E-ISSN : 2988-1986
https://ejournal.warunayama.org/kohesi

Kohesi: Jurnal Multidisiplin Saintek
Volume 6 No 11 Tahun 2025

# PENDEKATAN PERLINDUNGAN DATA YANG EFEKTIF DENGAN METODE DAN ALGORITMA KRIPTOGRAFI UNTUK MENINGKATKAN KERAHASIAAN DATA

**Muhammad Noval Rais[1], Kevin Nabil Mahardhika[2], Shakil Mardhika Azhar[3]**
[1,2,3] Informatics Engineering, Faculty of Computer Science, Esa Unggul University
West Jakarta, Indonesia
vallrais23@student.esaunggul.ac.id[1], kevinnabil234@student.esaunggul.ac.id[2],
mardhikazhar@student.esaunggul.ac.id[3]

***Abstract***

*In the growing digital era, data protection has become a very important aspect to maintain the confidentiality and integrity of information. Data security threats and internal and external attacks such as identity theft, hacking, and malware can result in losses and compromise data confidentiality. This article uses the narrative review research method to examine various effective data protection approaches by highlighting various cryptographic methods and algorithms that can be used to enhance data confidentiality, with the aim of providing in-depth insight into effective techniques or methods in protecting information from security threats. In addition, the article also highlights the importance of implementing effective cryptographic security to ensure data confidentiality. The results of the study show that the combined use of appropriate cryptographic algorithms, along with good key management and strict security policies, can significantly improve the security and reliability of the system. As such, this research makes an important contribution to the development of more effective data protection strategies in an increasingly complex digital age.*

***Keywords***: *Cryptography, Data Confidentiality, Security Threats, Cryptographic Methods, Data Protection*

**Abstrak**

Dalam era digital yang semakin berkembang, perlindungan data menjadi aspek yang sangat penting untuk menjaga kerahasiaan dan integritas informasi. Ancaman keamanan data dan serangan internal maupun eksternal seperti pencurian identitas, peretasan, dan malware dapat mengakibatkan kerugian dan mengganggu kerahasiaan data. Artikel ini menggunakan metode penelitian *narrative review* untuk mengkaji berbagai pendekatan perlindungan data yang efektif dengan menyoroti berbagai metode dan algoritma kriptografi yang dapat digunakan untuk meningkatkan kerahasiaan data, dengan tujuan memberikan wawasan mendalam mengenai teknik atau metode yang efektif dalam melindungi informasi dari ancaman keamanan. Selain itu, artikel ini juga menyoroti pentingnya penerapan keamanan kriptografi yang efektif untuk memastikan kerahasiaan data. Hasil kajian menunjukkan bahwa kombinasi penggunaan algoritma kriptografi yang tepat, bersama dengan manajemen kunci yang baik dan kebijakan keamanan yang ketat, mampu meningkatkan keamanan dan keandalan sistem secara signifikan. Dengan demikian, penelitian ini memberikan kontribusi penting bagi

**Article History**
Received: Januari 2025
Reviewed: Januari 2025
Published: Januari 2025

Plagirism Checker No 234
Prefix DOI : Prefix DOI : 10.8734/Kohesi.v1i2.365
**Copyright : Author**
**Publish by : Kohesi**

pengembangan strategi perlindungan data yang lebih efektif di era digital yang semakin kompleks.
**Kata Kunci**: Kriptografi, Kerahasiaan Data, Ancaman Keamanan, Metode Kriptografi, Perlindungan Data

## 1. PENDAHULUAN

Di era digital yang terus berkembang, tantangan terkait perlindungan data semakin kompleks dan memerlukan perhatian serius. Seiring dengan pesatnya perkembangan teknologi informasi, serta meningkatnya interaksi dan transaksi di dunia maya, ancaman terhadap keamanan data juga semakin beragam dan sulit diantisipasi. Berbagai jenis serangan, baik yang bersifat eksternal seperti peretasan, *malware*, dan *distributed denial of service* (DDoS), maupun ancaman internal seperti pencurian identitas, penyalahgunaan akses, dan kebocoran data oleh pihak yang berwenang, terus menjadi masalah yang kian mendesak (Andryanto Aman, 2023). Ancaman-ancaman ini memiliki potensi besar untuk merugikan individu atau kelompok baik secara finansial maupun dari sisi reputasi, sehingga perlindungan data menjadi prioritas utama dalam keamanan informasi. (Annisa Thahara, 2021).

Pengelolaan dan perlindungan data yang efektif tidak hanya dapat dicapai melalui langkah-langkah preventif seperti pengamanan jaringan dan sistem keamanan fisik, tetapi juga membutuhkan pendekatan yang lebih mendalam dan sistematis dalam mengimplementasikan teknologi keamanan modern. Salah satu pendekatan yang telah terbukti efektif adalah kriptografi, yang menggunakan metode enkripsi dan dekripsi untuk melindungi kerahasiaan dan integritas data. Kriptografi memungkinkan informasi sensitif diubah menjadi format yang hanya dapat dibaca oleh pihak yang memiliki kunci dekripsi yang tepat, sehingga mencegah akses tidak sah ke dalam data tersebut (Dola Ramalinda, 2024; Surya Kusuma, 2023). Dalam konteks ini, pemilihan algoritma kriptografi yang tepat, manajemen kunci yang baik, serta kebijakan keamanan yang ketat menjadi faktor penting untuk memastikan perlindungan data dari berbagai ancaman.

Pemilihan algoritma kriptografi yang tepat menjadi aspek krusial dalam menjaga keamanan data. Algoritma yang kuat dapat melindungi data dari berbagai bentuk serangan, sementara manajemen kunci yang baik memastikan bahwa kunci enkripsi tidak jatuh ke tangan yang salah. Di sisi lain, penerapan kebijakan keamanan yang ketat, yang mencakup pengelolaan akses, audit sistem, dan pemantauan aktif terhadap ancaman keamanan, turut berperan dalam meningkatkan keamanan sistem secara keseluruhan.

Penelitian ini bertujuan untuk memberikan wawasan yang mendalam mengenai pendekatan perlindungan data yang efektif, dengan menyoroti metode dan algoritma kriptografi yang dapat digunakan untuk meningkatkan kerahasiaan dan keamanan data. Kajian ini dilakukan melalui *narrative review* terhadap berbagai literatur yang relevan dalam bidang keamanan informasi. Fokus utama penelitian ini adalah mengidentifikasi teknik dan algoritma yang paling efektif dalam menjaga kerahasiaan informasi, serta memberikan panduan dalam menerapkan strategi perlindungan data yang lebih baik.

Melalui tinjauan ini, diharapkan dapat ditemukan strategi yang efektif dalam melindungi kerahasiaan data dari ancaman yang semakin kompleks di era digital. Hasil dari penelitian ini juga diharapkan dapat memberikan kontribusi bagi pengembangan kebijakan keamanan yang lebih baik dan penguatan sistem yang mampu menghadapi berbagai jenis serangan siber.

## 2. TINJAUAN PUSTAKA

### 2.1 PENGERTIAN KRIPTOGRAFI

Kriptografi adalah sebuah ilmu dan seni yang berhubungan dengan teknik-teknik pengamanan informasi dan komunikasi melalui penggunaan kode yang berhubungan erat dengan keamanan data (Rifky Priambudi, 2022), Kriptografi menjamin bahwa informasi hanya dapat diakses dan dipahami oleh pihak-pihak yang berwenang. Secara etimologis, istilah 'kriptografi' berasal dari bahasa Yunani, di mana 'kryptos' berarti 'tersembunyi' dan 'graphein' berarti

'tulisan'(Dimas Krisna Maulana, 2023). Kriptografi secara harfiah berarti “tulisan tersembunyi” atau teknik untuk menyembunyikan informasi sehingga akses yang tidak sah tidak dapat dilakukan.

