

Numéro d'anonymat :

Examen de RTA

Master Informatique

Partie de Cours de S. Chaumette

Année 2013-2014

Le 7 janvier 2014

Documents autorisés : aucun

Durée : 40 minutes.

Ce sujet comporte 4 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 d'un mot de longueur N donné construit sur l'alphabet constitué des caractères suivants : 'A', 'E', 'N', 'O', 'B', ' '. La donnée élémentaire considérée est le caractère.

- a. Donner un programme Gamma qui produit le message chiffré par décalage – on parle aussi de chiffre de César - du message initial (on prendra 3 comme valeur de clef) .

- b. Quelles sont les particules restant à la fin de l'exécution de votre programme avec le message initial suivant « BONNE ANNEE » ?

Numéro d'anonymat :

c. Donner l'invariant du programme proposé à la question a. et justifier qu'il termine.

Question2. Réseaux de Pétri.

Pour mémoire

« On dit qu'une transition est franchissable, si chaque place en entrée contient un nombre de jetons supérieur ou égal à la valuation de l'arc qui la relie à la transition »

On considère un digicode dont le code (non modifiable) ne comporte qu'un chiffre. Son clavier comporte lui les chiffres, de 0 à 9. Le système est câblé en dur et le code (de 1 chiffre donc) ne peut par conséquent pas être modifié. Ce digicode contrôle l'ouverture d'une porte et se bloque définitivement au bout de trois essais infructueux.

a. Modéliser le système décrit ci-dessus.

Numéro d'anonymat :

- b. Comment ferait on pour montrer que le système se bloque bien au bout de trois essais infructueux ? (il ne s'agit pas de le montrer mais d'expliquer comment on ferait pour le montrer)

- c. Ajoutez un système de reset à votre digicode permettant de le débloquent (en cas de blocage après trois essais).

Numéro d'anonymat :

Question 3. Cryptographie quantique

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

- b. A quoi sert l'algorithme BB84 ?

- c. Expliquez le principe de cet algorithme.

- d. Tracer sa courbe de robustesse (résistance aux attaques) en fonction de la puissance de calcul de l'attaquant.