BAB 1. PENDAHULUAN

1.1. Latar Belakang

1.1.1. Perkembangan Teknologi

Dalam beberapa dekade terakhir, kemajuan teknologi telah mengubah keamanan dokumen secara signifikan. Teknologi informasi dan telekomunikasi telah menjadi sangat penting bagi kehidupan manusia karena pertumbuhannya yang begitu cepat, termasuk dalam bidang administrasi pemerintahan, bisnis, dan sosial (Tasya Safiranita Ramli, 2019). Namun, teknologi ini juga dapat digunakan untuk melakukan tindakan melawan hukum, seperti kejahatan siber (Cyber crime), yang dapat membahayakan keamanan dokumen. Sehingga pemerintah dan lembaga terkait harus memperhatikan keamanan serta regulasi penggunaan jaringan dalam perspektif teknologi digital (Sandryones Palinggi, 2020). Selain itu, penggunaan teknologi enkripsi juga menjadi solusi untuk mencegah akses yang tidak sah ke dokumen. Algoritma enkripsi seperti AES dan CBC umumnya digunakan untuk mengenkripsi file. Dalam konteks pendidikan, teknologi juga dapat digunakan untuk meningkatkan keamanan dokumen. Sebagai contoh, MIN Tempel Yogyakarta telah menerapkan kurikulum 2013 dengan baik dan memanfaatkan teknologi untuk memudahkan penyampaian informasi dan pelayanan publik (Hairullah, 2021). Oleh karena itu, perkembangan teknologi dapat memberikan manfaat yang besar dalam meningkatkan keamanan dokumen, namun juga memerlukan perhatian dan pengaturan yang tepat untuk menghindari penyalahgunaan teknologi tersebut. Namun perkembangan teknologi yang pesat juga membawa risiko terhadap keamanan dokumen. Berikut adalah beberapa risiko yang dapat terjadi:

a. Kejahatan Siber: Perkembangan teknologi informasi dan telekomunikasi dapat digunakan untuk melakukan tindakan melawan hukum, seperti kejahatan siber, yang dapat membahayakan keamanan dokumen (Tasya Safiranita Ramli, 2019).
b. Kebocoran data: Dalam era digital, dokumen dapat dengan mudah disalin dan disebarluaskan tanpa izin. Hal ini dapat menyebabkan kebocoran data dan informasi rahasia (Sandryones Palinggi, 2020)
c. Penyalahgunaan teknologi: Dokumen dapat dilindungi dari penyalahgunaan oleh pihak yang tidak berhak dengan menggunakan

teknologi enkripsi namun dapat juga untuk menyembunyikan data berbahaya tanpa terdeteksi oleh otoritas pengatur keamanan.

d. Ketergantungan pada teknologi: Penggunaan teknologi dalam penyimpanan dan pengamanan dokumen dapat membuat pengguna terlalu bergantung pada teknologi tersebut, sehingga jika terjadi kerusakan atau kegagalan sistem, dokumen dapat hilang atau rusak (Affandi, 2022).

Oleh karena itu, perlu adanya pengaturan dan regulasi yang tepat dalam penggunaan teknologi untuk menjaga keamanan dokumen. Salah satu cara untuk melindungi dokumen dari akses yang tidak sah adalah dengan menggunakan teknologi enkripsi.

