Description du protocole du groupe *Protocool*

Lucas THOMAS, Matthieu PHAM et Emmanuel PERRIN

7 Octobre 2020

Notre protocole d'échange de clé secrète se décrit de la façon suivante :

$$\begin{array}{ll} A \longrightarrow B : & \{A, K\}_{pub(B)} \\ B \longrightarrow A : & \{\{N\}_{h(\{K\}_{pub(A)})}\}_{pub(A)} \\ A \longrightarrow B : & \{N\}_K \\ B \longrightarrow A : & \{K\}_{pub(A)} \end{array}$$

Connaissances initiales : Au début du protocole, on suppose que les agents A et B partagent deux clés : la clé publique pub(A) associée à A et pub(B) associée à B. Les agents A et B ont donc chacun également une clé privée associée : prv(A) et prv(B).
K est le message à envoyer (la clé secrète à échanger avec B).

Valeurs générées au cours du protocole : N est un nonce généré par B.

Description du protocole :

1. À la première étape du protocole, l'agent Alice envoie son nom A et le secret K à B, le tout chiffré avec $pub(B)$.

2. Bob génère un le nonce N et le chiffre avec le hash de K chiffré avec la clé publique de A puis chiffre le tout avec la clé publique de A (car c'est l'identifiant de l'envoyeur qu'il a reçu a l'étape une). Cela sert de challenge pour l'identification de A.

3. Alice reçoit le message de bob et déchiffre le tout et obtient le nonce N. Ce nonce N est correcte que si il est correctement déchiffré. Alice renvoie le nonce à Bob, chiffré avec le secret K. Cet échange permet l'authentification car seul B connaît N, c'est la réponse au challenge.

4. Bob envoie la clé comme acquittement si A à bien réussi le challenge (c'est à dire que B a reçu le bon nonce).

Propriétés de sécurité :

- Si B a fini pensant avoir reçu une clé K venant de A, alors A a bien envoyé K à B
- Si A a fini en ayant envoyé une clé K à B, alors B a bien reçu K de la part de A.
- La clé K est secrète entre A et B.

Poids du protocole : 90

- Règle 1 : $1 + 50 + 2 + 1 = 54$
- Règle 2 : $3 + 10 + 5 + 3 = 21$
- Règle 3 : $10 + 2 = 12$
- Règle 4 : $1 + 1 + 1 = 3$