École normale supérieure **2024-2025**
Département d'informatique **Ky Nguyen - ky.nguyen@ens.fr**

Introduction to Zero-Knowledge Proofs
DM n° 1 - Deadline : 23h59, le vendredi 18 octobre, 2024

Exercice 1 (**Non-résiduosité quadratique - 2 points).** Construire un protocole à divulgation nulle de connaissance face à un vérifieur honnête par lequel un prouveur qui connaît la factorisation d'un module RSA N prouve à un vérifieur polynomial que $x \in \mathbb{Z}_N^*$ n'est pas un carré modulo N.
Indication : connaissant la factorisation du module RSA N, il est possible de calculer si un entier donné est un carré modulo N en temps polynomial (en utilisant le symbole de Jacobi).

Exercice 2 (**Preuve de connaissance d'une représentation - 4 points).** Considérons un groupe $\mathbb{G}$ d'ordre premier q et g et h deux générateurs de $\mathbb{G}$. Soit $y = g^s h^t$. Proposer une preuve du couple (s, t) à divulgation nulle de connaissance face à un vérifieur honnête.

Exercice 3 (**Un vote électronique simple - 4 points).** Supposons que n personnes votent entre deux candidats, avec le protocole suivant.

- Une autorité de confiance choisit un chiffrement à clef publique, avec une paire clef privée/clef publique ElGamal ($sk = x, pk = g^x$), et publie pk.
- Chaque votant i choisit son candidat $v_i \in \{0, 1\}$ en chiffrant g_i^v avec ElGamal, et publie le résultat.
- Le résultat du vote est le produit des chiffrés (homomorphisme multiplicatif). L'autorité de confiance déchiffre le résultat $g^{v_1+\cdots+v_n}$ et publie une preuve que c'est bien le déchiffrement du produit des chiffrés.

1. Comment récupère-t-on le résultat effectif du vote $v_1 + \cdots + v_n$?
2. Argumenter que la dernière étape doit être correcte, sûre, et à divulgation nulle de connaissance.
3. Proposer une manière de réaliser cette dernière étape qui assure ces propriétés.
   Indication. Utilisez le protocole de Schnorr.