# Description du protocole Y

Team en Y

Décembre 2017

## 1 Protocole

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

$\mathrm{B} \rightarrow A : \{h(K, A, B, Nb)\}Na, \{Nb\}pk(A)$

$\mathrm{A} \rightarrow B : \{h(K, B, Na)\}Nb$

**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 deux parties distinctes : un message associé a un hash de son nom et d'un Nonce qu'elle génère, le tout chiffré avec la clé publique de Bob, et le Nonce généré qu'elle chiffre avec la clé publique de Bob.

Bob lui répond deux parties distinctes : un hash du message reçu associé au nom d'Alice, son nom et un Nonce qu'il génère, le tout chiffré avec le Nonce reçu, et il envoie le Nonce qu'il a généré et chiffré avec la clé publique d'Alice

Enfin, Alice renvoie le hash du message associé au nom de Bob et du Nonce qu'elle avait généré précédemment, le tout chiffré avec le Nonce de Bob.

**Propriétés de sécurité**

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

**Poids du protocole**

$\{\langle K, h(A, Na)\rangle\}pk(B)$ : Chiffrement d'une paire message/ hash avec la clé publique du destinataire : 1+50+1+1+5+1+1 = 60

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

$\{h(K, A, B, Nb)\}Na$ : Hash chiffré : 5+1+1+1+1+1+1=11

$\{h(K, B, Na)\}Nb$ : Hash chiffré : 5+1+1+1+1+1=10

On a ici un chiffrements de paire, deux chiffrement de Nonce, deux hash chiffrés. On obtient donc un total de 60+11+3x2+10 = 87