BAB 2. TINJAUAN PUSTAKA

2.1. Pertahanan

Pertahanan adalah upaya untuk melindungi diri dari serangan atau ancaman (Manurung, 2002). Ada banyak cara yang dapat digunakan dalam upaya pertahanan, baik secara fisik maupun non-fisik. Ada banyak cara untuk mempertahankan negara, baik secara fisik maupun non-fisik. Dalam konteks militer, pertahanan adalah upaya untuk melindungi diri dari serangan militer. Pertahanan militer dapat dilakukan dengan berbagai cara, seperti membangun kekuatan militer, memperkuat pertahanan negara, dan menjalin kerja sama pertahanan dengan negara lain. Dalam konteks nonmiliter, pertahanan adalah upaya untuk melindungi diri dari serangan nonmiliter. Serangan nonmiliter dapat berupa serangan ekonomi, serangan informasi, atau serangan siber. Pertahanan nonmiliter dapat dilakukan dengan berbagai cara, seperti memperkuat ekonomi, meningkatkan kesadaran keamanan, dan mengembangkan teknologi keamanan.

Pertahanan yang kuat adalah penting untuk menjaga keamanan dan kedaulatan suatu negara. Suatu negara memiliki pertahanan yang kuat tentunya dapat melindungi dirinya dari berbagai ancaman dan gangguan.(Prasetyo, 2021).

2.1.1. Pertahanan Negara

Segala usaha untuk mempertahankan kedaulatan, keutuhan wilayah, dan keselamatan seluruh warga negara dari ancaman atau gangguan terhadap kedaulatan dan keutuhan negara disebut pertahanan negara (Indonesia S. N., 2004). Pertahanan negara terdiri dari dua kategori yakni pertahanan militer dan pertahanan nonmiliter.

Segala upaya untuk mempertahankan kedaulatan, keutuhan wilayah, dan keselamatan seluruh negara dari ancaman dan gangguan tanpa menggunakan kekuatan militer disebut pertahanan nonmiliter. Sedangkan pertahanan militer adalah pertahanan yang bergantung pada TNI sebagai komponen utama pertahanan negara dan didukung oleh cadangan dan pendukung melalui mobilisasi yang direncanakan sejak dini untuk menghadapi ancaman.

Menurut Undang-Undang Nomor 3 Tahun 2002 tentang Pertahanan Negara, pertahanan negara memiliki peran penting dalam menjaga kelangsungan hidup dan kesejahteraan bangsa (Indonesia R. , undang-undang Nomor 3 Tahun 2002 tentang

Pertahanan Negara, 2002) menurut peraturan pemerintah pertahanan bertujuan untuk (Indonesia R. , Peraturan Pemerintah Nomor 32 Tahun 2004 tentang Penyelenggaraan Pertahanan Negara, 2004):

1. Menjaga kedaulatan negara dari ancaman dan gangguan baik dari luar dalam maupun dari luar negeri.
2. Mempertahankan keutuhan negara dari ancaman atau serangan dari dalam maupun luar negeri.
3. Melindungi keselamatan negara dari semua bahaya dan gangguan.
4. Mewujudkan keamanan dan ketertiban nasional yang kondusif bagi pembangunan dan kesejahteraan bangsa.

Pertahanan negara menghadapi sejumlah tantangan, antara lain:

1. Gangguan dan ancaman yang semakin kompleks, baik dalam maupun luar negeri. (Ningsih, 2022)
2. Keterbatasan sumber daya, baik manusia, material, maupun anggaran (Rifai, 2022).
3. Perkembangan teknologi yang semakin pesat.
4. Upaya Peningkatan Pertahanan Negara

2.1.2. Pertahanan Siber

Menurut Rizki (Rizki, 2022), segala cara atau usaha untuk melindungi dan mencegah gangguan terhadap kerahasiaan, integritas, dan ketersediaan informasi adalah keamanan siber atau pertahanan siber. Serangan siber dapat berupa pencurian data, penghancuran sistem, atau gangguan terhadap layanan. Pertahanan siber penting untuk melindungi aset-aset penting suatu negara, seperti infrastruktur kritis, sistem keuangan, dan informasi rahasia.

Pertahanan siber memiliki peran penting dalam keamanan nasional. Serangan siber dapat melumpuhkan infrastruktur kritis, mengganggu perekonomian, dan mencuri informasi rahasia negara. Oleh karena itu, pemerintah perlu memiliki strategi pertahanan siber yang komprehensif (Budi, 2021).

Strategi pertahanan siber nasional harus mencakup hal-hal berikut (Arianto, 2019):

a. Identifikasi aset-aset penting yang perlu dilindungi dari serangan siber dalam hal ini yang termasuk ke dalam infrastruktur informasi vital nasional.
b. Pengembangan dan penerapan kebijakan dan regulasi keamanan siber.

c. Penguatan kapasitas sumber daya manusia dalam bidang keamanan siber.
d. Pengembangan teknologi keamanan siber dalam negeri, salah satunya yakni dengan menerapkan teknologi-teknologi terbaru seperti penerapan enkripsi, penggunaan teknologi firewall, dll.
e. Peningkatan kerja sama dengan pihak lain dalam bidang keamanan siber.

Pemerintah Indonesia telah melakukan banyak hal untuk memperkuat pertahanan siber, salah satunya yakni dengan menerbitkan berbagai kebijakan dan regulasi keamanan siber, seperti Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, Peraturan Presiden Nomor 53 Tahun 2018 tentang Strategi Nasional Keamanan Siber, dan Peraturan Menteri Kominfo Nomor 18 Tahun 2016 tentang Standar Nasional Teknologi Informasi Keamanan Siber untuk Penyelenggara Sistem Elektronik.

2.2. Kriptografi

2.2.1. Sejarah Kriptografi

Kriptografi berasal dari bahasa Yunani yaitu crypto berarti rahasia (*secret*) dan *graphia* berarti tulisan (*writing*). Kriptografi secara umum berarti tulisan rahasia. Kriptografi, menurut definisinya, adalah seni dan ilmu untuk menjaga keamanan pesan saat dikirim. Selain itu, kriptografi adalah bidang yang mempelajari bagaimana menjaga kerahasiaan pesan agar isi pesan aman sampai ke orang yang menerimanya.

Menurut Ariyus (Ariyus, 2008), Sekitar 4000 tahun yang lalu, masyarakat Mesir memperkenalkan kriptografi melalui hieroglyph, yang pertama kali digunakan. Pada zaman Romawi kuno, Julius Caesar harus menggunakan kurir untuk mengirimkan pesan rahasia kepada seorang jendral di medan perang. Karena itu rahasia, Julius tidak ingin pesan itu diketahui orang lain saat dia di jalan. Kemudian, Julius Caesar mengacak pesan tersebut sehingga hanya jenderalnya sendiri yang dapat memahaminya.

Dari penjelasan di atas, berbagai istilah kriptografi digunakan untuk menandai tindakan rahasia yang dilakukan saat mengirim pesan. Enkripsi adalah teknik yang digunakan Julius Caesar untuk mengacak pesan. Disebut "dekripsi", proses yang dilakukan oleh Sang Jendral untuk merapikan pesan yang tidak teratur. Pesan acak

dan pesan yang telah dirapikan disebut plain text. Pesan acak dan pesan yang telah dirapikan disebut cipher text.

