Conception et analyse de protocoles cryptographiques

Protocole

A→S: A, senc(<<<A,B>,K>,Na>,Kas) (1)
S→B : S, senc(<<<A,S>,K>,Ns1>,Kbs) (2)
B →S : B, senc(<<senc(B,K),B>,Nb>,Kbs) (3)
S →A : S, senc(<senc(B,K),Ns2>,Kas) (4)

A : Alice
B : Bob
S : Serveur
K : clé secrète partagée
Na, Nb, Ns1, Ns2 : des valeurs générées par les émetteurs respectifs afin d'indiquer la date et l'heure à laquelle ils ont envoyé le message.

Coût

(1) = 157
(2) =157
(3) =157
(4) =57

(1)+(2) +(3) +(4)=528

Adeny Yannick Evrad
Youssef Zitan
Mamadou Bassirou Diallo