ANALISIS MODEL KRIPTOGRAFI UNTUK PROTEKSI ENKRIPSI DATA PADA JARINGAN KOMPUTER

Anjelina Hoar Seran[1], Serafina Safe[2], Mariana Seran[3], Maria Wilhelmina Usfinit[4], Siprianus Septian Manek[5]
anjelseran234@gmail.com[1], serafina34@gmail.com[2], marianaseran22@gmail.com[3], mariawilhelminausfinit@gmail.com[4], epimanek18@gmail.com[5]
Universitas Timor

ABSTRAK

Di era digital saat ini, pertukaran data melalui jaringan komputer memegang peranan penting di berbagai sektor seperti pemerintahan, bisnis, dan pendidikan. Namun, peningkatan lalu lintas data digital turut memperbesar potensi ancaman siber yang dapat mengganggu kerahasiaan, integritas, dan ketersediaan informasi. Penelitian ini mengevaluasi efektivitas penggunaan model kriptografi dalam enkripsi data sebagai mekanisme pertahanan terhadap serangan siber. Metode penelitian meliputi studi literatur, simulasi enkripsi, serta analisis terhadap potensi serangan umum seperti man-in-the-middle, penyadapan, dan brute force. Hasil penelitian menunjukkan bahwa penerapan algoritma kriptografi yang kuat seperti AES dan RSA secara signifikan memperkuat perlindungan jaringan. Penelitian ini mendukung pengembangan strategi keamanan jaringan berbasis pendekatan kriptografi yang lebih optimal.
Kata Kunci: Kriptografi, Enkripsi, Keamanan Jaringan, AES, RSA.

ABSTRACT

In today's digital landscape, data exchange over computer networks plays a vital role across multiple sectors such as governance, commerce, and education. However, the rising volume of digital communication increases the risk of cyber threats that may compromise data confidentiality, integrity, and availability. This study evaluates the effectiveness of data encryption using cryptographic models as a defense mechanism. The methodology combines literature review, encryption simulations, and analysis of vulnerability to common cyberattacks including man-in-the-middle, sniffing, and brute-force methods. Findings indicate that implementing robust cryptographic algorithms such as AES and RSA significantly strengthens network defense. This research supports the development of improved network security strategies through cryptographic techniques.
Keywords: *Cryptography, Encryption, Network Security, AES, RSA.*

PENDAHULUAN

Transformasi digital telah mendorong kebutuhan akan sistem keamanan informasi, termasuk di sektor pendidikan. Sekolah-sekolah seperti SMAN Wederok mulai mengadopsi teknologi informasi untuk mendukung kegiatan administratif dan pengelolaan data. Namun, digitalisasi ini juga membuka peluang bagi potensi ancaman keamanan seperti pencurian dan manipulasi data oleh pihak tak bertanggung jawab. Data sensitif seperti nilai siswa dan informasi internal sekolah perlu dijaga agar tetap aman dan utuh. Salah satu pendekatan yang efektif adalah penerapan teknologi kriptografi untuk mendukung proses enkripsi data dalam komunikasi jaringan.

Informasi seperti data pribadi siswa, nilai akademik, dan dokumen internal sekolah tergolong sangat sensitif dan rawan disalahgunakan. Oleh karena itu, upaya melindungi kerahasiaan serta integritas data menjadi hal yang krusial. Salah satu solusi strategis yang dapat diterapkan untuk mengatasi tantangan ini adalah dengan mengimplementasikan teknologi enkripsi berbasis kriptografi.

Kriptografi adalah metode pengamanan informasi dengan cara mengubahnya menjadi format yang tidak dapat dimengerti oleh pihak yang tidak memiliki otorisasi. Proses enkripsi memungkinkan data tetap aman saat dikirim melalui jaringan yang rentan terhadap

serangan. Oleh karena itu, model kriptografi harus dirancang untuk mampu menangkal berbagai jenis ancaman, baik yang bersifat pasif seperti penyadapan maupun aktif seperti manipulasi data.

