# Plagiarism Checker X Originality Report

**Similarity Found: 16%**

Date: Monday, June 05, 2023
Statistics: 966 words Plagiarized / 5933 Total words
Remarks: Low Plagiarism Detected - Your Document needs Optional Improvement.
---

PENERAPAN KEAMANAN FILE MENGGUNAKAN ALGORITMA BASE64 DAN AES (ADVANCED ENCRYPTION STANDARThar) 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 HALAMAN JUDUL.....i PERSETUJUAN PEMBIMBING ii DAFTAR ISI iii DAFTAR GAMBAR iv BAB I PENDAHULUAN 2 1.1 Latar Belakang 2 1.2 Perumusan Masalah 6 1.3 Batasan Penelitian 6 1.4 Tujuan Penelitian 6 1.5 Manfaat Penelitian 6 1.6 Sistematika Penulisan 7 BAB II LANDASAN TEORI 8 2.1. Tinjauan Studi 8 2.2.

Tinjauan Pustaka 10 2.2.1 Keamanan Informasi 10 2.2.2 Pertukaran Informasi 11 2.2.3 Ancaman Informasi 12 2.2.5 Enkripsi 14 2.2.6 Dekripsi 15 2.2.7 Algoritma Kriptografi 16 2.2.8 Algoritma Rail Fence Cipher 20 2.2.9 Evaluasi 25 2.3. Kerangka Pemikiran 26 BAB II METODOLOGI PENELITIAN 21 3.1. Gambaran Umum Penerapan Algoritma 21 3.2. Flowchart Enkripsi 22 3.3. Flowchart Dekripsi 22 3.4. Pengujian Penerapan Algoritma 23 DAFTAR PUSTAKA 24 DAFTAR GAMBAR Gambar 2.1. Diagram Alur Kriptografi 13 Gambar 2.2. Diagram proses enkripsi dan dekripsi algoritma simteris 15 Gambar 2.3. Diagram proses enkripsi dan dekripsi algoritma asimteris 16 Gambar 2.4. Algoritma Rail Fence Cipher 17 Gambar 3.1.

Flowchart enkripsi teks 21 Gambar 3.2. Flowchart enkripsi teks 22

BAB I PENDAHULUAN 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 dimana informasi (teks) atau data yang hendak dikirim diubah menjadi bentuk yang hampir tidak dikenali (acak), sedangkan Dekripsi adalah

mengubah kembali dari bentuk yang tidak dikenali tersebut menjadi informasi (teks) awal[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.

Perumusan Masalah Berdasarkan latar belakang masalah diatas maka perumusan masalah dalam penelitian ini adalah bagaimana mengamankan pertukaran informasi berupa file memanfaatkan teknik kriptografi? Batasan Penelitian Adapun batasan penelitian dalam pengerjaan penelitian ini adalah sebegai berikut : Metode yang digunakan dalam penelitian adalah metode base64 dan AES (Advanced Encryption Standart). Data yang digunakan dalam enkripsi hanya file berformat pdf. Data diambil dari data file pdf.

Penelitian ini tidak menerapkan penyandian dalam aplikasi tertentu. Pengujian / penerapan tidak mempertimbangkan jaringan internet. 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. Manfaat Penelitian Dari penelitian diatas diharapkan dapat memberikan manfaat sebagai berikut : Manfaat bagi peneliti Adapun manfaat bagi peneliti yaitu menambah ilmu pengetahuan khususnya pada keamanan dalam menggunakan algortima kriptografi.

Manfaat bagi pengirim dan penerima pesan Pengirim dan penerima pesan dapat menyandi file agar lebih aman saat berkomunikasi. Manfaat bagi pembaca Dapat menambah wawasan bagi pembaca dan dapat dipergunakan sebagai referensi untuk penelitian selanjutnya. Manfaat bagi keamanan informasi Dapat menjaga keamanan dalam bertukar informasi dengan menerapkan metode lebih 1 algoritma base64 dan AES (Advanced Encryption Standart). 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, lokasi penelitian, desain penelitian, pengumpulan data, metode pengembangan sistem, dan pengujian metode. BAB IV HASIL PENELITIAN DAN PEMBAHASAN Pada bab ini mejelaskan tentang penerapan dari 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 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)", dalam penelitian ini peneliti merancang sebuah aplikasi sistem informasi pada desa cipinang yang hanya mengandalkan system backup yang dimana tidak cukup efentif dan juga karyawan dapat mengubah data secara langsung tanpa adanya pengamanan pada sebuah data sehingga terdapat kekhawatiran kebocoran data kepada pihak yang tidak bertanggubng jawab sehingga diterapkanya pengamanan sebuah data file 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].

