BAB III
METODOLOGI PENELITIAN

Pada bagian ini menjelaskan metodologi yang digunakan dalam penelitian, langkah-langkahnya diuraikan sebagai berikut:

3.1 Masalah Kriptografi

Dalam perkembangan teknologi komunikasi masalah keamanan dan kerahasiaan pengiriman pesan menjadi aspek penting, maka diperlukannya ilmu atau seni untuk menjaga keamanan pesan yang disebut kriptografi. Namun banyak algoritma kriptografi yang telah dipecahkan dan dinilai sudah tidak aman lagi. Mengkomposisikan dua algorima kriptografi adalah salah satu cara agar pesan lebih sulit untuk dipecahkan dibandingkan dengan menggunakan satu algoritma saja. Algoritma kriptografi yang digunakan dalam penelitian ini adalah Vigenere *Cipher* dan algoritma *Knapsack* Merkle-Hellman.

3.2 Mengkaji Model Dasar

Vigenere *cipher* merupakan kriptografi simetri yang hanya memiliki satu kunci untuk proses enkripsi dan dekripsi. Arjana, dkk. (2012) mendefinisikan Vigenere *cipher* merupakan metode penyandian teks alfabet dengan menggunakan deret sadi caesar berdasarkan huruf-huruf pada kata kunci.

Sedangkan algoritma *Knapsack* Merkle-Hellman merupakan kriptografi asimetri yang menggunakan dua kunci, yaitu kunci publik untuk proses enkripsi dan kunci rahasia untuk proses dekripsi. Algoritma *Knapsack* Merkle-Hellman adalah algoritma yang bergantung pada sulitnya memecahkan *knapsack problem* dengan menggunakan barisan *superincreasing knapsack*, di mana barisan *superincreasing* merupakan barisan yang setiap nilai didalamnya lebih besar dari jumlah semua nilai sebelumnya. Namun algoritma *superincreasing knapsack* merupakan algoritma yang lemah, untuk mengatasi kelemahannya algoritma *superincreasing knapsack*

dimodifikasi menjadi *nonsuperincreasing knapsack,* di mana barisan *nonsuperincreasing knapsack* merupakan kunci publik yang digunakan untuk enkripsi dan barisan *superincreasing knapsack* merupakan kunci rahasia yang digunakan untuk dekripsi.

3.3 Mengembangkan Model Dasar

Model enkripsi dan dekripsi yang digunakan dalam penelitian ini adalah mengkomposisikan Vigenere *cipher* dan algoritma *Knapsack* Merkle-Hellman. Proses pertama dalam menenkripsi yaitu mengubah *plaintext* 1 menjadi *ciphertext* 1 menggunakan kunci Vigenere. Kedua, hasil *ciphertext* 1 dienkripsi menggunakan kunci publik *knapsack* yang menghasilkan *ciphertext* 2, di mana *ciphertext* 2 merupakan *ciphertext* yang akan dikirim sebagai pesan rahasia. Proses dekripsi, yaitu *ciphertext* 2 didekripsi dengan kunci rahasia *knapsack* menghasilkan *plaintext* 2 . Kemudian, *plaintext* 2 didekripsi dengan menggunakan kunci Vigenere, maka akan diperoleh *plaintext* 2 yang merupakan pesan yang sebenarnya.

3.4 Mengkonstruksi Program

Pada tahap ini akan dilakukan perancangan tampilan untuk program aplikasi enkripsi dan dekripsi. Rangcangan program aplikasi yang akan dibuat sebanyak dua tampilan, yaitu *view user* yang digunakan untuk pengguna program aplikasi kriptografi dan *view* validasi yang digunakan untuk menampilkan langkah-langkah hasil perhitungan program aplikasi. Kemudian, akan mengimplementasikan program aplikasi kriptografi sesuai dengan rancangan program yang telah dibuat. Pembuatan program aplikasi kriptografi dilakukan untuk mengubah model matematis kedalam bahasa pemograman. Program yang akan digunakan adalah pemograman Matlab R2013a dengan memanfaatkan fasilitas *Graphic User Interface* atau GUI yang digunakan untuk membuat tampilan berbentuk grafis sehingga hasil *output* lebih menarik.. Model yang dibuat dalam program adalah proses enkripsi dan dekripsi dari komposisi Vigenere *cipher* dan algoritma *Knapsack* Merkle-Hellman. Program aplikasi ini menggunakan kode ASCII. Jumlah kode ASCII yang digunakan adalah 95

karakter dari 127 karakter. Untuk itu dilakukan penyesuaian untuk kode ASCII, sehingga pada perhitungan kode ASCII yang asli akan dikurangkan 32, misalkan karakter spasi pada kode ASCII bernilai 32 dikurangkan 32 menjadi 0, karakter *a* pada kode ASCII bernilai 97 dikurangkan 32 menjadi 65.

3.5 Memvalidasi Program

Pada tahap ini akan dilakukan validasi program yang bertujuan untuk menguji hasil matematis yang dikerjakan sesuai dengan *output* program aplikasi.

3.6 Menarik Kesimpulan

Tahap terakhir yang dilakukan adalah menarik kesimpulan dari hasil penelitian yang telah dilakukan dan memberikan saran-saran kepada peneliti selanjutnya untuk lebih meningkatkan hasil penelitianya.