Penelitian ini bertujuan untuk mengevaluasi efektivitas penggunaan kriptografi dalam mengamankan data dari serangan siber melalui komunikasi jaringan komputer. Fokus studi dilakukan di lingkungan SMAN Wederok, sebagai representasi sekolah menengah yang telah terdigitalisasi. Selain itu, penelitian ini juga mengidentifikasi potensi celah keamanan serta menawarkan rekomendasi perlindungan berbasis enkripsi untuk meningkatkan ketahanan sistem informasi sekolah.

Dengan mengkaji penerapan algoritma enkripsi seperti Advanced Encryption Standard (AES) dan Rivest–Shamir–Adleman (RSA), penelitian ini diharapkan dapat memberikan kontribusi terhadap perumusan kebijakan keamanan jaringan yang lebih tangguh di sektor pendidikan, terutama dalam menghadapi kompleksitas ancaman digital masa kini.

METODE PENELITIAN

Penelitian ini mengadopsi metode deskriptif kualitatif, yang bertujuan untuk memberikan gambaran menyeluruh mengenai efektivitas penerapan model kriptografi dalam menjaga keamanan data yang dikirim melalui jaringan komputer. Fokus utama ditekankan pada identifikasi potensi celah keamanan dan pengujian sederhana terhadap algoritma enkripsi dalam konteks pendidikan, khususnya di SMAN Wederok.

1. Studi Literatur

   Langkah awal penelitian melibatkan penelusuran dan analisis terhadap berbagai referensi ilmiah, termasuk buku, jurnal akademik, dan dokumentasi teknis terkait kriptografi dan keamanan jaringan. Beberapa aspek penting yang menjadi landasan dalam kajian literatur ini antara lain:

   a. Konsep dasar kriptografi simetris dan asimetris
   b. Karakteristik algoritma enkripsi seperti AES dan RSA,
   c. Jenis-jenis serangan terhadap sistem enkripsi, seperti ciphertext-only, known-plaintext, dan chosen-ciphertext
   d. Standar keamanan jaringan dan kebijakan pengelolaan kunci dalam sistem informasi

   Kajian ini memberikan fondasi teoritis yang dibutuhkan untuk memahami tantangan dan solusi yang berkaitan dengan perlindungan data dalam komunikasi jaringan komputer.

2. Simulasi Enkripsi

   Untuk menilai efektivitas dari algoritma kriptografi yang dibahas, penulis melakukan simulasi teknis menggunakan dua algoritma utama, yaitu:

   a. AES (Advanced Encryption Standard): Sebagai representasi kriptografi kunci simetris.
   b. RSA (Rivest–Shamir–Adleman): Sebagai representasi kriptografi kunci publik atau asimetris.

   Simulasi dilakukan dalam skala kecil guna menguji bagaimana kedua algoritma tersebut bekerja dalam mengamankan data serta potensi performa dan efisiensinya dalam skenario jaringan komputer.

3. Analisis Kerentanan

   Penelitian ini juga mencakup evaluasi terhadap berbagai skenario serangan yang umum terjadi dalam komunikasi jaringan, seperti:

   a. Man-in-the-Middle (MitM) Attack
   b. Sniffing / Interception

c. Brute Force dan Dictionary Attack
d. Serangan terhadap protokol otentikasi dan pertukaran kunci

Analisis dilakukan untuk memahami sejauh mana algoritma kriptografi mampu menahan jenis serangan tersebut, serta bagaimana sistem dapat diperkuat untuk mencegah pelanggaran keamanan data.

4. Studi Kasus di SMAN WEDEROK

sebagai bagian dari implementasi konteks nyata, penelitian ini mengambil studi kasus di SMAN Wederok. Observasi dilakukan untuk memahami kebutuhan keamanan informasi yang berlaku di lingkungan sekolah, termasuk jenis data yang dikelola serta potensi risiko yang timbul apabila tidak dilindungi secara memadai. Analisis ini membantu menyusun rekomendasi praktis yang dapat diterapkan oleh institusi pendidikan dalam meningkatkan sistem keamanan berbasis kriptografi.

Seluruh metode di atas digunakan secara berurutan dan saling melengkapi untuk menghasilkan pemahaman teoritis sekaligus gambaran nyata mengenai perlindungan data menggunakan teknik enkripsi di lingkungan sekolah.

