

# Description du protocole du groupe *Protocol*

Lucas THOMAS, Matthieu PHAM et Emmanuel PERRIN

7 Octobre 2020

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

$$\begin{aligned} A &\longrightarrow S : A, B \\ S &\longrightarrow A : \{N\}_{ksa} \\ S &\longrightarrow B : \{N, A\}_{ksb} \\ A &\longrightarrow B : \{N, K\}_{\text{pub}(B)} \\ B &\longrightarrow A : \{N\}_{\text{pub}(A)} \end{aligned}$$

**Connaissances initiales :** Au début du protocole, on suppose que les agents  $A$  et  $B$  partagent deux clés : la clé publique  $\text{pub}(A)$  associée à  $A$  et  $\text{pub}(B)$  associée à  $B$ . Les agents  $A$  et  $B$  ont donc chacun également une clé privée associée :  $\text{prv}(A)$  et  $\text{prv}(B)$ .

On suppose aussi que  $A$  et  $B$  partagent chacun une clé symétrique avec le serveur  $S$  respectivement  $ksa$  et  $ksb$ .

$K$  est le message à envoyer (la clé secrète à échanger avec  $B$ ).

**Valeurs générées au cours du protocole :**  $N$  est un nonce généré par  $S$  pour  $A$  et  $B$ .

**Description du protocole :** À la première étape du protocole, l'agent Alice envoie son nom  $A$  et le nom de l'agent Bob  $B$  au serveur  $S$ .

Le serveur envoie à  $A$  un nonce  $N$  chiffré par la clé symétrique  $ksa$ . Ce  $N$  servira en quelque sorte d'identifiant de connexion.

Le serveur envoie ensuite à  $B$  le nonce et  $A$  chiffré par  $ksb$ .

Alice envoie alors  $N$  et  $K$  à Bob en les chiffrant avec la clé publique de Bob :  $\text{pub}(B)$ . Bob pourra déchiffrer avec sa clé privée  $\text{prv}(B)$ .

Enfin, Bob, ayant reconnu  $N$ , répond à Alice  $N$  chiffré par  $\text{pub}(A)$ . Cet échange remplit la fonction d'un acquittement.

**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 :** 135

- Règle 1 :  $1 + 1 = 2$
- Règle 2 :  $10 + 1 + 1 = 12$
- Règle 3 :  $50 + 1 + 1 + 10 + 1 + 1 = 64$
- Règle 4 :  $50 + 1 + 1 + 1 + 1 = 54$
- Règle 5 :  $1 + 1 + 1 = 3$