Proposition du groupe “Gros Pigeons”

Situation initiale :

- Alice possède une clé publique pub(A) et une clé secrète sec(A).
- Bob possède une clé publique pub(B) et une clé secrète sec(B).
- Alice connaît la clé publique de Bob et Bob connaît la clé publique d’Alice.

Protocole d’échange de clé symétrique créée par Alice :

A → B : $\{K\}_{pub(B)}$
B → A : $<h(k), \{n\}_{pub(A)}>$
A → B : h(n)

- Alice envoie à Bob la clé chiffrée avec la clé privée de Bob. Seul Bob peut déchiffrer le message et connaître la valeur de la clé. Alice garde en mémoire la clé K et le destinataire (Bob) dans un tableau.
- Bob envoie le hash de la clé à Alice. Il envoie également un nonce chiffré avec la clé publique d’Alice.
- Alice regarde dans son tableau si le hash reçu correspond à l’une des clés qu’elle a envoyée. Ensuite elle envoie le hash du nonce à Bob.
- Bob vérifie le hash du nonce et s’assure ainsi qu’il échange bien avec Alice.

Situation finale :

- La clé K est un secret partagé entre Alice et Bob.
- Bob est certain que c’est Alice qui lui a envoyé la clé K.
- Alice est certaine que Bob a bien reçu la clé K.

Coût du protocole :

f1 = 1 + 1 + 1 = 3
f2 = 5 + 1 + 1 + 1 + 1= 9
f3 = 5 + 1 = 6

C = f1 + f2 = 3 + 9 + 6 = 18