UNIVERSITÉ PARIS 8 VINCENNES-SAINT-DENIS

TD/TP N01

Partie 1 : Outils mathématiques pour la cryptographie

Exercice 1: **Nombre premier**

Objectif

- Apprendre à utiliser les fonctions mathématiques en cryptographique

Ecrire une fonction qui affiche les nombres premiers inférieurs à un nombre N :

1. Méthode par division:

Le principe de la méthode par division:

Pour N entier donné on va regarder, après avoir initialisé un vecteur p (p(1)=1,p(2)=2,p(3)=3),si le nombre k (partant de 5 à N) est divisible par tous les nombres premiers inférieurs à lui-même: s'il ne l'est pas alors k est premier et il est rajouté à la liste p des nombres premiers, sinon on ne fait rien et on passe à k+1.

Partie 2 : Chiffrement de César

Exercice 2 : En utilisant le langage Python :

Soit n un entier relatif. On souhaite écrire un programme qui code un mot en décalant chaque lettre de l'alphabet de n lettres. Par exemple pour n = +3, (chiffrement de César):

Le mot ***COUCOU*** devient ainsi ***fryfry***.
On ne s'occupera que des lettres.

1) Définir deux listes, alp_clair et alp_chiff, contenant toute les lettres dans l'ordre alphabétique.
On pourra au besoin utiliser chr(n), où n est le code ASCII de la lettre voulue (la commande inverse dechrestord).Codes:
«a» à «z»: 65 à 90.

2) Écrire une fonction cesar(n, texte) qui prend un entier n et une chaîne de caractères texte, et retourne la chaîne codée par la méthode décrite ci-dessus.

3) Tester votre fonction. Comment décoder le message que vous venez de coder ?'.

5. Proposer une méthode de résolution, et casser le code.