Crypto 2

Client C and server S share a secret password P. Furthermore, client C knows the server S' public key pubKS. Design a key establishment protocol that fulfils key authentication, key confirmation and is robust w.r.t. replay attack. Assume that client C and server S clocks are not synchronized.