

## Protocoles de sécurité

### Description du protocole des cotesdeporc

Moser Meven - Thébault Adrien - Trebon Landry

## Description du protocole de l'équipe cotesdeporc v1

Le protocole de l'équipe cotesdeporc à clef publique se décrit de la façon suivante :

$$\begin{aligned} A \rightarrow B : & \quad \langle A, \{N_1\}_{\text{pub}(B)}, \{K\}_{\text{pub}(B)}, h(\langle A, K \rangle) \rangle \\ B \rightarrow A : & \quad \langle \{N_2\}_{\text{pub}(A)}, h(\langle K, N_1, N_2, B \rangle) \rangle \\ A \rightarrow B : & \quad N_2 \end{aligned}$$

**Connaissances initiales :** au début du protocole, on suppose que les agents  $A$  et  $B$  connaissent la clef publique  $\text{pub}(C)$  associée à l'agent  $C$ , pour tout agent  $C$ .

### Valeurs générées au cours du protocole :

- $N_1$  est un nonce généré par  $A$
- $N_2$  est un nonce généré par  $B$

### Description du protocole :

Au début du protocole,  $A$  envoie à  $B$  le quadruplet contenant son identité, un nonce  $N_1$  chiffré avec la clef publique de  $B$ , le secret  $K$  chiffré avec la clef publique de  $B$  et un hash de la paire contenant l'émetteur ( $A$ ) et le secret  $K$ .

Lorsque  $B$  reçoit ce message, il déchiffre  $N_1$  et  $K$  et calcule le hash de la paire  $\langle A, K \rangle$  puis le compare avec celui qu'il a reçu. Si cela correspond, il répond avec une paire contenant un nonce  $N_2$  chiffré avec la clef publique de  $A$  et le hash du quadruplet contenant le secret  $K$ , le nonce  $N_1$  reçu précédemment, le nonce  $N_2$  qu'il a généré et son identité.

$A$  déchiffre ensuite  $N_2$ , calcule le hash du quadruplet  $K, N_1$  (qu'il a conservé en mémoire),  $N_2, B$  et le compare avec celui reçu. Si les hash sont égaux, il renvoie le nonce  $N_2$  à  $B$ .

Lorsque  $B$  reçoit  $N_2$ , il le compare avec celui qu'il a généré, s'ils sont égaux alors le protocole est terminé correctement.

### Propriétés de sécurité :

- *Confidentialité* : la donnée  $K$  reste secrète entre  $A$  et  $B$
- *Authentification* : à la fin du protocole,  $B$  est sûr que le secret  $K$  vient de  $A$
- A la fin du protocole,  $A$  est sûr que  $B$  a bien reçu le secret  $K$

### Poids du protocole : 24

- Message 1 :  $1 + (1 + 1) + (1 + 1) + (5 + 1 + 1) = 12$
- Message 2 :  $(1 + 1) + (5 + 1 + 1 + 1 + 1) = 11$
- Message 3 : 1