

Description du protocole de ATEAM v5

$$\begin{aligned}A &\rightarrow B : \{A, N_a\}_{\text{pub}(B)} \\B &\rightarrow A : \{B\}_{N_b}, \{\{N_b\}_{N_a}\}_{\text{pub}(A)} \\A &\rightarrow B : h(N_b)\end{aligned}$$

Connaissances initiales : Au début du protocole, on suppose que les agents A et B connaissent la clé publique $\text{pub}(C)$ 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 $\text{pub}(B)$. Ainsi, seul l'agent Bob est en mesure d'utiliser la clé privée associée à la clé publique $\text{pub}(B)$.

À la deuxième étape du protocole, Bob reçoit le message $\{A, N_a\}_{\text{pub}(B)}$ 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 son nom, chiffré symétriquement par le nonce N_b , qu'il a généré, avant d'envoyer ce même nonce chiffré symétriquement avec le nonce N_a puis asymétriquement avec la clé publique d'Alice, notée $\text{pub}(A)$.

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

Propriété de sécurité :

- *Authentication* : 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 : $1 + 1 + 10 + 1 + 10 + 1 + 1 + 1 = 26$

Règle 3: $1 + 5 = 6$

Total = 86