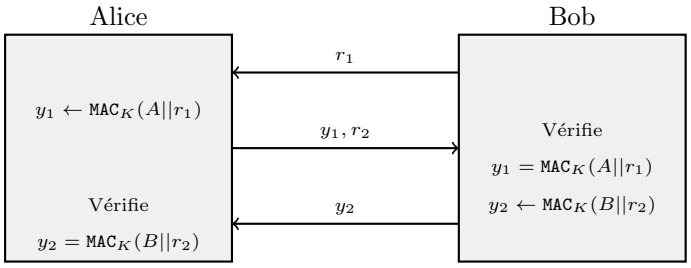
D31: Protocoles cryptographiques
TD 5: Schémas d'authentification

Exercice 1. Questions en vrac

1. Décrire un protocole d'identification simple utilisant une fonction `MAC` (challenge et réponse). Décrire une l'attaque par session parallèle sur ce protocole ainsi qu'une solution pour y remédier.
2. Décrire un protocole d'identification simple utilisant la cryptographie à clé publique. L'attaque par session parallèle fonctionne-t-elle?
3. Décrire les différentes étapes d'une connection `ssh`. Quelle est la plus grosse faille de sécurité du protocole?

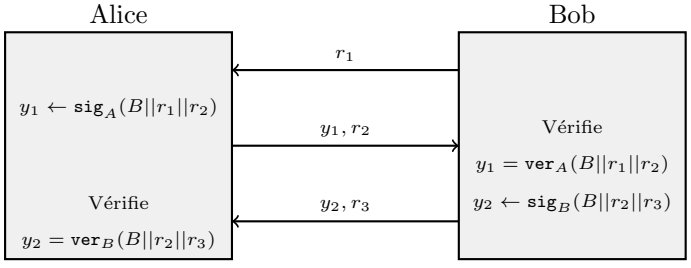
Exercice 2. Authentification mutuelle

1. Soit une fonction $\texttt{MAC}_K$ connue uniquement d'Alice est Bob. On considère le protocole d'authentification suivant:



   Montrer comment un attaquant peut facilement se faire passer pour Bob. Comment se protéger de cette attaque?

2. On considère le schéma d'authentification suivant:



   Proposer une attaque par session parallèle sur ce protocole où un attaquant peut se faire passer pour Bob au près d'Alice (on suppose que les fontions de vérification sont certifiées).

Exercice 3. Schéma d'identification Guillou-Quisquater

On considère la mise en place suivante:

(a) Une authorité de confiance choisit p et q deux grand nombres premiers et rend $n = pq$ public.

(b) Elle choisit un entier b, premier avec $\phi(n)$ de t bits où t est un paramètre de sécurité.

(c) Alice choisit un entier $u \leq n-1$ et calcule $v \equiv (u^{-1})^b \mod n$ et obtient de l'authorité de confiance la signature $s = \mathtt{sig}_{\mathtt{AC}}(A||v)$.

(d) n et b sont des paramètres publics, v est la clé publique d'Alice et u sa clé secrête.

Pour s'authentifier auprès de Bob Alice suit le protocole suivant:

(i) Alice génère $k < n-1$ aléatoirement, calcule $\gamma \equiv k^b \mod n$ et l'envoie à Bob.

(ii) Bob génère $0 \leq r < b-1$ aléatoirement et l'envoie à Alice.

(iii) Alice calcul $y = ku^r \mod n$ et l'envoie à Bob.

(iv) Bob vérifie que $\gamma \equiv v^r y^b \mod n$.

1. Prouver la consitence du protocole.
2. Sur quoi repose la sécurité du protocole?
3. Montrer qu'un attaquant qui connait à l'avance l'entier r peut se faire passer pour Alice.
4. On suppose qu'il existe une valeur de γ pour laquelle un attaquant est capable de calculer deux couples (y_1, r_1) et (y_2, r_2) lui permettant de faire passer pour Alice. Montrer alors qu'un tel attaquant est capable de calculer la clé privé u.