BAB IV
KESIMPULAN DAN SARAN

4.1 Kesimpulan

Setiap *latin rectangle* berukuran $k \times n$ dapat dilengkapkan menjadi *latin square* berukuran $n \times n$ dengan menambahkan baris secara bertahap. Dari proses ini diperoleh sedikitnya $n!\,(n-1)!\ldots 1!$ buah *latin square*. Dengan menambahkan *headline* dan *sideline* pada masing-masing *latin square*, akan dihasilkan sebanyak $n!\,(n-1)!\ldots 1!$ buah tabel *quasigroup* dengan himpunan pembangun yang sama namun operasi binernya berbeda.

Secara umum, *quasigroup cipher* terdiri atas enam buah komponen penyusun yakni himpunan alfabet A, operasi biner $*$, operasi biner $\backslash$ atau $/$, fungsi uner f_*, fungsi uner $f_\backslash$ atau $f_/$, dan *leader* a_1 yang berupa elemen sebarang di dalam A. *Quasigroup cipher* kiri dinotasikan dengan $(A,*,\backslash,a_1,f_*,f_\backslash)$, sedangkan *quasigroup cipher* kanan dinotasikan dengan $(A,*,/,a_1,f_*,f_/)$.

Komposisi antara fungsi *encipher* dan *decipher* akan menghasilkan suatu pemetaan identitas. Karena $f_\backslash \circ f_*$ dalam *quasigroup cipher* kiri menghasilkan pemetaan identitas di A^+, maka diambil $f_e = f_*$ sebagai fungsi *encipher* dan $f_d = f_\backslash$ sebagai fungsi *decipher*. Begitu juga dalam *quasigroup cipher* kanan, karena $f_/ \circ f_*$ menghasilkan pemetaan identitas di A^+, maka diambil $f_e = f_*$ sebagai fungsi *encipher* dan $f_d = f_/$ sebagai fungsi *decipher*.

Quasigroup cipher cocok untuk komunikasi *online*, tahan akan error, memiliki keamanan yang relatif kuat, serta dapat dikonstruksikan dalam jumlah yang banyak. *Quasigroup cipher* akan diketahui dengan mudah jika penyelundup mengetahui *plaintext* dan *ciphertext*. Untuk menanggulangi kelemahan ini, digunakanlah dua buah *quasigroup cipher* atau lebih sebagai kunci untuk proses *encipher* dan *decipher*. Semakin banyak jumlah *quasigroup cipher* yang digunakan, maka metode ini akan semakin aman.

4.2 Saran

Skripsi ini menjelaskan proses pembangkitan *quasigroup*, proses pembentukan *dual quasigroup*, proses *encipher* dan proses *decipher* secara manual. Akan membutuhkan waktu yang lama untuk mengkonstruksi *quasigroup cipher* dengan himpunan pembangun yang memiliki banyak elemen atau untuk mengkodekan *plaintext* yang sangat panjang. Bagi pembaca yang ingin membahas lebih lanjut tentang topik serupa, disarankan untuk merancang sebuah program dengan bahasa komputer guna mempercepat proses-proses tersebut.

Skripsi ini hanya membahas tentang aplikasi *quasigroup* dalam algoritma kriptografi konvensional. Pada kenyataannya, dalam beberapa makalah dijelaskan bahwa *quasigroup* juga dapat diterapkan dalam algoritma kriptografi kunci publik sehingga dapat dijadikan topik baru untuk penelitian dan analisis ke depannya.