Kriptografi digunakan untuk memastikan bahwa pesan, atau informasi, tidak dapat dilihat atau dibaca oleh orang yang tidak berhak. Metode penyandian pesan, yang juga dikenal sebagai kriptografi, telah berkembang seiring waktu.

Kemajuan teknologi yang begitu pesat sekarang memungkinkan orang berkomunikasi dan bertukar data secara jarak jauh, bahkan antar kota dan wilayah, bahkan antar benua. Oleh karena itu, kebutuhan akan perlindungan data yang saling dipertukarkan semakin meningkat. Banyak pengguna, termasuk perusahaan, departemen pertahanan, atau bahkan individu, tidak ingin informasi yang mereka berikan diketahui oleh pesaing, negara, atau orang lain. Oleh karena itu, dikembangkan satu bidang studi baru yang mempelajari bagaimana mengamankan data, atau disebut kriptografi.

2.2.2. Definisi Kriptografi

Menurut Ariyus (Ariyus, 2008), Kriptografi adalah seni dan ilmu yang memungkinkan pesan tetap aman saat dikirim. Fakta bahwa setiap orang mungkin memiliki metode yang berbeda untuk merahasiakan pesan. Pada masa-masa awal kriptografi adalah bersumber dari kata "seni" yang digunakan dalam definisi sebelumnya pada masa awal sejarah kriptografi. Setiap pelaku kriptografi menggunakan cara yang berbeda dan unik untuk menulis pesan rahasia, sehingga setiap pesan memiliki nilai estetika yang unik dan berbeda-beda, yang membuat kriptografi berkembang menjadi seni merahasiakan pesan.

Menurut JP Rizky Rachman (JP Rizky Rachman, 2011), dalam jurnalnya menyatakan keamanan penyimpanan data sangat penting, terutama ketika menggunakan media penyimpanan online. Kapasitas media penyimpanan harus digunakan lebih hemat karena kapasitasnya terbatas. Dimungkinkan untuk menyelesaikan kedua masalah tersebut dengan menjaga media penyimpanan online aman dan hemat biaya. Dengan kombinasi keduanya, gabungan kriptografi dan kompresi dapat membantu mengatasi masalah keamanan data. Dengan demikian, melindungi dan menghemat media penyimpanan online dapat menjadi solusi untuk kedua masalah tersebut.

Keamanan dari suatu kriptografi terletak pada kerahasiaan kunci. Selain itu, sistem kriptografi yang kuat membuat chipher teks acak untuk semua standar statistik

dan memiliki jangkauan kunci yang besar. Akibatnya, metode brute brute, yang mencoba semua kunci yang memungkin secara acak, akan mengalami kendala memecahkan hasil chipper teks atau setidaknya akan membutuhkan waktu yang lebih lama untuk memecahkannya.

2.2.3. Tujuan Kriptografi

Menurut UMA (LP2M, 2022, April 26), ilmu kriptografi memiliki empat tujuan utama yang berkaitan dengan keamanan informasi:

1. Kerahasiaan (*confidentiality*), untuk mencegah informasi yang telah disandi untuk dibuka atau diakses oleh siapa pun yang tidak memiliki otoritas atau kunci rahasia untuk melakukannya.
2. Integritas data (data *integrity*), untuk melindungi data dari perubahan yang tidak sah. Untuk menjaga integritas data, sistem harus memiliki kemampuan untuk mengidentifikasi orang yang tidak berhak yang mengubah data, seperti menambah, menghapus, dan memasukkan data lain ke dalam data sebenarnya.
3. Autentikasi (*authentiaction*), untuk mengidentifikasi informasi dan sistem itu sendiri. Dua belah pihak harus memperkenalkan diri. Semua informasi yang dikirim melalui kanal harus diperiksa untuk memastikan bahwa itu benar-benar asli. Faktor seperti waktu pengiriman dan isi data adalah bagian dari informasi ini.
4. Tanpa penolakan (non-*repudiation*), untuk menghindari penyangkalan pengiriman atau pembuatan informasi oleh orang yang mengirimkan atau membuatnya.

2.2.4. Terminologi dan Konsep Dasar Kriptografi

Beberapa istilah atau terminologi akan ditemukan dalam bidang kriptografi. Dalam ilmu kriptografi, istilah-istilah tersebut sangat sulit untuk dipahami. Berikut ini adalah penjelasan dari beberapa istilah-istilah penting dalam bidang kriptografi yang sering digunakan.

a. Plain text dan Cipher text

   Adalah pesan atau informasi yang dikirimkan baik dalam bentuk aslinya maupun dalam format yang mudah dibaca. Cipher teks adalah data atau pesan yang sudah dikodekan dan tidak dapat dibaca dengan mudah..

Keamanan algoritma yang digunakan untuk enkripsi atau dekripsi bergantung pada banyak hal. Sifat algoritma yang digunakan adalah salah satu faktor yang sangat penting. Pesan dapat berupa teks, video, gambar, dan sebagainya.

b. Enkripsi dan Dekripsi

Enkripsi adalah sebuah prosedur yang mengubah pesan dari yang mudah dipahami menjadi yang sulit dipahami, atau bisa disebut sebagai proses penyandian pesan. Dekripsi adalah proses yang menggunakan algoritma yang sama untuk mengembalikan informasi yang sudah teracak(ter-enkripsi) ke bentuk aslinya yang merupakan proses yang mengubah data yang sudah dienkripsi (cipher text) menjadi data asli (plain text).

c. Kriptologi dan Kriptanalisis

Kriptologi adalah bidang yang mempelajari kriptografi dan kriptanalisis. Kriptanalisis (cryptanalysis) adalah penelitian tentang cipher, cipher text, atau cyrptosystems. Tujuannya adalah untuk menemukan kelemahan sistem penyandian sehingga kita dapat mendapatkan teks biasa dari cipher text yang ada tanpa mengetahui kunci atau algoritma pembangunnya. Mereka yang melakukan kriptoanalisis disebut kriptoanalyst.

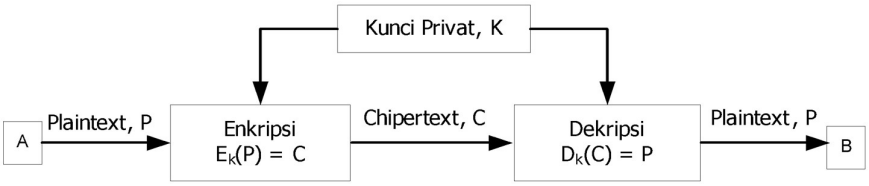
2.2.5. Jenis Algoritma Kriptografi

Dalam kriptografi, ada dua jenis algoritma digunakan yakni simetris dan asimetris (UMA., LP2M, 2022, April 26) (Paar, 2010)

A. Algoritma Simetris

Algoritma simetris, juga disebut algoritma kunci rahasia, adalah algoritma kriptografi yang menggunakan kunci enkripsi yang sama dengan kunci deskripsinya. Sebelum algoritma ini dapat berkomunikasi, kedua pihak harus menyetujui kunci tertentu. Keamanan algoritma simetris ditentukan oleh kuncinya. Agar komunikasi tetap aman, kunci harus tetap dirahasiakan. Karena sifat kunci tersebut sangat rahasia, pengirim kunci harus selalu memastikan bahwa orang yang ditunjuk untuk membawa kunci untuk dipertukarkan dapat dipercaya dan harus dapat memastikan teknik dan cara yang digunakan untuk mendistribusikan kunci tersebut haruslah aman.

