MATH EN INFO

Test de Rabin-Miller

FICHE EXPLICATION Nº 19

1 Descriptif

L'objectif de ce défi est d'implémenter la méthode principale du test de Rabin-Miller. Cette méthode, dont vous trouverez facilement l'algorithme sur internet, test si un nombre n donné est premier ou non. La particularité de ce test est d'être probabiliste. Sans rentrer dans les détails mathématiques, le test de Rabin-Miller cherche une "preuve" que le nombre donné n'est pas premier. Une telle preuve est appelée un "témoin" de Rabin-Miller. Après avoir fait quelques tests élémentaires (n non premier, n>1...), l'algorithme va choisir au hasard 25 nombres et tester si l'un d'eux est un témoin. Si c'est le cas, le nombre n'est pas premier, si ce n'est pas le cas, il est fortement probable que le nombre soit 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 : Test de Rabin-Miller –

   Ce message n'attend pas de réponse.
2. Le serveur envoie ensuite une série de nombres binaires.
3. Pour chaque nombre binaire le serveur doit recevoir en retour un booléen représentant si le nombre est premier 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.

- MOSO3 -
CRYPTAGE ET COMPRESSION

< -- Début du défi : Test de Rabin-Miller --
< 1010000100001101101
> false
< OK
< 100000100111111111
> false
< OK
< 10011101011011111
> true
< OK