HASIL DAN PEMBAHASAN

A. Analisis Celah Keamanan: Potensi Serangan dalam Sistem Kriptografi

Dalam proses enkripsi dan dekripsi, penggunaan kunci rahasia merupakan elemen krusial. Ada dua pendekatan utama dalam kriptografi: kriptografi simetris dan kriptografi asimetris. Pada pendekatan simetris, satu kunci yang sama digunakan baik untuk mengenkripsi maupun mendekripsi data. Sebaliknya, pendekatan asimetris menggunakan dua kunci berbeda — satu publik dan satu privat — untuk menjaga keamanan komunikasi.

Setiap metode enkripsi memiliki kerentanan terhadap berbagai bentuk serangan. Serangan tersebut pada dasarnya terbagi menjadi dua kategori:

1. Serangan Pasif: Penyerang hanya mengamati lalu lintas data tanpa mengubahnya. Tujuan utamanya adalah mengakses informasi tanpa diketahui oleh pengirim atau penerima.
2. Serangan Aktif: Penyerang secara langsung memodifikasi, menyisipkan, atau menghapus data selama proses transmisi. Serangan ini mengancam integritas dan keaslian informasi.

Penyerang umumnya berusaha untuk mengakses atau menebak kunci enkripsi agar dapat mengungkap isi pesan yang terlindungi. Berdasarkan strategi penyerangan, berikut adalah jenis-jenis serangan kriptografi yang umum dijumpai:

1. Ciphertext-only attack: Penyerang hanya memiliki data terenkripsi (ciphertext) dan mencoba menebak isi pesan.
2. Known-plaintext attack: Penyerang memiliki akses terhadap pasangan data plaintext dan ciphertext, yang digunakan untuk mengungkap kunci enkripsi.
3. Chosen-plaintext attack: Penyerang dapat memilih plaintext tertentu dan mengamati ciphertext hasil enkripsi untuk mempelajari pola.
4. Adaptive chosen-plaintext attack: Serangan lanjutan dari chosen-plaintext, di mana penyerang secara bertahap menyesuaikan plaintext berdasarkan hasil enkripsi sebelumnya.
5. Chosen-ciphertext attack: Penyerang mencoba menganalisis ciphertext yang dipilihnya untuk memperoleh plaintext dari sistem dekripsi.
6. Adaptive chosen-ciphertext attack: Penyerang mengakses perangkat dekripsi dan menyesuaikan ciphertext berdasarkan respons dekripsi yang diperoleh.

Pemahaman terhadap jenis-jenis serangan ini sangat penting untuk merancang sistem keamanan yang mampu menanggulangi risiko tersebut sejak tahap desain.

B. Evaluasi Perlindungan pada Sistem Kriptografi Kunci Publik dan Rahasia

Setelah mengidentifikasi berbagai ancaman yang mungkin muncul, langkah penting selanjutnya adalah menganalisis bagaimana sistem kriptografi dapat memberikan perlindungan yang efektif. Sistem kriptografi bekerja berdasarkan fungsi enkripsi-dekripsi yang dikendalikan oleh seperangkat parameter kunci. Sistem ini sering disebut sebagai cryptosystem, yang mencakup metode transformasi data dari bentuk asli ke bentuk terenkripsi dan sebaliknya.

Pada sistem dengan kunci tunggal (kriptografi simetris), tantangan utamanya adalah mendistribusikan kunci secara aman antara pengirim dan penerima. Jika proses distribusi tidak terlindungi dengan baik, maka kunci dapat diakses pihak tidak sah dan membahayakan integritas data.

Sebagai solusi, penggunaan kriptografi asimetris menjadi alternatif yang lebih aman. Dalam sistem ini, pesan dienkripsi menggunakan kunci publik dan hanya dapat didekripsi dengan kunci privat milik penerima. Dengan demikian, tidak ada kebutuhan untuk berbagi kunci rahasia secara langsung.