1.1.2. Infrastruktur Informasi Vital

Infrastruktur Informasi Vital (IIV) adalah sistem elektronik yang menggunakan teknologi informasi dan teknologi operasional yang saling ketergantungan dengan sistem elektronik lainnya, untuk mendukung sektor strategis. Jika infrastruktur terganggu, akan berdampak negative pada kepentingan umum, pelayanan publik, pertahanan dan keamanan, dan ekonomi nasional. Infrastruktur Informasi Vital (IIV) adalah infrastruktur yang sangat penting bagi kelangsungan suatu negara. IIV terdiri dari sistem informasi dan teknologi yang sangat penting untuk keberlangsungan suatu negara, seperti sistem keuangan, sistem transportasi, sistem kesehatan, dan lain-lain. Di dalam IIV tersebut memiliki jaringan komputer yang saling berhubungan di mana semua data (informasi dan dokumen) di transmisikan lewat jaringan komputer tersebut sehingga dibutuhkan sistem keamanan yang baik untuk mengamankan data (dokumen) penting yang di transmisikan tersebut untuk meminimalisasi risiko, Salah satu risiko negatif yang dapat terjadi adalah kebocoran data (dokumen digital). Dalam era digital, dokumen dapat dengan mudah disalin dan disebarluaskan tanpa izin. Hal ini dapat menyebabkan kebocoran data dan informasi rahasia (Tri Bagus Prabowo, 2023).

1.1.3. Keamanan Dokumen Digital

Salah satu cara untuk mengamankan dokumen rahasia dalam bentuk digital adalah dengan menggunakan Kriptografi. Dalam ilmu kriptografi, proses enkripsi digunakan untuk menyembunyikan isi dokumen sehingga orang lain tidak dapat mengetahuinya (D. Laoli, 2020). Selama pengiriman, informasi harus tetap rahasia

dan tetap utuh saat diterima. Untuk memenuhi hal tersebut, algoritma enkripsi seperti Advanced Encryption Standard 256 (AES-256), Rivest Code 4 (RC4) atau algoritma enkripsi lainnya digunakan untuk mengenkripsi dan mendekripsi dokumen yang akan dikirim.

Berdasarkan penjelasan di atas, penulis menggunakan bahasa pemrograman PHP untuk membuat sistem keamanan berbasis web untuk mengamankan dokumen rahasia pada infrastruktur informasi vital nasional menggunakan metode kriptografi dengan menggabungkan dua algoritma enkripsi yakni AES-256 dan RC4.

1.2. Identifikasi Masalah

Kebocoran dokumen rahasia merupakan masalah yang semakin mengkhawatirkan di era digital ini. Dokumen rahasia dapat berisi informasi yang sensitif, seperti rahasia negara, informasi keuangan, atau data pribadi. Kebocoran dokumen rahasia dapat menimbulkan berbagai dampak negatif, mulai dari kerugian finansial, kerusakan reputasi, hingga ancaman keamanan.

Ada berbagai faktor yang dapat menyebabkan kebocoran dokumen rahasia, antara lain:

1. Kesalahan manusia

   Kesalahan manusia, seperti kelalaian atau kecerobohan, merupakan penyebab kebocoran dokumen rahasia yang paling umum. Misalnya, seseorang yang meninggalkan dokumen rahasia di tempat umum atau mengirim dokumen rahasia melalui email yang tidak aman.
2. Serangan siber

   Serangan siber, seperti peretasan atau Fishing, dapat digunakan untuk mencuri dokumen rahasia.
3. Faktor lain

   Terdapat beberapa faktor lain yang dapat menyebabkan kebocoran dokumen rahasia antara lain:
   a) Kegagalan sistem keamanan
   b) Kolusi antar individu
   c) Sabotase

Dampak kebocoran dokumen rahasia dapat bervariasi, tergantung pada jenis dan isi dokumen yang bocor. Beberapa dampak kebocoran dokumen rahasia antara lain:

a) Kerugian finansial

Kebocoran dokumen rahasia dapat menyebabkan kerugian finansial karena data pribadi yang bocor digunakan untuk melakukan penipuan atau pencurian identitas.

b) Kerusakan reputasi

Kebocoran dokumen rahasia dapat merusak reputasi suatu organisasi atau individu.

c) Ancaman keamanan

Kebocoran dokumen rahasia dapat membahayakan keamanan suatu negara atau organisasi. Misalnya, dokumen rahasia tentang rencana pertahanan yang bocor dapat digunakan oleh pihak lawan untuk melakukan serangan.

