# BAB I
# PENDAHULUAN

## 1.1 Latar Belakang

Kriptografi memegang peranan yang penting seiring dengan perkembangan teknologi informasi dan komunikasi. Adanya internet membuat komunikasi jarak jauh menjadi cepat, mudah dan murah. Namun keberadaannya sebagai media komunikasi umum memungkinkan setiap orang untuk bisa mengaksesnya secara bebas sehingga menjadi sangat rentan terhadap penyadapan informasi yang dilakukan oleh pihak-pihak tak berwenang. Salah satu hal yang penting untuk menjamin keamanan informasi yang dilakukan melalui komputer dan jaringan adalah *cipher* dengan menggunakan algoritma kriptografi untuk mengkodekan pesan asli menjadi sebuah *ciphertext* yang sulit dimengerti (Budiyono, 2004).

Di sisi lain, beberapa teori dalam aljabar abstrak khususnya teori mengenai *quasigroup* telah dikembangkan secara luas mulai dari bentuk integrasinya dengan disiplin ilmu lain hingga aplikasinya dalam berbagai bidang. Menurut Yuliawan (2012), banyak teori *quasigroup* yang telah diterapkan dalam steganografi, teori pengkodean, dan kriptografi.

Sebagian ilmuwan yang meneliti terapan teori *quasigroup* dalam kriptografi adalah Smile Markovsky, Danilo Gligoroski dan Suzana Andova pada tahun 1997 melalui makalahnya yang berjudul *Using Quasigroups for One-one Secure Encoding*. Dalam makalah tersebut dibahas manfaat *quasigroup* untuk membentuk suatu kunci rahasia dalam algoritma kriptografi konvensional yang disebut dengan *quasigroup cipher*. Pembentukan *quasigroup cipher* dalam makalah ini diawali oleh proses pembangkitan *quasigroup* dengan menggunakan *latin square*. Pada tahun 2005, Jordan Bell melalui jurnalnya yang berjudul *An Introduction to SDR's and Latin Squares* menjelaskan salah satu aplikasi *latin square* dalam pengkonstruksian suatu tabel operasi agar diperoleh sebuah *quasigroup*.

Hasil penelitian yang dilakukan oleh para ilmuwan di atas mengenai proses pembangkitan *quasigroup* dengan menggunakan *latin square* dan pembentukan *quasigroup cipher* dijelaskan

dalam Bab Pembahasan pada skripsi ini. Selain itu akan dicantumkan pula beberapa pembuktian teorema dan lemma yang berhubungan dengan *latin square* dan *quasigroup*.

## 1.2 Rumusan Masalah

Berdasarkan uraian latar belakang di atas, dapat disusun beberapa rumusan masalah sebagai berikut.

1) Bagaimanakah cara mengkonstruksi *quasigroup* dengan menggunakan *latin square*?
2) Bagaimanakah cara mengkonstruksi kunci rahasia dalam bentuk *quasigroup cipher*?
3) Bagaimanakah cara mengkonstruksi fungsi *encipher* dan *decipher* dengan menggunakan *quasigroup cipher*?
4) Apakah kelebihan dan kelemahan metode kunci rahasia dengan menggunakan *quasigroup cipher*?

## 1.3 Tujuan Penulisan

Adapun tujuan penulisan skripsi ini adalah sebagai berikut.

1) Menjelaskan cara mengkonstruksi *quasigroup* dengan menggunakan *latin square*.
2) Menjelaskan cara mengkonstruksi kunci rahasia dalam bentuk *quasigroup cipher*.
3) Menjelaskan cara mengkonstruksi fungsi *encipher* dan *decipher* dengan menggunakan *quasigroup cipher*.
4) Menjelaskan kelebihan dan kelemahan metode kunci rahasia dengan menggunakan *quasigroup cipher*.