BAB 1

PENDAHULUAN

1.1 Latar Belakang

Dalam era digital yang berkembang pesat saat ini, informasi dan data menjadi aset yang sangat berharga. Perlindungan data telah menjadi prioritas utama di berbagai sektor, mulai dari pemerintahan, industri keuangan, hingga perusahaan teknologi. Namun, berdasarkan data dari BSSN, selama tahun 2023 terdapat sebanyak 1.417 aduan siber yang berasal dari berbagai sektor. Dari banyaknya aduan siber yang diterima, *cybercrime* menjadi kategori aduan siber tertinggi, yaitu sebanyak 1.216 aduan atau 86% dari total aduan siber. *Cybercrime* atau kejahatan siber adalah tindakan kriminal yang memanfaatkan teknologi, mulai dari perangkat hingga jaringan internet (Badan Siber dan Sandi Negara, 2023). Untuk mencegah adanya kejahatan siber, diperlukan keamanan siber atau *cyber security*. Keamanan siber dapat didefinisikan sebagai aktivitas, proses, kemampuan, atau kondisi dimana sistem informasi dan komunikasi, serta data yang ada di dalamnya, dilindungi dari kerusakan, penggunaan tanpa izin, perubahan, atau eksploitasi (Rahman, dkk., 2020). Dengan kata lain, keamanan siber bertujuan untuk melindungi informasi dan sistem digital dari segala bentuk ancaman yang dapat membahayakan integritas dan kerahasiaannya. Namun, jumlah tenaga profesional keamanan siber di Indonesia masih kurang karena minimnya pengetahuan masyarakat Indonesia terkait keamanan siber (Hapizon & Mahmuluddin, 2023). Kriptografi menjadi salah satu bagian dari keamanan

siber, sehingga penting bagi generasi masa kini untuk mulai mempelajari ilmu kriptografi agar dapat berperan aktif dalam memperkuat keamanan siber di era digital.

Menurut Schneier (1996), kriptografi merupakan ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data, serta otentikasi. Terdapat juga definisi lain menurut Meyer (1982), kriptografi merupakan ilmu dan seni untuk menjaga kerahasiaan pesan dengan cara melakukan penyandian pesan menjadi bentuk yang tidak dapat dipahami lagi maknanya (Munir, 2019).

Sebelum adanya teknologi canggih seperti zaman sekarang, kriptografi dilakukan dengan menggunakan alat sederhana seperti pensil dan kertas. Proses enkripsi dan dekripsi hanya dilakukan terhadap karakter yang ada di dalam pesan. Kriptografi yang menggunakan proses sederhana tersebut dikategorikan sebagai algoritma kriptografi klasik. Salah satu jenis cipher kriptografi klasik adalah cipher substitusi. Cipher susbtitusi mengubah setiap unit plainteks dengan satu unit cipherteks.

Suatu algoritma kriptografi perlu diperiksa keamanannya untuk memastikan apakah algoritma yang digunakan sudah aman dari serangan. Salah satu kelemahan dari cipher substitusi adalah kriptanalis dapat menerka huruf plainteks menggunakan tabel frekuensi kemunculan huruf karena huruf yang frekuensi kemunculannya paling tinggi di plainteks akan sering muncul juga pada cipherteks. Oleh karena itu, biasanya cipher substitusi dipecahkan oleh kriptanalis menggunakan metode analisis frekuensi. Jadi, metode analisis frekuensi termasuk salah satu metode untuk menganalisis keamanan suatu algoritma kriptografi. Jika algoritma kriptografi dapat menyembunyikan hubungan statistik antara huruf dalam plainteks dengan cipherteks, maka algoritma tersebut dapat dikatakan aman dari serangan metode analisis frekuensi.

