BAB 1

PENDAHULUAN

1.1 Latar Belakang

Di tengah percepatan era digital, peran data semakin penting dalam menunjang berbagai aktivitas manusia di berbagai sektor kehidupan, baik di sektor pemerintahan, bisnis, pendidikan, hingga individu (Chen et al., 2012). Meskipun digitalisasi memberikan banyak kemudahan, ketergantungan yang semakin tinggi terhadap sistem digital juga memunculkan tantangan baru, seperti pencurian dan penyalahgunaan data, yang sebagian besar disebabkan oleh rendahnya kesadaran akan pentingnya perlindungan informasi (Khando et al., 2021). Berdasarkan *National Cyber Security Index* (NCSI) 2023, Indonesia masih berada di peringkat ke-49 dari 176 negara dalam hal keamanan siber, menunjukkan bahwa kesiapan menghadapi ancaman digital belum optimal (e-Governance Academy Foundation, 2023).

Hal ini tercermin dalam kasus peretasan Pusat Data Nasional Sementara (PDNS) tahun 2024 oleh kelompok Brain Cipher, yang melumpuhkan layanan vital pemerintahan (Kompas, 2024). Kasus tersebut menunjukkan bahwa sistem pemerintahan yang seharusnya memiliki perlindungan tingkat tinggi pun masih memiliki celah yang bisa dimanfaatkan oleh pelaku kejahatan siber. Kejahatan siber (*cybercrime*) adalah tindakan ilegal yang memanfaatkan sistem digital seperti peretasan, pencurian data, atau penipuan online (Syalendro et al., 2025). Untuk menghadapinya, dibutuhkan keamanan siber (*cybersecurity*), yaitu sistem perlindungan yang

dirancang untuk menjaga informasi dan jaringan dari akses tidak sah maupun kerusakan (Imran et al., 2024).

Sayangnya, perkembangan transformasi digital di Indonesia belum diimbangi oleh kesiapan keamanan digital yang memadai, baik dari sisi teknologi, regulasi, maupun sumber daya manusianya (Bua & Idris, 2025). Banyak organisasi maupun individu masih belum memahami cara perlindungan data yang optimal, sehingga pendekatan keamanan digital yang menggabungkan berbagai teknik kriptografi menjadi semakin penting. Pemahaman terhadap dasar-dasar kriptografi pun menjadi langkah strategis dalam membangun sistem keamanan digital yang lebih tangguh dan berkelanjutan di masa depan.

Kriptografi merupakan cabang ilmu matematika yang mengkaji teknik pengamanan pesan dengan menggunakan operasi matematis seperti substitusi, permutasi, dan aljabar bilangan agar informasi hanya bisa dipahami oleh pihak yang memiliki hak akses (Hoffstein et al., 2008). Proses kriptografi pada dasarnya mencakup dua aktivitas penting, yaitu enkripsi dan dekripsi. Enkripsi merupakan proses pengubahan teks asli (*plaintext*) menjadi bentuk sandi (*ciphertext*) agar tidak dapat dipahami oleh pihak yang tidak berwenang. Sementara itu, dekripsi berfungsi untuk mengembalikan bentuk sandi (*ciphertext*) tersebut ke teks aslinya (*plaintext*) dengan menggunakan kunci yang sesuai. Berdasarkan penggunaan kunci, kriptografi terbagi menjadi dua jenis yaitu kriptografi simetris, yang menggunakan satu kunci yang sama untuk proses enkripsi dan dekripsi, serta kriptografi asimetris, yang melibatkan dua kunci berbeda yaitu kunci publik untuk proses enkripsi dan kunci privat untuk proses dekripsi (Al-Shammri, 2022).

