

## Tests :

### 1. Génération de la clef

- a. Nous entrons la suite super croissante suivante : 5 10 35 51 150 322 666 99999
- b. Nous entrons un entier  $m$  supérieur à 101238 tel que  $m = 1020000$
- c. Nous entrons un entier  $e$  inférieur à 1020000 différent de 0 et premier avec  $m$  tel que  $e = 1019999$
- d. On obtient la clé publique suivante : 920001 1019334 1019678 1019850 1019949 1019965 1019990 1019995 ainsi que la permutation 8 7 6 5 4 3 2 1

### 2. Chiffrement d'un message

- a. Nous entrons la clef publique générée précédemment
- b. Nous rentrons le message à crypter tel que : Le lys fut très présent dans le monde romain chrétien et le monde romain byzantin
- c. Nous rentrons un nombre  $n$  compris entre 2 et  $p$  tel que  $p$  soit égal au nombre de nombres dans la clé publique.  $n = 6$
- d. On obtient le message crypté suivant : 2959284 2039012 2039627 1019965 3979134 2959013 2959644 3979249 1019850 2039012 2959800 3979593 3979478 1019334 920001 3059592 3059477 3978978 2039528 1019965 3059477 2959013 1939851 3979249 2959800 3058961 3979765 3059592 1019850 2039012 1939950 1939966 3979134 3978978 2039528 1019965 3979134 2039012 2039627 1019965 3979134 3058961 4999443 4078827 2959800 2039012 2039627 1019965 3059477 3058977 4999443 3979494 2039799 3058961 2959644 4078827 1019850 2039012 2959529 2039815 3059477 3978978 1939950 2959816 2959800 3058961 3059764 1019965 2959800 3978962 1019949 1019965 3979134 2039012 2039627 1019965 3979134 3058961 4999443 4078827 2959800 2039012 2039627 1019965 3059477 3058977 4999443 3979494 2039799 3058961 2959644 4078827 1019850 2039012 1939851 3979765 4078811 3058977 1939679 4078827 3979478 2039012 2959644 4078827

### 3. Déchiffrement d'un message

- a. Nous entrons la suite super croissante donnée dans la génération de la clef
- b. Nous entrons le nombre  $e$  choisi dans la génération de la clef
- c. Nous entrons le nombre  $m$  choisi dans la génération de la clef
- d. Nous entrons la permutation donnée dans la génération de la clef
- e. Nous entrons le nombre  $n$  utilisé lors du cryptage
- f. Nous entrons le message crypté (suite de chiffres)
- g. On obtient le message en clair : Le lys fut très présent dans le monde romain chrétien et le monde romain byzantin