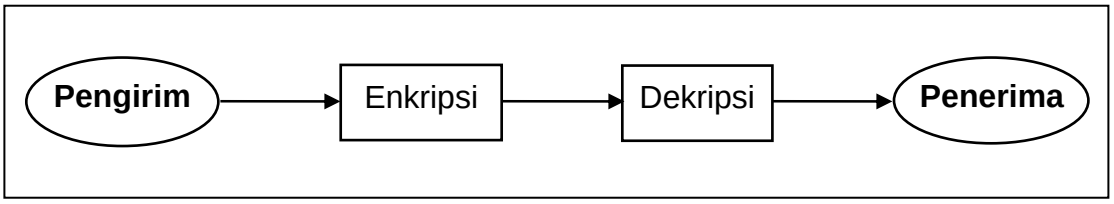
BAB I
PENDAHULUAN

1.1 Latar Belakang

Teknologi informasi memegang peranan yang sangat penting di era globalisasi saat ini, yaitu dalam penyampaian informasi dari satu pihak kepada pihak lain. Informasi yang disampaikan dapat bersifat umum dan dapat juga bersifat rahasia. Informasi yang bersifat umum dapat diketahui oleh pihak lain selain pihak pengirim informasi dan pihak penerima informasi. Sedangkan informasi yang bersifat rahasia hanya dapat diketahui oleh pihak pengirim informasi dan pihak penerima informasi.

Penyampaian berita melalui media seperti televisi, radio, dan surat kabar merupakan contoh dari penyampaian informasi yang bersifat umum. Sedangkan transaksi melalui ATM merupakan contoh dari penyampaian informasi yang bersifat rahasia.

Adapun proses penyampaian informasi rahasia tersebut dapat digambarkan sebagai berikut :



Gambar 1. Proses penyampaian informasi rahasia

Enkripsi adalah proses mengubah pesan/data/informasi yang dapat dibaca dan dimengerti maknanya menjadi bentuk pesan tersandi agar pesan tidak dapat dimengerti maknanya oleh pihak lain selain pihak pengirim dan penerima informasi. Sedangkan dekripsi adalah proses mengembalikan pesan tersandi menjadi pesan/data/informasi semula sehingga dimengerti maknanya oleh pihak penerima informasi.

Pada proses enkripsi dan dekripsi dibutuhkan suatu algoritma kesepakatan kunci, dimana dalam algoritma tersebut menggunakan suatu fungsi. Fungsi tersebut harus bersifat satu-satu supaya dapat ditemukan nilai inversnya sedemikian sehingga informasi yang dikirim oleh pihak pengirim tepat sama dengan informasi yang dibaca oleh pihak penerima. Salah satu fungsi yang digunakan adalah monomial x^n, dengan x positif.

Algoritma kesepakatan kunci dalam kriptografi yang menggunakan monomial x^n, dengan x positif adalah algoritma Diffie-Hellman. Penulis tertarik untuk mencoba mempelajari apakah ada polinomial yang dapat digunakan sebagai alternatif lain untuk algoritma tersebut. Polinomial yang dapat digunakan dalam algoritma kesepakatan kunci harus bersifat satu-satu atau disebut juga sebagai polinomial permutasi. Dalam aplikasinya, polinomial yang digunakan dalam algoritma kesepakatan kunci adalah polinomial permutasi di *ring* $\mathbb{Z}_n$. Tidak semua polinomial di *ring* $\mathbb{Z}_n$ merupakan polinomial permutasi, akan tetapi agar polinomial tersebut merupakan polinomial permutasi maka polinomial tersebut harus memiliki ciri-

ciri tertentu. Dalam algoritma Diffie-Hellman, selain menggunakan suatu monomial, juga dapat digunakan polinomial lain yang dikenal sebagai polinomial Chebyshev. Penulis akan melihat ciri-ciri dari polinomial Chebyshev yang merupakan polinomial permutasi di *ring* $\mathbb{Z}_n$.

1.2 Perumusan Masalah

Adapun permasalahan dalam skripsi ini adalah :

1. Bagaimana ciri-ciri dari suatu polinomial agar dapat dikatakan sebagai polinomial permutasi di *ring* $\mathbb{Z}_n$?
2. Bagaimana ciri-ciri dari polinomial Chebyshev yang merupakan suatu polinomial permutasi di *ring* $\mathbb{Z}_n$?

1.3 Tujuan Penulisan

Tujuan penyusunan skripsi ini adalah :

1. Menjelaskan ciri-ciri dari suatu polinomial permutasi di *ring* $\mathbb{Z}_n$.
2. Menjelaskan ciri-ciri dari polinomial Chebyshev yang merupakan suatu polinomial permutasi di *ring* $\mathbb{Z}_n$.

1.4 Batasan Masalah

Pada skripsi ini pembahasan mengenai polinomial permutasi di *ring* $\mathbb{Z}_n$ dibatasi pada $n = 2^w$, dengan $w \geq 1$.

1.5 Sistematika Penulisan

Sistematika penyusunan skripsi ini dimulai dengan Bab I Pendahuluan yang terdiri dari Latar Belakang, Perumusan Masalah, Tujuan Penulisan, Batasan Masalah, dan Sistematika Penulisan.

Bab II menunjukkan tentang landasan teori yang akan digunakan dalam pembahasan polinomial permutasi.

Polinomial permutasi dibahas pada Bab III yang dimulai dengan polinomial permutasi di *ring* $\mathbb{Z}_n$ dan dilanjutkan dengan polinomial Chebyshev yang merupakan contoh dari polinomial permutasi di *ring* $\mathbb{Z}_n$.

Bab IV membahas kesimpulan dari pembahasan polinomial permutasi.