Menurut (Kiki Andrea, 2023) Kriptografi memiliki tiga tujuan dasar aspek keamanan informasi, yaitu:

- Kerahasiaan, yang digunakan untuk menjaga isi informasi agar tetap terlindungi dan hanya dapat diakses oleh pihak yang berwenang. Prinsip ini memastikan bahwa informasi yang terenkripsi atau terkunci tidak diungkapkan tanpa izin.
- Integritas data, yang secara langsung melindungi data dari perubahan yang tidak sah. Sistem ini mampu mendeteksi adanya manipulasi atau perubahan data yang dilakukan oleh pihak yang tidak berwenang.
- Autentikasi, yaitu proses untuk memverifikasi suatu klaim, seperti memastikan identitas pengguna, guna menjaga keamanan. Proses ini melibatkan pemeriksaan keaslian data, waktu pengiriman, dan aspek relevan lainnya..

Kriptografi memainkan peran penting dalam menjaga keamanan informasi dan komunikasi melalui penggunaan teknik keamanan seperti enkripsi dan penyandian. Teknik kriptografi digunakan untuk memastikan bahwa data dijaga kerahasiaannya, utuh, dan diautentikasi sehingga hanya pihak yang berwenang yang dapat mengakses dan memodifikasinya.(Pratiwi et al., 2022) Dengan demikian, kriptografi membantu melindungi data dari akses yang tidak sah, manipulasi, dan ancaman lain yang dapat membahayakan keamanan informasi. Oleh karena itu, penggunaan teknik kriptografi sangat penting untuk menjaga keamanan informasi di era digital yang terus berkembang ini.

## 2.2 KERAHASIAAN DATA

Kerahasiaan data adalah elemen penting dalam upaya perlindungan informasi di era digital saat ini, yang semakin rawan terhadap ancaman seperti pencurian identitas, peretasan, dan malware. Dalam konteks ini, kriptografi menjadi solusi yang sangat efektif untuk menjaga kerahasiaan informasi. Metode kriptografi seperti **AES-256** dan **MD5** digunakan untuk mengamankan data sensitif perusahaan, seperti yang diimplementasikan dalam penelitian pengamanan data perusahaan teknologi. Kombinasi dari algoritma enkripsi ini terbukti ampuh melindungi dokumen dari ancaman internal maupun eksternal (Aldianto & Wibowo, 2023).

Selain itu, penerapan kriptografi dalam *smart grid* telah terbukti sangat efektif dalam menjaga keamanan data pelanggan yang dihasilkan dari interaksi antara perangkat cerdas dan sistem distribusi listrik. Dalam konteks *smart grid*, di mana sistem listrik tradisional terhubung dengan jaringan komunikasi digital, keamanan data menjadi sangat penting untuk mencegah gangguan dan potensi serangan siber yang dapat membahayakan operasional jaringan listrik serta privasi pengguna(Hafizh Fianto Putra, 2019).

Meskipun kriptografi sederhana seperti Caesar Cipher masih digunakan dalam skala kecil, metode ini tetap menunjukkan prinsip dasar bagaimana enkripsi dapat melindungi kerahasiaan data. Caesar Cipher, yang menggantikan setiap huruf dengan huruf lain berdasarkan pergeseran alfabet, mungkin tidak lagi cukup untuk melawan ancaman modern, tetapi metode ini memberikan gambaran tentang konsep enkripsi yang mendasar. Dalam konteks tertentu, seperti untuk pembelajaran atau enkripsi sementara, metode sederhana ini masih relevan. Ini menunjukkan bahwa setiap metode enkripsi, mulai dari yang paling dasar hingga yang paling kompleks, memiliki perannya masing-masing dalam melindungi informasi, tergantung pada tingkat keamanan yang dibutuhkan oleh sistem tersebut (Febrianingsih & Hafiz, 2019).

Di dunia digital yang semakin kompleks, metode kriptografi, baik melalui enkripsi sederhana maupun yang canggih, terbukti efektif dalam melindungi data sensitif dari akses yang tidak sah. Dengan menggunakan algoritma enkripsi yang sesuai dengan kebutuhan, mulai dari metode dasar seperti Caesar Cipher hingga yang lebih kompleks seperti AES-256 dan RSA, kriptografi mampu menjaga kerahasiaan informasi dan mengurangi risiko penyalahgunaan data.

## 2.3 ANCAMAN KEAMANAN DATA

Ancaman keamanan data adalah segala bentuk bahaya atau tindakan yang dapat menyebabkan kerusakan, kehilangan, atau akses tidak sah ke data yang disimpan, diproses, atau dikirim oleh suatu sistem. Ancaman ini dapat berasal dari berbagai sumber, baik internal maupun eksternal, dan dapat membahayakan orang, kelompok, atau perusahaan (Adisya Poeja Kehista, 2023).

Ada beberapa bentuk ancaman keamanan data yang umum meliputi:

- *Ransomware* adalah jenis *malware* yang mengenkripsi file dan dokumen sehingga tidak dapat diakses oleh pemiliknya. Kemudian, mereka meminta tebusan untuk mendapatkan kembali akses ke data.
- *Phishing*, yaitu serangan yang bertujuan untuk mencuri data sensitif dengan menyamar sebagai orang yang dapat dipercaya dalam pesan elektronik.
- Serangan *Denial-of-Service* (DoS) merupakan serangan yang membanjiri sistem dengan lalu lintas yang berlebihan untuk membuat layanan atau jaringan tidak tersedia bagi pengguna yang sah.
- Serangan *Brute Force Attack* adalah serangan di mana pelaku mencoba untuk menebak kredensial, seperti username dan password, dengan cara mencoba kombinasi yang berbeda secara berulang-ulang hingga menemukan kecocokan.
- Serangan *Data Breach* merupakan insiden keamanan di mana informasi sensitif atau pribadi yang dilindungi, seperti data pelanggan, informasi akun, atau data keuangan, berhasil diakses, dicuri, atau dipublikasikan oleh pihak yang tidak berwenang.

Dengan digitalisasi yang meningkat dan ancaman keamanan data yang semakin kompleks, penting bagi individu dan organisasi untuk mengambil tindakan proaktif untuk melindungi data mereka. Sebagai salah satu teknologi utama dalam keamanan data, kriptografi memainkan peran penting dalam menjaga kerahasiaan, integritas, dan autentikasi data. Dengan kombinasi teknik seperti enkripsi, tanda tangan digital, dan autentikasi multi-faktor, ditambah dengan pemantauan sistem secara *real-time*, ancaman keamanan dapat diminimalkan. Dengan menggunakan solusi berbasis kriptografi, Anda tidak hanya melindungi data dari serangan saat ini, tetapi juga membuat Anda siap untuk menghadapi tantangan di masa depan (Swetha Gadde, 2023).

## 2.4 METODE KRIPTOGRAFI

Berbagai teknik kriptografi digunakan untuk menjaga kerahasiaan, integritas, dan otentikasi data sensitif. Beberapa kategori utama algoritma ini termasuk enkripsi simetris dan asimetris, algoritma *hashing*, autentikasi dua faktor, enkripsi file, dan tanda tangan digital.
Menurut (Dina Atika Prima, 2018) dan (Indra et al., 2023) ada beberapa metode yang bisa diterapkan seperti :

1. Enkripsi Simetris
   Untuk enkripsi dan dekripsi data, enkripsi simetris menggunakan kunci yang sama, yang menjadikannya sangat populer karena cepat dan efektif, tetapi ada masalah dengan distribusi kunci yang aman. Algoritma seperti AES *(Advanced Encryption Standard)* adalah salah satu algoritma enkripsi simetris yang paling populer karena keamanannya dan kecepatan eksekusinya yang tinggi.
2. Enkripsis Asimetris
   Enkripsi asimetris menggunakan dua kunci - kunci publik untuk enkripsi dan kunci privat untuk dekripsi. Karena kunci privat tidak perlu dibagikan, metode ini lebih aman dalam hal distribusi kunci. Contoh enkripsi asimetris adalah algoritma seperti RSA *(Rivest-Shamir-Adleman)*. Untuk mengamankan data, algoritma ini sangat baik, terutama dalam situasi pengiriman data yang membutuhkan integritas dan otentikasi.
3. Algoritma Hashing
   Hashing menjaga keamanan data. Dengan algoritma *hashing*, input diubah menjadi *string* panjang tetap yang disebut hash, yang unik untuk setiap set data. Salah satu algoritma hashing yang paling umum digunakan adalah SHA-256 *(Secure Hash Algorithm)*, yang

digunakan untuk melindungi data dari perubahan ilegal selama penyimpanan atau pengiriman.

