

Description du protocole V4

Le protocole créé se décrit de la manière suivante :

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

Connaissances initiales :

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

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 : une paire contenant son nom et d'un nombre N_b généré aléatoirement, qui est chiffrée de manière asymétrique à l'aide de la clef publique de Alice. Le tout est ensuite chiffré de manière symétrique à l'aide de N_a .
- 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 haché du secret est envoyé à Bob pour que ce dernier 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 : 97

- Règle 1 : $1 + (1 + 1 + 1) = 4$
- Règle 2 : $10 + (1 + (50 + 1 + 1) + 1) = 64$
- Règle 3 : $(10 + 1 + (10 + 1 + 1)) = 23$
- Règle 4 : $5 + 1 = 6$