Jika n pengguna berkomunikasi secara bersamaan dan setiap pihak bertukar kunci, maka jumlah kunci rahasia yang harus ditukarkan secara aman adalah sebanyak (n-1)/2, maka masalahnya akan menjadi rumit. (Munir, 2006).



Gambar 2.1. Proses Algoritma Simetri (symmetric algorithm)

Algoritma aliran (Stream Cipher) dan blok (Block Cipher) adalah dua jenis algoritma simetris.

1. Algoritma aliran (*Stream Cipher*)

   Algoritma sandi yang dikenal sebagai stream cipher dapat digunakan untuk mengenkripsi sejumlah kecil data, seperti bit, byte, nible, atau per lima bit, dalam kasus di mana data yang dienkripsi dianggap sebagai data Boudout. Setiap kali satu set data dienkripsi, digunakan kunci yang dibuat dari kunci sebelumnya. Contoh stream cipher termasuk Caesar Cipher, One Time Pad, dan RC4 (Rivest Cipher 4).
2. Algoritma blok (Block cipher)

   Algoritma enkripsi block cipher adalah enkripsi yang membagi-bagi plain text yang akan dikirimkan dengan ukuran tertentu (disebut blok) dengan panjang t. Selain itu, kunci yang sama akan digunakan untuk mengenkripsi setiap blok. Oleh karena algoritma ini biasanya memproses teks biasa dengan panjang lebih dari 64 bit, pola serangan saat ini sulit untuk membongkar kunci. Contoh algoritma yang menggunakan metode blok cipher adalah DES, 3DES, CAST-128, RC5, RC6, AES, Blowfish, dan IDEA.

Kelebihan algoritma simetri adalah:

1. Enkripsi dan dekripsi menggunakan kriptografi simetri membutuhkan waktu yang singkat.
2. Ukuran kunci algoritma simetri relatif lebih pendek daripada algoritma asimetri.
3. Cipher teks yang diterima dapat digunakan untuk memastikan pengiriman pesan langsung karena kunci hanya diketahui oleh penerima dan pengirim.

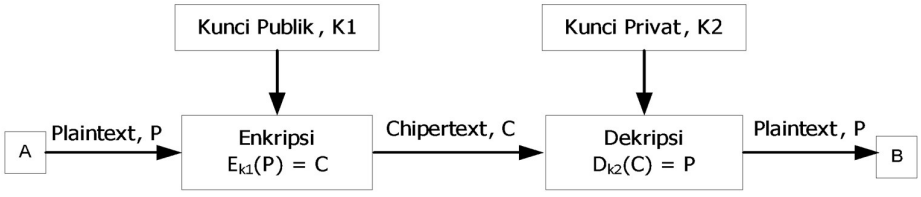
Kekurangan algoritma simetri adalah:

1. Ketika kunci simetri dikirim, saluran yang aman harus digunakan, dan kedua belah pihak harus memastikan bahwa kunci itu rahasia.
2. Setiap kali melakukan komunikasi, kunci harus diubah.
3. Pesan tidak dapat dibuka jika kunci hilang atau lupa.

B. Algoritma Asimetris

Dalam karya Diffie dan Hellman yang berjudul "New Directions in Cryptography" pada tahun 1976, algoritma asimetris pertama kali dipublikasikan. Berbeda dengan algoritma simetri, algoritma asimetris menggunakan dua jenis kunci untuk proses enkripsi dan deskripsinya. Algoritma ini menggunakan dua jenis kunci: kunci publik (public key) dan kunci rahasia (secret key). Ini dikenal sebagai algoritma kunci publik atau sandi kunci publik. Sementara kunci rahasia digunakan untuk mendekripsi pesan, kunci publik digunakan untuk mengenkripsinya. Kunci publik umum, yang berarti tidak dapat dirahasiakan sehingga siapa pun dapat melihatnya. Namun, kunci rahasia disimpan dalam rahasia dan hanya orang tertentu yang diizinkan untuk mengetahuinya, kunci ini digunakan untuk mengenkripsi pesan yang akan dikirimkan (UMA., LP2M, 2022, April 26).

Keunggulan utama algoritma asimetris adalah memberikan jaminan keamanan kepada semua orang yang melakukan transaksi data, terlepas dari situasi di mana orang-orang tersebut tidak mencapai kesepakatan sebelumnya tentang keamanan pesan atau tidak mengenal satu sama lain. Algoritma asimetris, adalah suatu algoritma yang menggunakan kunci yang berbeda untuk masing-masing proses enkripsi dan proses dekripsi.



Gambar 2.2. Proses Algoritma Asimetri (asymmetric algorithm)

Kelebihan algoritma asimetris adalah:

a. Algoritma asimetris menggunakan hanya kunci privat yang harus dijaga rahasia oleh setiap entitas yang berkomunikasi. sehingga tidak perlu mengirimkan kunci seperti yang dilakukan oleh algoritma kunci simetris.

b. Tidak perlu mengubah pasangan kunci publik dan privat dalam waktu yang lama..
c. Masalah distribusi keamanan kunci dapat diperbaiki.
d. Masalah pengelolaan kunci menjadi lebih mudah karena jumlah kunci yang lebih sedikit.

Kekurangan algoritma asimetris adalah:

a. Proses enkripsi dan dekripsi yang menggunakan bilangan besar dan operasi bilangan besar biasanya lebih lambat dari algoritma simetri.
b. Ukuran cipher text lebih besar dari plain text karena proses enkripsi yang dilakukan.
c. Membutuhkan dua kunci sekaligus, dan ukurannya relatif lebih besar daripada kunci simetri.

2.3. Kriptografi AES-256

Pemerintah Amerika Serikat telah menetapkan standar enkripsi kunci simetris yang dikenal sebagai Standar Enkripsi Lanjutan (AES). Standar AES-128, AES-192, dan AES-256 adalah tiga blok penyandian yang berasal dari kumpulan penyandian yang lebih besar yang pertama kali dirilis sebagai Rijndael. (Daemen, 2023) (Rogaway, 2022).

Karena kunci AES-256 memiliki panjang 256 bit, yang berarti bahwa serangan brute-force dapat membuka kunci dengan dua 256 upaya percobaan. Saat ini, algoritme enkripsi AES-256 dianggap sebagai salah satu yang paling aman. Namun, dengan tingkat komputasi saat ini, diperlukan jutaan tahun untuk meretas kunci AES-256.

Enkripsi AES 256 telah banyak digunakan, antara lain:

- Keamanan komunikasi
  Melindungi privasi informasi yang dikirim melalui jaringan seperti surel, dokumen, dan rekaman video.
- Keamanan penyimpanan
  Algoritma AES melindungi data yang disimpan pada perangkat penyimpanan seperti hard drive, SSD, dan kartu SD.
- Perlindungan perangkat lunak
  AES digunakan untuk menjaga data pribadi, kata sandi, kunci terenkripsi, dan informasi lainnya yang penting untuk perangkat lunak.

