# Sécurité des données TD 3

**Exercise 1** Proposez un code détecteur d'erreurs basé sur le protocole de partage de clé secrète de Shamir (Shamir's Secret Sharing Protocol).

**Exercise 2** Proposez une fonction de hachage basée sur

- l'arbre de Merkle, et
- le logarithme discret

**Exercise 3** Alice prouve à Bob qu'elle connaît une valeur $a$, sans divulgeur cette valeur.

**Protocole d'identification de Schnorr** : Après une étape préliminaire, où Alice et Bob s'accordent sur un nombre premier $p$ et un générateur $g$ de $\mathbb{F}_p = \{1, 2, \dots p-1\}$, Alice choisit $a$ (son secret) et émet la clé publique $A = g^a$. Cette clé publique est **certifiée**.

Alice (engagement) : engendre aléatoirement $b \in \mathbb{F}_p$, et transmet $B = g^b$ à Bob

Bob (défi) : engendre aléatoirement $r \in \mathbb{F}_p$, et transmet $r$ à Alice

Alice (réponse de Alice) : calcule $c = b + a \cdot r \in \mathbb{Z}$, et envoie $c$ à Bob

Bob : verifie que $B \cdot A^r = g^c$

**Question** Décrire ce protocole pour $p = 7$ et $g = 3$.

**Exercise 4** Un bureau militaire est composé de deux généraux et de deux colonels. Ils ont le contrôle d'un puissant missile, mais ils ne veulent pas le lancer à moins que :

- un général décide de le lancer, ou
- deux colonels décident de le lancer.

Décrivez le protocole SSS correspondant. Vous pouvez utiliser le 'grand' nombre premier $p = 13$.

**Exercise 5** Alice veut préparer des clés de chiffrement pour le protocole RSA. Elle choisit $p = 5$ et $q = 7$. Ensuite, elle calcule $(p-1)(q-1) = 4 \cdot 6 = 24$. Cependant, un défaut de sécurité permet de connaître cette valeur, $(p-1)(q-1) = 24$, qui n'est pas censée être publique.

- Cela compromet-il la sécurité du protocole ?
- Peut-on déduire facilement les valeurs de $p$ et $q$ à partir de cette information ?