Berikut ini adalah tabel beberapa kasus kejadian kebocoran dokumen diurutkan dari yang terbaru:

Tabel 1.1. Kasus Kebocoran Dokumen

Tahun	Negara	Kasus
2023	Indonesia [1]	**Instansi**: Kementerian ESDM **Jenis Dokumen**: Dokumen rahasia tentang kasus korupsi **Penyebab**: Kesalahan manusia **Dampak**: Kerugian keuangan
2023	Indonesia [2]	**Instansi**: Komisi Pemberantasan Korupsi **Jenis Dokumen**: Dokumen rahasia tentang kasus korupsi **Penyebab**: Kesalahan manusia **Dampak**: Kerugian reputasi
2022	Indonesia [3]	**Instansi**: Badan Intelijen Negara **Jenis Dokumen**: Dokumen rahasia tentang operasi intelijen **Penyebab**: Serangan siber **Dampak**: Kerugian keamanan

[1] https://www.cnbcindonesia.com/news/20230412084707-4-429148/heboh-dokumen-lidik-kpk-bocor-kementerian-esdm-buka-suara

[2] https://www.cnnindonesia.com/nasional/20230410152352-12-935777/dokumen-kpk-yang-bocor-diduga-terkait-izin-tambang-di-esdm

[3] https://www.kompas.com/tren/read/2022/09/09/140500865/data-nama-intel-badan-intelijen-negara-diduga-bocor-ini-kata-bin

2021	Indonesia [4]	**Instansi**: Kementerian Pertahanan **Jenis Dokumen**: Dokumen rahasia tentang rencana pertahanan **Penyebab**: Serangan siber **Dampak**: Kerugian keamanan
2021	Indonesia [5]	**Instansi**: BRI Life **Jenis Dokumen**: Data pribadi 463.000 nasabah **Penyebab**: Kesalahan manusia **Dampak**: Kerugian finansial
2020	Amerika Serikat[6]	**Instansi**: Pemerintahan **Jenis Dokumen**: Dokumen rahasia tentang rencana perang di Afghanistan **Penyebab**: Serangan siber **Dampak**: Kerugian keamanan
2020	Amerika Serikat[7]	**Instansi**: Pemerintahan **Jenis Dokumen**: Informasi rahasia pertahanan AS **Penyebab**: Serangan siber **Dampak**: Kerugian keamanan
2017	Amerika Serikat[8]	**Instansi**: CIA **Jenis Dokumen**: Dokumen rahasia tentang Vault 7 **Penyebab**: Serangan siber **Dampak**: Kerugian keamanan
2017	China[9]	**Instansi**: Pemerintahan **Jenis Dokumen**: Dokumen tentang strategi Tiongkok menghancurkan sejumlah operasi CIA di China **Penyebab**: Kesalahan manusia **Dampak**: Kerugian keamanan
2017	China[10]	**Instansi**: Pemerintahan **Jenis Dokumen**: Dokumen pengelolaan kamp muslim di xinjiang **Penyebab**: Serangan siber **Dampak**: Kerugian keamanan

Dikarenakan seringnya terjadi kebocoran dokumen baik itu karena kesalahan manusia atau karena serangan siber, maka perlu adanya pengamanan dokumen

[4] https://www.kompas.tv/nasional/179220/sayangkan-dokumen-raperpres-alpalhankam-yang-bocor-kemhan-akan-usut-sosok-yang-menyebarkan

[5] https://fokus.tempo.co/read/1488710/kebocoran-data-nasabah-bri-life-bukti-lemahnya-proteksi-dan-regulasi

[6] https://www.antaranews.com/berita/213414/dokumen-rahasia-perang-afghanistan-bocor

[7] https://www.bbc.com/indonesia/dunia-53816472

[8] https://dunia.tempo.co/read/854018/arti-kode-vault-7-di-dokumen-cia-hasil-bocoran-wikileaks

[9] https://www.liputan6.com/global/read/2959053/dokumen-sebut-operasi-cia-di-china-gagal-dan-puluhan-agen-dibunuh

[10] https://www.bbc.com/indonesia/dunia-61570181

tersebut sehingga meski terjadi kebocoran dokumen, dokumen tersebut tidak bisa digunakan lebih lanjut. Karena kebocoran dokumen sering terjadi, fokus penelitian ini adalah bagaimana menyimpan dan mengamankan dokumen dalam bentuk file digital di Infrastruktur Informasi Vital. (IIV) Nasional dari penyalahgunaan dengan melakukan kriptografi dengan menggunakan algoritma AES-256 dan RC4.

