BAB I

PENDAHULUAN

Bagian ini mencakup latar belakang masalah, rumusan masalah, batasan masalah, tujuan penelitian, metode penelitian, dan sistematika penulisan dalam pembahasan Algoritma El-Gamal Pada Teknik Kriptografi Affine-Hill Cipher dengan Pembangkit Kunci Matriks Multinacci.

1.1.Latar Belakang Masalah

Komunikasi adalah suatu proses di mana informasi, pikiran , ide, dan perasaan ditukar antara individu maupun kelompok. Komunikasi merupakan aspek fundamental dari interaksi manusia dan sangat penting untuk menyampaikan pesan, membangun hubungan, dan berbagi pengetahuan. Komunikasi yang efektif melibatkan pengirim dan penerima pesan, dan dapat dilakukan dalam berbagai bentuk, termasuk verbal (kata-kata yang diutarakan atau ditulis), non-verbal (gerak tubuh, bahasa tubuh, ekspresi wajah), dan visual (bagan, grafik, gambar).

Penyampaian pesan dalam komunikasi mengacu pada proses pengiriman pesan dari pengirim ke penerima. Proses ini melibatkan beberapa elemen dan pertimbangan utama untuk memastikan bahwa pesan disampaikan dan dipahami secara efektif.

Salah satu aspek yang paling dinamis dalam kehidupan manusia adalah evolusi metode dan alat komunikasi. Penyampaian pesan dahulu membutuhkan interaksi tatap muka antara pengirim dan penerima. Pesan hanya dapat disampaikan jika kedua belah pihak bertemu langsung. Namun, seiring berjalannya waktu, berbagai alat muncul untuk memfasilitasi komunikasi, seperti surat, telegraf, email dan smartphone. Bahkan hingga saat ini, metode dan alat ini terus berkembang. Meskipun kemajuan teknologi ini bermanfaat, namun hal ini juga memudahkan pesan untuk disadap atau diubah oleh orang yang tidak berwenang. Untuk mengatasi masalah ini, bidang kriptografi dikembangkan. Kriptografi adalah ilmu pengetahuan dan seni yang didedikasikan untuk menjaga pesan tetap aman dan rahasia.

Dalam kriptografi klasik, sandi Hill[9,17] adalah salah satu sandi substitusi poligrafik yang didasarkan pada sistem residu dan aljabar linier yang yang dikembangkan oleh matematikawan Lester Hill pada tahun 1929. MK Viswanath, et.al mengusulkan konsep kriptografi kunci publik menggunakan Hill's Cipher. Mereka mengembangkan kriptografi kunci publik dengan sistem cipher Hill menggunakan matriks persegi panjang dan untuk invers matriks kunci, mereka menggunakan metode Moore-Penrose Inverse (Pseudo Inverse). Belakangan ini, P. Sundarayya & G.V. Prasad[2] bekerja pada kertas yang sama[3], dan mereka mengusulkan metode yang meningkatkan keamanan sistem di atas dengan melibatkan dua atau lebih tanda tangan *(signature)* digital. Untuk meningkatkan keamanan Hill Cipher, Thilaka dan Rajalakshmi[4] memperluas konsep Hill Cipher dengan mengenkripsi string dengan panjang m menjadi string dengan panjang n $(n \geq m)$ menggunakan transformasi affine dan transformasi polinomial. Sementara di[5], Indivar Gupta, et.al menunjukkan bahwa ekstensi Hill Cipher ini rentan terhadap serangan *cryptanalytic* dan menyarankan bahwa modifikasi di Hill Cipher tidak membuatnya lebih kuat secara signifikan.

Dalam Skripsi ini, mengembangkan kriptosistem kunci publik menggunakan Affine-Hill Cipher dengan matriks Fibonacci yang diperumum (multinacci) dengan daya k yang besar, yaitu Q_λ^k sebagai matriks kunci. Metode ini cukup kuat dan dapat diimplementasikan dengan mudah.