Pada kriptografi simetris, terdapat algoritma *Autokey Cipher* dan *Affine Cipher*. *Autokey Cipher* merupakan salah satu algoritma kriptografi klasik dengan jenis cipher substitusi polialfabetik yang dikembangkan sebagai penyempurnaan dari algoritma *Vigenère Cipher* (Muslih & Handoko, 2022). Proses enkripsi pada algoritma ini serupa dengan *Vigenère Cipher*, namun

perbedaannya terletak pada pembentukan kunci. Pada *Autokey Cipher*, kunci tidak hanya bergantung pada kata kunci awal, melainkan juga diperluas menggunakan sebagian dari plainteks itu sendiri. Pendekatan ini bertujuan untuk menghindari pola pengulangan karakter pada cipherteks yang sering muncul dalam *Vigenère Cipher*, sehingga setiap huruf plainteks dienkripsi menggunakan kunci yang bersifat dinamis dan tidak berulang (Fadlan et al., 2021). Menurut Safei (2012), meskipun algoritma *Autokey Cipher* menawarkan keunggulan dibandingkan *Vigenère Cipher* karena dapat menyamarkan pola berulang, algoritma ini tetap memiliki kelemahan dalam keamanan kunci, terutama jika kunci memiliki pola yang terlalu sederhana dan mudah ditebak. Penggunaan sebagian plainteks sebagai bagian dari kunci membuatnya rentan terhadap upaya peretasan. Oleh karena itu, sebaiknya kunci awal *Autokey* bervariasi seperti gabungan huruf, angka, simbol dan karakter lainnya. Serta algoritma *Autokey Cipher* dapat dikombinasikan dengan algoritma lain agar dapat meningkatkan keamanan data.

Sedangkan *Affine Cipher* merupakan salah satu algoritma kriptografi klasik sebagai pengembangan dari *Caesar Cipher*, yang mengalikan plainteks dengan sebuah nilai dan menambahkannya dengan sebuah pergeseran (Munir, 2019). *Affine Cipher* memiliki keunggulan dalam hal kecepatan pemrosesan enkripsi dan dekripsi karena tergolong sederhana dan mudah diimplementasikan, namun tingkat keamanannya cukup rendah jika digunakan tanpa dikombinasikan dengan algoritma lain. Hal ini disebabkan karena sifatnya yang termasuk ke dalam cipher substitusi monoalfabetik, di mana satu karakter plainteks selalu dikonversi ke karakter cipherteks yang sama. Selain itu, karena kunci *Affine* menggunakan pasangan kunci (a, b) maka ruang kuncinya terbatas tergantung dengan jumlah karakter yang digunakan, hal tersebut menjadikan algoritma ini mudah diretas menggunakan metode *Brute Force Attack* (Gusmana et al., 2022).

Pada kriptografi asimetris, terdapat algoritma RSA *(Rivest–Shamir–*

Adleman) yang merupakan salah satu algoritma kunci publik paling populer dan banyak diimplementasikan sampai saat ini (Munir, 2019). Pada proses pengamanan data, RSA menggunakan pasangan kunci berbeda, yaitu kunci publik untuk proses enkripsi dan kunci privat untuk dekripsi. Algoritma RSA memiliki keunggulan dalam sulitnya memfaktorkan bilangan bulat besar menjadi faktor-faktor prima, pemfaktoran tersebut dilakukan untuk mengetahui kunci privat (Alamsyah et al., 2024). Penelitian yang dilakukan Wicaksono (2013), melakukan analisis terhadap ketahanan RSA menggunakan metode *Brute Force Attack* dengan menguji tiga variasi nilai bilangan prima p dan q. Penelitian ini menunjukkan bahwa semakin besar nilai modulus n (hasil perkalian p dan q), maka semakin besar pula kunci privat d yang dihasilkan. Dalam percobaan ketiga dengan nilai $p = 25799$ dan $q = 12899$, diperoleh kunci d sepanjang 56 bit yang diperkirakan membutuhkan waktu hingga 1.142 tahun untuk dipecahkan. Temuan ini memperlihatkan bahwa RSA dengan ukuran kunci besar memiliki ketahanan yang tinggi terhadap metode *Brute Force Attack*. Namun, algoritma RSA tergolong lamban dalam pemrosesannya karena melibatkan operasi matematika yang kompleks, sehingga RSA tidak cocok digunakan untuk mengenkripsi data dalam jumlah besar atau ukuran pesan yang panjang.

