Université de Cergy-Pontoise **2006-2007**
Introduction à la cryprographie **UE libre**

Examen du 1er Juin 2007

Exercice 1 :
1. A quelle condition nécessaire et suffisante un élément de $\mathbb{Z}/28\mathbb{Z}$ est-il inversible ?
2. Calculer $\varphi(28)$.
3. Déterminer tous les éléments inversibles de $\mathbb{Z}/28\mathbb{Z}$.

Exercice 2 : Un phare émet un signal jaune toutes les 15 minutes et un signal rouge toutes les 28 minutes. On aperçoit le signal jaune à 0h02 et le signal rouge à 0h08. A quelle heure verra-t-on pour la première fois, les deux signaux émis en même temps ?

(On notera x la durée en minutes séparant 0h00 et le moment de la première coincidence et on énoncera de façon précise le théorème utilisé.)

Exercice 3 : Bob utilise le protocole RSA et fait connaître 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 $\varphi(N) = 160$, retrouver la factorisation de N puis la clé privée de Bob.

Exercice 4 : Bob et Bart ont pour clés publiques RSA respectivement : (N, e_1) et (N, e_2) avec e_1 et e_2 premiers entre eux. Alice envoie le même message m crypté par les clés publiques RSA de Bob et Bart en C_1 et C_2.
1. Montrer qu'il existe deux réels u et v tels que $u \cdot e_1 + v \cdot e_2 = 1$.
2. Expliquer comment Oscar qui connait $C_1 = m^{e_1} \mod N$ et $C_2 = m^{e_2} \mod N$, peut retrouver le message m sans connaître les clés privées de Bob et Bart.