Secara matematis, proses ini dapat dirumuskan sebagai:

E_K(M) = C → enkripsi pesan M dengan kunci K menghasilkan ciphertext C

D_K(C) = M → dekripsi C menggunakan K akan mengembalikan pesan asli M

Dalam proses enkripsi, pesan M disandikan menggunakan kunci K sehingga menghasilkan ciphertext C. Sebaliknya, pada proses dekripsi, ciphertext C diuraikan kembali dengan menggunakan kunci K untuk memperoleh pesan M yang identik dengan pesan aslinya. Oleh karena itu, keamanan suatu pesan sangat bergantung pada kunci atau kombinasi kunci yang digunakan, bukan pada algoritma enkripsinya. Hal ini memungkinkan algoritma yang digunakan untuk dipublikasikan dan dianalisis secara terbuka, serta memungkinkan pengembangan produk yang mengimplementasikannya secara massal. Dengan demikian, tidak menjadi masalah apabila seseorang mengetahui algoritma yang digunakan. Selama kunci yang digunakan tetap dirahasiakan, pihak tersebut tetap tidak akan mampu membaca isi pesan yang telah dienkripsi.

Teknik enkripsi asimetris memiliki kecepatan yang jauh lebih rendah dibandingkan dengan enkripsi menggunakan kunci simetris. Oleh karena itu, dalam praktiknya, enkripsi asimetris biasanya tidak digunakan untuk menyandikan pesan secara langsung. Sebagai gantinya, kunci simetris dienkripsi terlebih dahulu menggunakan kunci asimetris, kemudian pesan utama dikirim setelah dienkripsi dengan kunci simetris tersebut.

Public-key CryptoSystems memiliki dua fungsi utama, yaitu enkripsi dan tanda tangan digital. Dalam sistem ini, setiap individu memiliki sepasang kunci, yaitu kunci publik dan kunci privat. Kunci publik dipublikasikan secara terbuka, sementara kunci privat dijaga kerahasiaannya. Kunci privat ini juga dikenal dalam kriptografi sebagai Secret-key Cryptography. Secret-key Cryptography, yang kadang disebut sebagai Symmetric Cryptography, adalah bentuk kriptografi yang lebih tradisional, di mana satu kunci tunggal digunakan untuk mengenkripsi dan mendekripsi pesan. Selain digunakan dalam enkripsi, Secret-key Cryptography juga berhubungan dengan otentikasi. Salah satu teknik dalam kategori ini adalah message authentication codes.

Masalah utama yang dihadapi oleh sistem Secret-key Cryptography adalah bagaimana memastikan bahwa pengirim dan penerima dapat sepakat mengenai kunci rahasia tanpa pihak ketiga mengetahui kunci tersebut. Hal ini memerlukan metode yang memungkinkan kedua pihak berkomunikasi dengan aman, tanpa takut disadap. Dibandingkan dengan

Public-key Cryptography, Secret-key Cryptography memiliki kelebihan dalam hal kecepatan. Beberapa teknik yang paling umum digunakan dalam Secret-key Cryptography meliputi block ciphers, stream ciphers, dan message authentication codes.

Dalam sistem ini, kebutuhan untuk pengirim dan penerima untuk berbagi informasi rahasia dihilangkan. Semua komunikasi hanya melibatkan kunci publik, sementara kunci privat tidak pernah dikirimkan atau digunakan bersama. Dengan demikian, tidak ada lagi kebutuhan untuk mengandalkan keamanan peralatan komunikasi. Yang diperlukan hanya kunci publik yang terasosiasi dengan penggunanya melalui cara yang dapat dipercaya dan telah diotentikasi (misalnya, melalui direktori yang tepercaya). Setiap orang dapat mengirimkan pesan rahasia hanya dengan menggunakan kunci publik, namun pesan tersebut hanya dapat didekripsi dengan kunci privat yang dimiliki oleh penerima yang dituju. Lebih lanjut, Public-key Cryptography tidak hanya dapat digunakan untuk menjaga kerahasiaan pesan (enkripsi), tetapi juga untuk otentikasi (seperti tanda tangan digital) serta aplikasi lainnya.