4. Enkripsi File
   Enkripsi file memastikan bahwa file yang disimpan aman dari ancaman internal dan eksternal karena file tidak dapat dibaca tanpa alat khusus. Seseorang hanya dapat mengakses file tersebut jika mereka memiliki kunci yang tepat. Untuk melindungi informasi pribadi yang disimpan pada perangkat atau server, metode ini sangat penting (Alfiah et al., n.d.)
5. Tanda Tangan Digital
   Tanda tangan digital memverifikasi identitas pengirim dan memastikan integritas pesan dengan membuat "sidik jari" dokumen menggunakan algoritma hashing dan enkripsi asimetris. Teknologi ini memungkinkan penerima untuk memastikan bahwa pesan yang mereka terima adalah asli.

Metode-metode ini dapat melindungi data sensitif dari berbagai ancaman, baik internal maupun eksternal. Penggunaan metode kriptografi yang tepat sangat penting untuk memastikan keamanan dan kerahasiaan data dalam sistem informasi yang semakin kompleks.

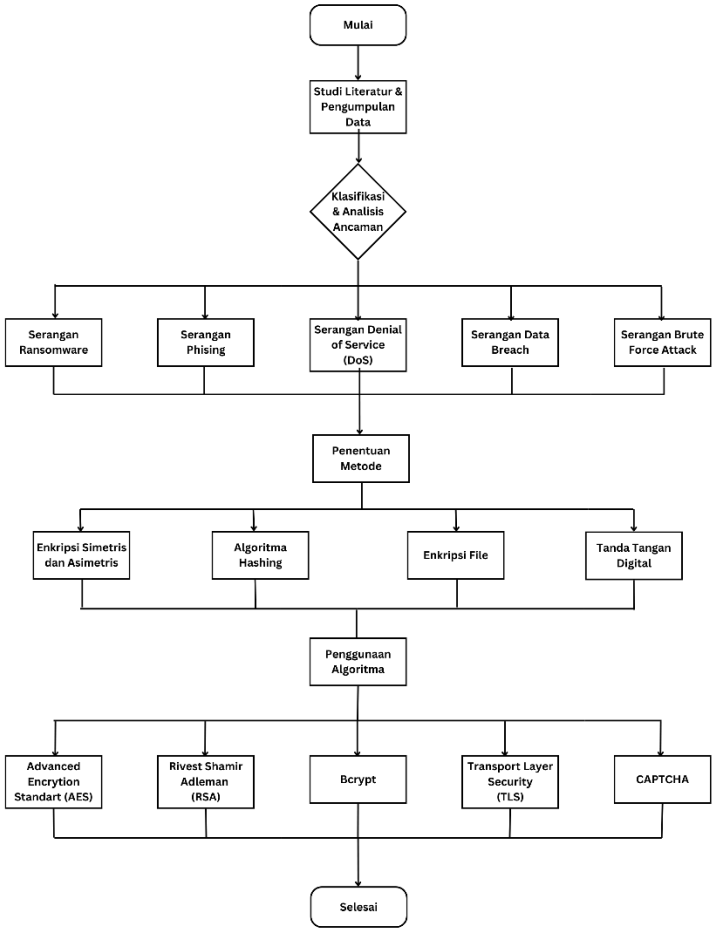
## 2.5 PERLINDUNGAN DATA

Perlindungan data adalah sebuah proses yang bertujuan untuk melindungi data agar tidak diakses secara tidak sah, kebocoran, perubahan, pencurian, dan kerusakan. Tujuan utama perlindungan data adalah untuk melindungi kerahasiaan, integritas, dan ketersediaan data. Perlindungan data ini penting tidak hanya untuk organisasi besar, tetapi juga untuk individu, untuk memastikan bahwa informasi pribadi yang sensitif tetap aman. Sejumlah teknologi telah dikembangkan untuk mengatasi tantangan keamanan data, salah satunya adalah kriptografi (Ramalinda & Rachmat Raharja, 2024).

Kriptografi dalam perlindungan data sangat dibutuhkan karena dapat memberikan solusi yang kuat dan teruji untuk mengamankan informasi dari akses tidak sah. Kriptografi menggunakan teknik enkripsi yang mengubah data menjadi kode yang hanya dapat dibaca oleh pihak yang memiliki kunci dekripsi yang sah, sehingga meskipun data dicuri atau disadap, isinya tetap tidak dapat dimengerti. Selain itu, kriptografi juga berperan penting dalam memastikan integritas data, yaitu memastikan bahwa data tidak diubah selama penyimpanan atau transmisi (Robertus Silalahi, 2021). Teknologi ini juga mendukung autentikasi pengguna, memastikan bahwa hanya pihak yang berwenang yang dapat mengakses informasi tertentu, dan memberikan verifikasi keaslian data melalui tanda tangan digital. Dalam konteks keamanan informasi dan privasi, kriptografi sangat esensial untuk memastikan bahwa data sensitif hanya dapat diakses oleh mereka yang berhak, serta untuk melindungi data dari ancaman yang dapat merusak atau mencuri informasi tersebut.

## 3. METODE PENELITIAN

Dalam penelitian ini, kami mengadopsi metodologi *narrative review*. *Narrative review* merupakan metode yang digunakan untuk merangkum dan mengevaluasi literatur yang relevan dengan topik penelitian secara komprehensif (Leysan Nurgalieva, 2023). *Narrative review* dipilih karena metode ini memungkinkan peneliti untuk menyusun rangkuman dan sintesis dari berbagai literatur yang relevan.




**Gambar 1. Metode Penelitian**

- Studi Literatur & Pengumpulan Data
  Penelitian ini diawali dengan studi literatur yang bertujuan untuk mengumpulkan data mengenai berbagai metode dan algoritma kriptografi serta perlindungan data yang telah diterapkan dalam berbagai studi sebelumnya. Studi literatur ini mencakup buku, jurnal ilmiah, artikel, dan laporan penelitian terkait keamanan data dan kriptografi. Data yang dikumpulkan akan digunakan sebagai dasar untuk memahami ancaman keamanan yang ada serta pendekatan-pendekatan perlindungan yang relevan.
- Klasifikasi & Analisis Ancaman
  Setelah data terkumpul, dilakukan klasifikasi dan analisis ancaman. Proses ini melibatkan identifikasi berbagai jenis ancaman terhadap keamanan data, seperti serangan *ransomware*, *phishing*, *Data Breach*, *Denial-of-Service (DoS)*, ancaman dari dalam *(insider threats)* dan serangan lainnya. Analisis ini bertujuan untuk memahami karakteristik setiap ancaman dan dampaknya terhadap kerahasiaan data.
- Penentuan Metode
  Berdasarkan hasil analisis ancaman, dilakukan penentuan teknik perlindungan data yang paling efektif. Metode - metode yang dianalisis meliputi enkripsi simetris, enkripsi asimetris, algoritma *hashing*, enkripsi file, dan tanda tangan digital. Pemilihan teknik ini didasarkan pada kemampuan masing-masing metode dalam menghadapi ancaman yang telah diidentifikasi sebelumnya.