Keamanan AES-256 berakar pada dua prinsip pokok:

1. Kunci berukuran besar yang dienkripsi dengan kunci 256 bit memberikan tingkat keamanan yang sangat tinggi.
2. Serangan terhadap algoritme AES-256 sangat sulit karena Tingkat kompleksitasnya.

Tidak ada serangan yang mampu mengalahkan kunci AES-256 dengan tingkat keberhasilan yang signifikan, meskipun AES telah diuji secara menyeluruh. Dalam dunia keamanan data, AES-256 memiliki beberapa keunggulan yang signifikan. Dengan tingkat enkripsi yang sangat tinggi, AES-256 dapat melindungi informasi sensitif dari serangan peretas yang paling canggih. Standar enkripsi ini juga menawarkan tingkat keamanan yang tinggi dan sangat sulit untuk ditembus, sehingga Anda dapat menggunakan AES-256 dengan kepercayaan tinggi. (Bertoni, 2022) (Bogdanov, 2021)

AES-256 memiliki beberapa kelebihan jika dibandingkan dengan algoritme enkripsi lainnya, seperti:

- AES-256 merupakan algoritme enkripsi yang memiliki tingkat keamanan tertinggi pada saat ini.
- Karena kecepatannya yang tinggi, AES-256 dapat digunakan dengan cepat di perangkat keras dan perangkat lunak kontemporer.
- Salah satu keuntungan menggunakan AES-256 adalah penggunaan memori yang lebih efisien.

Terlepas dari kenyataan bahwa AES-256 dianggap sebagai salah satu algoritma enkripsi yang paling aman, ada beberapa hal yang perlu diperhatikan untuk memastikan keamanannya. (Saputra, 2023) (Anggraini, 2022), yaitu:

- Keamanan kunci

  Kunci AES-256 harus disimpan dengan aman dan tidak boleh diambil oleh orang yang tidak berwenang sehingga Sangat penting untuk menjaga agar kunci AES-256 disimpan dengan aman. Jika bocor, data yang terenkripsi dengannya dapat diretas dengan mudah.
- Implementasi

  Untuk memastikan keamanan AES-256, Implementasi harus dilakukan dengan cara yang tepat. Keamanan AES-256 dapat berkurang jika tidak dilakukan dengan benar.

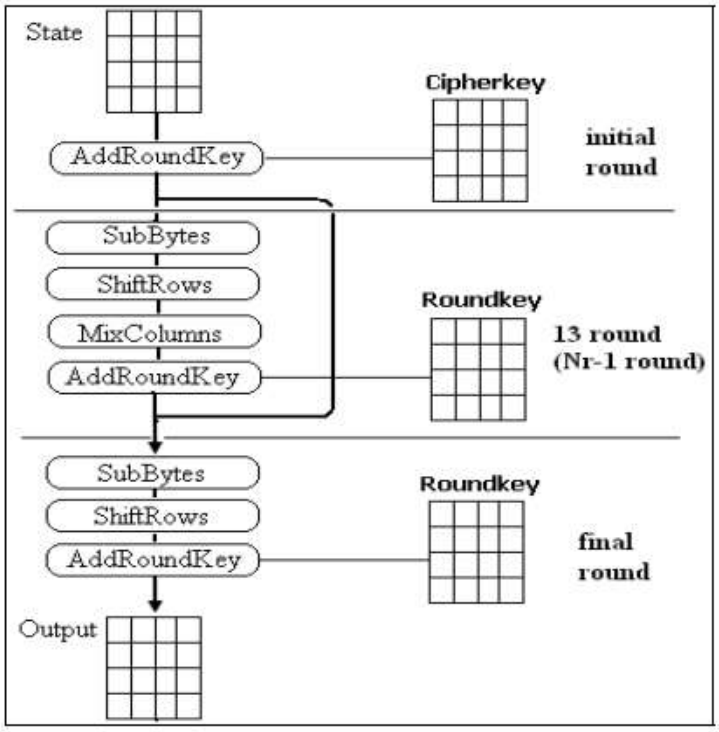
- Keamanan perangkat

  Perangkat yang digunakan untuk mendekripsi dan mengenkripsi data dengan AES-256 harus aman dari serangan fisik. Jika perangkat diretas, data yang terenkripsi dengan AES-256 juga dapat diretas.

AES-256 mengenkripsi dan mendekripsi data dengan menggunakan kunci 256-bit. Metode ini didasarkan pada algoritma kriptografi kunci simetris yang sangat kuat, dan dianggap aman untuk digunakan dalam berbagai aplikasi keamanan data. Karena kunci 256-bitnya, AES-256 menawarkan perlindungan yang sangat baik terhadap serangan kriptanalisis dan membantu menjaga kerahasiaan data yang telah terenkripsi. Aplikasi keamanan sistem informasional banyak menggunakan AES-256. Dengan prinsip kerja yang canggih dan keamanan yang kuat, AES-256 menjadi salah satu pilihan yang populer untuk melindungi data sensitif.

Dengan menggunakan kunci 256 bit, AES-256 mampu memberikan perlindungan yang sangat baik terhadap serangan kriptanalisis dan membantu menjaga kerahasiaan data yang terenkripsi. AES-256 telah banyak digunakan dalam aplikasi keamanan sistem informasi, termasuk dalam penyimpanan data, transfer file, dan komunikasi kriptografi.

Komponen AES selalu memiliki inversi dengan panjang blok 128 bit, sehingga merupakan sistem penyandian blok non-Feistel. Proses yang digunakan oleh kunci AES disebut sebagai ronde, dan proses itu sendiri merupakan transformasi terhadap keadaan. Pertama, teks asli disusun sebagai keadaan dalam blok 128 bit.



Gambar 2.3. Ilustrasi Proses Enkripsi AES (Munir, 2006)

Enkripsi AES adalah modifikasi situasi berulang. Teks asli dibuat sebagai keadaan pada awal proses enkripsi. Ronde ke-k menerima state yang keluar dari ronde k+1. Kemudian, sebelum ronde pertama, blok teks asli dicampur dengan kunci ronde ke-0 melalui transformasi yang dikenal sebagai AddRoundKey. Kemudian, ronde ke-1 berlanjut sampai ronde ke-(Nr-1), di mana Nr adalah jumlah ronde. AES menggunakan empat kategori transformasi, yaitu:

1) SubBytes, sebagai transformasi substitusi.
2) ShiftRows, sebagai transformasi permutasi.
3) MixColumns, sebagai transformasi pengacakan.
4) AddRoundKey, sebagai transformasi penambahan kunci.

Pada ronde ke-Nr, ronde terakhir, terjadi transformasi yang sebanding dengan ronde lain, tetapi tidak ada transformasi MixColumns. Secara ringkas, algoritma deskripsi adalah kebalikan dari algoritma enkripsi AES. Algoritma dekripsi AES menggunakan transformasi inversi untuk semua transformasi dasar yang digunakan dalam algoritma enkripsi AES (Shazhaq, 2023). Contoh transformasi inversi ini adalah InvSubBytes, InvShiftRows, dan InvMixColumns. Dengan menggunakan dikunci yang sama, AddroundKey adalah transformasi yang bersifat self-invers.

Penggunaan enkripsi AES 256 karena tingkat kesulitan membobol hasil enkripsi AES 256. Menurut penjelasan Vasileios A. Memos (Memos, 2015) diperlukan waktu 3,31 x 10^{56} tahun untuk membobol hasil enkripsi AES 256, seperti yang ditunjukkan pada gambar berikut.