Hill Cipher adalah algoritma kriptografi klasik jenis cipher substitusi yang menggunakan matriks transformasi pada proses enkripsi dan dekripsinya

dimana matriks tersebut dijadikan sebagai kuncinya. *Hill Cipher* memiliki keunggulan dalam analisis frekuensi jika dilakukan analisis per karakter, namun algoritma ini masih lemah dalam analisis frekuensi jika dilakukan analisis dalam bigram atau trigam karena blok plainteks yang sama menghasilkan blok cipherteks yang sama juga. Untuk mengatasi kelemahan tersebut akan dilakukan kombinasi dengan algoritma kriptografi yang memiliki kelebihan dalam menyembunyikan pola dalam analisis frekuensi bigram atau trigram.

Algoritma *Hill Cipher* memiliki kunci dalam bentuk matriks. Namun, tidak semua matriks dapat dijadikan sebagai kunci pada *Hill Cipher*. Kunci yang dapat digunakan dalam *Hill Cipher* adalah matriks yang *invertible*, yaitu matriks yang determinannya tidak sama dengan nol dan nilai determinannya harus relatif prima terhadap banyaknya karakter yang dapat dijadikan plainteks (Sujarwo, 2024). Liew & Nguyen (2020) pada penelitiannya mengubah matriks *skew-symmetric* menjadi matriks ortogonal yang *invertible* sebagai matriks kunci pada *Hill Cipher*. Varian yang dirancang berhasil mengurangi waktu komputasi dalam proses dekripsi.

Salah satu cara untuk menyembunyikan pola atau hubungan statistik antara plainteks dengan cipherteks yang dapat diketahui oleh kriptanalis menggunakan analisis frekuensi pada cipher substitusi adalah dengan menggunakan cipher substitusi homofonik, dimana teknik enkripsinya menggunakan fungsi *ciphering* yang memetakan satu-ke-banyak atau *one to many*, sehingga satu karakter yang ada di plainteks dapat dienkripsi menjadi lebih dari satu kemungkinan karakter cipherteks (Munir, 2019). Beragamnya bentuk cipherteks yang dihasilkan oleh skema pemetaan *one-to-many* menyebabkan proses kriptanalisis menjadi lebih sulit dilakukan (Wowor & Susanto, 2023). Algoritma kriptografi yang pemetaannya *one to many* ini dapat dibuat dengan mengaplikasikan konsep koset dalam aljabar ke dalam algoritma kriptografi klasik, seperti yang telah dilakukan oleh Yulianti & Wijaya (2022) dalam penelitiannya. Hasil pengujian analisis frekuensi pada enkripsi menggunakan kriptografi klasik dengan penerapan konsep koset tidak terlihat

hubungan antara sebaran kemunculan huruf di plainteks dengan kemunculan huruf di cipherteks, sehingga kriptanalis tidak dapat menebak aturan enkripsi yang digunakan. Namun, pada penelitian tersebut, hanya menggunakan 26 huruf abjad, sehingga belum bisa mengenkripsikan plainteks yang memiliki angka dan simbol. Dalam penelitian ini akan digunakan kode ASCII pada algoritma kriptografi klasik dengan konsep koset tersebut agar dapat digunakan pada plainteks yang lebih kompleks dan menghasilkan cipherteks yang lebih kompleks pula.

Pada penelitian terdahulu, Hassan, dkk. (2022) mencoba meningkatkan keamanan data dengan menggunakan kombinasi *Hill Cipher* dan *Transposition Cipher*. Plainteks akan dienkripsi menggunakan teknik *Hill Cipher* biasa dan dienkripsi lagi menggunakan *Transposition Cipher* sehingga kombinasi keduanya menghasilkan teks sandi yang lebih kompleks dan lebih aman daripada algoritma dalam bentuk biasa dari masing-masing cipher.

