

## DESCRIPTION DU PROTOCOLE DES VOLEURS DE POMMES

Nous proposons le protocole suivant :

$$\begin{aligned} A \rightarrow S : & \quad < A, \text{enc}(< B, k >, k_{AS}) > \\ S \rightarrow B : & \quad < S, \text{enc}(< A, k >, k_{BS}) > \\ B \rightarrow A : & \quad < B, \text{enc}(B, k) > \end{aligned}$$

**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 (identité de la personne qui veut communiquer avec B qui est ici A, clé  $k$  avec laquelle A veut communiquer) 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.

Les trois étapes de notre protocole suivent le schéma suivant :

expéditeur  $\rightarrow$  destinataire : (identité de l'expéditeur, message chiffré avec une clé commune à l'expéditeur et au destinataire).

De cette façon, le destinataire peut savoir avec quelle clé déchiffrer le message composant le deuxième membre de la paire. Si jamais la clé du premier membre du message ne permet pas de déchiffrer le deuxième membre du message (cad la clé associée à l'identité annoncée dans le message et la clé utilisée pour chiffrer le deuxième morceau du message ne correspondent pas), le destinataire détecte que le message est mal formé et le protocole est interrompu.

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

**Coût du protocole :** On rappelle que les paires "extérieures" ne sont pas sujettes au malus de 50.

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