Tinjauan Pustaka 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]. 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]. 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]. 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. 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: Plaintext (M) adalah pesan yang hendak dikirimkan (berisi data asli). Ciphertext (C) adalah pesan ter-enkrip (tersandi) yang merupakan hasil enkripsi. Enkripsi (E) adalah proses pengubahan plaintext menjadi ciphertext.

Dekripsi (D) adalah kebalikan dari enkripsi yakni mengubah ciphertext menjadi plaintext, sehingga berupa data awal atau asli. 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) 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. 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. Algoritma Kriptografi 2.2.9.1. 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: Kecepatan operasi lebih tinggi bila dibandingkan dengan algoritma asimetrik. Karena kecepatannya yang cukup tinggi, maka dapat digunakan pada sistem real-time Kekurangan algoritma kriptografi simetris adalah: 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 2.2.9.2.

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 : Masalah keamanan pada distribusi kunci dapat lebih baik Masalah manajemen kunci yang lebih baik karena jumlah kunci yang lebih sedikit Kelemahan algoritma kriptografi asimetris: Kecepatan yang lebih rendah bila dibandingkan dengan algoritma simetris. Untuk tingkat keamanan sama, kunci yang digunakan lebih panjang dibandingkan dengan algoritma simetris.

Contoh algoritma : RSA, ECC, ElGamal 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. / 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. 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 : Teks yang akan dienkripsi adalah “Hello” sebagai plaintext. Untuk mendapatkan hasil enkripsi, konversi plainteks diatas kedalam bentuk biner menggunakan kode ASCII dari “Hello”. Selanjutnya dari hasil konversi ASCII dirubah menjadi dalam bentuk biner 8bit yang menghasilkan 'H' = 01001000, 'e' = 01100101, 'l' = 01101100, 'l' = 01101100, 'o' = 01101111. Gabungkan biner menjadi satu urutan 01001000 01100101 01101100 01101100 01101111.

Bagi menjadi grup dengan panjang 6 bit 010010 000110 010110 001100 011011 110. Konversi grup ke dalam bentuk desimal 18 6 22 12 27 62. Konversi desimal ke dalam bentuk karakter Base64 SGVsbG8=. Contoh proses dekripsi : Teks yang akan didekripsi adalah “Hello” sebagai chipertext. 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. 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.

Bagi menjadi grup dengan panjang 6 bit 01001000 01100101 01101100 01101100 01101111. Konversi grup ke dalam bentuk sesuai dengan tabel ASCII 01001000 = 'H', 01100101 = 'e', 01101100 = 'l', 01101100 = 'l', 01101111 = 'o'. Konversi dan gabungkan ke dalam bentuk karakter Base64 Hello. 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: SubBytes, sebgai tranformasi subtutusi. shiftRows, sebgai tranformasi permutasi. MixColumns, sebagai tranformasi pengaacakan. AddRoundKey, sebegai tranformasi penambahan kunci. Pada ronde terakhir yaitu ronde ke-Nr dilakukan tranformasi serupa dengan ronde lain namun tanpa tranformasi serupa dengan ronde lain namun tanpa mixColumns. / 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. / 2.4. 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. Berikut adalah langkah-langkah untuk melakukan ekspansi kunci: 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]). Untuk elemen keluaran selanjutnya W[i] dengan i ={4,...,43} dihitung sebagai berikut:\ Salin W [i-1] pada word t.

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]. 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]. Evaluasi 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. Kerangka Pemikiran

BAB III METODOLOGI PENELITIAN 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. 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. Analisa Data Analisis data merupakan bagian dari proses penyelesaian masalah keamanan, yang melibatkan tahap analisis data. Dalam analisis data, dilakukan langkah-langkah sebagai berikut: Pengumpulan data yang berfungsi untuk memperoleh data yang diperlukan dalam pengujian program. Pengelompokan data sesuai dengan jenis dan fungsinya. Mencari data dalam berjenis teks (.txt .pdf) yang akan dienkripsi dalam penelitian.

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.