Key Size	Time to Crack
56-bit (DES)	399 seconds
128-bit (AES)	1,02 x 10^{18} years
192-bit (AES)	1,872 x 10^{37} years
256-bit (AES)	3,31 x 10^{56} years

Gambar 2.4. Waktu Yang Diperlukan Untuk Memecahkan Suatu Enkripsi

2.4. Kriptografi RC4

Untuk masalah transmisi query basis data seperti ini, RC4 adalah algoritma stream cipher yang paling cocok dibandingkan dengan algoritma stream cipher yang lain. Ini karena proses enkripsi RC4 yang sangat sederhana, dengan hanya beberapa operasi yang dilakukan pada setiap byte. Menurut AlFardan (AlFardan, 2013) algoritma RC4 memerlukan dua ribu jam untuk diselesaikan.

Salah satu algoritma kriptografi kunci simetris yang dikembangkan oleh RSA Data Security Inc. (RSADSI) adalah Rivest Code 4 (RC4), juga dikenal sebagai Rivest Cipher 4, yang ditemukan oleh Ronald L. Rivest pada tahun 1987. RSADSI juga membuat algoritma kunci simetris dalam bentuk cipratan alur. Tiga orang dari Massachusetts Institute of Technology, Ron Rivest, Adi Shamir, dan Len Adleman, menciptakan algoritma ini pada tahun 1977. Nama singkatan RSA berasal dari inisial mereka.

Algoritma ini merupakan salah satu algoritma stream cipher yang paling populer dan digunakan dalam berbagai aplikasi aplikasi, seperti jaringan nirkabel (Wi-Fi, Bluetooth, dan sebagainya), protokol keamanan (TLS, SSL, WPA, dan sebagainya), dan aplikasi lainnya, menggunakan algoritma stream cipher ini. (Khairul Anwar, 2022) (Ridwan, 2022)

RC4 membuat tabel sepanjang 256 byte dengan panjang kunci dari 1 hingga 256 byte. Tabel ini digunakan untuk generasi berikutnya dari pseudo acak, yang menghasilkan cipher teks dengan menggunakan XOR dengan plain text. Minimal satu elemen dari tabel ditukarkan satu sama lain.

RC4 adalah jenis stream cipher yang dapat memproses unit atau data masukan, pesan, atau informasi sekaligus. Data atau unit biasanya berupa byte, atau bahkan bit (dalam hal RC4), sehingga enkripsi dan dekripsi dapat dilakukan pada panjang yang berbeda. Algoritma ini tidak perlu menunggu jumlah data, pesan, atau informasi tertentu sebelum diproses, atau ia tidak perlu mengenkripsi dengan menambahkan byte tambahan.

Menurut Arianto (2019), algoritma RC4 menggunakan array 256 yang mengandung permutasi dari 0 hingga 255. Selain itu, ada S-Box kedua yang mengandung permutasi yang merupakan fungsi dari kunci dengan panjang yang berubah. RC4 adalah cipher aliran yang umum digunakan untuk sistem keamanan, seperti protokol Secure Socket Layer (SSL). Algoritma kriptografi ini tidak rumit dan dapat digunakan dengan mudah. Untuk mengenkripsi atau mendeskripsi data, Ron Rivest membuat RC4 di laboratorium RSA.

RC4 menghasilkan kunci aliran yang dienkripsi dengan teks biasa saat dienkripsi (atau dienkripsi dengan bit teks ter sandi saat didekripsi). RC4 berbeda dari streamer normal karena memproses data dalam blok. RC4 memproses data terlebih dahulu dalam ukuran byte (1 byte = 8 bit). RC4 menggunakan dua kotak substitusi, atau S-box, dari array 256-byte, berisi substitusi bernomor 0-255, dan S-box kedua berisi substitusi aktivitas induk dalam indeks..

Namun, algoritma RC4 memiliki kelemahan. Di mana pada array S bisa saja ada nilai yang mempunyai nilai yang sama. Ini karena karakter kunci disalin. RC4 mudah diserang dengan serangan kata sederhana yang diketahui jika browser mengetahui banyak bagian dari kata-kata tertulis dan tertulis Anda. Ada beberapa cara untuk memperbaiki masalah ini:

a. Menggunakan kunci yang panjang (minimal panjang kunci kurang lebih 3 karakter dan maksimal lebih kurang dari 255 karakter) mengurangi kemungkinan menambahkan kunci berulang kali ke tabel kunci dan menggunakan kombinasi yang berbeda.
b. Jika ingin mengenkripsi file yang berbeda, usahakan untuk tidak menggunakan kunci yang sama.
c. Jika kita menggunakan kunci yang sama setiap kali kita mengenkripsi file, kita memerlukan vektor inisialisasi (IV) pada kunci rahasia. Jika IV yang digunakan dalam setiap proses enkripsi tidak pernah sama, maka akan

dihasilkan cipher text yang berbeda walaupun plain text yang dienkripsi sama.

d. Mengacak (mengurutkan ulang) plain text sebelum mengubahnya menjadi cipher text, sehingga jika penyerang menerima 1 byte data dari plain text, maka penyerang tidak dapat melakukan XOR 2 buah cipher text dan satu byte data yang diketahui.
e. Mengubah metode pengisian kunci menjadi kumpulan(himpunan/array) kunci. Metodenya adalah dengan mengisi kumpulan kunci hanya sekali, lalu mengisi variabel kunci lainnya dengan nilai yang dihasilkan secara acak.

Keamanan RC4 bergantung pada panjang kunci yang digunakan. Kunci dengan panjang 128 bit atau lebih dianggap aman dari serangan brute force. Namun, kunci dengan panjang 40 bit atau kurang dianggap tidak aman.

Berikut adalah kelebihan dan Kekurangan algoritma RC4 (Saifullah, 2022):

a) Kelebihan RC4 antara lain:

- Sederhana dan mudah diimplementasikan
- Efisien dalam penggunaan sumber daya.
- Dapat digunakan dengan panjang kunci yang variabel.

b) Kekurangan RC4 antara lain:

- Tidak tahan terhadap serangan tertentu, seperti serangan differential cryptanalysis.
- Memiliki pola yang berulang, yang dapat meningkatkan kemungkinan serangan.

2.5. Secure Hash Algorithm (SHA)

SHA-1, atau Secure Hash Algorithm 1, adalah fungsi hash yang digunakan dalam kriptografi untuk membuat nilai hash unik untuk setiap input. Nilai hash ini biasanya berupa 40 digit huruf heksadesimal (Nugraha, 2020).

Fungsi hash mengambil data masukan, membaginya menjadi blok-blok kecil, dan kemudian menerapkan operasi matematika ke blok-blok tersebut. Operasi matematika ini menghasilkan nilai hash yang unik. (Wibowo, 2022).

Panjang keluaran SHA-1 adalah 160 bit, yang membuatnya cukup kuat untuk berbagai aplikasi keamanan informasi. Namun pada tahun 2017, tim peneliti berhasil menemukan serangan tabrakan terhadap SHA-1. Serangan ini menunjukkan bahwa dua input berbeda dapat menghasilkan nilai hash yang sama. Meskipun demikian, SHA-1 masih dianggap cukup aman untuk sebagian besar aplikasi. Namun, aplikasi

yang memerlukan keamanan sangat tinggi (seperti tanda tangan digital) harus menggunakan fungsi hash yang lebih kuat, seperti SHA-256 atau SHA-512.