1.3. Batasan Masalah

Batasan yang terkait dengan masalah penelitian ini adalah sebagai berikut:

a) Enkripsi file dengan menggunakan algoritma AES-256.
b) Enkripsi kunci dengan men*ggunakan Rivest Code 4 (RC4)*.
c) File yang dapat diamankan dalam sistem ini adalah dengan file dalam bentuk digital bisa berupa file Office, Video, Gambar, atau file digital lainnya.
d) Kunci dalam pada proses enkripsi bisa menggunakan kunci yang diperoleh dari pengguna atau menggunakan kata sandi yang dibangkitkan oleh sistem.
e) Sistem yang dibangun berbasis web dan menggunakan bahasa pemrograman PHP.
f) Maksimal jumlah file sejenis yang akan bisa dienkripsi untuk satu kali enkripsi adalah 5 file dengan ukuran maksimal 3MB per file, hal ini dikarenakan keterbatasan kemampuan komputer yang digunakan penulis.

1.4. Rumusan Masalah

Dari permasalahan tersebut di atas dan Berdasarkan batasan-batasan masalah yang telah ditentukan, maka rumusan masalah penelitian ini adalah sebagai berikut:

1. Bagaimana desain dan penerapan enkripsi AES 256 dan RC4 untuk meningkatkan keamanan dokumen digital berklasifikasi?

   Tujuannya adalah untuk membuat sistem dan antarmuka yang akan digunakan untuk dapat memproses enkripsi dan dekripsi dokumen digital berkalsifikasi.
2. Seberapa efektif desain dan penerapan enkripsi AES256 dan RC4 untuk meningkatkan keamanan dokumen digital berklasifikasi ?

   Tujuan dari pertanyaan ini adalah untuk menentukan tingkat keberhasilan penggunaan enkripsi yang digunakan melalui pengujian. Untuk mengetahui

tingkat efektivitas desain dan penerapan desain yang digunakan, diukur dengan uji penetrasi baik secara offline maupun online. Jika dokumen dapat dengan mudah disalahgunakan maka dapat dikatakan bahwa efektivitas penerapannya rendah.

1.5. Obyek Penelitian

Penelitian ini akan menggunakan dokumen digital dalam bentuk file sebagai objek yang akan di teliti. Dokumen digital adalah dokumen yang dibuat, disimpan, dan didistribusikan dalam format digital (Saleh, 2014). Berikut adalah beberapa karakteristik dokumen digital:

1. Terdiri dari kumpulan data digital

   Dokumen digital terdiri dari kumpulan data digital, seperti teks, gambar, audio, dan video. Data-data tersebut disimpan dalam format biner (byte), yang merupakan representasi dari data dalam bentuk angka 0 dan 1. Nilai desimal, seperti 0 hingga 255, dapat diwakili dengan satu byte. Dalam penelitian ini penulis akan melakukan enkripsi terhadap byte file tersebut dengan menggunakan algoritma enkripsi AES 255 dan mengenkripsi teks kunci dengan RC4.
2. Dapat diakses dan diubah dengan mudah

   Dokumen digital dapat diakses dan diubah dengan mudah menggunakan perangkat komputer atau perangkat telepon seluler. Dokumen digital juga dapat dibagikan dengan mudah melalui berbagai media, seperti email, media sosial, dan cloud storage. Dalam penelitian ini dokumen digital akan diubah dengan menggunakan perangkat komputer.
3. Dapat dilindungi dengan enkripsi.

   Enkripsi dapat digunakan untuk mencegah pihak yang tidak berwenang mengakses dokumen digital. Enkripsi mengubah data menjadi kode-kode rahasia yang hanya bisa digunakan oleh penerima yang memiliki kunci setelah melakukan dekripsi.
4. Dapat dicetak atau dikonversi ke format lain.

