Master CSI 2 2013-2014

Crypto avancée : TD 1

– Exercice 1. Problèmes de calcul et problèmes de décision

a) Le problème de calcul du log discret prend en entrée deux éléments α et y de $\mathbb{F}_p^*$, et exige en sortie un élément x de $\mathbb{F}_p^*$ tel que $\alpha^x = y$.
Donner un problème de décision associé, et estimer le nombre d'appels au problème de décision nécessaire pour obtenir une solution au problème de calcul.

b) Une *coloration* d'un graphe en k couleurs est une partition des sommets du graphe en k parties, chacune coloriée d'une seule couleur, de telle sorte que deux sommets adjacents soient coloriés par des couleurs différentes.
Ramener, d'une manière raisonnable, la recherche d'une k-coloration d'un graphe à un problème de décision.

– Exercice 2. Discuter l'appartenance à NP des problèmes suivants :

a)
- I : un ensemble d'entiers $\{x_1, \ldots, x_k\}$, un entier z
- Q : exite-t-il un sous-ensemble $\{y_1, \ldots, y_\ell\} \subset \{x_1, \ldots, x_k\}$ tel que

$$\sum y_i = z \ ?$$

b)
- I : une machine reconnaissant en temps polynomial l'appartenance à un langage L, deux mots s et t de L de même longueur
- Q : existe-t-il une suite $s_1, \ldots, s_n$ de mots de L de même longueur, avec $s_1 = s$, $s_n = t$, et telle que pour tout i, les mots s_i et s_{i+1} diffèrent d'une seule lettre ?

– Exercice 3.

a) Montrer que la classe P est close par réunion et concaténation, Ceci veut dire que
- Si L et L' sont deux langages dans P alors le langage $L \cup L'$ est dans P
- Si L et L' sont dans P alors $L \circ L' = \{xx', x \in L, x' \in L'\}$ est dans P.

b) Montrer que si L et L' sont dans NP, alors $L \cup L'$, $L \circ L'$ le sont aussi.

c) Montrer que si L est dans NP alors L^* l'est aussi.

– Exercice 4.

a) Le problème suivant est-il dans NP ?

– I : un entier n
– Q : n est-il composé (non-premier) ?

b) Le problème suivant est-il dans NP ?
– I : un entier n
– Q : n est-il premier ?
On pourra se rappeler le théorème de Lucas : n est premier si et seulement s'il existe un entier a tel que $a^{n-1} = 1 \bmod n$ et si pour tout diviseur premier q de $n-1$, $a^{(n-1)/q} \neq 1 \bmod n$.

– EXERCICE 5.

a) La formule booléenne suivante est-elle satisfaisable ?

$$(x \vee y) \wedge (x \vee \overline{y}) \wedge (\overline{x} \vee y) \wedge (\overline{x} \vee \overline{y})$$

b) Montrer que la formule booléenne $x \vee y$ est réalisée (vaut 1) si et seulement si la formule

$$(x \vee y \vee z) \wedge ((x \vee y \vee \overline{z}))$$

l'est.

c) Montrer que la formule $x_1 \vee x_2 \vee x_3 \vee x_4$ est réalisée si et seulement s'il existe une valeur de y qui réalise

$$(x_1 \vee x_2 \vee y) \wedge (x_3 \vee x_4 \vee \overline{y}).$$

d) Exhiber une transformation polynomiale f de SAT vers 3-SAT.

– EXERCICE 6. Une *fonction booléenne* est une fonction $f : \{0,1\}^n \to \{0,1\}$. Elle peut être représentée par une table, par exemple :

x_1	x_2	x_3	f
0	0	0	1
0	0	1	0
0	1	0	0
0	1	1	1
1	0	0	1
1	0	1	1
1	1	0	0
1	1	1	0

Un *circuit* de calcul est un graphe orienté, dont les sommets sont étiquetés par un des termes $0, 1, \vee, \wedge, \neg, \mathbf{x}_1, \ldots, x_n$, «sortie». De plus,
– Les sommets étiquetés $0, 1, x_i$ ont 0 comme degré rentrant.
– Les sommets étiquetés $\neg$ ont 1 comme degré rentrant.
– Les sommet étiquetés $\vee, \wedge$ ont 2 comme degré rentrant.

– Il y a un unique sommet étiqueté «sortie», il a 1 comme degré rentrant, et 0 comme degré sortant.

a) Écrire un circuit qui calcule la fonction f donnée par la table ci-dessus.

b) Donner une procédure qui construit, à partir d'une table définissant une fonction booléenne f, un circuit calculant f. Que peut-on dire de la taille du circuit ?