## 4. HASIL DAN PEMBAHASAN

### 4.1. KLASIFIKASI DAN ANALISIS ANCAMAN

1. Serangan Ransomware

   Menurut (Surya Kusuma, 2023), *Ransomeware* salah satu bentuk malware yang dirancang untuk mengenkripsi data penting pada sistem komputer korban, sehingga

data tersebut tidak dapat diakses tanpa kunci dekripsi. Setelah proses enkripsi selesai, pelaku serangan biasanya mengajukan tuntutan pembayaran tebusan, sering kali dalam bentuk mata uang kripto, sebagai syarat untuk memperoleh akses kembali ke data yang terkunci.(Anasrullah, 2024) . *Ransomware* kerap memblokir akses ke data atau sistem yang telah terinfeksi dan hanya menyediakan "kunci" atau dekripsi kepada korban setelah pembayaran tebusan dilakukan. *Ransomeware* dapat mengenkripsi atau merusak berbagai jenis file, seperti dokumen, foto, video, serta data penting lainnya.

Penelitian (Diana Afifah, 2023) mengenai serangan siber ransomware pada PT Bank Syariah Indonesia (Bank BSI) mengidentifikasi dua isu penting dalam perlindungan konsumen di sektor jasa keuangan. Pertama, terdapat masalah transparansi informasi yang disampaikan oleh Bank BSI kepada nasabah, di mana informasi yang diberikan tidak memadai dan dapat menimbulkan ketidakpercayaan. Kedua, serangan *ransomware* mengancam kerahasiaan data pribadi nasabah, termasuk informasi sensitif seperti identitas dan nomor rekening, yang dapat menyebabkan kerugian finansial dan gangguan dalam akses ke akun serta transaksi keuangan sehari-hari. Penelitian ini menunjukkan bahwa serangan siber ransomware dapat mengakibatkan kerugian yang signifikan bagi lembaga keuangan dan nasabah. *Ransomware* memiliki kemampuan untuk mengenkripsi data penting dan meminta tebusan, sehingga mengganggu operasional bank dan mengancam kerahasiaan informasi pribadi nasabah. Dengan adanya serangan *ransomware*, nasabah berisiko mengalami kerugian finansial, kehilangan akses ke akun mereka, dan terancamnya data sensitif seperti informasi identitas dan nomor rekening. Oleh karena itu, penting bagi bank dan lembaga keuangan untuk memahami dan menerapkan strategi keamanan yang efektif guna mengurangi risiko serangan siber dan melindungi data pribadi nasabah mereka

2. Serangan Phising

Menurut (Efendy et al., 2019) Phishing didefinisikan sebagai Aktivitas kejahatan siber yang memanfaatkan teknik rekayasa sosial dan metode penipuan bertujuan mencuri data identitas serta informasi kredensial akun keuangan. Skema ini sering dilakukan melalui email palsu yang mengklaim berasal dari institusi bisnis terpercaya, yang dirancang untuk mengarahkan korban ke situs web tiruan. Di situs web tersebut, Korban akan diarahkan untuk memberikan informasi keuangan mereka, termasuk *username* dan *password* (Gupta et al., 2024). Selain itu, teknik *subterfuge* teknis juga digunakan, di mana *crimeware* ditanamkan ke dalam komputer untuk mencuri informasi secara langsung, sering kali dengan mengelabui pengguna agar memasukkan data mereka ke dalam situs web yang tidak sah atau melalui proxy yang dikendalikan oleh penyerang *(phiser)* untuk memantau dan mengintersepsi informasi konsumen.

Penelitian yang dilakukan oleh (Dewanto et al., 2024) mengenai penipuan penambah *followers* Instagram dan analisis serangan *phishing* serta dampaknya terhadap keamanan data. Penelitian ini menunjukkan bahwa serangan *phishing* merupakan ancaman yang semakin meningkat, di mana penyerang menggunakan situs web palsu untuk menipu pengguna agar memberikan informasi sensitif seperti *username* dan *password*. Penelitian ini menekankan pentingnya edukasi dan kesadaran masyarakat mengenai kejahatan siber, khususnya *phishing,* untuk mencegah pencurian identitas dan penyalahgunaan data pribadi. Selain itu, jurnal tersebut juga menggarisbawahi bahwa serangan *phishing* dapat dilakukan dengan cara yang sederhana, seperti menggunakan BOT Telegram untuk mengumpulkan data korban.

3. Serangan Denial of Service (Dos)

Menurut (Haris et al., 2022) , *Denial of Service* (DoS) adalah ancaman siber serius yang bertujuan untuk melumpuhkan target dengan membanjiri jaringan atau sistem dengan lalu lintas data dalam jumlah besar. Serangan ini bekerja dengan cara membanjiri target dengan sejumlah besar paket data atau menggunakan metode spesifik, seperti *deauthentication attack* pada jaringan Wi-Fi, yang menyebabkan pengguna terputus secara terus-menerus (Yusuf et al., 2022) . DoS dapat menyebabkan

dampak signifikan pada performa sistem, terutama pada CPU dan latensi jaringan, serta dapat mengakibatkan reputasi dan kerugian finansial yang besar. Metode penanganannya melibatkan penggunaan *firewall*, deteksi serangan dengan IDS, atau pendekatan khusus lainnya seperti *Defense-through-deception* untuk meningkatkan keamanan jaringan.

Berdasarkan penelitian (Yusuf et al., 2022) mengenai analisis keamanan jaringan Wi-Fi Indihome terhadap serangan *Denial of Service* (DoS), penelitian ini menggunakan metode serangan deauthentication attack untuk menguji keamanan jaringan. Penelitian ini dilakukan dengan memanfaatkan tools pada sistem operasi Kali Linux, seperti airodump-ng untuk identifikasi target, dan aireplay-ng untuk meluncurkan serangan DoS. Hasil analisis mengungkap bahwa jaringan Wi-Fi Indihome yang menggunakan enkripsi WPA2-PSK dan protokol jaringan IEEE 802.11n masih rentan terhadap serangan DoS. Penelitian ini menunjukkan bahwa serangan siber *Denial of Service* (DoS) dapat mengakibatkan gangguan yang signifikan pada stabilitas jaringan dan kenyamanan pengguna layanan Wi-Fi. DoS memiliki kemampuan untuk membanjiri jaringan dengan paket data berlebihan, seperti melalui metode *deauthentication attack*, yang menyebabkan pengguna terputus secara berulang dari jaringan Wi-Fi.

4. Serangan Data Breach

Menurut (Muhammad Chandraca Hutagalung et al., 2024) *data breach* atau kebocoran data adalah kejadian di mana informasi pribadi atau sensitif yang tidak seharusnya diakses atau dibagikan, jatuh ke tangan pihak yang tidak berwenang. Hal ini dapat melibatkan pencurian, pengungkapan, atau akses tanpa izin terhadap data yang dilindungi oleh organisasi atau individu, pelanggaran data merupakan risiko serius yang mengancam keamanan data pengguna(Yuswanto et al., 2024). Data breach sering kali terjadi akibat serangan siber, seperti peretasan atau *malware*, namun juga bisa terjadi karena kelalaian atau kesalahan manusia, seperti kesalahan konfigurasi sistem atau pengelolaan data yang buruk.

