

Description du protocole V2

Le protocole créé se décrit de la manière suivante :

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

Connaissances initiales :

A connaît la clef publique $\text{pub}(B)$ de B et B connaît la clef publique $\text{pub}(A)$ 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 :

- 1^{ère} 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
- 2^{ème} étape : Bob envoie N_a chiffré de manière asymétrique à l'aide de $\text{pub}(A)$, suivi d'un nombre N_b généré aléatoirement et ensuite chiffré de manière asymétrique à l'aide de la clef publique de Alice
- 3^{ème} 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 $\text{pub}(A)$.
- 4^{ème} étape : le secret est envoyé à Alice avec un chiffrement asymétrique (avec $\text{pub}(A)$) pour que cette dernière puisse vérifier que Bob a bien reçu le secret (pas d'interception). Le secret est récupéré car Bob connaît 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 : 36

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