Algoritme SHA-1 relatif lebih lambat dibandingkan versi SHA yang lebih baru seperti SHA-256 dan SHA-3, dan meskipun lebih kompleks, para ahli juga mengindikasikan kemungkinan serangan *spoofing* terhadap SHA-1, yaitu menemukan dokumen tertentu yang menghasilkan. nilai hash yang ditentukan. (Aoki, 2014). Namun, terlepas dari kelemahan ini, SHA-1 memiliki desain algoritma yang relatif sederhana dan mudah diimplementasikan pada berbagai platform komputasi, dan SHA-1 pernah menjadi fungsi hash yang sangat populer dan banyak digunakan dalam berbagai protokol dan aplikasi, oleh karena itu kompatibilitas dan dukungan perangkat lunak masih tersedia. (Potenz, 2020)

Dalam penelitian ini, SHA-1 digunakan untuk memperoleh nilai hash dari dokumen yang akan di enkripsi, untuk selanjutnya hash tersebut divalidasi Kembali pada saat proses dekripsi, hal ini dilakukan untuk menjaga integritas dokumen yang di enkripsi.

2.6. Infrastruktur Informasi Vital

Infrastruktur Informasi Vital yang selanjutnya disingkat IIV adalah sistem elektronik yang memanfaatkan teknologi informasi dan/atau teknologi operasional baik secara mandiri maupun dikombinasikan dengan sistem elektronik (SE) lainnya untuk mendukung sektor-sektor strategis jika terjadi gangguan, kerusakan, dan/atau kehancuran. Infrastruktur yang bersangkutan mempunyai dampak yang signifikan terhadap kepentingan umum, pelayanan publik, pertahanan dan keamanan atau perekonomian nasional. (Indonesia R. , Peraturan Presiden Nomor 82 Tahun 2022, 2022).

Bidang-bidang yang ditetapkan dalam Peraturan Presiden Nomor 82 Tahun 2022 tentang Perlindungan Infrastruktur Informasi Penting, menurut undang-undang, mengacu pada Pasal 99 Peraturan Pemerintah Nomor 71 Tahun 2019 tentang PSTE Pasal 99 ayat (2): Kantor atau fasilitas yang menyimpan informasi elektronik strategis yang harus dilindungi sesuai ketentuan pada ayat (l), meliputi:

a. Sektor administrasi pemerintahan.
b. Sektor energi dan sumber daya mineral.
c. Sektor transportasi.
d. Sektor keuangan.

e. Sektor kesehatan.
f. Sektor teknologi informasi dan komunikasi.
g. Sektor pangan.
h. Sektor pertahanan
i. Sektor lain yang ditetapkan oleh Presiden.

Adapun tujuan dari perlindungan IIV adalah:

a. Melindungi kelangsungan operasi IIV dengan cara yang aman, andal, dan dapat dipercaya;
b. Mencegah kerusakan, kerusakan, dan/atau kerusakan IIV karena serangan siber dan ancaman/kerentanan lainnya; dan
c. Meningkatkan kesiapan untuk menghadapi insiden siber dan mempercepat pemulihan.

2.7. Penelitian Terdahulu

Penelitian yang relevan dengan penelitian ini pernah dilakukan oleh beberapa peneliti terdahulu, antara lain:

Aditia Rahmat Tulloh (Tulloh, 2016) telah melakukan penelitian tentang Kriptografi Standar Penyandian Tinggi (AES) untuk Penyandian Dokumen File Dalam algoritma kriptografi AES 128(128 bit), Proses enkripsi dimulai dengan mengubah teks biasa menjadi kode ASCII dalam bentuk bilangan heksadesimal. Kemudian, state, matriks byte berukuran empat kali empat, disusun. Enkripsi AES 128 menggunakan transformasi state sepuluh kali. Data biner adalah yang digunakan untuk memproses setiap putaran.

AES menggunakan empat transformasi utama: subbytes, shiftrows, mixcolumns, dan addroundkey. Untuk setiap ronde, satu hasil generasi kunci diperlukan. Namun, transformasi-transformasi dilakukan dengan urutan invshiftrows, invsubbytes, addroundkey, dan invmixcolumns selama proses dekripsi. Dokumen yang telah dipastikan memiliki lebih dari 16 karakter akan dienkripsi dan didekripsi setiap 128 bit atau 16 karakter.

Akibatnya, dekripsi dan enkripsi AES dilakukan secara bersamaan. Namun, file teks dengan kurang dari 16 karakter tidak akan memiliki padding. Penggunaan karakter ASCII nul untuk mengisi lebih sedikit karakter sehingga dapat diproses tanpa mengubah hasil enkripsi atau dekripsi dikenal sebagai padding.

Irfan Kurnia Nurhareza (Nurhareza, 2022) telah melakukan penelitian tentang penerapan algoritma kriptografi AES 256. Dalam penelitian ini, algoritma kriptografi AES 256 digunakan untuk mengamankan dokumen berbasis web Kelurahan Belendung.Hasilnya menunjukkan bahwa penggunaan metode ini berhasil mengubah dan mengembalikan isi dokumen Kelurahan Belendung.

Sistem web dapat mengamankan isi dokumen dengan baik dan hasil dari proses enkripsi menjadikan isi dokumen tidak dapat terbaca. Hasil pengujian sistem menunjukkan bahwa ukuran dokumen rata-rata 2496069,1 byte, lama proses 1181000 millidetik, dan hasil dekripsi rata-rata 2496128 byte. Ini menunjukkan bahwa sistem web berhasil mengembalikan isi dokumen yang telah dienkripsi ke bentuk aslinya.

Beberapa saran yang dapat menjadi pertimbangan kedepannya untuk mengembangkan sistem ke tingkat yang lebih lanjut adalah: Menambahkan fungsi pada sistem online, seperti tombol kembali untuk kembali ke halaman utama dan tombol KIRIM untuk mengirim file melalui internet sehingga bisa lebih mempermudah pengguna dan aplikasi web bisa. mengakses tidak hanya dokumen PDF dan TXT, tetapi juga semua format file lainnya.

Berita Estu Widodo (Widodo, 2020) telah melakukan penelitian tentang implementasi Advanced Encryption Standard pada enkripsi dan dekripsi dokumen rahasia di INTELKAM polda DIY, yang diperoleh dari penelitian itu adalah Sistem kriptografi dokumen "Akrid" memanfaatkan metode kriptografi Advance Encryption Standard (AES) untuk enkripsi dan dekripsi dokumen dalam format seperti doc, docx, xls, xlsx, pdf, dan txt. Hasil pengujian menunjukkan bahwa ukuran dokumen memengaruhi waktu yang dibutuhkan untuk enkripsi dan dekripsi. Semakin besar ukuran dokumen, waktu yang diperlukan lebih lama. Proses enkripsi membutuhkan waktu antara 0,010 dan 0,014 detik untuk dokumen per 1Kb, sedangkan proses dekripsi membutuhkan waktu antara 0,011 dan 0,013 detik untuk dokumen per 1Kb.

