Crypto 2

Client C and server S share a secret password P. Furthermore, client C knows the server S' public encryption 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.

SOLUZIONE

M1: S→C : S, C, nS
M2: C → S : C, E_{pubKS}(C, S, P, nS, nC, K).
M3: S→C : S, E_K(S, C, H(nC), nS)

In case KCS is compromised, the attacker gets hold on H(nC) but not nC. So the attacker cannot perform a password attack against M2.