Université Bordeaux 1 **M1 CSI, Cryptologie**
Mathématiques, Informatique Année 2019–2020

# FEUILLE D'EXERCICES n° 10

## Protocoles divers

**Exercice 1** – Il y a quatre personnes dans une pièce et l'une d'entre elles est un espion. Les trois autres utilisent le protocole de partage de secret de Shamir avec $n = 5$, $k = 2$ et $p = 11$. L'espion a construit son couple au hasard. Les quatre couples sont $s_1 = (1, 7)$, $s_2 = (3, 0)$, $s_3 = (5, 10)$ et $s_4 = (7, 9)$. Retrouver l'espion et le secret.

**Exercice 2** – Donner un exemple concret du protocole de jeu de pile ou face par téléphone de Blum.

**Exercice 3** – Soit $n = pq$, où $p, q \equiv 3 \bmod 4$ sont deux grands premiers distincts. P (le prouveur) veut convaincre V (le vérificateur) qu'il connaît la factorisation de $n$ sans révéler d'information sur les facteurs. Ils utilisent le protocole suivant. P et V répètent 30 fois :

(1) V choisit au hasard un entier $x$ premier avec $n$, calcule $y = x^2 \bmod n$ et envoie $y$ à P.

(2) P calcule les 4 racines carrées de $y$, en choisit une au hasard, notée $r$ et l'envoie à V.

(3) V vérifie que $y = r^2 \bmod n$.

V accepte si et seulement si les 30 vérifications ont été couronnées de succès. S'agit-il d'une preuve sans transfert de connaissance ?

**Exercice 4** – On s'intéresse ici au protocole d'identification de Fiat-Shamir. Le secret de P est un $k$-uplet $(x_1, x_2, \ldots, x_k) \in \{0, 1, \ldots, n-1\}^k$ avec $\mathrm{pgcd}(x_i, n) = 1$, où $n$ est le produit de deux grands premiers distincts $p$ et $q$ ($n$ est public, $p$ et $q$ sont tenus secrets). L'identité de P est spécifiée par les $k$ résidus quadratiques $I_1 = x_1^2, I_2 = x_2^2, \ldots, I_k = x_k^2 \bmod n$. P prouve son identité en montrant qu'il connaît les racines carrées $x_1, x_2, \ldots, x_k$ de $I_1, I_2, \ldots, I_k$ modulo $n$. Le protocole est le suivant.

(1) P choisit un entier $r$ aléatoire et calcule $t = r^2 \bmod n$. Il communique $t$ à V.

(2) V choisit un $\varepsilon = (\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_k) \in \{0, 1\}^k$ et le communique à P.

(3) P calcule $x = r x_1^{\varepsilon_1} x_2^{\varepsilon_2} \cdot s x_k^{\varepsilon_k} \bmod n$ et le donne à V.

(4) V vérifie que $x^2 = t I_1^{\varepsilon_1} I_2^{\varepsilon_2} \cdots I_k^{\varepsilon_k} \bmod n$.

Montrer que ce protocole est sans transfert de connaissance et qu'un imposteur connaissant seulement $n$ et les $I_i$ ne peut tromper ce protocole qu'avec une probabilité $\leqslant 1/2^k$.