**EST –Béni Mellal** **TD 3** **DUT-GI2/ARI2**

# (Cryptographie à clé publique : RSA)

## Exercice 1 :

On considère l'ensemble $Z_{30} = \{0, 1, 2, . . . , 29\}$ des entiers modulo $30$. Rappelons qu'un élément $a \in Z_{30}$ est inversible si, et seulement si, $pgcd(a, 30) = 1$.

1) Calculer $\phi(30)$, *puis é*numérer tous les éléments de $Z_{30}$ inversibles.
2) Calculer l'inverse des éléments trouvés à la question précédente.

## Exercice 2 :

Bob utilise le protocole RSA et publie sa clé publique $n = 187$ et $e = 3$.

1) Encoder le message $m = 15$ avec la clé publique de Bob.
2) En utilisant le fait que $\phi(n) = 160$, retrouver la factorisation de $n$, puis la clé privée de Bob.

## Exercice 3 :

Alice utilise un système RSA construit utilisant $p = 13$, $q = 19$.

1) Quelles sont les valeurs de $n$ et $\phi(n)$?
2) Si Alice doit choisir la deuxième plus petite valeur valide qui sert comme exposant de chiffrement. Quelle est la valeur adéquate de $\boldsymbol{e}$ et celle de la clé publique à utiliser dans ce cas ?
3) Quelle sera sa clé privée correspondante ?
4) Bob veut transmettre le message clair $\boldsymbol{m = 11}$ à Alice, quel est le message chiffré $\boldsymbol{c}$ correspondant ?
5) Quel est le message clair $\boldsymbol{m}$ correspondant au message chiffré $\boldsymbol{c = 23}$?

Considérons le cas où Bob possède le même module $\boldsymbol{n}$ que Alice, mais avec un exposant de chiffrement $\boldsymbol{e' \neq e}$ et $\boldsymbol{pgcd(e, e') = 1}$. Supposons que Alice et Bob chiffrent et s'échangent un même message $\boldsymbol{m}$ et que Oscar intercepte les deux cryptogrammes $\boldsymbol{c_A = m^e \bmod n}$ et $\boldsymbol{c_B = m^{e'} \bmod n}$, qu'elle sait être deux chiffrements du même message $\boldsymbol{m}$.

6) Montrez qu'Oscar peut alors très facilement découvrir le message $m$.