ABSTRAK

Algoritma caesar merupakan sistem persandian klasik berbasis substitusi yang sederhana pada enkripsi dan dekripsi sebuah sistem persandian caesar menggunakan operasi shift. Operasi shift adalah mensubstitusi suatu huruf menjadi daftar alfabet berbeda yang digunakan untuk keamanan dan kerahasiaan pesan untuk mengubah pesan asli (Plainteks) menjadi chiperteks agar tidak dapat dibaca pesan aslinya. Hal ini telah tebukti pada saat zaman Romawi kuno dikisahkan pada suatu saat, ketika Julius Caesar ingin mengirimkan satu pesan rahasia kepada orang Jendral di medan perang. Pesan tersebut harus dikirimkan melalui seseorang kurir, tetapi karena pesan tersebut mengandung rahasia, Julius Caesar tidak ingin pesan tersebut terbuka ditengah jalan. Di sini Julius Caesar memikirkan bagaimana mengatasinya yaitu dengan cara mengacak pesan tersebut menjadi suatu pesan yang tidak dapat dipahami oleh siapapun kecuali hanya dapat dipahami oleh Jenderalnya saja. Tentu sang Jendral telah diberi tahu sebelumnya cara membaca pesan yang teracak tersebut, karena telah mengetahui kuncinya. Yang dilakukan Julius Caesar adalah mengganti semua susunan alfabet. Maka dalam hal ini untuk menguji coba mengimplementasikan antara Algoritma caesar dengan chatting, agar tidak dapat dibaca pesan aslinya dalam pengiriman dan menerima pesan pada saat berada dalam lalulintas jaringan.

Kata Kunci : Algoritma caesar, Chatting, Enkripsi, Dekripsi, Client-Server, LAN (Local Area Network).