Protocole: Needham-Schroeder asymétrique Ce protocole se base sur un algorithme de chiffrement et de signature à clé publique. Plus précisément, K_{UA} et K_{RA} sont respectivement la clé publique de chiffrement et la clé secrète de déchiffrement d'Alice (de même pour Bob avec K_{UB} et K_{RB}) alors que K_{RS} est la clé secrète de signature pour le serveur et K_{US} la clé publique de vérification de la signature.

1- A →S : A, B

Alice demande la clé publique de Bob au serveur.

2- S → A : $\{K_{UB}, B\}K_{RS}$

Le serveur répond à Alice avec la clé publique de Bob en même temps que son identité, le tout étant signé par la clé du serveur.

3- A → B : $\{NA, A\}K_{UB}$

Alice choisit un nonce, le chiffre avec la clé publique de Bob avant de lui envoyer.

4- B →S : B, A

Bob demande la clé publique d'Alice au serveur.

5- S → B : $\{K_{UA}, A\}K_{RS}$

Le serveur répond à Bob avec la clé publique d'Alice en même temps que son identité, le tout étant signé par la clé du serveur.

6- B→ A : $\{NA, NB\}K_{UA}$

Bob choisit un nonce, le chiffre avec la clé publique de Alice en même temps que le nonce que celle-ci a généré afin de prouver qu'il a pu déchiffrer le message envoyé à l'étape.

7- A →B : $\{NB\}K_{UB}$

Alice envoie NB à Bob pour prouver qu'elle a pu déchiffrer le message envoyé à l'étape précédente.

Questions :

- Expliquez pourquoi ici on pourrait dire que le serveur d'authentification joue l'équivalent du rôle d'une autorité de certification qui peut sur demande produire des certificats contenant l'identité et la clé publique d'un participant ?
- Une fois que le protocole est terminé, comment est-ce qu'Alice et Bob peuvent générer une clé de session partagée à partir des deux nonces NA et NB ?
- Proposez une attaque de type homme-du-milieu sur ce protocole où un imposteur I qui a réussi à convaincre A d'initier une session avec lui peut utiliser cela pour réussir à convaincre B qu'il discute avec A dans une autre session.
- Modélisez et analysez le protocole en scyther.
- Discuter les attaques.
- Proposez un changement au protocole permettant de contrer les attaques trouvées.