

Laboratoire 6 – RSA

But :

Construire un algorithme permettant de crypter un message alphabétique (pas de majuscule, espace ou accent) en utilisant le système RSA

Consignes :

Le programme doit valider les données reçues (le message, p, q et e) et afficher des messages d'erreurs conséquents. La saisi du message peut être faite lettre par lettre.

- p est premier
- q est premier
- $p \cdot q \geq 1000$
- e est premier avec $(p-1) \cdot (q-1)$

Le message doit d'abord être transformé en nombre pour ensuite être groupé par 3 chiffres (par la droite).

Vous devez tester votre algorithme avec un jeu d'essais montrant la validation des données reçues.

Critères d'évaluation

Validation des données reçues	20 pts
Transformation du message en nombre	10 pts
Groupeement par 3 chiffres	20 pts
Encryptage	20 pts
Jeu d'essais	10 pts
Commentaires	10 pts
Affichage 10pts	10 pts

Un nombre ou une qualité de tests insuffisant(e) entraînera une pénalité pouvant aller jusqu'à 10%.

Dans tous les cas, si le programme compile avec erreur, au moins 50% des points seront retranchés.

10% par jour de retard seront retranchés.

Valeur relative : 1%