Quentin Guillard

Description du protocole

Le protocole créé se décrit de la manière suivante :

$A \rightarrow B$: A, $\{N_a\}_{pub(B)}$
$B \rightarrow A$: $SYM\{B\}_{Na}$, $\{N_b\}_{pub(A)}$
$A \rightarrow B$: $SYM\{scrt\}_{SYM\{Nb\}Na}$
$B \rightarrow A$: h(scrt)

Connaissances initiales :
A connait la clef publique pub(B) de B et B connait la clef publique pub(A) de A.

Valeurs générées au cours du protocole :
N_a est un nonce généré par A. N_b est un nonce généré par B.
scrt est le secret qui doit être partagé entre les deux parties.

Description du protocole :

- 1ère étape : Alice envoie son nom, et un nombre N_a généré aléatoirement et chiffré de manière asymétrique à l'aide de la clef publique de Bob
- 2ème étape : Bob envoie son nom chiffré de manière symétrique à l'aide de N_a (puisqu'il a la clef privée associée à pub(B)), suivi d'un nombre N_b généré aléatoirement et ensuite chiffré de manière asymétrique à l'aide de la clef publique de Alice
- 3ème étape : Alice envoie le secret chiffré de manière symétrique à partir de la clef générée par N_b chiffré de manière symétrique par N_a . N_b est connu car Alice possède la clef privée associée à pub(A).
- 4ème étape : Bob envoie le hash du secret à Alice pour que cette dernière puisse vérifier que ce dernier à bien reçu le secret (pas d'interception). Le secret est récupéré car Bob connait N_b et N_a et peut donc ouvrir le message.

Propriété de sécurité :

- Si B a fini pensant avoir reçu une clef 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 : 48

- Règle 1 : 1 + (1 + 1 + 1) = 4
- Règle 2 : (10 + 1 + 1) + (1 + 1 + 1) = 15
- Règle 3 : (10 + 1 + (10 + 1 + 1)) = 23
- Règle 4 : 5 + 1 = 6