Description du protocole Y

Team en Y

Décembre 2017

1 Protocole

$A \rightarrow B : \{\langle K, A\rangle\}pk(B), h(k), \{Na\}pk(B)$

$\mathrm{B} \rightarrow A : \{\langle Nb, B\rangle\}pk(A), Na$

$\mathrm{A} \rightarrow B : Nb$

Connaissances initiales

Au début du protocole, on suppose que A et B connaissent les clefs publique pk(B) et pk(A). Ils ont aussi la connaissance de la méthode de hashage utilisée.

Valeurs générées au cours du protocole

Na est un nonce généré par A et Nb est un nonce généré par B.

Description du protocole

Alice initie la communication en envoyant trois parties distinctes : un message avec son nom, le tout chiffré avec la clé publique de Bob, un hash du message, et un Nonce qu'elle génère puis qu'elle chiffre avec la clé publique de Bob.

Bob lui répond deux parties distinctes : un Nonce qu'il génère et son nom le tout chiffré avec la clé publique d'Alice, et le Nonce d'Alice pour attester la bonne réception du message précédent

Enfin, Alice renvoie le Nonce que Bob lui a envoyé afin d'attester la bonne réception du message précédent également.

Propriétés de sécurité

Confidentialité du message, intégrité du message et authenticité des communicants assurés

Poids du protocole

$\{\langle K, A\rangle\}pk(B)$: Chiffrement d'une paire message/expediteur avec la clé publique du destinataire : 1+50+1+1+1 = 54

$\{Na\}pk(B)$: Chiffrement d'un Nonce avec la clé publique du destinataire : 1+1+1 = 3

$h(k)$: Hash du message : 5+1=6

Na : Envoie d'un Nonce : 1

On a ici deux chiffrements de paire, un chiffrement de Nonce, un hash, et deux envois de Nonce. On obtient donc un total de 2x54+3+6+2x1 = 119