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 3.1. 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 rail fence cipher sehingga keluaran dari teks yang terenkripsi menjadi ciphertext. Flowchart Dekripsi Flowchart untuk dekripsi dapat dilihat pada gambar 3.2. / Gambar 3.2. Flowchart dekripsi teks Berdasarkan Gambar 3.2, Penjabaran dari flowchart dekripsi adalah teks yang terenkripsi (ciphertext) akan didekripsi menggunakan proses metode algoritma rail fence cipher, yang mana ciphertext akan dirubah menjadi plaintext kembali.

Hasil keluaran dari dekripsi merupakan teks yang bisa dibaca secara normal. 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.

INTERNET SOURCES:

---

AJEMEN_KEAMANAN_INFORMASI
<1% -
https://ultraintelijen.wordpress.com/2020/06/01/rekognisi-sigint-signal-intelligence/
<1% -
https://beritapolisi.id/kegiatan-yang-dilakukan-untuk-mengubah-data-menjadi-informasi-baru-yang-dapat-digunakan-dalam-membuat-kesimpulan-berdasarkan-pertanyaan-tersebut-adalah-penjelasan-tentang/
<1% - https://ejournal.unib.ac.id/index.php/pseudocode/article/download/1042/874
<1% - http://staffnew.uny.ac.id/upload/132319971/pendidikan/sistem+keamanan.pdf
<1% - https://gudangssl.id/blog/enkripsi-adalah/
<1% - https://academy.binance.com/id/articles/symmetric-vs-asymmetric-encryption
<1% -
https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2007-2008/Makalah1/MakalahIF5054-2007-A-021.pdf
<1% - https://e-journals.unmul.ac.id/index.php/SAKTI/article/download/1844/pdf
<1% -
http://seminar.uny.ac.id/semnasmatematika/sites/seminar.uny.ac.id.semnasmatematika/files/full/T-41.pdf
<1% - https://angkasa.co.id/apa-itu-kriptografi-ini-jenis-dan-contohnya/
<1% -
https://journal.universitassuryadarma.ac.id/index.php/jmm/article/download/585/556
<1% -
https://www.academia.edu/68890716/Enkripsi_Teks_dengan_Algoritma_Affine_Cipher
<1% - https://qastack.id/programming/3538021/why-do-we-use-base64
<1% - https://ejournal.unisba.ac.id/index.php/matematika/article/view/4067
<1% -
https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi-dan-Koding/2022-2023/Makalah2023/Makalah-KriptoKoding-2023%20(27).pdf
<1% -
https://mediaindonesia.com/ekonomi/407990/pertukaran-data-dan-informasi-kian-penting-di-masa-pandemi
<1% - http://eprints.ums.ac.id/32469/6/BAB%20I.pdf
<1% - http://repository.upi.edu/21868/6/S_IND_1008973_Chapter3.pdf
<1% -
https://www.academia.edu/6430721/PERUMUSAN_MASALAH_DAN_TUJUAN_PENELITIAN
<1% -
https://www.kompas.com/skola/read/2021/12/03/173213569/apa-itu-komunikasi-yang-efektif-dan-bagaimana-contohnya
<1% - http://scholar.unand.ac.id/8998/2/2.%20BAB%201.pdf

