ABSTRAK

Sistem data Encryption dengan kunci publik atau lebih dikenal dengan sebutan sistem kripto dengan kunci publik, yang memiliki keunggûlan dalam pengaturan kunci dibanding dengan metode data *Encryption* yang konvensional. Metode data *encryption* yang konvensional hanya memiliki satu kunci yang digunakan untuk men-*encrypt* juga digunakan untuk men-*decrypt*. Sehingga kebutuhan kunci pada suatu jaringan komputer dengan n *user* punya kompleksitas $O(n^2)$. Sedangkan sistem kripto dengan kunci publik, kunci untuk men-*encrypt* tidak digunakan untuk men-*decrypt* karena masing-masing memiliki kunci sendiri-sendiri. Dan kebutuhan kunci pada suatu jaringan dengan n *user* punya kompleksitas O(n). Selain keunggulan dalam pengaturan kunci, sistem data *Encryption* dengan kunci publik ini menjamin keaslian pesan yang dikirim oleh seorang *user*.

Penulis membuat program pengiriman pesan pada jaringan (LAN) dengan menggunakan metode RSA (Rivest-Shamir-Adleman) dalam bahasa pemrograman Turbo Pascal, yang dijalankan dengan sistem operasi NetWare pada Lokal Area Network, sehingga dapat digunakan oleh setiap *user* yang telah mendaftarkan dirinya untuk memakai fasilitas pengiriman pesan.