Berdasarkan penelitian (Muhammad Chandraca Hutagalung et al., 2024) ditemukan bahwa kebocoran data yang terjadi di Bank Syariah Indonesia (BSI) akibat serangan ransomware memberikan dampak signifikan terhadap nasabah dan kredibilitas bank. Dalam kasus ini, data pribadi nasabah, termasuk nomor telepon, alamat, dan informasi rekening, berhasil dicuri oleh kelompok *hacker* seperti LockBit, yang kemudian mengancam untuk merusak sistem lebih lanjut dengan meminta tebusan. Kebocoran data ini menunjukkan pentingnya perlindungan konsumen, terutama dalam aspek keamanan data pribadi dan transaksi keuangan yang sangat rentan terhadap ancaman kejahatan siber. Dalam penelitian *data breach* ini dapat menyebabkan penyalahgunaan informasi sensitif oleh pihak yang tidak berwenang, yang berpotensi merugikan nasabah secara finansial dan merusak reputasi perusahaan. Kebocoran data ini sering kali mengincar informasi yang sangat bernilai, seperti kredensial login, informasi pribadi, serta data keuangan yang dapat disalahgunakan untuk penipuan atau pencurian identitas.

5. Serangan Brute Force Attack

Menurut (Rahmah, 2023) *Brute Force Attack* adalah jenis serangan siber yang dilakukan dengan mencoba semua kemungkinan kombinasi kata sandi atau kunci enkripsi hingga menemukan yang sesuai. Tujuan dari serangan ini adalah untuk memperoleh akses tidak sah ke sistem, akun, atau data yang terlindungi. Metode *brute force* memanfaatkan kecepatan dan ketelitian komputer untuk menjalankan percobaan sistematis terhadap semua kemungkinan hingga menemukan kecocokan. Contohnya, penyerang dapat mencoba berbagai kombinasi kata sandi untuk membobol otentikasi pada protokol HTTP atau akun pengguna tertentu. Penyalahgunaan *Brute Force Attack* sering digunakan untuk meretas otoritas administrator sistem, yang memberikan akses penuh ke pengaturan, file, dan data penting.

Berdasarkan penelitian (Rahmah, 2023) mengenai efektivitas penerapan algoritma *brute force* dan penyalahgunaannya dalam sistem berbasis web, penelitian ini menjelaskan bagaimana *Brute Force Attack* digunakan oleh penyerang untuk mendapatkan akses tidak sah ke sistem dengan mencoba semua kombinasi kata sandi atau kunci enkripsi yang mungkin. Penelitian ini menggunakan studi literatur dan studi kasus untuk menganalisis penerapan teknik *brute force* baik sebagai alat keamanan maupun sebagai ancaman siber. Hasil analisis menunjukkan bahwa *Brute Force Attack* sering digunakan untuk meretas otentikasi HTTP, di mana penyerang memanfaatkan alat seperti *WebCracker* untuk mencoba kombinasi *username* dan *password* hingga menemukan kecocokan. Penyerangan ini dapat memberikan akses penuh kepada penyerang untuk mengontrol sistem, mengakses data sensitif, dan bahkan memodifikasi informasi penting. Penelitian ini menyoroti bahwa *Brute Force Attack* dapat mengancam keamanan situs web dan pengguna, terutama jika kata sandi yang digunakan terlalu sederhana atau protokol keamanannya tidak diperbarui. Oleh karena itu, penting untuk meningkatkan langkah-langkah keamanan, seperti menggunakan enkripsi kuat, otentikasi multi-faktor, dan membatasi upaya login yang gagal, guna mengurangi risiko serangan dan melindungi integritas sistem.

## 4.2. PENENTUAN METODE UNTUK KERAHASIAAN DATA

1. Enkripsi Simetris dan Asimetris

   Penulis menegaskan bahwa enkripsi simetris dan asimetris merupakan dua metode kriptografi yang esensial dalam menjaga kerahasiaan data. Enkripsi simetris, seperti yang diimplementasikan dengan algoritma AES, menawarkan kecepatan dan efisiensi yang tinggi dalam pemrosesan data, menjadikannya pilihan ideal untuk aplikasi yang memerlukan pengolahan volume data besar dan luas (Hadi Wiyono, 2023). Di sisi lain, enkripsi asimetris, seperti RSA, memberikan lapisan keamanan tambahan melalui penggunaan dua kunci (publik dan privat), memungkinkan verifikasi identitas pengirim serta integritas data yang lebih baik (Dyta Bagus Nawawi, 2024). Enkripsi simetris dan asimetris tetap menjadi metode penting dalam kriptografi modern, terutama untuk aplikasi yang memerlukan kecepatan dan efisiensi tinggi (Laurentinus, 2020). Namun, perhatian harus diberikan pada manajemen dan distribusi kunci untuk menjaga kerahasiaan data.

2. Algoritma Hashing

   Algoritma hashing digunakan untuk menghasilkan nilai *hash* yang unik dari data atau informasi tertentu, yang sulit dikembalikan ke bentuk aslinya. *Hashing* sangat berguna untuk memverifikasi integritas data dan dalam penyimpanan *password* yang aman (Salmon, 2024). Dalam penggunaan yang tepat, hasil hash tidak dapat diprediksi atau dibalikkan, menjadikannya metode yang efisien untuk memverifikasi data tanpa mengungkapkan informasi sensitif. Beberapa algoritma *hashing* yang populer adalah SHA-256 *(Secure Hash Algorithm)* dan MD5, meskipun MD5 sekarang dianggap kurang aman.

3. Enkripsi File

   Enkripsi file melibatkan pengamanan data dalam file tertentu, dengan mengenkripsi seluruh isi file agar tidak dapat dibaca tanpa kunci dekripsi yang sesuai. Ini melindungi data pada perangkat atau selama transfer melalui jaringan. File yang terenkripsi hanya bisa dibuka dengan kunci yang benar (Ali Rohman, 2023), menjamin kerahasiaan isi file tersebut meskipun file tersebut jatuh ke tangan yang salah. Aplikasi yang menggunakan enkripsi file umumnya seperti perangkat lunak untuk penyimpanan *cloud* yang menawarkan enkripsi *end-to-end*.

4. Tanda Tangan Digital

   Tanda tangan digital merupakan metode untuk memverifikasi identitas pengirim dan integritas data dalam dokumen elektronik. Tanda tangan digital menggunakan enkripsi asimetris, di mana pengirim menandatangani data menggunakan kunci privat

mereka (Gafrun, 2024). Penerima kemudian dapat memverifikasi tanda tangan dengan menggunakan kunci publik pengirim untuk memastikan bahwa data tersebut tidak diubah sejak ditandatangani dan bahwa data tersebut benar-benar berasal dari pengirim yang sah. Ini sangat penting untuk transaksi online, kontrak digital, dan komunikasi aman.

Dari hasil analisis ini, dapat disimpulkan bahwa kombinasi berbagai metode kriptografi enkripsi simetris dan asimetris, algoritma *hashing*, enkripsi file, serta tanda tangan digital merupakan pendekatan yang efektif untuk meningkatkan kerahasiaan dan keamanan data. Implementasi yang tepat dari metode-metode ini dapat secara signifikan mengurangi risiko pencurian data dan memastikan integritas serta keaslian informasi yang ditransmisikan.

### 4.3. PENGGUNAAN ALGORITMA UNTUK MENINGKATKAN KERAHASIAAN DATA

1. Advanced Encrytion Standard (AES)

   Menurut (Akhmad Sahal Mabruri, 2020) AES merupakan algoritma enkripsi simetris yang paling banyak digunakan dan diakui sebagai standar *de facto* untuk melindungi data elektronik. AES menggunakan blok data berukuran 128 bit dan mendukung kunci dengan panjang 128, 192, atau 256 bit. Keunggulan utama dari AES adalah kecepatannya dalam memproses data serta kemampuannya untuk memberikan tingkat keamanan yang tinggi. Dengan implementasi yang tepat, AES dapat melindungi data dari serangan kriptografi yang dikenal, menjadikannya pilihan ideal untuk aplikasi yang memerlukan kerahasiaan tinggi, seperti dalam sistem perbankan dan komunikasi aman.