C. Peran Sertifikasi Kunci Publik dalam Keamanan Enkripsi

Dalam sistem kriptografi kunci publik, penting untuk memastikan bahwa kunci publik yang digunakan benar-benar milik entitas yang dimaksud. Untuk itu, sistem sertifikasi digital melalui Certificate Authority (CA) digunakan sebagai pihak ketiga yang menjamin keaslian identitas pemilik kunci.

CA menerbitkan sertifikat digital yang memuat informasi identitas pengguna, kunci publik, serta validitas dan otentikasi digital. Sertifikat ini ditandatangani secara digital menggunakan kunci privat milik CA, sehingga validitasnya dapat diverifikasi oleh siapa pun melalui kunci publik CA.

Sertifikat digital juga dapat berisi elemen tambahan seperti alamat email, nama organisasi, dan hash data tertentu. Mekanisme ini sangat penting dalam mencegah serangan man-in-the-middle, di mana penyerang berpura-pura menjadi pihak yang sah untuk memperoleh akses.

Jika sebuah sertifikat tidak lagi valid, maka akan dicantumkan dalam Certificate Revocation List (CRL), yang merupakan daftar resmi dari CA tentang sertifikat yang telah dicabut karena kompromi atau alasan administratif lainnya.

Secara teori, salah satu keunggulan tanda tangan digital adalah kemampuannya untuk melakukan otentikasi secara offline. Pemeriksa cukup memiliki kunci publik dari sistem operasi utama untuk memverifikasi keabsahan kunci publik lawan bicaranya. Untuk meningkatkan keamanan, kunci publik sistem operasi utama juga dapat diintegrasikan dalam program aplikasi. Namun, dalam praktiknya, ada kemungkinan sertifikat digital hilang, dicuri, atau identitas pemiliknya berubah (misalnya perubahan alamat email atau nomor KTP). Oleh karena itu, sertifikat digital perlu diverifikasi keabsahannya dengan memeriksa daftar sertifikat yang dicabut (Certificate Revocation List) yang disimpan oleh sistem operasi.

Secara umum, sistem kriptografi dapat dipahami melalui tiga dimensi independen. Pertama, jenis operasi yang digunakan untuk mengubah plaintext menjadi ciphertext. Semua algoritma enkripsi didasarkan pada dua prinsip dasar: substitution, di mana setiap elemen dalam plaintext (seperti bit, huruf, atau kelompoknya) dipetakan ke elemen lainnya, dan transposition, di mana elemen-elemen dalam plaintext diatur ulang (rearranged). Persyaratan mendasar adalah tidak ada informasi yang hilang, sehingga setiap operasi harus bersifat dapat dibalik (reversible). Kedua, jumlah kunci yang digunakan. Jika pengirim dan penerima menggunakan kunci yang sama, sistem ini disebut simetris, atau enkripsi kunci tunggal. Jika pengirim dan penerima menggunakan kunci yang berbeda, sistem ini disebut asimetris, atau enkripsi kunci publik. Ketiga, cara pemrosesan plaintext. Dalam blok cipher,

sebuah blok elemen input diproses pada satu waktu untuk menghasilkan satu blok output. Sedangkan dalam stream cipher, elemen-elemen input diproses secara berkelanjutan untuk menghasilkan elemen output satu per satu.

D. Analisa Generalisasi Standar Keamanan Data pada Kriptografi

Standar sangat penting dalam kriptografi untuk menciptakan interoperabilitas dalam dunia keamanan informasi. Pada dasarnya, standar merujuk pada kondisi dan protokol yang dirancang untuk memastikan keseragaman dalam komunikasi, transaksi, dan berbagai aktivitas virtual. Perkembangan teknologi informasi yang terus-menerus mendorong pengembangan lebih banyak standar, yang berfungsi sebagai panduan dalam proses evolusi ini. Tujuan utama dari standar adalah untuk memungkinkan teknologi dari berbagai penyedia untuk "berbicara dengan bahasa yang sama", sehingga dapat berinteraksi dengan efektif.

