Protocole Proto-Chorale V4

Clément Bidault, Loïc Cardinaël, Elise Klein

Notre protocole se décrit comme suit :

$$\begin{aligned} A &\rightarrow B : A, \{N_a\}_{pub(B)} \\ B &\rightarrow A : \{\{N_b\}_{pub(B)}\}_{pub(A)}, \{\{N_b\}_{pub(A)}\}_{N_a} \\ A &\rightarrow B : \{N_b\}_{pub(B)} \end{aligned}$$

Connaissances initiales : Au début du protocole on suppose que A et B connaissent les clé publiques *pub(C)* de tout agent C.

Valeurs générées au cours du protocole : Les nonces N_b et les messages secrets N_a sont générés à chaque nouvelle conversation.

Description du protocole :

1. A entame la conversation en envoyant à B son nom ainsi son message secret chiffré avec la clé publique de B. Le message sera spécial à cette conversation.
2. B répond en envoyant 2 éléments, le premier est son nonce N_b qu'il a généré pour cette conversation qu'il va chiffrer avec *pub(B)* le tout chiffré avec *pub(A)*. Le deuxième morceau est à nouveau N_b mais cette fois chiffré avec *pub(A)* puis avec le N_a qu'il aura reçu du premier message.
3. A reçoit ce message et peut déchiffrer le deuxième élément avec N_a et sa clé privée. Il obtient ainsi N_b. Ensuite il déchiffre le premier avec sa clé privée, et vérifie que ce qu'il trouve est égal au N_b qu'il vient de trouvé, chiffré avec *pub(B)*. Si ce n'est pas le cas il arrête la conversation.
4. Si l'étape d'avant s'est bien passée, A envoie à B N_b chiffré avec *pub(B)*. Si B reçoit bien son nonce il finit sinon il sait qu'il y a eu un problème et ne finit pas.

Propriétés de sécurité :

— *Authentification :* Lorsque B reçoit le message du serveur il sait que c'est Alice qui lui parle, et quand Alice envoie la clé à B, elle est sûre que B a reçu la clé.
— *Confidentialité :* Les 2 agents sont seuls à connaître N_a.

Poids du protocole : 26

— Règle 1 : $1 + 1 + 1 + 1 = 4$
— Règle 2 : $1 + 1 + 1 + 1 + 1 + 1 + 10 + 1 + 1 + 1 = 19$
— Règle 3 : $1 + 1 + 1 = 3$