<1% -
https://elibrary.unikom.ac.id/id/eprint/788/8/13.%20UNIKOM_41814107_MUHAMAD%20AZHARI%20PERMADY_BAB%20II%202%20(13-75).pdf
<1% - http://etheses.uin-malang.ac.id/843/7/11510078%20Bab%203.pdf
<1% -
https://lib.ui.ac.id/file?file=digital/126768-RB13C33a-Analisis%20subyek-Analisis.pdf
<1% - http://repository.upi.edu/25588/8/D_MAT_1303391_Chapter5.pdf
<1% - http://eprints.unisnu.ac.id/id/eprint/2905/3/1312400000091_BAB%20II.pdf
<1% -
https://www.academia.edu/86581523/Implementasi_Algoritma_Base64_Sebagai_Tingkat_Keamanan_Data_Pada_Website_Sistem_Informasi_Pencatat_Barang
<1% - https://garuda.kemdikbud.go.id/documents/detail/2402547
<1% -
https://elibrary.unikom.ac.id/1468/13/UNIKOM_MOH%20YUNUS_JURNAL%20DALAM%20BAHASA%20INDONESIA.pdf
<1% -
https://123dok.com/document/y4w685r5-implementasi-pengamanan-menggunakan-algoritma-kriptografi-advanced-encryption-standard.html
<1% -
https://garuda.kemdikbud.go.id/journal/view/11756?issue=Vol%205,%20No%201%20(2021):%20Jurnal%20Rekayasa%20Teknologi%20Informasi%20(JURTI)
<1% - http://digilib.uinsgd.ac.id/1969/2/2_abstrak.pdf
<1% -
https://www.academia.edu/en/63938068/Penerapan_Kriptografi_Caesar_Chiper_Pada_Aplikasi_Chatting_Berbasis_Local_Area_Network
<1% -
https://rofendymanalu.blogspot.com/2012/12/aplikasi-chatting-multi-user-pada-local.html
<1% -
https://garuda.kemdikbud.go.id/journal/view/22108?page=1&issue=Vol%202%20No%201%20(2022):%20Journal%20of%20information%20Technology
1% - https://www.researchgate.net/figure/TEA-Decryption-Process_fig4_261181145
<1% -
https://www.researchgate.net/publication/359396506_Review_Algoritma_Kriptografi_Sistem_Keamanan_SMS_di_Android
<1% -
https://retizen.republika.co.id/posts/215554/pengamanan-data-sains-melindungi-privasi-dan-keamanan-informasi-dalam-era-big-data
<1% - https://www.asdf.id/7-aspek-keamanan-komputer-yang-harus-diperhatikan/
1% -

https://www.academia.edu/31898811/Makalah_PBX_MUHAMMAD_REZA_and_HAFIZ_RAHMAD
<1% - https://www.researchgate.net/publication/329177345_KEAMANAN_INFORMASI
<1% - https://www.jagoanhosting.com/blog/kriptografi-adalah/
<1% -
https://informatika.stei.itb.ac.id/~rinaldi.munir/Matdis/2010-2011/Makalah2010/MakalahStrukdis2010-059.pdf
<1% - https://www.hostinger.co.id/tutorial/tls-adalah
<1% - https://www.gurupendidikan.co.id/proses-komunikasi/
<1% - https://creatormedia.my.id/peranan-teknologi-informasi-dalam-perusahaan/
<1% - https://diskominfo.badungkab.go.id/artikel/18212-keamanan-jaringan
<1% - https://qwords.com/blog/social-engineering-adalah/
<1% - https://www.logique.co.id/blog/2019/09/03/serangan-social-engineering/
<1% -
https://www.researchgate.net/publication/337316007_SISTEM_INFORMASI_MANAJEMEN_KEAMANAN_INFORMASI
<1% - https://investor.id/investory/295998/apa-itu-kriptografi-dan-contohnya
<1% -
https://lp2m.uma.ac.id/2022/04/26/mengenal-kriptografi-definisi-tujuan-dan-jenis-jenisnya/
1% -
http://staffnew.uny.ac.id/upload/198412092015041001/pendidikan/Dasar-dasar%20keamanan%202rev%201.pdf
<1% -
https://repository.dinus.ac.id/docs/ajar/file_2013-08-19_23:02:32_Heru_Lestiawan,_M.Kom__Bab_4.2_keamanan-komputer_KRIPTOGRAFI.ppt
<1% - https://id.wikipedia.org/wiki/Enkripsi
<1% - https://www.websiterating.com/id/cloud-storage/what-is-aes-256-encryption/
<1% -
https://www.researchgate.net/publication/323962079_Implementasi_Kriptografi_Pengamanan_Data_Pada_Pesan_Teks_Isi_File_Dokumen_Dan_File_Dokumen_Menggunakan_Algoritma_Advanced_Encryption_Standard/fulltext/5ab50552aca2722b97c9bd02/Implementasi-Kriptografi-Pengamanan-Data-Pada-Pesan-Teks-Isi-File-Dokumen-Dan-File-Dokumen-Menggunakan-Algoritma-Advanced-Encryption-Standard.pdf
<1% -
https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2014-2015/Makalah2-2015/Makalah2_Kripto_IF4020_2015_022.pdf
<1% -
https://www.websiterating.com/id/vpn/glossary/what-is-asymmetric-symmetric-encryption/

