Protocoles de sécurité

Description du protocole des cryptopathes

Le protocole se décrit de la façon suivante :

$$A \rightarrow B : \{k\}_{p(B)}$$

$$B \rightarrow A : h(<B,n>), \{ \{n\}_k \}_{p(A)}$$

$$A \rightarrow B : \{n\}_{p(B)}$$

Connaissances initiales : Au début du protocole, on suppose que les agents A et B connaissent la clé publique p(C) de tout agent C.

Valeurs générées au cours du protocole : k est une clé de session générée par A. n est un nonce généré par B.

Description du protocole :

Au début du protocole, A génère une clé de session et la chiffre à l'aide d'un algorithme de chiffrement asymétrique en utilisant la clé publique de B (donc seul B peut la déchiffrer). A envoi ce message chiffré à B.

Une fois que B a reçu le message contenant la clé chiffrée, il le déchiffre. Il va générer un nonce n et calculer le hash de <B,n>. Il va envoyer ce hash ainsi que le nonce chiffré par la clé de session k, puis par la clé publique de A.

Quand A reçoit ce message, il déchiffre le deuxième message afin de retrouver le nonce, et calcul le hash de <B,n> afin de s'assurer de son intégrité. Il lui suffit de alors de renvoyer n chiffré à l'aide de la clé publique de B afin d'accuser sa réception (et que B soit assuré que A a reçu le bon n).

Propriétés de sécurité :

- Authentification : Lorsque B reçoit $\{n\}_{p(B)}$, il est certains que le message vient de A. De même quand A reçoit $h(<B,n>), \{ \{n\}_k \}_{p(A)}$, il est certains que ça vient de B
- Confidentialité : Seul A et B ont connaissance de la clé de session k.

Poids du protocole : 18

- Règle 1 : 1 + 1 + 1 = 3
- Règle 2 : (5 + 1 + 1) + (1 + (1 + 1 + 1)+ 1) = 12
- Règle 3 : 1 + 1 + 1 = 3