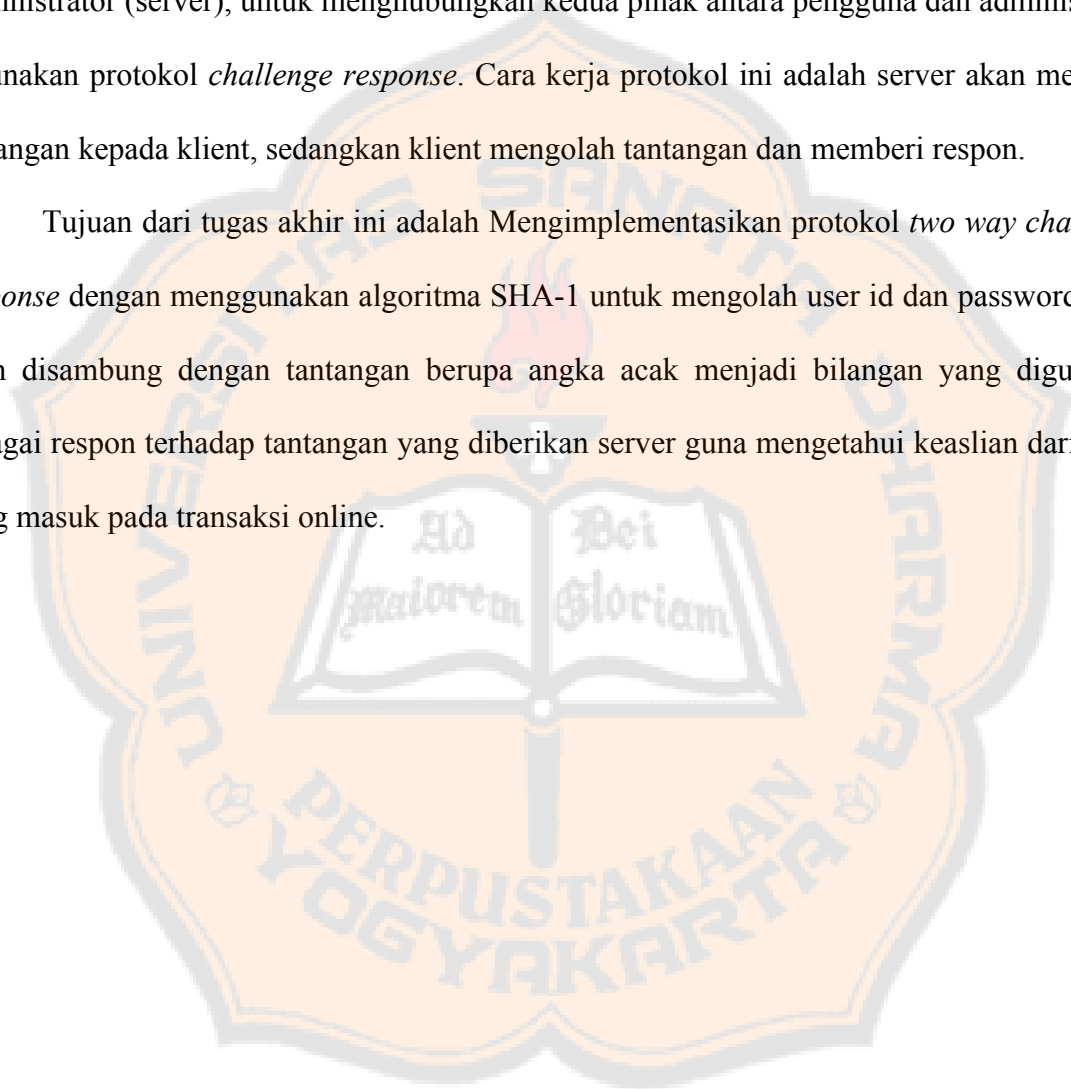


INTISARI

SHA 1 adalah salah satu algoritma fungsi has untuk proses enkripsi, pada sistem autentikasi ini dibangun untuk dua pihak yaitu pihak pengguna (klient) dan pihak administrator (server), untuk menghubungkan kedua pihak antara pengguna dan administrator digunakan protokol *challenge response*. Cara kerja protokol ini adalah server akan memberi tantangan kepada klient, sedangkan klient mengolah tantangan dan memberi respon.

Tujuan dari tugas akhir ini adalah Mengimplementasikan protokol *two way challenge response* dengan menggunakan algoritma SHA-1 untuk mengolah user id dan password yang akan disambung dengan tantangan berupa angka acak menjadi bilangan yang digunakan sebagai respon terhadap tantangan yang diberikan server guna mengetahui keaslian dari klien yang masuk pada transaksi online.



ABSTRACK

SHA 1 is one of the any other hash algorithm to encryption, this authentication system was built for two sides namely client side and server side, challenge response protocol is used to connect between client and server. In this challenge response protocol, server will give challenge to client, and client will generate challenge and send response.

The purpose of this final assignment is to see the implementation of challenge response protocol with used SHA 1 algorithm for generate user id and password with challenge like random number to be response as challenge be given by server to know authenticity from client in online transaction.

