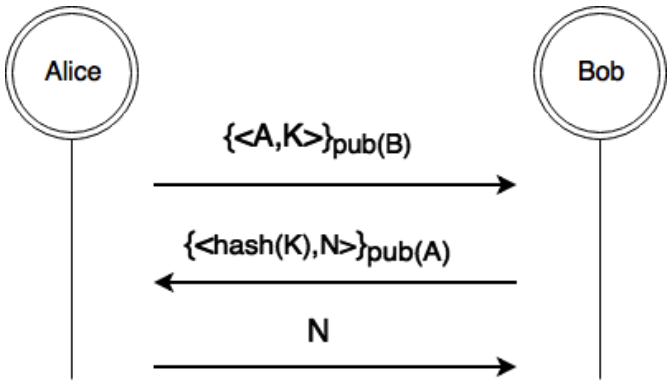
Réalisation d'un protocole de sécurité

HUANG Manutea
LEVEQUE Lucile
LE GORANDE Raphaël

Novembre 2018

1 Le protocole



Connaissances initiales : Au début du protocole, on suppose que les agents A et B connaissent la clef publique pub(C) associée à l'agent C, pour tout agent C.

Description du protocole : À la première étape du protocole, l'agent Alice envoie son nom A et la donnée K. Ce message est chiffré par un algorithme de chiffrement asymétrique avec la clef publique de B (notée pub(B)), c'est-à-dire que seul l'agent Bob connaît la clef privée correspondant à la clef pub(B).

À la deuxième étape du protocole, Bob reçoit le message envoyé par Alice. Comme il a la clef privée lui permettant d'ouvrir le message, il renvoie à Alice un hash des données ainsi qu'un nonce N, le tout chiffré avec la clef publique pub(A) d'Alice.

À la troisième étape du protocole, Alice déchiffre le message reçu puis renvoie à Bob le nonce N dont elle a désormais connaissance.

Propriétés de sécurité :

- *Authentification* : L'identité A est présente dans le premier message, et le nonce renvoyé lors de la dernière étape ne peut être obtenu que par Alice en connaissance de sa clef privée (permettant de déchiffrer le message 2).
- *Confidentialité* : Les deux agents Alice et Bob sont seuls à connaître la donnée K.

1.1 Calcul du coût

Le coût de ce protocole est calculé à partir des fonctions données en énoncé. Ici il est de $54 + 58 + 1 = \mathbf{113}$.