École normale supérieure **2018-2019**
Département d'informatique

Introduction à la cryptologie
TD n° 4 : Preuves à Divulgation Nulle de Connaissance, Signatures.

Exercice 1 (Isomorphisme de graphes)**.** Construire un protocole à divulgation nulle de connaissance par lequel un prouveur prouve à un vérifieur honnête qu'il connaît une permutation π réalisant un isomorphisme entre deux graphes G_0 et G_1.

Exercice 2 (Non-isomorphisme de graphes)**.** Construire un protocole à divulgation nulle de connaissance face à un vérifieur honnête par lequel un prouveur non borné calculatoirement prouve à un vérifieur polynomial que deux graphes G_0 et G_1 ne sont pas isomorphes.

Exercice 3 (Non-résiduosité quadratique)**.** 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 4 (Preuve de connaissance d'un logarithme discret)**.** Considérons un groupe $\mathbb{G}$ d'ordre premier q et g un générateur de $\mathbb{G}$ et $y = g^x \in \mathbb{G}$. Considérons le protocole suivant par lequel Alice veut prouver sa connaissance de x.

Engagement : Alice tire uniformément aléatoirement $k \in \mathbb{Z}_q^*$ et calcule $r = g^k \in \mathbb{G}$. Elle envoie r à Bob.

Challenge : Bob répond en envoyant un élément $c \in \mathbb{Z}_q$ tiré uniformément aléatoirement.

Réponse : Alice répond en envoyant $s = k - cx \bmod q$ et Bob accepte si $r = g^s y^c$ dans le groupe $\mathbb{G}$.

Montrons qu'il s'agit d'une preuve de connaissance de x à divulgation nulle de connaissance face à un vérifieur honnête.

Exercice 5 (Preuve de connaissance d'une représentation)**.** 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 de connaissance du couple (s, t) à divulgation nulle de connaissance face à un vérifieur honnête.

Exercice 6 (Un vote électronique simple)**.** Supposons que deux personnes, Alice et Bob, votent pour deux candidats, avec le protocole suivant.

- Une autorité de confiance choisit un chiffrement à clef publique, avec une paire clef privée/clef publique (sk, pk), et publie pk. On suppose que le chiffrement choisi est tel que pour pk donné, sk est unique.
- Alice et Bob chiffrent leur choix de candidat avec pk et publient le résultat.
- L'autorité de confiance déchiffrent les deux choix et publie le résultat des deux déchiffrements, dans un ordre aléatoire (pour ne pas révéler qui de Alice ou Bob a voté pour quoi, s'ils ont fait un choix différent).

1. On propose d'utiliser un chiffrement déterministe. Qu'en pensez-vous ?
2. On souhaite que tout le monde puisse vérifier que l'autorité n'a pas triché, i.e. les résultats publiés sont bien ceux d'Alice et Bob. Proposer un protocole qui réalise ce souhait (toujours sans révéler qui a voté pour quoi).
   Indication : on rappelle qu'on sait réaliser des preuves *zero knowledge* pour tous les langages NP (dont par exemple SAT).
3. Généraliser votre idée à n votants.