   Serangan *brute force* melibatkan percobaan semua kemungkinan kombinasi kunci untuk mendekripsi data yang terenkripsi. Meskipun serangan ini menjadi tantangan yang sulit pada ukuran kunci AES yang lebih besar (128, 192, atau 256 bit), peningkatan kekuatan komputasi dapat mengurangi tingkat kesulitan serangan ini (Indra Gunawan, 2023). Namun, dengan ukuran kunci yang cukup besar, AES tetap dianggap aman terhadap serangan *brute force* dalam praktiknya.

   Kriptoanalisis adalah upaya untuk menemukan kelemahan dalam algoritma enkripsi dengan tujuan mengeksploitasi celah tersebut. Meskipun terdapat penelitian yang mencoba menemukan kelemahan dalam AES, hingga saat ini belum ada serangan yang berhasil mengungkapkan kelemahan signifikan pada algoritma ini. AES telah diuji secara ekstensif dan masih dianggap sangat aman (Uci Julya Ningsih, 2024).

   Dengan demikian, algoritma AES merupakan alat yang efektif untuk melindungi data dari berbagai ancaman serangan siber. Meskipun tidak ada sistem yang sepenuhnya kebal terhadap serangan, penggunaan ukuran kunci yang tepat, mode operasi yang aman, dan praktik terbaik dalam implementasi dapat secara signifikan meningkatkan keamanan data dan melindungi informasi sensitif dari akses tidak sah.

2. Rivest Shamir Adleman (RSA)

   Menurut (Maria SD.Dairi, 2023) RSA merupakan algoritma enkripsi asimetris yang menggunakan pasangan kunci publik dan privat. Kunci publik dapat dibagikan kepada siapa pun, sedangkan kunci privat harus dirahasiakan oleh pemiliknya. Keamanan RSA bergantung pada kesulitan faktorisasi bilangan bulat besar. RSA sering digunakan dalam situasi di mana kepercayaan dan autentikasi penting, seperti dalam pengiriman email aman dan transaksi online. Dengan kemampuannya untuk mendukung tanda tangan digital, RSA juga berperan penting dalam memastikan integritas dan keaslian data.

   RSA sangat efektif dalam mencegah serangan MitM, di mana penyerang mencoba untuk mengintersepsi komunikasi antara dua pihak. Dengan menggunakan enkripsi asimetris, RSA memastikan bahwa hanya pihak yang memiliki kunci privat yang dapat mendekripsi pesan yang dienkripsi dengan kunci publik. Ini membantu menjaga kerahasiaan dan integritas data yang ditransmisikan (Chiradeep Gupta, 2022).

   Menurut (Budi Satria Muchlis, 2017) Serangan *timing* berusaha mengeksploitasi waktu yang diperlukan untuk melakukan operasi enkripsi atau dekripsi pada RSA.

Dengan menganalisis perbedaan waktu dalam proses ini, penyerang dapat mencoba menebak informasi tentang kunci privat. Untuk mengurangi risiko ini, implementasi RSA harus dirancang sedemikian rupa sehingga waktu eksekusi tidak tergantung pada nilai input atau kunci.

Secara keseluruhan, algoritma RSA memainkan peran penting dalam menjaga keamanan data dalam komunikasi digital dengan melindungi dari berbagai jenis serangan siber. Dengan menggunakan kunci publik dan privat serta menerapkan praktik terbaik dalam pemilihan kunci dan implementasi, RSA dapat memberikan tingkat keamanan yang tinggi terhadap ancaman-ancaman tersebut.

3. Bcrypt

Menurut (Mochamad Dandi Akbar, 2022) Bcrypt merupakan algoritma hashing yang dirancang khusus untuk menyimpan password dengan aman. Berbeda dengan algoritma hashing lainnya, bcrypt menggunakan teknik *salting* yang menambahkan data acak ke *password* sebelum proses *hashing*, sehingga menghasilkan hash unik untuk setiap *password* meskipun *password* tersebut identik. Keunggulan bcrypt terletak pada kemampuannya untuk memperlambat proses *hashing* melalui pengaturan faktor biaya, sehingga membuat serangan *brute force* menjadi lebih sulit dilakukan. Ini menjadikannya pilihan yang sangat baik untuk penyimpanan *password* dalam aplikasi web.

Bcrypt secara efektif melindungi terhadap serangan *rainbow table* dengan menggunakan salt, yaitu data acak yang ditambahkan ke kata sandi sebelum proses *hashing*. Dengan cara ini, meskipun dua pengguna memiliki kata sandi yang sama, hasil hash yang dihasilkan akan berbeda karena salt yang berbeda. Hal ini mencegah penyerang dari menggunakan tabel hash pra-komputasi untuk mencocokkan hash dan mendapatkan kata sandi asli (Mochamad Dandi Akbar, 2022).

Dengan demikian, bcrypt merupakan algoritma *hashing* yang sangat efektif untuk melindungi kata sandi dari berbagai jenis serangan siber, termasuk *brute force* dan *rainbow table*. Penggunaan salt dan kemampuan adaptifnya dalam meningkatkan kompleksitas hashing seiring waktu menjadikannya pilihan utama dalam pengamanan data sensitif seperti kata sandi pengguna.

4. Transport Layer Security (TLS)

TLS adalah protokol kriptografi yang mengamankan komunikasi di jaringan komputer dengan mengenkripsi data yang ditransmisikan antara klien dan server. Protokol ini memastikan kerahasiaan, integritas, dan autentikasi data selama transmisi, melindungi informasi sensitif dari akses tidak sah dan manipulasi. TLS juga mendukung fitur seperti *forward secrecy*, di mana kunci sesi unik dihasilkan untuk setiap koneksi, sehingga bahkan jika satu kunci sesi dikompromikan di masa depan, komunikasi sebelumnya tetap aman.

TLS sangat efektif dalam mencegah serangan MitM, di mana penyerang mencoba untuk mengintersepsi komunikasi antara dua pihak. Dengan menggunakan enkripsi, TLS memastikan bahwa data yang ditransmisikan tidak dapat dibaca atau dimodifikasi oleh pihak ketiga (Rival Moh. Wahyudi, 2024), bahkan jika data tersebut berhasil diintersepsi. Proses autentikasi dalam TLS juga membantu memastikan bahwa kedua belah pihak dalam komunikasi adalah siapa yang mereka klaim. TLS juga melindungi integritas data dengan memastikan bahwa informasi yang dikirim tidak dapat diubah tanpa terdeteksi. Jika data diubah selama proses transmisi, TLS akan mendeteksi perubahan tersebut dan mencegah data yang telah dimodifikasi diterima oleh penerima. Ini sangat penting untuk aplikasi seperti perbankan online dan e-commerce, di mana bahkan perubahan kecil pada data dapat memiliki konsekuensi serius.

Dengan demikian, penggunaan algoritma TLS sangat penting dalam menjaga keamanan komunikasi di internet. Dengan melindungi data dari serangan seperti MitM, penyadapan, dan pemalsuan data, TLS berfungsi sebagai lapisan pertahanan utama dalam menjaga kerahasiaan dan integritas informasi sensitif selama transmisi.

Implementasi TLS yang tepat membantu organisasi dan individu untuk membangun kepercayaan dalam interaksi digital mereka.