Berikut ini adalah metrik penelitian yang sudah pernah dilakukan beserta gap (celah) dengan penelitian ini.

Tabel 2.1. Metrik Gap Penelitian

Penulis	Judul	Hasil Penelitian	Gap
Djong, H. S., & Siswanto, S. (Djong, 2022)	Implementasi Kriptografi Dengan Menggunakan Metode RC4 dan AES-256 Untuk Mengamankan File Dokumen pada PT Varnion Technology Semesta	Penelitian ini berhasil mengimplementasikan algoritma kriptografi dengan metode RC4 dan AES-256 pada file dokumen yang berekstensi .txt, .pdf, .doc, .docx, .xls, dan .xlsx dengan ukuran maksimal 3MB.	Penelitian ini menggunakan kunci yang diberikan oleh pengguna sehingga rentan dengan kemungkinan kunci tersebut hilang atau digunakan oleh pihak lain
Wardhana (Wardhana, 2023)	Analisis Perbandingan Kinerja Enkripsi Algoritma RC4 dan AES	Penelitian ini menunjukkan bahwa RC4 memiliki kecepatan enkripsi lebih baik, sementara AES memerlukan waktu lebih lama. Ukuran file yang dienkripsi dengan RC4 tetap sama, sementara AES menghasilkan ukuran yang berbeda.	Penelitian ini membandingkan kinerja enkripsi AES 256 dan RC4 bukan penggabungan 2 jenis enkripsi, bukan penggabungan 2 enkripsi sekaligus
Imron, M., & Pratama, A. (Imron, 2022)	Pengamanan E-Dokumen Berbasis Steganografi Dengan Kombinasi Advanced Encryption Standard (AES) 128 Bit	Penelitian ini berhasil mengimplementasikan algoritma kriptografi dengan metode AES-128	Penelitian ini hanya menggunakan satu jenis enkripsi yakni AES 128
(Nurhareza, Penerapan Algoritme Kriptografi AES 256 Untuk Mengamankan Dokumen Berbasis Web Pada Kelurahan	Penerapan Algoritme Kriptografi AES 256 Untuk Mengamankan Dokumen Berbasis Web Pada Kelurahan Belendung	Penelitian ini berhasil mengimplementasikan algoritma kriptografi dengan metode AES-256 pada file dokumen pada Kelurahan Belendung	Penelitian ini hanya menggunakan enkripsi AES 256 bukan penggabungan 2 enkripsi sekaligus

Belendung, 2022)			
A. A. R. Al-Marzoqi, A. F. Al-Ghamdi, dan A. S. Al-Ghamdi (2021)	A Comparative Study of RC4 and AES Algorithms for Data Encryption	Penelitian ini membandingkan kinerja algoritma RC4 dan AES untuk enkripsi data. Hasil penelitian menunjukkan bahwa AES memiliki tingkat keamanan yang lebih baik daripada RC4, tetapi AES memerlukan waktu lebih lama untuk melakukan enkripsi.	Penelitian ini membandingkan kinerja enkripsi AES 256 dan RC4 bukan penggabungan 2 jenis enkripsi, bukan penggabungan 2 enkripsi sekaligus
Berita Estu Widodo (Widodo, 2020)	Implementasi Advanced Encryption Standard Pada Enkripsi Dan Dekripsi Dokumen Rahasia Ditintelkam Polda DIY	Penelitian ini berhasil mengimplementasikan algoritma kriptografi dengan metode AES-256 pada file dokumen di Ditintelkam Polda DIY dengan waktu enkripsi 0,212 second untuk dokumen ukuran 19,212 Kb dan 20,533 second untuk dokumen ukuran 1.966 Kb	Penelitian ini hanya menggunakan enkripsi AES 256 bukan penggabungan 2 enkripsi sekaligus
M. M. Khan, S. A. Khan, dan M. I. Khan (2019)	A Survey on the Security Analysis of RC4 and AES Algorithms	Penelitian ini memberikan survei tentang analisis keamanan algoritma RC4 dan AES. Hasil penelitian menunjukkan bahwa AES memiliki tingkat keamanan yang lebih baik daripada RC4, tetapi AES lebih rentan terhadap serangan brute force.	Penelitian ini membandingkan tingkat keamanan enkripsi AES 256 dan RC4 bukan penggabungan 2 jenis enkripsi, bukan penggabungan 2 enkripsi sekaligus
M. A. S. Al-Fahad, M. M. Al-Hajry, dan A. S. Al-Ghamdi (2018)	A Comparative Study of RC4 and AES Algorithms for Data Encryption	Penelitian ini membandingkan kinerja algoritma RC4 dan AES untuk enkripsi data. Hasil penelitian menunjukkan bahwa AES memiliki tingkat keamanan yang lebih baik daripada RC4,	Penelitian ini membandingkan kinerja enkripsi AES 256 dan RC4 bukan penggabungan 2 jenis enkripsi, bukan

		tetapi AES memerlukan waktu lebih lama untuk melakukan enkripsi.	penggabungan 2 enkripsi sekaligus
Aditia Rahmat Tulloh (2016)	Kriptografi Advanced Encryption Standard (AES) Untuk Penyandian File Dokumen	Penelitian ini berhasil mengimplementasikan algoritma kriptografi dengan metode AES-256 pada file dokumen	Penelitian ini hanya menggunakan enkripsi AES 256 bukan penggabungan 2 enkripsi sekaligus
V. Indriyanta dan G. Indriyanta (2009)	Enkripsi dan Dekripsi dengan Algoritma AES 256 untuk Semua Jenis File	Penelitian ini menunjukkan bahwa AES 256 dapat digunakan untuk mengenkripsi semua jenis file, termasuk file dokumen.	Penelitian ini hanya menggunakan enkripsi AES 256 bukan penggabungan 2 enkripsi sekaligus

Dari penelitian yang ada di atas, untuk pengamanan data tingkat yang aman belum dirasa cukup, sehingga kami menawarkan metode yang lebih kuat dalam pengamanan dokumen berklasifikasi.

2.8. Metrik Efektivitas Desain dan Penerapan Enkripsi

Salah satu komponen penting dalam menilai keamanan algoritma kriptografi adalah metrik pengukuran enkripsi. Beberapa elemen termasuk dalam metrik ini, seperti tingkat keamanan yang dihitung berdasarkan ketahanan terhadap serangan kriptografis, yang mencakup brute force dan analisis kripto. Serangan brute force adalah upaya menggunakan semua kombinasi kunci atau kata sandi yang mungkin untuk mendapatkan akses tidak sah ke data (Verma, 2022). Sebaliknya, kriptoanalisis adalah proses menganalisis sistem kriptografi untuk menemukan kelemahan atau kerentanan yang dapat digunakan untuk memecahkan enkripsi (Popat, 2019). Teknik analisis formal, seperti ketahanan terhadap serangan dan masalah komputasi, digunakan untuk memverifikasi secara matematis kebenaran kriptosistem (Çevik, 2019). Metrik juga digunakan untuk mengevaluasi seberapa efektif algoritma kriptografi, terutama dalam menghadapi ancaman baru seperti komputer kuantum. Tujuan metrik ini adalah untuk membantu pengambilan keputusan saat memilih jenis kriptografi.

