Protocoles de sécurité

Description du protocole de Pikachu

Le protocole de Pikachu à clefs publiques se décrit de la façon suivante :

A → B: $<\{A\}_K, \{K\}_{pub\ (B)}>$

B → A: $<\{B\}_n, \{\{n\}_K\}_{pub(A)}>$

A → B: $\{n\}_{pub(B)}$

Connaissances initiales : Au début du protocole, on suppose que les agents A et B connaissent la clef publique pub(C) associée à l'agent C, pour tout agent C.

Valeurs générées au cours du protocole : K est un nonce généré par A. n est un nonce généré par B.

Description du protocole : À la première étape du protocole, l'agent Alice envoie son nom A chiffré par la clef K qu'elle l'a générée et la clef K est chiffrée par un algorithme de chiffrement asymétrique avec la clef publique de B (notée pub(B)), c'est-à-dire que seul l'agent Bob connaît la clef privée correspondant à la clef pub(B).

À la deuxième étape du protocole, Bob reçoit le message $<\{A\}_K, \{K\}_{pub(B)}>$ envoyé par Alice. Comme il a la clef privée (prv(B)) lui permettant d'ouvrir le message, il renvoie son nom chiffré par un nonce n généré par lui-même, n est chiffré une première fois par la clef K et une deuxième fois par la clef publique de A noté pub(A).

À la troisième étape du protocole, Alice reçoit le message

$<\{B\}_n, \{\{n\}_K\}_{pub(A)}>$, elle renvoie alors le nonce n chiffrée par la clef publique de B .

Propriétés de sécurité :

– *Authentification :*Lorsque Bob reçoit le message $<\{A\}_K, \{K\}_{pub(B)}>$ il est sûr que celui-ci vient d'Alice car il déchiffre la clé K par sa clé privée et déchiffre le nom de A par la clé qu'il a trouvé .

– *Confidentialité :* Les deux agents Alice et Bob sont seuls à connaître le nonce n et la clé K.

Poids du protocole : 17

- Règle 1 : 3+3=6
- Règle 2 :3+1+3+1 =8
- Règle 3: 3