Dalam kriptografi, standarisasi memiliki tujuan tambahan, yaitu untuk menyediakan dasar bagi pengembangan teknik-teknik kriptografi. Protokol yang kompleks cenderung mengandung kelemahan dalam desainnya. Dengan menerapkan standar yang telah teruji, industri dapat menghasilkan produk yang lebih dapat diandalkan. Bahkan protokol yang sudah dianggap aman pun akan lebih dipercaya oleh pelanggan setelah diadopsi sebagai standar, karena telah melalui proses verifikasi yang ketat.

Pemerintah, sektor industri swasta, dan berbagai organisasi lainnya turut berperan besar dalam pengembangan standar-standar kriptografi. Beberapa standar yang dihasilkan di antaranya berasal dari ISO, ANSI, IEEE, NIST, dan IETF. Terdapat berbagai jenis standar, ada yang digunakan dalam industri perbankan, beberapa berskala internasional, dan lainnya digunakan oleh pemerintah. Proses standarisasi ini membantu pengembang dalam merancang standar baru, yang memungkinkan mereka untuk mengikuti pedoman yang telah ada dalam proses pengembangan. Dengan cara ini, pelanggan memiliki kebebasan untuk memilih produk atau layanan yang bersaing dan memenuhi standar tersebut.

Dalam sebuah perusahaan atau sekolah, penting untuk menyadari perlunya mekanisme enkripsi password yang lebih aman, terutama jika kebutuhan keamanan data semakin tinggi. Salah satu solusi yang dapat diterapkan adalah penggunaan mekanisme One Time Password (OTP) untuk menggantikan mekanisme password statis yang kurang aman.

Keunggulan dari mekanisme One Time Password (OTP) adalah bahwa password hanya dapat digunakan sekali setiap kali pengguna melakukan log in ke sistem. Meskipun seorang penyerang berhasil memperoleh password tersebut, ia tidak akan bisa menggunakannya lagi untuk mengakses sistem. Teknik enkripsi yang dapat diterapkan dalam mekanisme ini adalah teknik enkripsi simetris atau kunci rahasia.

Ada banyak algoritma yang dapat digunakan untuk mengenkripsi password, seperti DES, AES, Blowfish, RC6, dan lainnya. Hal utama yang dibutuhkan adalah sumber daya manusia yang memiliki kemampuan untuk mengimplementasikan algoritma-algoritma ini, salah satunya melalui PEM (Privacy-Enhanced Mail). PEM mendukung enkripsi dan otentikasi untuk email di Internet. Penggunaan perangkat baru ini bertujuan untuk mengurangi potensi celah keamanan yang dapat dimanfaatkan untuk mencuri data, meskipun kriptografi sudah digunakan dalam proses pengiriman data. Untuk enkripsi pesan, PEM menggunakan Triple DES-EDE dengan pasangan kunci simetris. Algoritma Hash seperti RSA, MD2, atau MD5 digunakan untuk menghasilkan message digest, sementara enkripsi kunci publik TSA digunakan untuk implementasi tanda tangan digital dan distribusi kunci rahasia. PEM juga menggunakan sertifikat yang berdasarkan standar X.509 yang dihasilkan oleh CA (Certificate Authority) formal.

Untuk memperjelas permasalahan terkait ancaman terhadap data email, penulis perlu menambahkan bahwa aplikasi kriptografi lainnya yang dapat diimplementasikan dalam

perusahaan adalah enkripsi email. Enkripsi email penting untuk melindungi surat-surat penting yang dikirimkan, baik yang masuk maupun keluar dari perusahaan. Contohnya adalah pengiriman data laporan rugi-laba suatu perusahaan kepada pihak penagih pajak, atau pengiriman surat-surat berharga lainnya.

Untuk mengimplementasikan enkripsi email, perusahaan harus terhubung dengan Internet. Salah satu aplikasi enkripsi email yang dapat diadopsi adalah Pretty Good Privacy (PGP), yang tersedia secara gratis. Selain digunakan untuk mengenkripsi email, PGP juga dapat dimanfaatkan untuk tanda tangan digital jika perusahaan membutuhkan tingkat keamanan yang lebih tinggi.

