# LePoteauColle

Na, Nb sont des clefs générées aléatoirement pour chaque nouvel échange :

A -> B : {A,Na}pub(B)

B -> A : B, h(Na,B), {Nb}pub(A)

A -> B : A, h(Nb),{secret}Na

B -> A : B, h(secret)

Coût:

52 + 12 + 19 + 7 = 90

Commentaire :

1 – A envoi son identité et un nonce à B chiffré avec la clef publique de B. B récupère Na et associe le nonce à sa communication avec A. A et B ajoutent le tuple (A,B,Na) à leur table.

2 – B répond à A avec son identité, le hash du nonce et son identité (B) suivit d'un autre nonce chiffré avec la clef public de A. A vérifie avec h(Na,B) que le tuple (A,B,Na) existe dans sa table. Si le tuple existe, A ajoute Nb au tuple.

3 – A envoi son secret en envoyant d'abord son identité en claire, suivit du nonce de B et le secret chiffré avec Na qui joue le rôle de clef symétrique. Avant d'accepter le secret, B vérifie le h(Nb) associé à la communication avec A, puis déchiffre le secret avec le Na du tuple associé.

4 – Pour finir B renvoi le hash du secret avec son identité. A vérifie que le hash du secret envoyé à B est bon avant de valider l'échange.

A la fin de l'échange, A et B partagent « secret » qui est resté confidentiel.