Selain itu, penting untuk mempertimbangkan ukuran dan kompleksitas kunci; kunci yang lebih besar dan lebih kompleks biasanya menawarkan keamanan yang lebih tinggi. Parameter seperti kompleksitas dan karakteristik kunci digunakan untuk mengukur kompleksitas kunci (Gideon, 2018) (Ou, 2010). Kekuatannya ditentukan melalui analisis korelasi dan keacakan kunci. Ukuran kunci—yang merujuk pada jumlah bit kunci—juga merupakan faktor yang dipertimbangkan saat menilai tingkat keamanan. Keadaan keamanan kunci dapat diperkirakan secara objektif dan andal, memastikan keamanan sistem informasi, dengan menggabungkan ukuran dan kompleksitas kunci.

Selanjutnya, throughput (atau kecepatan enkripsi dan dekripsi) juga diukur untuk mengetahui seberapa baik algoritma memproses data. Untuk mengevaluasi efisiensi algoritma dalam penggunaan sumber daya, juga dipertimbangkan penggunaan sumber daya seperti CPU dan memori. Salah satu algoritma ideal yang menyeimbangkan kinerja yang efisien dengan keamanan yang kuat, evaluasi ini membantu menentukan kepraktisan dan kecocokan algoritma enkripsi dalam berbagai situasi.

2.9. Kerangka Berpikir

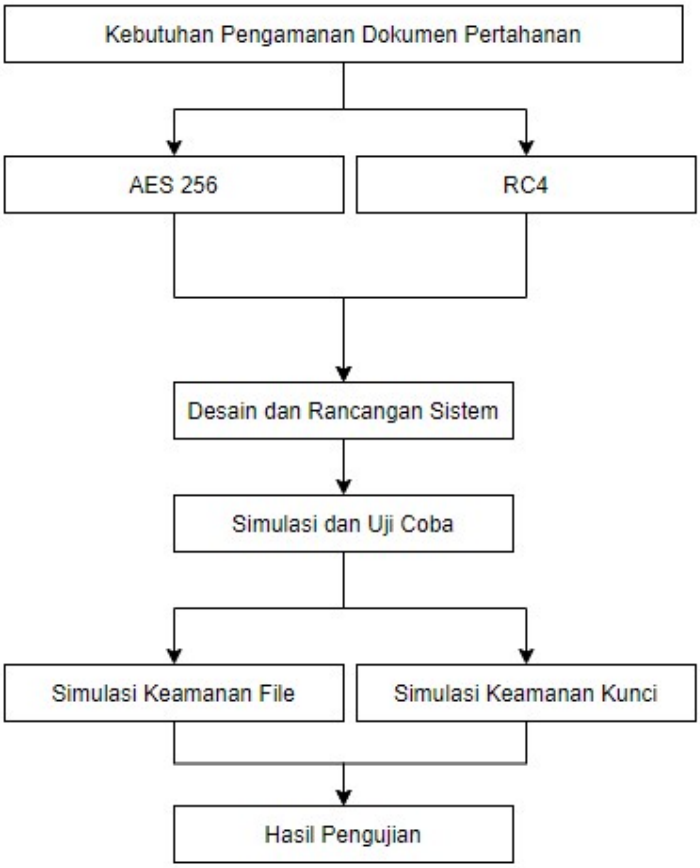
Penelitian Ini mencoba mencari tahu kendala dan memberikan solusi yang relevan yang dihadapi oleh instansi terkait khususnya dalam keamanan data. Untuk mencari tahu jawaban penelitian tersebut, didapatlah dari studi literatur terkait dengan study kasus yang berkesinambungan sehingga penelitian ini akan menerapkan solusi yang di inginkan untuk keamanan data di instansi terkait. Untuk mempersiapkan sistem pengamanan dokumen yang memerlukan metode AES 256 bit, analisis masalah harus dilakukan.

Setelah itu, sesuai dengan hasil analisis sistem, desain sistem, terutama proses enkripsi dan dekripsi dan desain antarmuka. Metode Waterfall akan digunakan dalam pengembangan perangkat lunak konvensional. Setiap tahap dalam model ini harus diselesaikan secara menyeluruh sebelum melanjutkan, dan hasil dari masing-masing tahap harus dicatat dengan baik. Karena model ini mensyaratkan penyelesaian suatu tahap secara tuntas sebelum beranjak pada tahap selanjutnya.

Setelah tahap perancangan sistem selesai, masuk ke tahap implementasi, di mana di tahap ini, algoritma dari AES-256 dan RC4 akan di terapkan untuk mengubah file/data yang sebelumnya dapat dengan mudah di baca menjadi sulit dibaca.

Terakhir, tahap pengujian, tujuan dari tahap ini adalah untuk menentukan apakah sistem sesuai dengan hasil analisis dan desain serta menghasilkan kesimpulan apakah sistem tersebut sesuai dengan yang diharapkan berdasarkan masalah dan atasan masalah. Untuk mencapai tujuan ini, metode pengujian yang berbentuk parameter atau ukuran diperlukan untuk memastikan bahwa sistem telah mencapai tujuan. Metode pengujian digunakan untuk memastikan bahwa file yang telah dienkripsi menjadi tidak dapat diakses karena keterbatasan akses. Selain itu, memastikan bahwa file yang telah dienkripsi masih dapat dibaca kembali ke metode dekripsi oleh pengguna dengan akses.

Berikut adalah diagram kerangka berpikir dari penelitian yang dilakukan:



Gambar 2.5. Diagram Kerangka Berpikir

2.9. Hipotesis Operasional

Salah satu cara penting untuk mengkomunikasikan informasi adalah melalui teknologi komputer, khususnya Infrastruktur Informasi Vital Nasional (IIVN). Berbagai data atau informasi yang diperoleh akan digunakan dan dibagikan untuk berbagai

tujuan. Jika tidak ada media fisik, pertukaran data atau informasi menjadi lebih mudah. Namun, terkadang keamanan pertukaran data atau informasi tidak diperhatikan dengan serius. Pencurian data atau informasi adalah salah satu efek negatif dari kemajuan teknologi komputer. Infrastruktur Informasi Vital Nasional (IIVN) sangat perlu untuk memperhatikan keamanan pertukaran data atau informasi untuk menghindari pencurian data atau informasi dalam bentuk digital.

Data atau informasi memerlukan perlakuan yang lebih khusus, khusus, dan terlindungi karena telah menjadi aset yang sangat berharga dan penting. Selain itu, telah terjadi kemajuan besar dalam bidang pengembangan sistem operasi komputer dan utilitasnya. Akibatnya, kinerja, keandalan, dan fleksibilitas perangkat lunak menjadi prioritas utama dalam proses pengembangan perangkat lunak. Sudah pasti akan semakin mudah bagi peretas, penyusup, dan penyadap untuk terus bereksperimen atau mengeksploitasi kelemahan dalam konfigurasi sistem karena pentingnya informasi atau data yang terus meningkat karena kemajuan teknologi.

Salah satu cara untuk memastikan bahwa data atau informasi aman adalah dengan melakukan rekayasa keamanan data dengan menggunakan teknik kriptografi untuk memastikan bahwa file rahasia aman dan dapat digunakan oleh orang lain yang tidak memiliki otorisasi. Cara lain untuk memastikan bahwa informasi atau data aman adalah dengan mengacak atau membuat informasi tersebut tidak dapat dibaca oleh pihak yang tidak berwenang.