APLIKASI *QUASIGROUP* DALAM PEMBENTUKAN KUNCI RAHASIA PADA ALGORITMA KRIPTOGRAFI KONVENSIONAL

ABSTRAK

Skripsi ini membahas tentang cara mengkonstruksi *latin square* untuk memperoleh *quasigroup* dengan menggunakan modifikasi teorema Marshal Hall. Dengan menambahkan *headline* dan *sideline* pada *latin square* dapat diperoleh tabel operasi *quasigroup*. *Quasigroup* memiliki sifat yang berguna dalam proses *encipher* dan *decipher* sehingga bisa dijadikan kunci rahasia yang kemudian disebut *quasigroup cipher*. *Quasigroup cipher* kanan terdiri atas enam buah komponen penyusun yakni himpunan alfabet *A*, operasi biner $*$ dan $/$, fungsi uner f_* dan $f_/$, serta *leader* a_1 yang berupa elemen sebarang di dalam *A*. *Quasigroup cipher* kiri juga terdiri atas enam buah komponen penyusun, perbedaannya dengan *quasigroup cipher* kanan terletak pada operasi biner dan fungsi uner yang digunakan yakni operasi biner $*$ dan $\backslash$, serta fungsi uner f_* dan $f_\backslash$. Komposisi dua fungsi uner dalam *quasigroup cipher* kanan dan kiri menghasilkan suatu pemetaan identitas, sehingga salah satu dijadikan sebagai fungsi *encipher* dan yang lainnya sebagai fungsi *decipher*. Metode kunci rahasia ini memiliki beberapa kelebihan diantaranya: pertama, *quasigroup cipher* dapat dikonstruksikan dalam jumlah yang banyak, kedua, cocok untuk komunikasi *online*, ketiga, tahan akan error, keempat, memiliki keamanan yang relatif kuat. Namun terdapat kelemahan jika penyelundup mengetahui *plaintext* dan *ciphertext*, maka *quasigroup* dapat diketahui dengan mudah. Untuk menanggulangi kelemahan ini, digunakanlah dua buah *quasigroup cipher* atau lebih sebagai kunci untuk proses *encipher* dan *decipher*.

Kata kunci : *quasigroup*, *quasigroup cipher*, *latin square*, kunci rahasia.