BAB I

PENDAHULUAN

1.1 Latar belakang masalah

Di era digital yang berkembang pesat ini, data telah menjadi komoditas paling berharga(Disemadi et al., 2023). Hampir semua aspek kehidupan manusia kini terdigitalisasi—mulai dari transaksi keuangan, informasi pribadi, sistem pemerintahan, hingga infrastruktur vital seperti rumah sakit dan energi. Perkembangan teknologi informasi yang masif telah melahirkan sistem informasi berbasis jaringan yang memungkinkan pengiriman dan penerimaan data secara cepat dan efisien. Namun, kemajuan ini diikuti pula oleh meningkatnya risiko keamanan, terutama yang berkaitan dengan kerahasiaan, integritas, dan ketersediaan data(Setyowati et al., 2021).

Ancaman terhadap keamanan data digital tidak lagi bersifat konvensional. Serangan siber seperti *phishing*, *man-in-the-middle attack*, *brute force*, *dictionary attack*, hingga *quantum attack* menjadi ancaman nyata yang dapat merusak sistem dan mencuri informasi sensitif(Chopra et al., 2024). Kasus kebocoran data pribadi masyarakat Indonesia dari beberapa instansi besar menunjukkan lemahnya sistem keamanan digital yang ada. Bahkan lembaga besar seperti kementerian dan operator seluler tidak luput dari serangan tersebut(Sorisa et al., 2024). Situasi ini menegaskan pentingnya penguatan keamanan data digital, khususnya dalam proses transmisi dan penyimpanan data(Hoshmand et al., n.d.).

Salah satu pendekatan utama dalam menjaga keamanan data adalah dengan menggunakan teknologi kriptografi(Adee & Mouratidis, 2022). Kriptografi merupakan ilmu dan seni mengamankan data melalui proses penyandian, sehingga informasi hanya dapat dibaca oleh pihak yang memiliki kunci yang sesuai(Gençoğlu & Gençoğlu, n.d.). Seiring berjalannya waktu, berbagai algoritma kriptografi telah dikembangkan, baik yang bersifat simetris maupun asimetris. Masing-masing memiliki kelebihan dan kekurangan tersendiri(Navid Bin Anwar et al., 2019).

Algoritma One-Time Pad (OTP) merupakan salah satu algoritma kriptografi simetris yang dikenal sangat aman secara teoretis (Ao et al., 2018). Diperkenalkan pada awal abad ke-20, OTP menggunakan kunci acak yang panjangnya sama dengan pesan. Dalam kondisi ideal, OTP dianggap sulit untuk dipecahkan (unbreakable) karena sifat kunci yang benar-benar acak dan hanya digunakan sekali. Keamanan OTP sangat bergantung pada panjang dan keacakan kunci, yang berarti juga tergantung pada panjang plaintext yang akan dienkripsi. Namun demikian, algoritma OTP memiliki beberapa kelemahan. Salah satunya adalah ketergantungan pada sinkronisasi waktu antara dua pihak. OTP tidak dapat melakukan autentikasi pengguna dengan baik jika waktu antara pengirim dan penerima tidak tersinkronisasi secara akurat. Oleh karena itu, nilai OTP biasanya hanya berlaku dalam jangka waktu yang sangat singkat, dan setelah waktu tersebut, nilai OTP akan berubah secara otomatis. Selain itu, jika plaintext yang akan dienkripsi sangat panjang, maka kunci yang dibutuhkan juga harus sangat panjang. Hal ini tidak hanya menyulitkan dalam hal pembuatan dan distribusi kunci, tetapi juga memperlambat proses sinkronisasi. Oleh karena itu, algoritma OTP kurang ideal untuk digunakan dalam penyandian pesan yang berukuran besar atau panjang secara real-time(Hoyul Choi, 2015). Jika kunci yang digunakan tidak cukup panjang atau tidak sepenuhnya acak, maka tingkat keamanan OTP dapat terganggu dan berisiko dieksploitasi. Meskipun algoritma kriptografi seperti OTP sulit dipecahkan secara teoritis, dalam praktiknya, jika jumlah plaintext (pesan) terbatas, maka jumlah kunci yang dibutuhkan juga cenderung sedikit(Krianto Sulaiman et al., 2020). Hal ini membuka kemungkinan celah keamanan karena penyerang dapat mencoba mengeksploitasi pola dari kunci yang terbatas. Oleh karena itu, untuk meminimalisir kelemahan akibat keterbatasan jumlah kunci, pendekatan kombinasi dengan algoritma Cramer-Shoup dapat digunakan. Algoritma Cramer-Shoup yang merupakan algoritma kriptografi asimetris dikenal tahan terhadap serangan adaptif, sehingga dapat meningkatkan tingkat keamanan secara signifikan ketika dikombinasikan dengan OTP. Pendekatan kombinasi ini mampu meningkatkan perlindungan terhadap data digital secara lebih efektif.

Di sisi lain, algoritma Cramer-Shoup merupakan salah satu algoritma kriptografi asimetris modern yang dirancang untuk mengatasi kelemahan algoritma sebelumnya, seperti ElGamal *(Jain, 2017)*. Cramer-Shoup menawarkan keamanan yang lebih tinggi dalam komunikasi dua arah dan pengiriman pesan sensitif di lingkungan publik. Algoritma ini juga mendukung penerapan dalam sistem digital seperti *blockchain*, *e-voting*, dan sistem transaksi online yang membutuhkan jaminan integritas dan autentikasi data(Dr. S. Raju, 2014).

