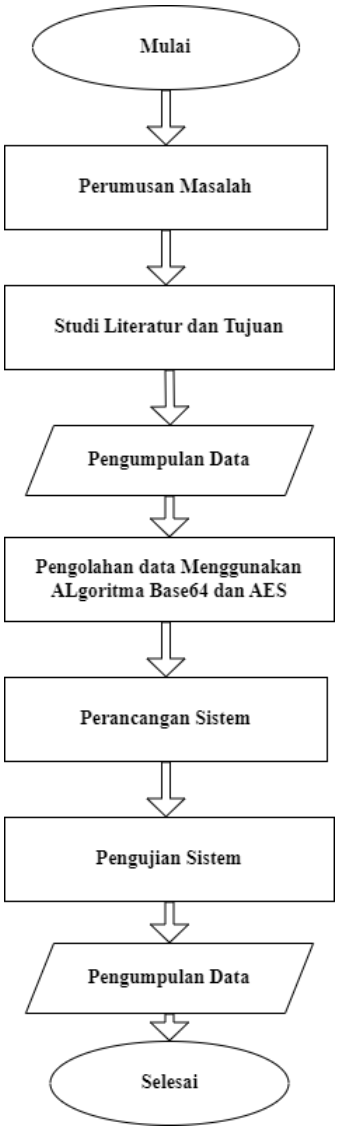
METODOLOGI PENELITIAN

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



3.1 Gambar Flowchart Penelitian

3.2. Pengumpulan Data

Saat mengumpulkan sumber data, peneliti mengumpulkan sumber data dari dataset Kaggle berupa data file. Kaggle Data Set adalah 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 teks secara online di kumpulan data Kaggle, 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:

a. Pengumpulan data yang berfungsi untuk memperoleh data yang diperlukan dalam pengujian program.
b. Pengelompokan data sesuai dengan jenis dan fungsinya.
c. Mencari data dalam berjenis teks (.txt .pdf) yang akan dienkripsi dalam penelitian.

