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

Introduction à la cryptologie
TD n° 10 : Calcul multi-partie.

Dans tous les protocoles qui suivent, on suppose que les participants sont honnêtes.

Exercice 1 (Calcul de produit à n joueurs)**.** Soit $\mathbb{G} = \langle g \rangle$ un groupe fini d'ordre p. On considère n joueurs $P_1, \ldots, P_n$, disposant respectivement d'une donnée $x_1, \ldots, x_n \in \mathbb{Z}_p$. Le but est de leur révéler la valeur de $x_1 \cdots x_n \bmod p$ sans révéler d'information sur les valeurs respectives.

1. Montrer que le chiffrement d'El Gamal est multiplicativement homomorphe, autrement dit, montrer qu'étant donné deux chiffrés c_x, c_y de x et de y respectivement, on peut calculer un chiffré de $x \cdot y$.
2. En utilisant de la cryptographie distribuée, en déduire un protocole pour résoudre le problème.

Exercice 2 (Transfert inconscient [1])**.** Le but de l'exercice est de construire un protocole d'*oblivious transfer* à partir d'un échange de clef Diffie-Hellman modifié. Soit $\mathbb{G}$ un groupe cyclique d'ordre premier p, et g un générateur fixé de $\mathbb{G}$. On définit les deux problèmes suivants.
Problème 1. Étant donnés g^a et g^b pour a, b quelconques dans $\mathbb{Z}_p$, calculer g^{ab}.
Problème 2. Étant donné g^a pour a quelconque dans $\mathbb{Z}_p$, calculer g^{a^2}.
On dit qu'un algorithme est efficace s'il est polynomial en $\log p$.

1. Donner des algorithmes efficaces pour :
   — étant donné $x \in \mathbb{G}$, calculer un inverse de x ;
   — étant donné $x \in \mathbb{G}$, calculer une racine carrée de x (trouver y tel que $y^2 = x$).
2. Montrer qu'il existe un algorithme efficace pour le problème 1 ssi il existe un algorithme efficace pour le problème 2.
   Indication. Utiliser g^{a+b}.
3. En déduire que si le problème de Diffie-Hellman (calculatoire) est difficile dans $\mathbb{G}$, alors le problème suivant est difficile : étant donnés b, g^a et mg^{a^2+ab} pour $a, b \in \mathbb{Z}_p$ et $m \in \mathbb{G}$ quelconques, calculer m.
   Question facultative. Est-ce que la réciproque est vraie ?
4. Rappeler le protocole d'échange de clef Diffie-Hellman, et comment on utilise une fonction de hachage H pour dériver du secret commun une clef symmétrique utilisée ensuite pour chiffrer les échanges entre Alice et Bob.
5. On propose de dévier du protocole précédent en faisant la chose suivante : soit $x \in \{0, 1\}$ le bit de Bob. Au lieu d'envoyer $B = g^b$ lors de l'échange de clef, Bob envoie $B = g^b$ si $x = 0$, et $B = A \cdot g^b$ si $x = 1$, où A représente le premier message de l'échange de clef DH envoyé par Alice à Bob. Déterminer un protocole d'oblivious transfer commençant ainsi, avec un échange supplémentaire (envoi de deux messages par Alice en chiffrant avec deux clefs bien choisies).

Exercice 3 (Dîner de cryptologues)**.** N cryptologues sont invités à un dîner à la Tour d'Argent. À la fin du repas, le serveur annonce que l'addition est déjà payée. Les cryptologues voudraient savoir si c'est l'un d'entre eux qui a payé, ou si c'est une entité extérieure (comme la NSA). Mais si c'est l'un d'entre eux, soucieux de vie privée, ils ne veulent pas que cette personne ait à se révéler.

1. Ne pas confondre avec le transfert en psychanalyse.

Voilà comment ils procèdent : si le cryptologue $i \in [\![1, N]\!]$ a payé le repas, on pose $p_i = 1$, sinon $p_i = 0$. Chaque paire (i, j) de cryptologues se met d'accord sur une valeur secrète uniformément aléatoire $x_{i,j} \in \{0, 1\}$ (en tirant secrètement à pile ou face par exemple [2]). Finalement, chaque cryptologue i publie

$$p_i + \sum_{j \neq i} x_{i,j} \bmod 2.$$

1. À partir des valeurs publiées, comment savoir si un des cryptologues a payé le repas ?
2. Un sous-ensemble K de cryptologues sont dans la poche du KGB, et voudraient savoir qui a payé le repas parmi les convives (si ce n'est pas la NSA). Ils mettent donc en commun toutes leurs valeurs secrètes $x_{i,j}$, et essaient de déduire un maximum d'information sur l'identité du payeur. Montrer qu'ils n'apprenent rien de plus ce faisant que ce qu'ils peuvent déduire purement du résultat du protocole (autrement dit, les autres valeurs qu'ils apprennent via le protocole ne révèlent rien de plus).
3. Au lieu d'échanger une valeur secrète avec tous les autres cryptologues, les cryptologues se mettent en cercle et échangent un secret commun $x_{i,j}$ seulement avec leur deux voisins immédiats. En fin de compte le cryptologue i publie donc $x_{i,i-1}+x_{i,i+1}+p_i \bmod 2$. La propriété de la question précédente est-elle vérifiée ? (Si on représente les cryptologues comme les sommets d'un graphe, avec une arête ssi ils communiquent, on utilise donc un graphe cyclique au lieu d'un graphe complet.)
4. Plus généralement, est-il possible d'inventer une protocole où cette propriété est vérifiée, mais où le graphe n'est pas complet ?

Exercice 4 (Un peu de complexité pour conclure)**.**
Supposons qu'il existe un schéma de chiffrement à clef publique sûr (mettons IND-CPA). Supposons pour simplifer qu'une clef publique correspond à une unique clef secrète. Montrer que P $\neq$ NP.

2. Alternativement, voir TD précédent pour un protocole qui permet de le faire à distance !