Berdasarkan pembahasan algoritma Autokey Cipher, Affine Cipher, dan RSA, secara umum algoritma simetris dan asimetris memiliki keunggulan dan kelemahan masing-masing. Algoritma kriptografi simetris, memiliki keunggulan pada kecepatan proses enkripsi dan dekripsi karena perhitungannya relatif sederhana, sehingga algoritma ini efektif digunakan untuk mengenkripsi pesan panjang atau data berukuran besar. Namun, kelemahannya terletak pada distribusi kunci yang rawan disadap sehingga mengharuskan kedua pihak menjaga kerahasiaan kunci bersama dan juga kunci harus sering diubah. Sementara itu, algoritma kriptografi asimetris lebih aman dalam hal distribusi kunci karena menggunakan dua pasangan kunci yang berbeda yaitu kunci publik dan privat,

sehingga tidak mengharuskan perubahan kunci secara berkala, tetapi proses enkripsi dan dekripsi lebih lambat akibat kompleksitas perhitungan matematis yang melibatkan penggunaan bilangan bulat berukuran besar dan terdapatnya operasi perpangkatan (Munir, 2019). Untuk mengatasi kelemahan tersebut, digunakan pendekatan yang memadukan keunggulan dari kedua jenis algoritma, yang dikenal sebagai Kriptografi Hibrida. Metode ini mengamankan data dengan menggabungkan algoritma simetris dan asimetris dalam satu sistem (Jamaludin dan Romindo, 2020). Pada kriptografi hibrida, algoritma simetris digunakan untuk proses enkripsi dan dekripsi pesan, sedangkan algoritma asimetris digunakan untuk proses enkripsi dan dekripsi kunci yang dipakai oleh algoritma simetris tersebut. Dengan menggabungkan algoritma simetris dan asimetris, sistem ini dapat memaksimalkan keunggulan dari kedua jenis algoritma untuk mendapatkan sistem keamanan yang lebih efektif (Munir, 2019).

Beberapa penelitian terdahulu telah mengimplementasikan pendekatan Kriptografi Hibrida sebagai upaya untuk memperkuat sistem pengamanan data. Penelitian oleh Jamaludin dan Romindo (2020), yaitu *"Implementation of Combination Vigenere Cipher and RSA in Hybrid Cryptosystem for Text Security"*, membahas penerapan kriptografi hibrida dengan mengombinasikan algoritma *Vigenere Cipher* untuk enkripsi pesan dan algoritma RSA untuk enkripsi kunci *Vigenere*. Penelitian ini bertujuan mengatasi kelemahan masing-masing algoritma, yaitu *Vigenere Cipher* yang mudah ditebak karena pola kuncinya berulang dan lambatnya proses RSA. Hasil penelitian ini menunjukkan bahwa pendekatan kriptografi hibrida yang memadukan algoritma *Vigenere Cipher* dan RSA mampu meningkatkan efisiensi proses enkripsi maupun dekripsi, sekaligus memberikan perlindungan yang lebih optimal terhadap data teks.

Penelitian oleh Gultom (2021), yang berjudul *"Penerapan Algoritma Hybrid Affine Cipher dan RSA Terhadap Sistem Keamanan"*, mengimplementasikan kriptografi hibrida dengan merancang sebuah aplikasi perlindungan keamanan file yang memadukan algoritma

Affine Cipher dan RSA. Aplikasi dikembangkan menggunakan bahasa pemrograman Delphi 7.0. Dalam proses enkripsi, data file terlebih dahulu dienkripsi menggunakan kunci *Affine* untuk menghasilkan *cipherfile*. Selanjutnya, kunci *Affine* tersebut juga dienkripsi menggunakan kunci publik RSA, sehingga diperoleh *cipherkey Affine*. Kedua hasil ini kemudian digabungkan menjadi *file_secure* yang aman. Pada tahap dekripsi, *file_secure* dibuka dengan terlebih dahulu mendekripsi *cipherkey* menggunakan kunci privat RSA untuk memperoleh kembali kunci *Affine*, yang selanjutnya digunakan untuk mendekripsi *cipherfile* dan menghasilkan data asli. Hasil penelitian menunjukkan bahwa sistem mampu mengenkripsi dan mendekripsi data dengan baik, serta menunjukkan bahwa pendekatan hibrida ini efektif menjaga kerahasiaan data file teks meskipun waktu enkripsi bergantung pada ukuran file yang diproses.