3.4. Gambaran Umum Penerapan Algoritma

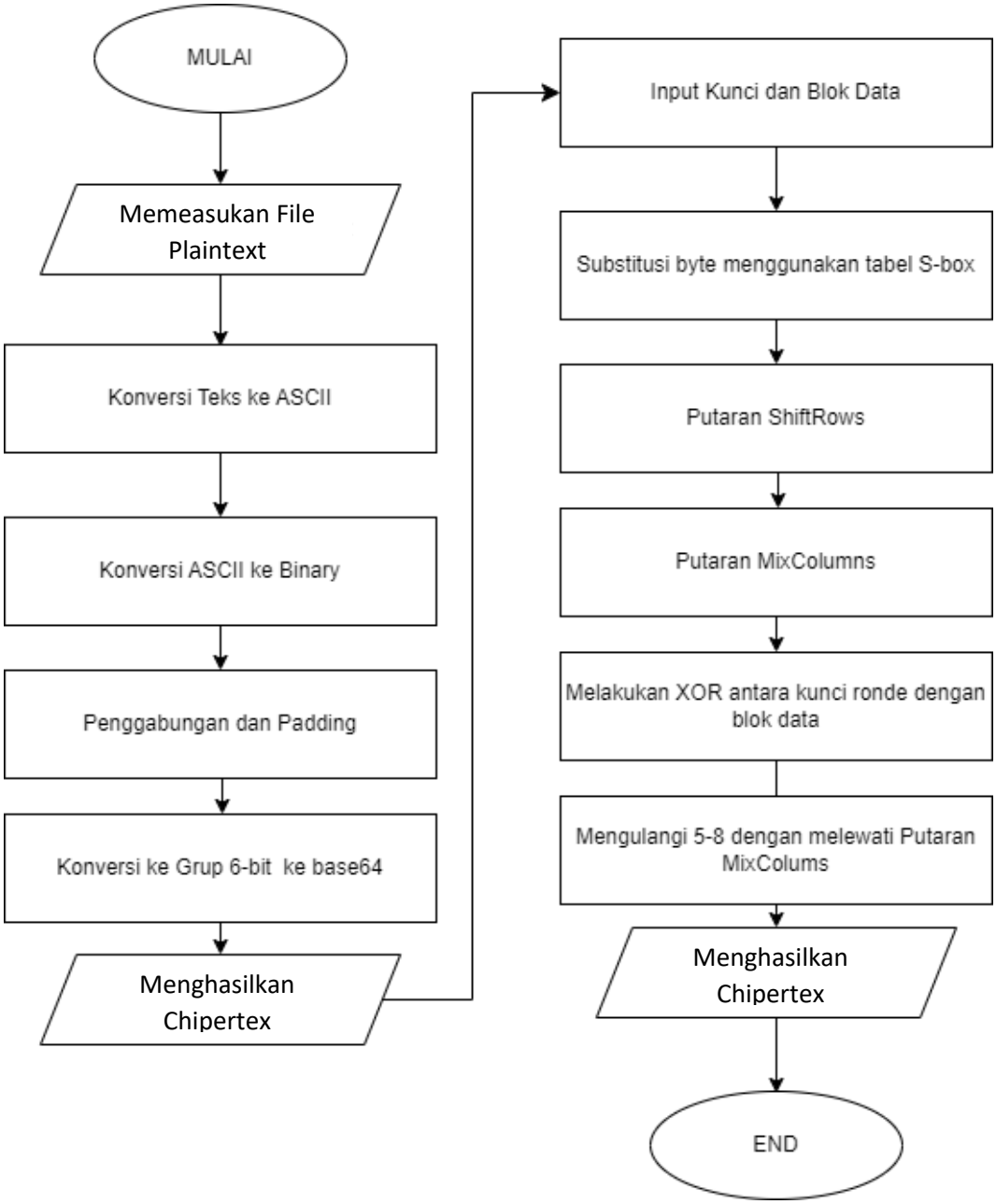
Penerapan algoritma dalam keamanan teks digunakan untuk melindungi kerahasiaan, integritas, dan otentikasi informasi yang dikirim melalui media elektronik seperti email, pesan teks, dll. Salah satu algoritme yang sering digunakan adalah algoritme kriptografi, yang tujuannya adalah untuk mengubah suatu 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

