

Numéro d'anonymat :

Examen de RTA

Master Informatique

Partie de Cours de S. Chaumette

Année 2011-2012

Le 10 janvier 2012

Documents autorisés : aucun

Durée : 45 minutes

Ce sujet comporte 5 pages.

Les réponses seront données sur ce document et uniquement dans les zones prévues à cet effet.

Question 1. Gamma.

On s'intéresse ici à la manipulation des mots. La donnée élémentaire considérée est la lettre.

- a. Donner un programme Gamma qui calcule le mot miroir d'un mot donné de longueur $2n$.

- b. Donner l'invariant de ce programme et justifier qu'il termine. On notera, si besoin est, $\sim m$ le mot miroir de m et $.$ la concaténation de lettres et/ou de mots.

Numéro d'anonymat :

Question2. Réseaux de Pétri.

On considère deux processus P1 et P2 qui fonctionnent sur le même *smart phone*. Ce *smart phone* dispose d'une connexion réseau et d'une carte SD. Le comportement du processus P1 est le suivant : il acquière la carte SD, y lit une valeur, acquière le réseau, émet sur le réseau la valeur lue sur la carte, puis libère le réseau et enfin la carte SD. Le comportement du processus P2 est le suivant : il acquière le réseau, reçoit une valeur sur celui-ci, acquière la carte SD, écrit sur la carte la valeur reçue, libère la carte SD, puis le réseau.

L'objectif de cette question est de modéliser ce système à l'aide du modèle des réseaux de Pétri puis de l'étudier.

Note : on modélise une ressource partagée par une place, dotée d'un nombre de jetons égal au nombre d'utilisateurs simultanés qu'elle peut encore supporter.

- a. Modéliser la carte SD du smart phone dans une configuration où cette ressource ne peut pas être partagée (i.e. un seul utilisateur simultané possible). Faites de même pour la carte réseau.

- b. Modéliser le comportement du système comprenant P1 et P2 en présence des ressources partagées qui sont la carte SD et la connexion réseau.

Numéro d'anonymat :

- c. Construire le *graphe des marquages* du réseau de Pétri résultant (i.e. graphe d'évolution entre les états globaux possibles du réseau).

- d. Comment voit-on qu'un *deadlock* est possible dans le système résultant.

Question 3. Cryptographie quantique

- a. Quand on parle de cryptographie quantique à quoi fait-on réellement référence ?

Numéro d'anonymat :

b. Donner la table de vérité d'un C-NOT. Expliquer son action en une phrase.

c. Quelle est la particularité et l'intérêt de deux particules enchevêtrées ?

d. Que signifie BB84 ?

e. Expliquez le principe de cet algorithme.

f. Quel est l'avantage de ce type d'algorithme en termes de robustesse par rapport à un algorithme classique ?

Numéro d'anonymat :

Question 4. Smart dust et terminaux du futur.

Dans un appel à projets (débutant en février 2012) et intitulé « *Cyber-Physical Systems (CPS)* » (http://www.nsf.gov/funding/pgm_summ.jsp?pims_id=503286), la NFS (*National Science Foundation*) Américaine écrit :

« *Cyber-physical systems (CPS) are engineered systems that are built from and depend upon the synergy of computational and physical components. Emerging CPS will be coordinated, distributed, and connected, and must be robust and responsive. The CPS of tomorrow will need to far exceed the systems of today in **mot1, mot 2, mot 3, mot4, mot 5 and mot 6.** Examples of the many CPS application areas include **ex 1, ex2, ex 3, ex4, ex 5 and ex 6.** CPS will transform the way people interact with engineered systems, just as the Internet transformed the way people interact with information. »*

Faites des propositions pour remplacer **mot 1** à **mot 6** et **ex 1** à **ex 6** qui ont été effacés dans le texte ci-dessus.

Mot1 :
Mot 2:
Mot 3:
Mot 4:
Mot 5:
Mot 6 :

Ex 1 :
Ex 2 :
Ex 3 :
Ex 4 :
Ex 5 :
Ex 6 :