5. CAPTCHA

CAPTCHA adalah mekanisme perlindungan yang dirancang untuk membedakan antara pengguna manusia dan bot otomatis. Dengan memberikan tantangan yang harus diselesaikan oleh pengguna (seperti pengenalan karakter atau gambar), CAPTCHA membantu mencegah penyalahgunaan layanan *online* oleh program otomatis. CAPTCHA dirancang untuk mencegah pengiriman spam dalam jumlah besar yang sering dilakukan oleh bot. Tanpa CAPTCHA, situs web dapat dengan mudah diserang oleh bot yang membuat akun palsu atau mengirim pesan spam, yang dapat merusak reputasi dan integritas layanan online. Dengan menggunakan CAPTCHA pada halaman *login*, sistem dapat mencegah bot dari melakukan serangan *brute force* untuk menebak kata sandi pengguna (Muhammad Rayza, 2023) . Ini membantu melindungi data akun pengguna dari akses tidak sah dan pencurian identitas.

Dengan demikian, penggunaan algoritma CAPTCHA sangat penting dalam menjaga keamanan situs web dan aplikasi dari berbagai ancaman siber yang melibatkan bot otomatis. Implementasi CAPTCHA membantu menciptakan lingkungan online yang lebih aman dengan memastikan bahwa hanya pengguna manusia yang dapat mengakses layanan tertentu, sehingga melindungi data pribadi dan integritas sistem secara keseluruhan.

## 5. KESIMPULAN

Kesimpulan dari jurnal ini menegaskan bahwa perlindungan data merupakan aspek yang sangat penting di era digital yang terus berkembang. Ancaman keamanan yang semakin kompleks, seperti *ransomware*, *phishing*, *Denial of Service* (DoS), *Data Breach* , serta serangan *brute force attack*, menuntut adanya solusi yang efektif dan adaptif untuk menjaga kerahasiaan dan integritas informasi. Dalam konteks ini, metode kriptografi memainkan peran sentral. Teknologi seperti enkripsi simetris (contohnya AES), enkripsi asimetris (contohnya RSA), algoritma hashing (seperti SHA-256 dan bcrypt), serta tanda tangan digital telah terbukti mampu memberikan tingkat keamanan yang tinggi terhadap ancaman-ancaman tersebut. Kombinasi teknik-teknik ini, ketika diterapkan bersama dengan manajemen kunci yang efisien dan kebijakan keamanan yang ketat, tidak hanya mengurangi risiko pencurian data tetapi juga memastikan keandalan dan keabsahan sistem dalam berbagai skenario, mulai dari perlindungan data pribadi hingga aplikasi pada sektor bisnis dan layanan publik.

Selain itu, penelitian ini menekankan pentingnya pemilihan algoritma yang tepat sesuai dengan kebutuhan spesifik dan kondisi operasional. Misalnya, AES unggul dalam kecepatan dan efisiensi untuk mengamankan data dalam jumlah besar, sedangkan RSA memberikan lapisan autentikasi tambahan dalam pengiriman data yang membutuhkan keamanan tingkat tinggi. Praktik terbaik, seperti penerapan autentikasi multi-faktor, penggunaan tanda tangan digital untuk memastikan integritas dokumen, dan pemantauan sistem secara *real-time*, juga menjadi rekomendasi utama dalam pengelolaan keamanan data. Dengan langkah-langkah tersebut, sistem dapat lebih siap menghadapi serangan siber yang semakin canggih, termasuk serangan berbasis teknik manipulasi sosial. Penelitian ini memberikan kontribusi yang signifikan terhadap pengembangan strategi perlindungan data yang lebih komprehensif dan dapat diterapkan di berbagai sektor. Dengan pendekatan ini, perlindungan data di era digital yang terus berubah dapat dilakukan secara lebih efektif, menjamin keamanan informasi, dan memberikan rasa aman bagi pengguna maupun organisasi.

## DAFTAR PUSTAKA

Adisya Poeja Kehista, A. F. A. T. I. P. N. A. F. S. K. V. B. D. (2023). Analisis Keamanan Data Pribadi pada Pengguna E-Commerce: Ancaman, Risiko, Strategi Kemanan (Literature Review). *Jurnal Ilmu Manajemen Terapan*, *4*.

Akhmad Sahal Mabruri, A. (2020). Data Security System of Text Messaging Based on Android Mobile Devices Using Advanced Encryption Standard Dynamic S-BOX. *Journal Soft Computing Exploration*.

Aldianto, D., & Wibowo, A. (2023). *IMPLEMENTASI KRIPTOGRAFI DENGAN AES 256 DAN MD 5 UNTUK MENGAMANKAN DATA DI PT. EBDESK TEKNOLOGI* (Vol. 2, Issue 2).

Alfiah, F., Sudarji, R., & Taqiyyuddin Al Fatah, D. (n.d.). *Aplikasi Kriptografi Dengan Menggunakan Algoritma Elgamal Berbasis Java Desktop Pada Pt. Wahana Indo Trada Nissan Jatake*.

Ali Rohman, A. M. (2023). IMPLEMENTASI ENKRIPSI FILE BERBASIS CRYPTOGRAPHY UNTUK KEAMANAN DATA DI WINDOWS 10 MENGGUNAKAN ALGORITMA (AES). *Jurnal Ilmiah Sistem Informasi* , *3*.

Anasrullah, F. (2024). PENCEGAHAN RANSOMWARE PADA SERVER ON PREMISE MENGGUNAKAN TEKNIK SECURITY HARDENING. *Jurnal Informatika Dan Teknik Elektro Terapan*, *12*(3). https://doi.org/10.23960/jitet.v12i3.5105

Andryanto Aman. (2023). Pengujian Keamanan Jaringan Nirkabel Melalui Simulasi Serangan Man In The Middle Attack Di Sekolah XYZ. *Digital Transformation Technology (Digitech)*, *3*.

Annisa Thahara, I. T. S. (2021). Implementasi Kriptografi untuk Keamanan Data dan Jaringan menggunakan Algoritma DES. *JURTI*, *5*.

Budi Satria Muchlis, M. A. B. D. R. (2017). Teknik Pemecahan Kunci Algoritma Rivest Shamir Adleman (RSA) dengan Metode Kraitchik. *Jurnal & Penelitian Teknik Informatika*, *2*.

Chiradeep Gupta, N. V. S. R. (2022). Enhancement of Security of Diffie-Hellman Key Exchange Protocol using RSA Cryptography. *Journal of Physics: Conference Series*, *2*.

Dewanto, M. A. B., Fathurrahman, M., Firdaus, D. R., & Setiawan, A. (2024). Penipuan Penambah Followers Instagram: Analisis Serangan Phising dan Dampaknya pada Keamanan Data. *Journal of Internet and Software Engineering*, *1*(4), 11. https://doi.org/10.47134/pjise.v1i4.2672

Dimas Krisna Maulana, S. M. T. R. S. R. A. I. (2023). Penerapan Kriptografi Vigenere Cipher Pada Kekuatan Kata Sandi. *Jurnal Jurnal Sains Dan Teknologi (JSIT)*, *3*.

Dina Atika Prima, S. (2018). *DIGITAL SIGNATURE DENGAN ALGORITMA SHA-1 DAN RSA SEBAGAI AUTENTIKASI* (Issue 021).

Dola Ramalinda, J. A. R. Raharja. (2024). Strategi Perlindungan Data Menggunakan Sistem Kriptografi Dalam Keamanan Informasi. *Journal of International Multidisciplinary Research*, *2*.

Dyta Bagus Nawawi, M. M. H. T. P. (2024). Perbandingan Enkripsi Advanced Encryption Standard dan Enkripsi Rivest Shamir Adleman. *Jurnal Teknologi Terapan*, *8*.

Efendy, Z., Putra, I. E., & Saputra, R. (2019). ASSET RENTAL INFORMATION SYSTEM AND WEB-BASED FACILITIES AT ANDALAS UNIVERSITY. *Jurnal Terapan Teknologi Informasi*, *2*(2), 135–146. https://doi.org/10.21460/jutei.2018.22.103

Febrianingsih, R., & Hafiz, A. (2019). IMPLEMENTASI KRIPTOGRAFI BERBASIS CAESAR CHIPER UNTUK KEAMANAN DATA. In *Jurnal Informasi Dan Komputer* (Vol. 7, Issue Thn).

