# Description du protocole de ATEAM

$$A \rightarrow B : \{A, N_a\}_{pub(B)}$$
$$B \rightarrow A : h(N_a), \{N_b\}_{pub(A)}$$
$$A \rightarrow B : h(N_b)$$

**Connaissances initiales :** Au début du protocole,on suppose que les agents A et B connaissent la clé publique pub(C) associée à l'agent C, pour tout agent C. On suppose également que tout agent C connaît la méthode de hachage utilisée dans ce protocole.

**Valeurs générées au cours du protocole :** $N_a$ et $N_b$ sont des nonces générés respectivement par A et B. $N_b$ correspond alors à la clé échangée entre A et B.

**Description du protocole :**

À la première étape, Alice envoie son nom A et un nombre aléatoire $N_a$. Ce message est chiffré par un algorithme de chiffrement asymétrique avec la clé publique de Bob, notée pub(B). Ainsi, seul l'agent Bob est en mesure d'utiliser la clé privée associée à la clé publique pub(B).

À la deuxième étape du protocole, Bob reçoit le message $\{A, N_a\}_{pub(B)}$ envoyé par Alice. Comme il a la clé privée lui permettant d'ouvrir le message, il lui renvoie le haché de nonce d'Alice ($N_a$) suivi d'un nouveau nonce $N_b$ qu'il vient d'engendrer qu'il chiffre alors avec la clé publique d' Alice, notée pub(A).

À la troisième étape du protocole, Alice reçoit le message $\{N_b\}_{pub(A)}$ et le haché de son nonce $N_a$ ainsi en hachant son nonce, elle vérifie que le haché envoyé par B est bien identique au sien. Elle envoie donc le haché du nonce $N_b$ à B.

**Propriété de sécurité :**

- *Authentification* : Alice étant la seule (autre que Bob) à connaître $N_b$, en renvoyant son haché, elle permet à Bob de s'assurer que c'est elle qui a reçu son nonce.
- *Confidentialité* : Seul Alice et Bob connaissent le nonce $N_b$.

**Coût du protocole :**

Règle 1 : 1 + 50 + 1 + 1 + 1 = 54
Règle 2 : 5 + 1 + 1 +1 +1 = 9
Règle 3 : 5 + 1 = 6
Total = 69