VERSION 1 DU PROTOCOLE DES VOLEURS DE POMMES

Nous proposons le protocole suivant :

$$\begin{array}{ll} A \to S : & < A, \text{enc}(< B, k >, k_{AS}) > \\ S \to B : & < S, \text{enc}(< k, A >, k_{BS}) > \\ B \to A : & < B, \text{enc}(B, k) > \end{array}$$

Connaissances initiales des agents : Initialement on considère que le serveur de confiance S est un agent honnête et qu'il partage avec chaque agent A_i une clé de chiffrement symétrique notée k_{A_iS}

Description du protocole :

- A commence par créer une clé symétrique k. Il veut la partager avec B. Il commence par envoyer au serveur S une paire constituée de son identité et d'un message chiffré avec k_{AS}, à savoir la paire (identité du destinataire de la clé qui est ici B, clé k).
- Après déchiffrement de ce premier message, le serveur se retrouve en possession de k et du destinataire souhaité par A de cette clé, ici B. Le serveur envoie alors à B un message chiffré avec k_{BS}, à savoir la paire (clé k avec laquelle A veut communiquer, identité de la personne qui veut communiquer avec B qui est ici A) accompagné de son identité S.
- Après réception de ce message, B le déchiffre et se retrouve en possession de la clé k. Il envoie alors un message de confirmation à A : son identité et son identité chiffrée avec k, maintenant connue de A et de B.

On remarque que les messages chiffrés lors du premier et du deuxième échange ne sont plus de la même forme (puisque n'importe qui peut distinguer le nom d'un agent d'une chaîne correspondant à une clé) ce qui brise la symétrie qui permettait aux attaques de Balec et Brocoli de fonctionner.

Propriétés de sécurité : Ce sont les trois points exigés dans l'énoncé du projet.

Coût du protocole : Le coût de ce protocole version 1 n'est pas changé par rapport à la version 0. En effet, nous avons simplement échangé les places de k et A dans le deuxième échange.
Coût de la première règle = 50 + 1 + 1 + 1 + 1 + 1 = 55
Coût de la deuxième règle = 50 + 1 + 1 + 1 + 1 + 1 = 55
Coût de la troisième règle = 1 + 1 + 1 + 1 = 4
Coût total du protocole = 114