Description du protocole de ATEAM v4

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

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.

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 chiffrés 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 peut récupérer le nonce d'Alice : N_a. Il envoie ensuite le nonce N_b , qu'il a généré, d'abord symétriquement avec le nonce N_a le tout chiffré asymétriquement avec la clé publique d' Alice, notée pub(A).

À la troisième étape du protocole, Alice peut déchiffrer le message envoyé par Bob et récupérer ainsi le nonce N_b. Elle envoie pour finir un acquittement en envoyant le haché de N_b.

Propriété de sécurité :

- *Authentification* : Si le protocole abouti, on est certains que Alice a bien communiqué avec Bob et inversement.
- *Confidentialité* : Alice et Bob sont les seuls à connaître les nonce N_b et N_a .

Coût du protocole :

Règle 1 : 1 + 1 + 1 + 1 + 50 = 54
Règle 2 : 1 +10 + 1 + 1 + 1 = 14
Règle 3: 1 + 5 = 6
Total = 74