Master CSI 2 — 2011-2012

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 $\cancel{\mathbb{F}_p^*}$ $\mathbb{N}$ 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. La formule booléenne suivante est-elle satisfaisable ?

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

– Exercice 3. 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 4.

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 5.

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 $n-1$, $a^{(n-1)/q} \neq 1 \bmod n$.