Protocole Cryptographique

A → S : A , senc (< < < A , B > , K > , Na1 > , Kas) **(1)**

S → B : S , senc (< < < A , S > , K > , Ns1 > , Kbs) **(2)**

B → S : B , senc (< < senc (< B , C > , K) , B > , Nb > , Kbs) **(3)**

S → A : S , senc (< senc (< B , C > , K) , Ns2 > , Kas) **(4)**

A → S : A , senc (< C , Na2 > , Kas) **(5)**

S → B : S , senc (< C , Ns2 > , Kbs) **(6)**

Coût

(1) : 157
(2) : 157
(3) : 159
(4) : 107
(5) : 55
(6) : 55

Total : 690

A : Alice

B : Bob

S : Serveur

K : Clé Partagée

Kas : Clé de Session entre A et S

Kbs : Clé de Session entre B et S

Na1, Na2, Nb, Ns1, Ns2 : Nonces