Master CSI 2 2013-2014

Cryptographie avancée : DS du 21 octobre 2013

Durée : 1h30. Sans document. Les exercices sont indépendants.

– EXERCICE 1. On rappelle qu'un graphe non orienté à n sommets est dit hamiltonien s'il existe un cycle (un chemin se terminant en son origine) de longueur n passant par tous les sommets du graphe. Un tel cycle est dit «hamiltonien».

Montrer que si P=NP, alors il existe un algorithme polynomial qui prend en entrée un graphe (non orienté) G à n sommets et qui
– répond «non hamiltonien» si G est non hamiltonien,
– *détermine* (exhibe) un cycle hamiltonien de G si G est hamiltonien.
On pourra exhiber un algorithme qui utilise comme sous-programme un algorithme auxiliaire $\mathcal{A}_{\text{aux}}$ qui *décide* si G est hamiltonien.

– EXERCICE 2. On considère une formule booléenne en n variables sous la forme conjonctive

$$f = C_1 \wedge C_2 \wedge \ldots \wedge C_k$$

où chaque clause C_i est un «ou inclusif» de termes. On dira qu'une telle formule est *presque satisfaisable* s'il existe une instanciation des variables dans $\{0,1\}^n$ telle que toutes les clauses C_i soient satisfaites, *sauf une*. Soit L le langage constitué des formules booléennes presque satisfaisables.

a) Montrer que $L \in$NP.

b) Montrer que L est NP-complet en exhibant une transformation de SAT vers L et en montrant qu'il s'agit d'une réduction polynomiale.

– EXERCICE 3. Soit g un élément de $\mathbb{Z}/p\mathbb{Z}$ d'ordre premier q connu. Soit $P = g^x \mod p$.

a) Montrer que le protocole suivant démontre, sans divulgation de connaissance, l'existence et la connaissance de $x \mod q$.
- le prouveur P envoie au vérificateur V un entier $t \mod p$,
- le vérificateur V renvoie un bit $\varepsilon \in \{0,1\}$,
- le prouveur P envoie un entier $z \mod q$ et
  - si $\varepsilon = 0$ alors V vérifie que $g^z = t \mod p$,
  - si $\varepsilon = 1$ alors V vérifie que $P^z = t \mod p$.

On montrera séparément la complétude, la validité et le caractère sans divulgation du protocole.

b) On suppose maintenant que le prouveur possède deux entiers P et Q modulo p, et qu'il souhaite démontrer qu'il existe un $x \bmod q$ tel que simultanément :
- $P = g^x \mod p$,
- $Q = g^{(x^{-1} \bmod q)} \mod p$.

Montrer que le protocole suivant démontre, sans divulgation de connaissance, l'existence et la connaissance de $x \mod q$.
- le prouveur P envoie au vérificateur V trois entier $a, b, t \mod p$,
- le vérificateur V renvoie un bit $\varepsilon \in \{0, 1\}$,
- le prouveur P envoie deux entiers $y, z \mod q$ et
  - si $\varepsilon = 0$ alors V vérifie que $g^y = a \bmod p$, $g^z = b \bmod p$, et $g^{yz} = t \bmod p$,
  - si $\varepsilon = 1$ alors V vérifie que $P^y = a \bmod p$, $Q^z = b \bmod p$, et $g^{yz} = t \bmod p$.

On montrera séparément la complétude, la validité et le caractère sans divulgation du protocole.

– Exercice 4. On considère le protocole suivant, destiné à démontrer qu'un graphe G à n sommets $\{1, 2, \ldots, n\}$ et m arêtes est hamiltonien.
- Le prouveur P donne m enveloppes au vérificateur V (qui peuvent éventuellement être matérialisées par des fonctions cryptographiques),
- le vérificateur V donne au prouveur un bit $\varepsilon \in \{0, 1\}$,
- si $\varepsilon = 0$ alors le prouveur P donne au vérificateur une permutation π de $\{1, 2, \ldots, n\}$ et P et V ouvrent les enveloppes. Le vérificateur V vérifie que chaque enveloppe contient une paire d'entiers de $\{1, 2, \ldots, n\}$, et que pour toute arête $\{i, j\}$ du graphe G, la paire $\{\pi(i), \pi(j)\}$ apparait bien dans une des enveloppes. En d'autres termes, V vérifie que les enveloppes contiennent bien les arêtes d'un graphe isomorphe à G.
- si $\varepsilon = 1$, alors le prouveur P ouvre exactement n enveloppes. Le vérificateur vérifie que les arêtes contenues dans les n enveloppes font apparaître un circuit de longueur n, par exemple, dans le cas $n = 7$,

$$\{3, 7\}, \{7, 5\}, \{5, 2\}, \{2, 4\}, \{4, 6\}, \{6, 1\}, \{1, 3\}.$$

Montrer que ce protocole est complet, valide, et sans divulgation : est-ce au sens parfait ou calculatoire ?