Selanjutnya, penelitian yang dilakukan oleh Pangaribuan dan Simbolon (2021) berjudul *"Kriptografi Hibrida Menggunakan Algoritma Hill Cipher dan RSA untuk Keamanan Pengiriman Informasi pada Email"*, menerapkan metode kriptografi hibrida, di mana pesan teks dienkripsi menggunakan algoritma *Hill Cipher* yang telah dimodifikasi, sedangkan pengamanan distribusi kunci *Hill Cipher* dilakukan dengan menggunakan algoritma RSA. Dari hasil penelitian diketahui bahwa tingkat keamanan pesan meningkat melalui penerapan kombinasi kriptografi hibrida, karena sistem ini menggunakan kunci yang berbeda antara proses enkripsi dan dekripsi. Selain itu, kompleksitas kunci yang dikirim kepada penerima menyulitkan pihak luar untuk menebak kunci asli, karena jumlah karakter kunci yang diterima tidak mencerminkan panjang kunci sebenarnya.

Berdasarkan penelitian-penelitian terdahulu, kriptografi hibrida umumnya menggabungkan satu algoritma simetris dan satu algoritma asimetris, sehingga pada penelitian ini mengusulkan sebuah kriptografi hibrida yang menggabungkan dua algoritma simetris, *Autokey Cipher* dan *Affine Cipher*, untuk mengenkripsi pesan secara berlapis, serta algoritma asimetris RSA untuk mengenkripsi kunci dari kedua algoritma simetris

tersebut. Proses dimulai dengan enkripsi pesan menggunakan algoritma *Autokey Cipher-Affine Cipher*, lalu kunci dari kedua algoritma tersebut dienkripsi menggunakan RSA. Pada tahap dekripsi, algoritma RSA terlebih dahulu digunakan untuk mendekripsi kunci algoritma simetris yang sebelumnya telah dienkripsi, sehingga diperoleh kembali bentuk kunci aslinya. Kemudian dilanjutkan dengan proses dekripsi pesan sesuai urutan algoritma. Pendekatan ini bertujuan agar sistem enkripsi yang dibangun tidak hanya menjaga kerahasiaan pesan melalui enkripsi berlapis menggunakan algoritma simetris, tetapi juga memberikan lapisan perlindungan tambahan terhadap kunci algoritma simetris, sehingga proteksi data yang diberikan lebih menyeluruh. Pada penelitian ini juga akan dilakukan analisis keamanan dari dua aspek yang berbeda, yaitu analisis keamanan pesan dan analisis keamanan kunci. Analisis keamanan pesan dilakukan menggunakan *Shannon Entropy* untuk menilai kualitas *cipherteks* yang dihasilkan oleh kombinasi algoritma simetris *Autokey Cipher* dan *Affine Cipher* berdasarkan tingkat keacakan cipherteksnya. Sementara itu, analisis keamanan kunci dilakukan menggunakan *Brute Force Attack* untuk menilai ketahanan kunci pada kombinasi algoritma simetris *Autokey Cipher*, *Affine Cipher*, dan algoritma asimetris RSA, berdasarkan kompleksitas waktu yang diperlukan untuk menemukan kunci yang benar.

1.2 Perumusan Masalah

Berikut ini adalah uraian dari rumusan masalah penelitian ini berdasarkan latar belakang yang telah dipaparkan di atas:

1. Bagaimana mengimplementasikan kriptografi hibrida menggunakan algoritma simetris *Autokey Cipher* dan *Affine Cipher* untuk pengamanan pesan, serta algoritma asimetris RSA untuk pengamanan kunci algoritma simetris?