   Dokumen digital dapat dicetak atau dikonversi ke format lain, seperti dokumen PDF atau dokumen teks, dokumen video, audio atau format dokumen digital lainnya.

Penelitian dirancang untuk menggunakan dokumen berklasifikasi yang terdapat pada instansi-instansi vital nasional secara khusus pada Kementerian

pertahanan republik Indonesia. Beberapa jenis dokumen berklasifikasi seperti dokumen-dokumen kebijakan strategi pertahanan, dokumen personal, dan dokumen-dokumen terkait alutsista pertahanan. Namun karena sifat dokumen-dokumen tersebut sangat rahasia sehingga untuk menghindari kesalahan dan kebocoran selama proses rekayasa dan uji coba maka penulis memilih untuk menggunakan dokumen-dokumen yang terdapat pada instansi yang menjadi lokasi penelitian kami yakni Fakultas Sain dan Teknologi Pertahanan, Universitas Pertahanan Republik Indonesia. Dengan tanpa membatasi jenis dan ukuran dokumen yang akan di proses, sehingga diharapkan setelah dilakukan rekayasa, sistem yang dirancang dapat digunakan di instansi-instansi nasional seperti Kementerian Pertahanan Republik Indonesia

1.6. Tujuan Penelitian

Penelitian ini bertujuan untuk mengetahui seberapa efektif algoritma enkripsi AES 256 dan RC4 untuk melindungi dokumen digital. Pada akhirnya, penelitian ini diharapkan dapat memberikan informasi dan gambaran yang lebih baik tentang seberapa efektif algoritma tersebut dalam mencegah akses pihak yang tidak berwenang, mengurangi kemungkinan kebocoran data, dan meningkatkan kinerja keamanan dokumen.

Berikut adalah tujuan dalam penelitian ini:

1. Mengkaji bagaimana bentuk desain dan alur sistem yang dapat mengombinasikan enkripsi AES-256 dan RC4 untuk meningkatkan keamanan dokumen digital berklasifikasi pada infrastruktur informasi vital nasional.
2. Mengkaji efektivitas desain dan penerapan kombinasi enkripsi AES 256 dan RC 4 untuk meningkatkan keamanan dokumen digital berklasifikasi pada infrastruktur informasi vital nasional dengan melakukan serangkaian testing dan pengujian terhadap desain yang sudah dibuat.
3. Melakukan rekayasa keamanan file dengan menggunakan teknik kriptografi untuk mengamankan file rahasia supaya menjadi aman dan bisa digunakan oleh pengguna lain yang tidak memiliki otorisasi.

1.7. Manfaat Penelitian

Salah satu manfaat yang diharapkan dari penelitian ini adalah untuk memberikan gambaran tentang desain dan implementasi sistem keamanan file dengan menggabungkan algoritma teknologi enkripsi *Advanced Encryption Standard 256* (AES-256) dan *Rivest Code 4* (RC4) sehingga dapat meningkatkan sistem keamanan dokumen digital pada infrastruktur informasi vital nasional (IIVN). Dengan adanya rekayasa keamanan file yang menggunakan teknik kriptografi membuat file rahasia lebih aman sehingga tidak bisa digunakan oleh orang lain yang tidak memiliki otorisasi. Diharapkan bahwa penelitian ini akan memberikan manfaat sebagai berikut:

1. Memberikan informasi tentang metode dan teknik yang bisa digunakan untuk meningkatkan keamanan dokumen digital menggunakan algoritma enkripsi AES 256 dan RC4, terutama untuk sektor infrastruktur informasi penting di seluruh negeri.
2. Sebagai landasan standarisasi untuk memperkuat keamanan dokumen digital untuk pertahanan siber nasional.
3. Memperkaya literatur tentang keamanan informasi, khususnya tentang penggunaan algoritma enkripsi AES 256 dan RC4 untuk mengamankan dokumen digital.