

## Protocoles

### Exercice 1 (Protocole BAN-Yahalom)

Le protocole de **BAN-Yahalom** comporte deux participants  $A$  et  $B$  et un serveur, noté  $S$ . Le serveur peut être considéré comme un participant mais dont l'intrus ne peut pas prendre l'identité. Il partage en général des secrets avec chacun des participants, ici une clef symétrique, notée  $K_{as}$  pour la clef partagée entre le serveur et  $A$ .

Protocole BAN-Yahalom

1.  $A \rightarrow B : A, N_a$
2.  $B \rightarrow S : B, N_b, \{A, N_a\}_{K_{bs}}$
3.  $S \rightarrow A : N_b, \{B, K_{ab}, N_a\}_{K_{as}}, \{A, K_{ab}, N_b\}_{K_{bs}}$
4.  $A \rightarrow B : \{A, K_{ab}, N_b\}_{K_{bs}}, \{N_b\}_{K_{ab}}$
5.  $B \rightarrow A : \{secret\}_{K_{ab}}$

1. Quel est le message renvoyé par  $B$  à la 2e étape s'il reçoit le message  $A, \{A, N_a\}_{K_{as}}$  ?
2. Que fait  $A$  à la 4e étape si elle vient de recevoir le message  $N_b, \{B, K_{ab}, N_a\}_{K_{as}}, \{A, K', N'\}_{K_{bs}}$  au lieu du message normal ?
3. Que fait  $A$  à la 4e étape si elle vient de recevoir le message  $N_b, \{B, K_{ab}, K'_{ab}, N_a\}_{K_{as}}, \{A, K_{ab}, N_b\}_{K_{bs}}$  au lieu du message normal ?
4. Que fait  $A$  à la 4e étape si elle vient de recevoir le message  $N_b, \{B, K_{ab}, N'\}_{K_{as}}, \{A, K_{ab}, N_b\}_{K_{bs}}$  au lieu du message normal ?
5. Calculer le "coût" du protocole, pour la fonction de coût décrite dans la présentation du projet.

---

### Exercice 2

On considère le protocole suivant (version erronée du Wide-Mouth-Frog Protocol) :

$$\begin{aligned} A &\rightarrow S : A, B, \{K_{ab}\}_{K_{as}} \\ S &\rightarrow B : A, B, \{K_{ab}\}_{K_{bs}} \end{aligned}$$

$A$  envoie au serveur une clef de session  $K_{ab}$  à l'aide d'une clef partagée  $K_{as}$  avec le serveur, en indiquant son identité et celle de  $B$ . Le serveur  $S$  répond en transmettant la clef de session à  $B$  à l'aide de sa clef partagée  $K_{bs}$ . On souhaite bien sûr que la clef de session reste secrète entre  $A$  et  $B$  (et le serveur).

1. Calculer le "coût" du protocole, pour la fonction de coût décrite dans la présentation du projet
  2. Montrer que ce protocole peut être attaqué.
  3. Quelle(s) correction(s) proposez-vous ?
-

**Exercice 3 (Protocole de Dolev)**

A et B s'échangent un secret de manière authentifiée.

$$\begin{aligned} A &\rightarrow B \quad \{A, M\}_{pub(B)} \\ B &\rightarrow A \quad \{B, M\}_{pub(A)} \end{aligned}$$

On souhaite renforcer la sécurité en ajoutant une couche de chiffrement.

$$\begin{aligned} A &\rightarrow B \quad \{A, \{M\}_{pub(B)}\}_{pub(B)} \\ B &\rightarrow A \quad \{B, M\}_{pub(A)} \end{aligned}$$

- Montrer qu'il existe une attaque sur le protocole ainsi modifié.
- Calculer le "coût" des deux protocoles, pour la fonction de coût décrite dans la présentation du projet

**Exercice 4 (attaque de type sur Needham-Schroeder-Lowe)**

On considère une variante du protocole de Needham-Schroeder, où l'identité de B est placée à gauche du message.

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

1. Calculer le "coût" du protocole, pour la fonction de coût décrite dans la présentation du projet.
2. Montrer qu'il existe à nouveau une attaque sur le secret du nonce  $N_b$ .  
*Indication : L'attaque repose sur la confusion de type entre un agent et un nonce.*
3. À quel point cette attaque est-elle réaliste ?