Description du protocole de ATEAM v2

$$A \rightarrow B : \{A, N_a\}_{pub(B)}$$
$$B \rightarrow A : sym\{N_a\}_{nb}, \{N_b\}_{pub(A)}$$
$$A \rightarrow B : sym\{secret\}_{nb}$$

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 lui renvoie le nonce d'Alice (N_a) chiffré symétriquement avec un nouveau nonce N_b qu'il vient d'engendrer qu'il envoie de manière chiffré assymétriquement 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 chiffré de son nonce N_a, généré symétriquement avec la clef N_b. Ainsi en déchiffrant le chiffré symétrique avec la clef N_b trouvé dans le message chiffré avec sa clef publique, elle vérifie que le nonce N_a envoyé par B est bien identique à celui envoyé dans la première étape. Elle envoie donc le secret en le chiffrant symétriquement avec le nonce N_b.

Pour finir, on considère que A n'enverra jamais N_a comme secret à B. Si B reçoit un secret ayant comme contenu N_a il l'ignore sachant qu'il pourrait provenir d'une autre personne (trivial).

Propriété de sécurité :

- *Authentification* : Alice étant la seule (autre que Bob) à connaître N_a, lorsque B transmet N_a chiffré symétriquement avec N_b il lui permet de s'assurer que B à bien reçu son nonce et qu'il est bien à l'origine du tout juste message reçu.
- *Confidentialité* : Seul 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 : 10 + 1 + 1 + 1 + 1 + 1 = 15
Règle 3 : 10 + 1 + 1 = 12
Total = 81