Untuk meningkatkan keamanan algoritma, maka pada penelitian ini akan dilakukan kombinasi antara *Hill Cipher* dan cipher substitusi dengan koset. Setelah itu, akan dilakukan analisis keamanan dari kombinasi tersebut dengan teknik analisis frekuensi. Analisis frekuensi dilakukan dalam bigram dan trigam karena masalah keamanan dalam *Hill Cipher* dimulai pada analisis frekuensi bigram sedangkan N-Gram dengan ukuran lebih besar dari trigram cenderung menghasilkan data yang jarang berulang sehingga memiliki kemungkinan menghasilkan diagram sebaran frekuensi yang seragam dan kurang efektif untuk dianalisis secara statistik.

1.2 Perumusan Masalah

Berdasarkan latar belakang yang dituliskan sebelumnya, rumusan masalah dari penelitian ini, yaitu:

1. Bagaimana analisis keamanan pesan tersandi menggunakan kombinasi *Hill Cipher* dilanjutkan dengan cipher substitusi dengan koset pada pesan teks?

2. Bagaimana analisis keamanan pesan tersandi menggunakan kombinasi cipher substitusi dengan koset dilanjutkan dengan *Hill Cipher* pada pesan teks?

3. Bagaimana pengaruh perbedaan urutan kombinasi terhadap hasil analisis keamanan?

1.3 Batasan Masalah

1. Analisis keamanan dilakukan dengan metode analisis frekuensi bigram dan trigram yang dilihat dari diagram sebaran frekuensi, nilai *Shannon entropy*, dan nilai *Min-entropy*.

2. Analisis keamanan dilakukan menggunakan plainteks berikut:

> Untuk mendapatkan kode brankas, pecahkan teka-teki berikut ini dengan cermat dan teliti. Pertama, hitung ada berapa banyak bilangan prima dalam himpunan X = { x | 1 ≤ x < 50 }. Kedua, perhatikan bentuk bangun datar ini [redacted] dan cari tahu jumlah sisinya, lalu kalikan dengan 1000, setelah itu hitung 2% dari hasilnya. Ketiga, tentukan nilai dari operasi matematika ((4! ÷ 6) + √36)², kemudian jumlahkan semua digit hasil akhirnya. Terakhir, gabungkan semua hasil dari langkah pertama, kedua, dan ketiga secara berurutan untuk mendapatkan kodenya.

3. Matriks *skew-symmetric* ukuran 2×2 dan ukuran 3×3 yang digunakan untuk membentuk kunci *Hill Cipher* adalah sebagai berikut:

$$A_{2\times 2} = \begin{pmatrix} 0 & 10 \\ -10 & 0 \end{pmatrix}$$

$$A_{3\times 3} = \begin{pmatrix} 0 & 11 & 21 \\ -11 & 0 & -32 \\ -21 & 32 & 0 \end{pmatrix}$$

4. Kunci cipher substitusi dengan koset yang digunakan adalah $K_{CSK} = 30$

1.4 Tujuan Penelitian

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

1. Mengetahui hasil analisis keamanan pesan tersandi menggunakan kombinasi *Hill Cipher* dilanjutkan dengan cipher substitusi dengan koset pada pesan teks.
2. Mengetahui hasil analisis keamanan pesan tersandi menggunakan kombinasi cipher substitusi dengan koset dilanjutkan dengan *Hill Cipher* pada pesan teks.
3. Mengetahui pengaruh perbedaan urutan kombinasi terhadap hasil analisis keamanan.

1.5 Manfaat Penelitian

Penelitian ini diharapkan dapat bermanfaat bagi para pembaca, yaitu:

1. Bagi Mahasiswa
   - Memahami konsep dan algoritma kriptografi klasik.
   - Memahami cara mengombinasikan algoritma kriptografi.
   - Memahami cara menganalisis keamanan algoritma kriptografi.
2. Bagi Program Studi Matematika
   Hasil penelitian dapat dijadikan sebagai referensi untuk bahan ajar tentang kriptografi dan peran matematika dalam suatu algoritma kriptografi.
3. Bagi Masyarakat Umum
   Memberikan wawasan kepada masyarakat mengenai pentingnya kriptografi dan bagaimana peran kriptografi dalam menjaga keamanan data.