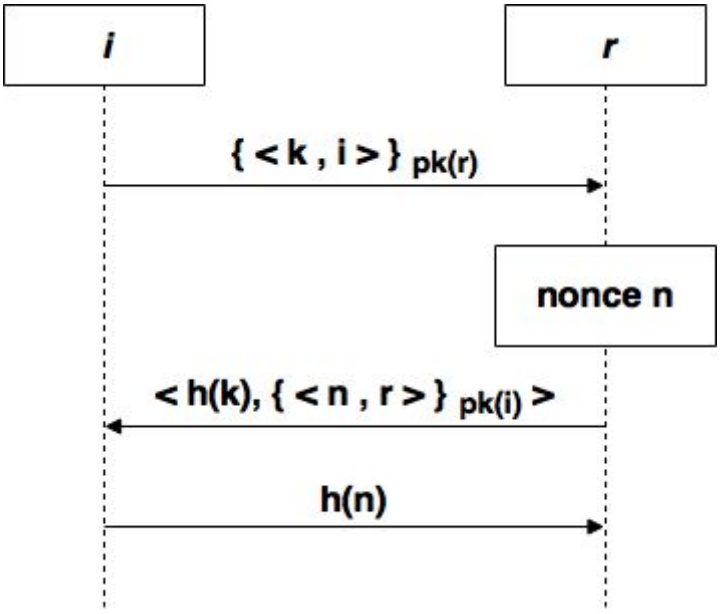
Protocole du groupe “Gros Pigeons” - V1

Situation initiale :

- ***i*** possède une clé publique ***pk(i)*** et une clé secrète ***sk(i).***
- ***r*** possède une clé publique ***pk(r)*** et une clé secrète ***sk(r).***
- ***i*** connaît la clé publique de ***r*** et ***r*** connaît celle de ***i.***

Protocole d’échange de clé symétrique générée par ***i*** :



- ***i*** génère une clé ***k*** et envoie à ***r*** la paire **< *k, i* >** chiffrée avec la clé publique de ***r***. Seul ***r*** peut alors déchiffrer ce message et connaître la valeur de la clé ainsi que l’identité présumée du créateur du message.
- ***r*** envoie le hash de la clé à ***i***. Il envoie également la paire **< *n,r* >** chiffrée avec la clé publique de ***i*** où ***n*** est un nonce.
- ***i*** vérifie le hash de la clé afin de s’assurer que ***r*** l’a bien reçue. Il envoie ensuite le hash du nonce ***n*** à ***r***.
- ***r*** vérifie le hash du nonce et s’assure ainsi qu’il échange bien avec ***i***.

Situation finale :

- La clé ***k*** est un secret partagé entre ***i*** et ***r***.
- ***r*** est certain que ***i*** lui a envoyé la clé ***k***.
- ***i*** est certain que ***r*** a bien reçu la clé ***k***.

Coût du protocole : 54 + 55 + 6 = 115