<1% - https://ejournal3.undip.ac.id/index.php/transient/article/viewFile/22/1812
<1% - https://www.academia.edu/9786951/KRIPTOGRAFI_keamanan_jaringan
<1% -
https://indahbian.blogspot.com/2011/03/apa-sih-kriptografi-simetris-asimetris.html
<1% -
http://download.garuda.kemdikbud.go.id/article.php?article=2503592&val=23920&title=Penerapan%20Algoritma%20Kriptografi%20Twofish%20Untuk%20Mengamankan%20Data%20File
<1% -
https://www.sosial79.com/2021/08/pengertian-alphanumeric-fungsi-karakter.html

<1% -
https://support.microsoft.com/id-id/office/menyisipkan-simbol-dan-karakter-berbasis-ascii-atau-unicode-latin-d13f58d3-7bcb-44a7-a4d5-972ee12e50e0
<1% -
https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2006-2007/Makalah1/Makalah1-040.pdf
<1% - https://id.wikipedia.org/wiki/Enkripsi_basis_data
<1% - https://jurnal.uisu.ac.id/index.php/infotekjar/article/viewFile/300/pdf
<1% - https://id.wikihow.com/Mengubah-Biner-Menjadi-Desimal
<1% -
https://informatika.stei.itb.ac.id/~rinaldi.munir/AljabarGeometri/2015-2016/Makalah-2015/Makalah-IF2123-2015-111.pdf
<1% - https://stackoverflow.com/questions/64760954/binary-to-text-decryption
<1% -
https://klinikinformatikacyber.blogspot.com/2016/03/pengertian-dan-sistem-kerja-aes-iii.html
<1% -
https://informatika.stei.itb.ac.id/~rinaldi.munir/Matdis/2008-2009/Makalah2008/Makalah0809-090.pdf
<1% - https://id.wikipedia.org/wiki/National_Institute_of_Standards_and_Technology
<1% -
https://informatika.stei.itb.ac.id/~rinaldi.munir/Matdis/2017-2018/Makalah-2017/Makalah-Matdis-2017-107.pdf
<1% -
http://download.garuda.kemdikbud.go.id/article.php?article=735757&val=10384&title=Implementasi%20Algoritme%20Advance%20Encryption%20Standard%20AES%20pada%20Enkripsi%20dan%20Dekripsi%20QR-Code
<1% - https://ejournal.unisba.ac.id/index.php/matematika/article/download/4067/2398
<1% - http://digilib.uinsgd.ac.id/30825/1/11-Article%20Text-20-1-10-20180117_2.pdf

<1% -
https://karyailmiah.unisba.ac.id/index.php/matematika/article/download/4580/pdf
1% - https://ejournal.unisba.ac.id/index.php/matematika/article/viewFile/4067/2398
<1% -
https://text-id.123dok.com/document/7q07229xz-menghitung-dekripsi-aes-contoh-perhitungan.html
<1% -
https://www.researchgate.net/publication/265364513_ENKRIPSI_DAN_DEKRIPSI_DENGAN_ALGORITMA_AES_256_UNTUK_SEMUA_JENIS_FILE
<1% -
https://dqlab.id/macam-macam-metode-analisis-data-2-macam-metode-penting-dalam-mengolah-data
<1% - https://eprints.umm.ac.id/66352/4/BAB%20III.pdf
<1% - https://glints.com/id/lowongan/enkripsi-adalah/
<1% -
https://garuda.kemdikbud.go.id/author/view/201796?page=1&jid=9538&jname=InfoTekJar%20(Jurnal%20Nasional%20Informatika%20dan%20Teknologi%20Jaringan)
<1% -
http://download.garuda.kemdikbud.go.id/article.php?article=2966953&val=17623&title=Kombinasi%20Metode%20Kriptografi%20Subsitusi%20Dalam%20Pengaman%20Pesan%20dan%20Informasi
<1% -
https://www.researchgate.net/publication/370075528_PENGAMANAN_DATA_INFORMASI_DENGAN_MEMANFAATKAN_KRIPTOGRAFI_KLASIK
<1% - https://journal.ipb.ac.id/index.php/jika/article/download/32973/21682
<1% -
https://www.researchgate.net/publication/362100253_Pengamanan_Dokumen_Teks_Dengan_Menerapkan_Kombinasi_Algoritma_Kriptografi_Klasik
<1% - http://journal.upgris.ac.id/index.php/JIU/article/view/3212/2529
<1% - https://jom.fti.budiluhur.ac.id/index.php/SKANIKA/article/view/884/1144
<1% - https://senafti.budiluhur.ac.id/index.php/senafti/article/view/218