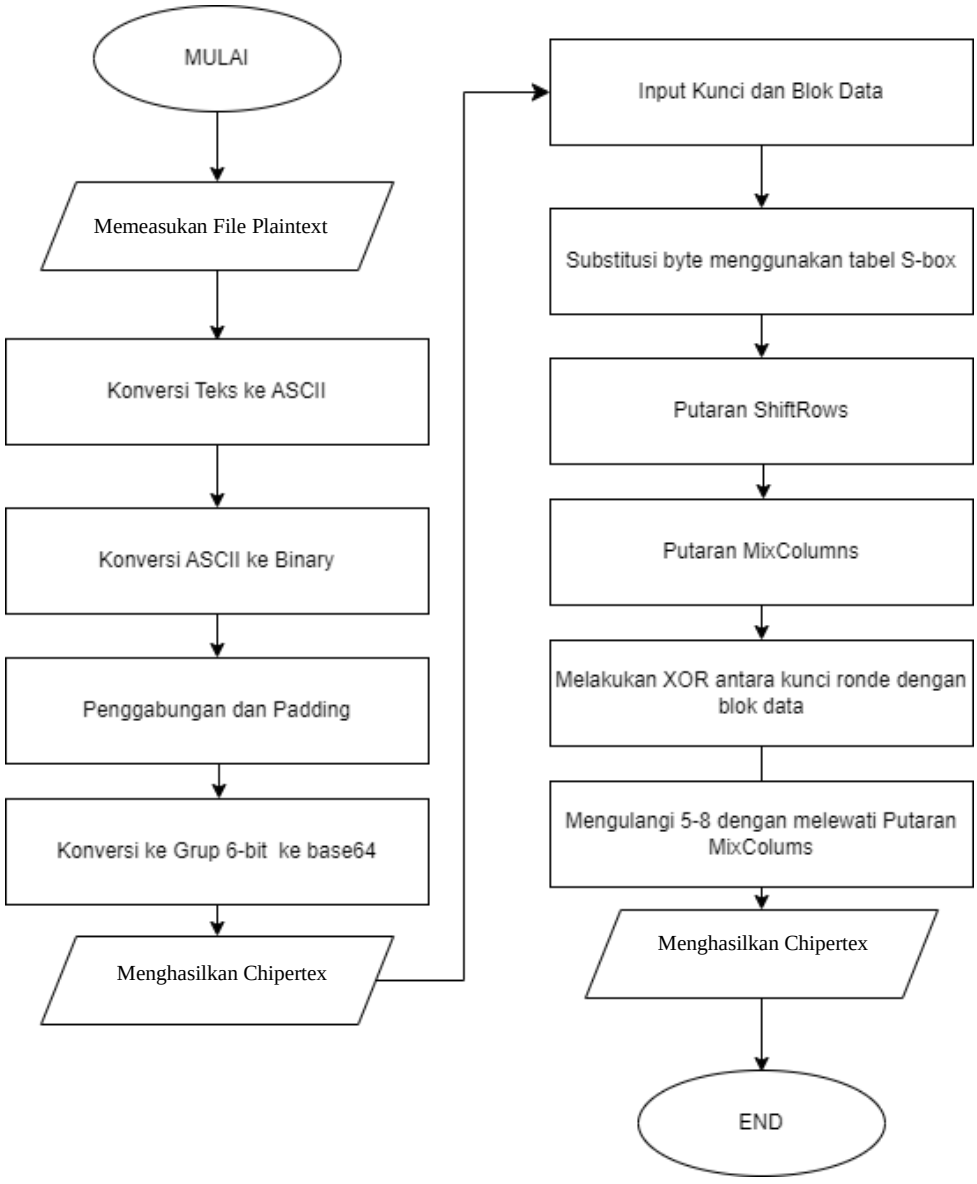
Flowchart sistem mennggambarkan urutan proses secara mendetail dan hubungan antara satu proses dengan proses lainnya. *Flowchart* sistem untuk enkripsi data dapat dilihat pada Gambar 3.1.



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 teks

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 Penerapan 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.

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] L. D. Simatupang and U. D. Bengkulu, "Pengamanan Dokumen Teks Dengan Menerapkan Kombinasi Algoritma Kriptografi Klasik," vol. 07, pp. 133–140, 2022.

[6] 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.

[7] W. P. Abdul Kodir, "IMPLEMENTASI KRIPTOGRAFI DENGAN MENGGUNAKAN METODE RC4 DAN BASE64 UNTUK MENGAMANKAN DATABASE SEKOLAH PADA SDN GROGOL

UTARA 10,” vol. 4, no. 1, pp. 7–14, 2021.

[8] E. Dokumen, G. Geulis, and E. Abadi, “Penerapan Algoritma AES (Advance Encryption Standart) 128 untuk,” vol. 5, pp. 1–10, 2022.

[9] 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.

[10] 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.

[11] 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.

[12] 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.

[13] P. Kriptografi and C. Chiper, “APLIKASI CHATTING BERBASIS LOCAL AREA NETWORK,” vol. 4, no. 1, pp. 1–10, 2021.

[14] 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.

[15] 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.

[16] 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.

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

[18] R. C. Halim and S. Sugiarto, “Penerapan Algoritma AES dalam Perancangan Aplikasi Media Sosial Berbasis Android,” *Enter*, pp. 368–379, 2018, [Online]. Available: http://www.sisfotenika.stmikpontianak.ac.id/index.php/enter/article/view/821%0Ahttps://www.sisfotenika.stmikpontianak.ac.id/index.php/enter/article/viewFile/821/585.

[19] 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.

[20] 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.

[21] 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.

[22] A. Handayani, N. Budi Nugroho, and R. I. Ginting, “Implementasi Kriptografi Dengan Metode AES(Advance Encryption Standard) Untuk Mengamankan Data Penjualan Di Toko Sweet Amirah,” *J. CyberTech*, vol. 2, no. 2, pp. 297–311, 2019, [Online]. Available: https://ojs.trigunadharma.ac.id/.