2. Bagaimana proses enkripsi dan dekripsi dilakukan dalam dua urutan kombinasi algoritma simetris (*Autokey-Affine* dan *Affine-Autokey*)

untuk pengamanan pesan, serta algoritma asimetris RSA untuk pengamanan kunci algoritma simetris?

3. Bagaimana tingkat keamanan pesan berdasarkan kualitas *cipherteks* yang dihasilkan oleh kombinasi algoritma simetris *Autokey Cipher* dan *Affine Cipher* melalui analisis *Shannon Entropy*?

4. Bagaimana tingkat keamanan kunci berdasarkan ketahanan kombinasi kunci *Autokey Cipher*, *Affine Cipher*, dan RSA yang dianalisis menggunakan metode *Brute Force Attack* ditinjau dari kompleksitas waktu yang diperlukan untuk menemukan kunci yang benar?

1.3 Pembatasan Masalah

Untuk mencegah agar pembahasan penelitian tidak menjadi terlalu luas, diberikan batasan masalah, yaitu:

1. Menggunakan kode ASCII 256 karakter.
2. Algoritma yang digunakan terbatas pada:
   (a) Algoritma simetris yaitu *Autokey Cipher* dan *Affine Cipher* digunakan untuk enkripsi dan dekripsi pesan teks.
   (b) Algoritma asimetris RSA digunakan untuk enkripsi dan dekripsi kunci *Autokey* dan kunci *Affine* (a, b).
3. Enkripsi pesan menggunakan dua kombinasi urutan:
   (a) *Autokey Cipher–Affine Cipher*
   (b) *Affine Cipher–Autokey Cipher*
4. Evaluasi keamanan terbatas pada:
   (a) Analisis keamanan pesan dengan *Shannon Entropy*
   (b) Analisis keamanan kunci dengan *Brute Force Attack*

5. Implementasi dilakukan menggunakan bahasa pemrograman *Python* di lingkungan *Google Colab*.

1.4 Tujuan Penelitian

Berdasarkan rumusan masalah yang telah diberikan sebelumnya, tujuan dari penelitian ini adalah sebagai berikut:

1. Mengimplementasikan kriptografi hibrida menggunakan algoritma simetris *Autokey Cipher* dan *Affine Cipher* untuk pengamanan pesan, serta algoritma asimetris RSA untuk pengamanan kunci algoritma simetris.
2. Melakukan proses enkripsi dan dekripsi dilakukan dalam dua urutan kombinasi algoritma simetris (*Autokey-Affine* dan *Affine-Autokey*) untuk pengamanan pesan, serta algoritma asimetris RSA untuk pengamanan kunci algoritma simetris.
3. Menganalisis keamanan pesan menggunakan *Shannon Entropy* untuk menilai kualitas *cipherteks* yang dihasilkan oleh kombinasi algoritma simetris *Autokey Cipher* dan *Affine Cipher* berdasarkan tingkat keacakannya.
4. Menganalisis keamanan kunci menggunakan *Brute Force Attack* untuk menilai ketahanan kombinasi kunci *Autokey Cipher*, *Affine Cipher*, dan RSA berdasarkan kompleksitas waktu yang diperlukan untuk menemukan kunci yang benar.

1.5 Manfaat Penelitian

Terdapat beberapa manfaat penelitian bagi para pembaca, yaitu:

1. Memahami konsep pengamanan data teks dengan pendekatan kriptografi hibrida yang menggabungkan algoritma simetris dan asimetris untuk meningkatkan keamanan data.

2. Memahami tahapan proses enkripsi dan dekripsi pesan menggunakan dua urutan kombinasi algoritma simetris (*Autokey–Affine* dan *Affine–Autokey*), serta proses pengamanan kunci menggunakan algoritma asimetris RSA.

3. Memahami metode analisis keamanan pada kriptografi hibrida melalui analisis *Shannon Entropy* dan *Brute Force Attack*.