Kedua algoritma tersebut OTP dan Cramer-Shoup mewakili dua pendekatan yang berbeda namun saling melengkapi. OTP unggul dalam hal kerahasiaan mutlak, sementara Cramer-Shoup memberikan keamanan yang kokoh terhadap jenis serangan tertentu di dunia nyata. Namun, hingga saat ini, belum banyak penelitian yang mencoba menggabungkan keduanya dalam satu pendekatan terpadu. Padahal, jika dikombinasikan dengan bijak, pendekatan ini berpotensi memberikan perlindungan yang jauh lebih tinggi terhadap ancaman yang terus berkembang.

Penelitian ini muncul dari kebutuhan mendesak akan mekanisme perlindungan data digital yang lebih kuat dan adaptif. Kombinasi algoritma OTP dan Cramer-Shoup dalam satu sistem mampu menciptakan model enkripsi hybrid yang tidak hanya menjaga kerahasiaan, tetapi juga ketahanan terhadap manipulasi data dan serangan canggih lainnya. Dengan memanfaatkan kekuatan OTP dalam hal *confidentiality* dan keunggulan Cramer-Shoup dalam *non-malleability* dan *adaptive security*, pendekatan ini dapat menjadi solusi inovatif dalam meningkatkan kualitas keamanan informasi.

Untuk mengatasi kelemahan yang ditemukan pada algoritma yang disebutkan sebelumnya, peneliti mengusulkan Peningkatan Kunci. Pendekatan ini bertujuan untuk memperketat keamanan kunci OTP dari serangan dan mempercepat operasi kriptografi seperti enkripsi dan dekripsi pada Cramer-Shoup. Berdasarkan masalah dia atas maka peneliti melakukan penelitian yang berjudul **"Peningkatan Keamanan Data Digital Dengan Pendekatan Kombinasi Algoritma Kriptografi Otp Dan Cramer Shoup".**

1.2 Rumusan masalah

Berdasarkan adanya kelemahan pada algoritma One-Time Pad (OTP) yang rentan terhadap serangan pada kunci serta kompleksitas proses enkripsi dan dekripsi pada algoritma Cramer-Shoup, maka rumusan masalah dalam penelitian ini adalah bagaimana merancang dan mengimplementasikan pendekatan peningkatan kunci untuk memperkuat keamanan OTP terhadap serangan serta mengoptimalkan efisiensi kriptografi pada algoritma Cramer-Shoup, sehingga kombinasi kedua algoritma tersebut mampu meningkatkan keamanan data digital secara lebih efektif dan efisien.

1.3 Batasan Masalah

Berikut merupakan batasan masalah dari penelitian yang akan dilakukan:

1. Algoritma kriptografi yang di gunakan algoritma kriptografi One-Time Pad (OTP) dan Cramer-Shoup
2. Proses enkripsi dan dekripsi dalam penelitian ini diimplementasikan menggunakan bahasa pemrograman Python
3. Penelitian ini secara spesifik hanya berpusat pada proses enkripsi dan dekripsi untuk pengamanan ganda berkas digital, khususnya dokumen teks berekstensi .txt/docx.
4. Studi ini tidak akan membahas atau menganalisis serangan kriptanalisis secara menyeluruh.

1.4 Tujuan penelitian

Tujuan dari penelitian ini adalah untuk merancang, mengembangkan, dan menganalisis pendekatan hibrida berbasis kombinasi algoritma kriptografi One-Time Pad (OTP) dan Cramer-Shoup dalam rangka peningkatan keamanan data digital. Penelitian ini bertujuan untuk:

1. Memperkuat kerangka teoritis keamanan kriptografi dengan mengusulkan mekanisme hibrida yang mampu meminimalkan kelemahan inheren OTP terkait distribusi kunci serta keterbatasan efisiensi Cramer-Shoup dalam proses enkripsi dan dekripsi.

2. Menghasilkan model konseptual sistem kriptografi hibrida yang tidak hanya berfokus pada aspek teknis implementasi, tetapi juga pada landasan matematis, efisiensi algoritmik, dan tingkat resistansi terhadap berbagai serangan kriptanalisis, termasuk serangan berbasis kunci dan plaintext.
3. Mengevaluasi secara komprehensif kinerja dan tingkat keamanan pendekatan yang diusulkan melalui simulasi, analisis perbandingan, serta uji validasi terhadap skenario ancaman nyata dalam keamanan siber.
4. Memberikan kontribusi ilmiah berupa konsep kriptografi hibrida yang dapat menjadi rujukan pengembangan sistem keamanan data digital, serta membuka peluang untuk penelitian lanjutan pada integrasi algoritma kriptografi modern dengan teknologi keamanan lainnya.

1.5 Manfaat penelitian

Penelitian ini dapat memberikan beberapa manfaat, baik secara teoritis maupun praktis. Secara teoritis, penelitian ini memberikan kontribusi terhadap pengembangan ilmu pengetahuan di bidang kriptografi, khususnya dalam merancang model kombinasi algoritma yang mengintegrasikan keunggulan One-Time Pad (OTP) dalam menjaga kerahasiaan data dengan keunggulan Cramer-Shoup dalam melindungi terhadap serangan adaptive chosen ciphertext. Penelitian ini juga memperkaya literatur mengenai teknik peningkatan keamanan kunci dan efisiensi proses enkripsi-dekripsi dalam sistem kriptografi modern.

Secara praktis, hasil dari penelitian ini dapat diterapkan dalam sistem keamanan data digital yang digunakan oleh lembaga pemerintahan, sektor pendidikan, layanan kesehatan, serta perusahaan yang membutuhkan perlindungan tinggi terhadap informasi sensitif. Model kombinasi algoritma yang dikembangkan juga dapat dijadikan dasar bagi pengembangan aplikasi keamanan data berbasis Python, serta sebagai solusi alternatif untuk meningkatkan ketahanan sistem informasi terhadap berbagai ancaman siber yang semakin kompleks