KESIMPULAN

Sebagai simpulan, meskipun enkripsi memiliki potensi sebagai senjata ampuh dalam meningkatkan sistem keamanan, ia juga memiliki lubang-lubang keamanan yang perlu diwaspadai. Seiring dengan kemajuan teknologi dan penggunaan data vital seperti email, yang sering menjadi sasaran serangan dari pihak-pihak yang tidak bertanggung jawab, meskipun sudah diterapkan model kriptografi dan enkripsi, tetap ada kebutuhan untuk memperbarui dan menggunakan perangkat terbaru.

Dalam hal ini, penggunaan PEM (Privacy Enhanced Mail) sangat dianjurkan. PEM adalah standar yang diusulkan oleh IETF (Internet Engineering Task Force) untuk mematuhi standar kriptografi kunci publik (PKCS). PEM ini dikembangkan oleh konsorsium besar yang melibatkan Microsoft, Novell, dan Sun Microsystems, untuk meningkatkan keamanan komunikasi email melalui enkripsi dan otentikasi yang lebih kuat.

Dengan mengadopsi standar ini, sekolah dan individu dapat memitigasi potensi risiko keamanan yang terkait dengan pengiriman data sensitif melalui email.

Secara umum, penerapan mekanisme kriptografi di perusahaan dapat dilakukan dengan relatif mudah tanpa memerlukan banyak modifikasi, karena banyak algoritma enkripsi yang sudah tersedia secara gratis dan dapat diakses dengan mudah. Hal ini memungkinkan perusahaan untuk mengembangkan dan mengimplementasikan sistem enkripsi sesuai dengan lingkungan dan kebutuhan spesifik mereka.

Pengembangan sistem enkripsi ini dapat dilakukan secara in-house jika perusahaan memiliki divisi TI yang mampu menangani hal tersebut, atau bisa juga dilakukan dengan menggunakan outsource jika perusahaan memilih untuk bekerja sama dengan pihak ketiga yang memiliki keahlian dalam bidang tersebut.

Penerapan kriptografi ini tentunya harus mempertimbangkan tingkat urgensi dan kerahasiaan data yang akan dienkripsi. Pemilihan teknik enkripsi dan jenis data yang akan dienkripsi disesuaikan dengan kebutuhan keamanan perusahaan. Misalnya, data sensitif seperti informasi keuangan atau data pelanggan harus dilindungi dengan metode enkripsi yang lebih kuat dan sesuai dengan standar keamanan yang berlaku.

DAFTAR PUSTAKA

Amalya, N., Sopiana Silalahi, S. M., Nasution, D. F., Sari, M., & Gunawaan, I. (2023a). JURNAL MEDIA INFORMATIKA [JUMIN] Kriptografi dan Penerapannya Dalam Sistem Keamanan Data.

Amalya, N., Sopiana Silalahi, S. M., Nasution, D. F., Sari, M., & Gunawaan, I. (2023b). JURNAL MEDIA INFORMATIKA [JUMIN] Kriptografi dan Penerapannya Dalam Sistem Keamanan Data.

Arif, Z., & Nurokhman, A. (2023). Analisis Perbandingan Algoritma Kriptografi Simetris Dan Asimetris Dalam Meningkatkan Keamanan Sistem Informasi Comparative Analysis of Symmetric and Asymmetric Cryptographic Algorithms in Improving Information System Security. In JTSI (Vol. 4, Issue 2).

Fithria, N. (n.d.). Jenis-Jenis Serangan terhadap Kriptografi.

Kautsar, A., & Ikhsan, M. (n.d.). Sistemasi: Jurnal Sistem Informasi Implementasi Algoritma Advanced Encryption Standard (AES) dan Teknik Steganografi Bit Plane Complexity Segmentation (BPCS) dalam Eskalasi Keamanan File Teks Implementation of the Advanced Encryption Standard (AES) Algorithm and Bit Plane Complexity Segmentation (BPCS) Steganography Technique for Enhancing Text File Security. http://sistemasi.ftik.unisi.ac.id

Sulastri, S., Defi, R., & Putri, M. (n.d.). Implementasi Enkripsi Data Secure Hash Algorithm (SHA-256) dan Message Digest Algorithm (MD5) pada Proses Pengamanan Kata Sandi Sistem Penjadwalan Karyawan.