UNIVERSITE ABDELMALEK ESSAADI
ECOLE NATIONALE DES SCIENCES APPLIQUEES
TANGER

DEPARTEMENT : MATH-INFO

TP : Algorithme RSA et conception d'une application de chat sécurisée

- Un correspondant « A » choisit deux nombres premiers **p** et **q**. Il doit garder ces nombres secrets.

- « A » forme le produit de l'un par l'autre et obtient ici **N=pq**. Il doit choisir un autre nombre e < n et il doit faire en sorte que **e et (p-1)*(q-1) soient premiers** entre eux. *Appliquer pour cela l'algorithme d'Euclide.*

- « A » peut maintenant diffuser e et N par le moyen approprié. Ces deux nombres étant nécessaires pour le chiffrement, ils doivent être disponibles pour toute personne ayant à crypter un message pour « A ».

- Pour crypter un message, celui-ci doit d'abord être converti en un nombre M. Par exemple, un mot est traduit en bits selon le code ASCII, ou un autre codage. et ces bits sont considérés comme l'écriture du nombre M. Celui-ci est alors crypté pour obtenir le texte chiffré.

- Pour crypter ce message, cet expéditeur commence par chercher la clef publique de « A », et trouve N et e. Cela lui procure la formule de chiffrement requise pour crypter les messages pour « A » :

C:=M^e mod(N);

- Il très difficile de repartir de C pour retrouver le message original M. Mais « A » peut le déchiffrer, car il dispose de e, p et de q.
  Il calcule un nombre **d**, la clef de déchiffrement, encore appelée **clef privée**.
  Le nombre d est calculé selon la formule suivante: **ed=1 mod((p-1)(q-1)),** *pour cela, résoudre une «équation modulaire ».*

- Pour décrypter le message, on applique la formule suivante.

M:=C^d mod(N);

Etapes pour valider l’algorithme

1) Coder le message
2) attribuer des valeurs à p, q et e.
3) lancer la procédure de cryptage.
4) Décrypter le message obtenu et vérifier ce qu'on retrouve.

Préparation des clés

Faites connaître vos clefs publiques. Pour cela, ouvrez un fichier intitulé **clé_nom** , recopiez vos clefs publiques (pas la privée bien sûr !), et envoyez le dans un dossier partagé ou mettez le dans une base de donnée accessible.
Pour envoyer un message à quelqu'un, chercher ses clefs publiques, les copier dans votre répertoire crypter et envoyer.

Deuxième test

Réaliser une application de chat sécurisée avec RSA (validation sur machine virtuelle ou réseau local).