MATH EN INFO

Témoin de Rabin-Miller

FICHE EXPLICATION Nº 16

1 Descriptif

L'objectif de ce défi est d'implémenter la méthode témoin de Rabin-Miller. Cette méthode, dont vous trouverez facilement l'algorithme sur internet, test si un nombre a donné est un témoin de Rabin-Miller pour le nombre n donné. Sans rentrer dans les détails mathématiques, un témoin de Rabin-Miller est une "preuve" que n est composé (n'est pas premier).

2 Protocole

1. Une fois la connexion établie, le serveur commence par envoyer un premier message annonçant le début du défi :

   -- Début du défi : Temoin de Rabin-Miller --

   Ce message n'attend pas de réponse.
2. Le serveur envoie ensuite une série de couples (n,a) où n et a sont des nombres binaires.
3. Pour chaque couple (n,a), le serveur doit recevoir en retour un booléen représentant si a est un témoin de Rabin-Miller pour n ou non.
4. Après chaque réponse, le serveur enverra un message commençant par "OK" ou "NOK" suivant si la réponse est correcte ou non.
5. A la fin du défi, le serveur enverra un message indiquant "Défi validé" ou "Défi échoué !". Aucune réponse n'est attendue.
6. Le serveur terminera la communication par le message "FIN", votre client devra alors fermer la socket. Aucune réponse n'est attendue.

3 Exemple de communication

Voici un exemple (incomplet) d'une communication pour ce défi. Dans cet exemple les "<" et ">" indiquent le sens de transfert de chaque message et ne doivent pas être présents dans la communication.

< -- Début du défi : Temoin de Rabin-Miller --
< 1110101101000111111100001100001110011010111110100101
< 1000100011010000011011101001101110101001110100011
> true
< OK
< 1000100011000001100100111110111101011110110011
< 1100101111100001111010101111000011100101111100
> true
< OK
< 1001111110010101110000001000001110010011001111111
< 1111000101110110011101010000111010111000010000
> false
< OK