1.2. Rumusan Masalah

Rumusan masalah yang akan dibahas dalam tugas akhir ini didasarkan pada latar belakang yang telah dijelaskan sebelumnya, yaitu:

1. Bagaimana algoritma El-Gamal untuk pembangkitan kunci matriks multinacci ?
2. Bagaimana enkripsi dan dekripsi dalam teknik Affine-Hill Cipher ?
3. Bagaimana simulasi pengiriman dan penerima pesan menggunakan Affine-Hill Cipher ?

1.3. Batasan Masalah

Terdapat beberapa aspek yang membatasi ruang lingkup masalah dalam penelitian ini, yaitu:

1. Penggunaan barisan dari matriks Fibonacci yang diperumum (matriks multinacci).
2. Teknik enkripsi - dekripsi dari Affine Hill-Cipher menggunakan matriks multinacci.
3. Pembangkitan kunci dengan El-Gamal dengan modulo yang digunakan 127.

1.4. Tujuan Penelitian

Dengan mempertimbangkan latar belakang dan rumusan masalah yang telah diuraikan, penelitian ini bertujuan :

1. Untuk mengetahui bagaimana penggabungan Affine Cipher dengan Hill Cipher.
2. Untuk mengetahui bagaimana enkripsi-dekripsi Affine-Hill Cipher.
3. Untuk mengetahui bagaimana pertukaran kuncinya.
4. Untuk mengetahui bagaimana barisan dari matriks multinacci.
5. Untuk mengetahui bagaimana penggunakan algoritma El-Gamal pada teknik kriptografi Affine-Hill Cipher dengan pembangkit kunci matriks multinacci.

1.5. Metode Penelitian

1. Studi Literatur

   Pada tahap ini mengumpulkan topik penelitian, data penelitian dan landasan teori berkaitan dengan algoritma kriptografi. Sumber ini dapat diperoleh dari berbagai sumber seperti buku, jurnal, paper, dan artikel terkait.

2. Analisis

   Pada langkah ini, algoritma yang telah direpresentasikan akan dianalisis untuk menemukan kunci yang kompleks, sehingga dapat diperoleh suatu metode yang optimal dari masing-masing algoritma tersebut.

3. Simulasi

Tahap ini melakukan simulasi untuk mengetahui efektivitas skema. Simulasi menunjukan proses algoritma El-Gamal enkripsi dan dekripsi pesan dalam skema algoritma dari pengiriman dan pengamanan pesan.

1.6. Sistematika Penulisan

Skripsi ini terdiri dari lima bab dengan sistematika penulisan yang mencakup:

BAB I : PENDAHULUAN

Pada bab pendahuluan, umumnya berisikan beberapa elemen penting, seperti latar belakang masalah, rumusan masalah, batasan masalah, tujuan penelitian, ruang lingkup penelitian, dan sistematika penulisan.

BAB II : LANDASAN TEORI

Pada bab landasan teori, terdapat penjelasan mendalam mengenai berbagai teori yang relevan dan menjadi dasar dari pembahasan mengenai kriptografi secara umum, termasuk prinsip-prinsip dasar kriptografi, penjelasan khusus mengenai Affine cipher dan Hill cipher, serta algoritma enkripsi-dekripsi yang digunakan.

BAB III : PEMBANGKITAN KUNCI MATRIKS MULTINACCI MENGGUNAKAN ALGORITMA EL-GAMAL PADA TEKNIK KRIPTOGRAFI AFFINE-HILL CIPHER

Bab ini mencakup pembahasan utama dari skripsi yang diteliti, yaitu mengenai Pembangkitan Kunci Matriks Multinacci Menggunakan Algoritma El-Gamal Pada Teknik Kriptografi Affine-Hill Cipher Dengan Affine-Hill Cipher.

BAB IV : STUDI KASUS DAN ANALISIS

Bab ini berisi pembahasan dan analisis mendalam terhadap permasalahan yang dikaji dalam penelitian ini. Pembahasan mencakup implementasi algoritma untuk menghitung nilai yang relevan serta penggunaan aplikasi software seperti Excel dan Jupyter untuk mencari solusi yang optimal.

BAB V : PENUTUP

Bab ini memuat kesimpulan dari pembahasan yang telah dikaji. Selain itu, terdapat juga saran yang diajukan untuk pengembangan lebih lanjut topik pembahasan skripsi ini.

DAFTAR PUSTAKA

LAMPIRAN