Soit le protocole de sécurité suivant :

$A \rightarrow B : A$

$B \rightarrow S : B, \{A, N_b\}k_{bs}$

$S \rightarrow A : \{B, N_b, k_{ab}\}k_{as}, \{K_{ab}\}k_{bs}$

$A \rightarrow B : \{k_{ab}\}k_{bs}, \{N_b, N_a\}k_{ab}$

$B \rightarrow A : \{N_a\}k_{ab}$

Connaissances initiales :

Au début du protocole, on suppose que les agents A et B ont une clef symétrique partagée avec un serveur S.

Valeurs générées au cours du protocole :

– N_a est un nonce généré par A.

– N_b est un nonce généré par B.

– K_{ab} est une clé générée par le serveur S

Description du protocole :

L'agent A demandé à l'agent B d'engager une conversation avec lui en envoyant son identité A.

L'agent B va envoyer au serveur son identité pour que le serveur sache de qui provient le message ainsi qu'un message chiffré symétriquement avec la clé k_{bs} contenant l'identité de A pour que le serveur sache à qui envoyer le prochain message et le nonce de l'agent B.

Le serveur envoie un message chiffré symétriquement avec la clé k_{as} contenant l'identité de B, le nonce de B et une clé symétrique $k_{ab,}$ et un message chiffré symétriquement avec la clé k_{bs} contenant la clé symétrique $k_{ab.}$

L'agent A va envoyer le message chiffré symétriquement avec la clé k_{bs} contenant la clé symétrique k_{ab} reçu précédemment ainsi qu'un message chiffré symétriquement avec la clé k_{ab} contenant le nonce de B et un nonce généré par A.

B va d'abords déchiffré le premier message avec la clé k_{bs} pour récupérer la clé k_{ab} puis va déchiffre le second message voir que le premier nonce est le sien pour ensuite renvoyer le deuxième nonce à l'agent A chiffré avec la clé k_{ab}

Propriétés de sécurité :

– Authentification : Lorsque Bob reçoit l'avant dernier message il sait qu'il parle à Alice et Alice sait qu'elle parle à Bob quand elle reçoit le dernier message car seul Bob peut déchiffrer le message contenant la clé secrète et donc retourner N_a.

– Confidentialité : Les deux agents Alice et Bob sont seuls à connaître la clé k_{ab}.

Poids du protocole : 278

– Règle 1 : 1

– Règle 2 : 1 + 10 + 50 + 1 + 1 + 1 = 64

– Règle 3 : 10 + 50 + 1 + 50 + 1 + 1 + 1 + 10 + 1 + 1 = 126

– Règle 4 : 10 + 1 +1 + 10 + 50 + 1 + 1 + 1 = 75

– Règle 5 : 10 + 1 + 1 = 12