MATH EN INFO

Nombre Premier

FICHE EXPLICATION Nº 23

1 Descriptif

L'objectif de ce défi est d'implémenter une méthode de recherche de grand nombre premier utilisant l'algorithme de Rabin-Miller. Pour trouver un grand nombre premier, on se fixe un grand nombre au hasard (donné en paramètre de la méthode), et tant que celui-ci n'est pas premier, on l'augmente de 1. Notez cependant qu'il n'est pas nécessaire de tester si un nombre pair est premier.

La méthode à implémenter doit donc renvoyer le premier nombre premier plus grand que le nombre donné en paramètre.

Cette méthode peut sembler naïve, mais il est possible de démontrer que statistiquement, elle est très efficace. Elle permet facilement de trouver de très grands nombres premiers (en lui laissant un peu de temps bien sûr).

2 Protocole

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

   -- Debut du defi : Nombre Premier --

   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 le premier nombre premier plus grand que le nombre donné en paramètre.
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 "Defi valide" ou "Defi echoue !". 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.

< -- Debut du defi : Nombre Premier --
< 1100000000011010000100000110010010010111000101100100010000
> 1100000000011010000100000110010010010111000101100101000011
< OK
< 1101000011101010100110111011011111000101011100011111110000100
> 1101000011101010100110111011011111000101011100011111110100011
< OK
< 1000000101001001101101001100101010101011110001010010010110 0
> 1000000101001001101101001100101010101011110001010010010110 0001
< OK