BAB I

PENDAHULUAN

1.1. Latar Belakang

Di era teknologi jaman sekarang, informasi merupakan hal yang penting dan vital untuk setiap orang. Apabila suatu informasi berupa percakapan bocor ke orang yang tidak berhak, hal tersebut dapat memberikan kerugian yang sangat besar kepada kedua belah pihak terkait. Terlebih lagi, dengan perkembangan pesat teknologi internet, celah untuk mencuri informasi data perusahaan lebih besar.

Untuk mengatasi celah keamanan tersebut, dibutuhkan ilmu kriptografi yang berguna untuk menyembunyikan informasi secara rahasia. Menurut sejarahnya, kriptografi sudah lama digunakan oleh tentara Sparta di Yunani pada permulaan tahun 400 SM. Mereka menggunakan alat yang disebut scytale. Alat ini terdiri dari sebuah pita panjang dari daun papyrus yang dililitkan pada sebuah batang silinder.

Algoritma Kriptografi dibagi menjadi dua, yaitu algoritma simetris dan algoritma asimetris. Algoritma simetris adalah suatu algoritma yang menggunakan kunci enkripsi sama dengan kunci dekripsi. Contoh algoritma simetris adalah algoritma hill cipher dan algoritma vigenere. ***Hill cipher*** merupakan penerapan aritmatika modulo pada kriptografi. Teknik kriptografi ini menggunakan sebuah matriks persegi berukuran m x m sebagai kunci yang digunakan untuk melakukan enkripsi dan dekripsi.

Kekurangan pada kriptografi hill cipher adalah keterbatasan karakter yang dipakai yaitu hanya menggunakan karakter alphabet dan matriks kunci yang digunakan dalam enkripsi dan deskripsi sama. Selain itu, dengan menggunakan metode *known plaintext attack*, kriptografi hill cipher sudah bisa ditembus sehingga tingkat keamanan metode kriptografi ini sudah tidak aman. Salah satu cara untuk memperkuat keamanan dari kriptografi dengan menggunakan matriks sirkulan

Penggunaan matriks sirkulan terdapat di AES (*Advanced Encryption System*) pada tahap MixColoumns. Selain itu, matriks sirkulan juga terdapat pada

kriptografi WHIRLPOOL yaitu pada tahap ShiftColoumns. Kelebihan dari matriks sirkulan pada kriptografi adalah mengurangi kunci yang semula berjumlah $n^2 \in Z_p$ menjadi *n* buah elemen sehingga pada program mengurangi memori yang digunakan dan mempercepat waktu dalam perkalian matriks.

Oleh karena itu, dalam penelitian ini penulis mencoba untuk mengembangkan kriptografi hill cipher yang dimodifikasi dengan matriks sirkulan.

1.2. Rumusan Masalah

Berdasarkan latar belakang yang penulis uraikan, maka dirumuskan pokok permasalahan pada penelitian ini yaitu:

1. Bagaimana konsep dan algoritma kriptografi *Hill-cipher* yang dimodifikasi dengan matriks sirkulan ?
2. Bagaimana pembangkitan kunci publik pada kriptografi *Hill-cipher* yang dimodifikasi dengan matriks sirkulan ?
3. Bagaimana pengimplementasian algoritma kriptografi *Hill-cipher* yang dimodifikasi dengan matriks sirkulan ?

1.3 Tujuan Masalah

Tujuan penelitian ini antara lain:

1. Mengetahui konsep dan algoritma kriptografi *Hill-cipher* yang dimodifikasi dengan matriks sirkulan
2. Mengetahui pembangkitan kunci publik pada kriptografi *Hill-cipher* yang dimodifikasi dengna matriks sirkulan
3. Menganalisis pengimplementasian algoritma kriptografi *Hill-cipher* yang dimodifikasi dengan matriks sirkulan

1.4 Manfaat Masalah

Manfaat yang hendak dicapai dari penelitian ini adalah sebagai berikut.

1. Memberikan sumbangsih kepada masyarakat pada umumnya dan dunia kriptografi pada khususnya tentang pengimplementasian modifikasi kriptografi *Hill Cipher* dengan matriks sirkulan
2. Dalam penelitian ini dikembangkan sebuah aplikasi yang bertujuan untuk membantu proses pembangkitan kunci, enkripsi dan dekripsi pada modifikasi kriptografi *Hill Cipher* dengan matriks sirkulan.

1.5 Batasan Masalah

1. Matriks yang dipakai yaitu berukuran 2x2
2. Enkripsi dan dekripsi pada kriptografi ini menggunakan teks.