Gafrun, Y. S. (2024). ALGORITMA TANDA TANGAN DIGITAL UNTUK MENINGKATKAN KEAMANAN PESAN. *JURNAL SISTEM INFORMASI DAN TEKNIK KOMPUTER*, *9*.

Gupta, S., Pritwani, M., Shrivastava, A., Mohana, Moharir, M., & Ashok Kumar, A. R. (2024). A Comprehensive Analysis of Social Engineering Attacks: From Phishing to Prevention - Tools, Techniques and Strategies. *2nd International Conference on Intelligent Cyber Physical Systems and Internet of Things, ICoICI 2024 - Proceedings*, 42–49. https://doi.org/10.1109/ICoICI62503.2024.10696444

Hadi Wiyono, A. B. K. I. S. (2023). Perancangan Aplikasi Keamanan data Rekam Medis menggunakan Algoritma AES (Advanced Encryption Standard). *Journal on Pustaka Cendekia Informatika*, *1*.

Hafizh Fianto Putra, W. dan O. P. (2019). Penerapan Blockchain dan Kriptografi untuk Keamanan Data pada Jaringan Smart Grid. *JURNAL TEKNIK ITS* , *8*.

Haris, A. I., Riyanto, B., Surachman, F., & Ramadhan, A. A. (2022). Analisis Pengamanan Jaringan Menggunakan Router Mikrotik dari Serangan DoS dan Pengaruhnya Terhadap Performansi. *Komputika : Jurnal Sistem Komputer*, *11*(1), 67–76. https://doi.org/10.34010/komputika.v11i1.5227

Indra, D., Hts, G., Ridho Aldizar, M., & Hutasuhut, G. (2023). *PERBANDINGAN ALGORITMA KRIPTOGRAFI SIMETRIS DAN ASIMETRISCOMPARISON OF SYMMETRIC AND ASYMMETRIC CRYPTOGRAPHIC ALGORITHMS*. https://fe.ekasakti.org/index.php/UJIS

Indra Gunawan. (2023). Peningkatan Pengamanan Data File Menggunakan Algoritma Kriptografi AES Dari Serangan Brute Force. *JURNAL MEDIA INFORMATIKA [JUMIN]*, *4*.

Kiki Andrea, A. W. B. S. W. A. I. (2023). Penerapan Kriptografi Caesar Cipher Pada Fitur Aplikasi Chatting Whatsapp. *Jurnal Hasi Penelitian Dan Pengkajian Ilmiah Eksakta* , *2*.

Laurentinus, H. A. P. D. Y. S. F. P. J. (2020). Perbandingan kinerja RSA dan AES terhadap kompresi pesan SMS menggunakan algoritme Huffman. *Jurnal Teknologi Dan Sistem Komputer*, *8, no. 3*.

Leysan Nurgalieva, A. F. G. D. (2023). A Narrative Review of Factors Affecting the Implementation of Privacy and Security Practices in Software Development. *ACM Computing Surveys*, *55*.

Maria SD.Dairi, M. S. A. K. (2023). Implementasi Algoritma Kriptografi RSA Dalam Aplikasi Sistem Informasi Perpustakaaan. *Jurnal Ilmu Komputer Dan Sistem Informasi (JIRSI)*, *2*.

Mochamad Dandi Akbar, A. (2022). Aplikasi Absensi Pegawai pada Dinas Komunikasi dan Informatika Kabupaten Deli Serdang dengan QR Code Menggunakan Algoritma Bcrypt. *Jurnal Teknik Informatika*, *1*.

Muhammad Chandraca Hutagalung, A., Rhaesa Marendra, N., & Ul Hosnah, A. (2024). *PERLINDUNGAN TERHADAP KONSUMEN DALAM KASUS KEBOCORAN DATA BANK SYARIAH INDONESIA*. *2*(1), 156–165. https://doi.org/10.18415/ijmmu.v10i4.4643

Muhammad Rayza, A. U. A. B. (2023). Keamanan Jaringan Hotspot Mikrotik Menggunakan Metode Otentikasi Pengguna dengan Captcha dan IP-Binding Untuk Filtering User. *Jurnal Ilmu Komputer Dan Sistem Informasi (JIRSI)*, *2*.

Pratiwi, R., Utami, L. C., & Sakti, R. B. (2022). *Perancangan Keamanan Data Pesan Dengan Menggunakan Metode Kriptografi Caesar Cipher*. *3*(4), 367–373. https://doi.org/10.47065/bit.v3i1

Rahmah, S. A. (2023). *JCBD JOURNAL OF COMPUTERS AND DIGITAL BUSINESS Efektifitas Penerapan Algoritma Brute Force dan Penyalahgunaannya Dalam Sistem Berbasis Web*. *2*(3), 112–119. https://doi.org/10.56427/jcbd.v2n3.235

Ramalinda, D., & Rachmat Raharja, A. (2024). Strategi Perlindungan Data Menggunakan Sistem Kriptografi Dalam Keamanan Informasi. *Journal of International Multidisciplinary Research*, *2*. https://journal.banjaresepacific.com/index.php/jimr

Rifky Priambudi, J. dan C. Nugrahaeni. (2022). Penerapan Algoritma Kriptografi AES (Advanced Encryption Standard) dan Algoritma Kompresi RLE (Run Length Encoding) Untuk Pengamanan File Dokumen. *Ilmu Komputer Universitas Pembangunan Nasional Veteran Jakarta*, *11*.

Rival Moh. Wahyudi, A. N. S. G. R. P. M. R. N. M. A. Q. A. Y. S. N. M. R. A. A. E. Pinem. (2024). Mengimplementasikan SSL/TLS pada Web Server Apache di dalam Jaringan Internal Praktikum untuk Pengembangan Web Server. *JURNAL MAJEMUK*, *3*.

Robertus Silalahi, I. P. S. I. G. dan W. (2021). *Implementasi Algoritma Caesar Cipher dan Algoritma RSA untuk Keamanan Data*. http://sostech.greenvest.co.id

Salmon, S. L. N. R. A. (2024). Penerapan Algoritma Hash Based Terhadap Penentuan Rule Asosiasi Transaksi Penjualan Sparepart Sepeda Motor. *JURNAL MEDIA INFORMATIKA BUDIDARMA*, *8*.

Surya Kusuma, R. (2023). Forensik Serangan Ransomware Ryuk pada Jaringan Cloud. In *Forensik Serangan Ransomware Ryuk pada Jaringan Cloud JURNAL MULTINETICS* (Vol. 9, Issue 2).

Swetha Gadde, G. S. R. V. S. V. M. Y. R. S. M. L. P. (2023). Secure Data Sharing in Cloud Computing: A Comprehensive Survey of Two-Factor Authentication and Cryptographic Solutions. *IIETA*, *28*.

Uci Julya Ningsih, S. S. I. H. D. S. I. G. (2024). Pendekripsian Caesar Chiper Dengan Menggunakan Teknik-Teknik Kriptanalisis. *Jurnal ILKOMEDIA*, *1*.

Yusuf, A., Azmi, F., Gusti, J., & Wahyudi, E. (2022). *ANALISIS NETWORK SECURITY PADA LAYANAN WIFI INDIHOME TERHADAP SERANGAN DENIAL OF SERVICE (DOS)* (Vol. 19, Issue 1).

Yuswanto, A., Wibowo, B., & Hafiz, L. (2024). A Review Method for Analysis of the Causes of Data Breach in the Pasca Pandemic. *Jurnal Komputer Dan Elektro Sains*, *3*(1), 1–5. https://doi.org/10.58291/komets.v3i1.205