Université de Cergy-Pontoise **2007-2008**
Introduction à la cryprographie **UE libre**

Examen du 19 Mai 2008 : deuxième session

Exercice 1 :
1. Donner la définition du chiffrement affine.
2. En utilisant la correspondance $A \leftrightarrow 0, \ldots, Z \leftrightarrow 25$, numériser le message suivant : UNE MAISON.
3. Chiffrer le message numérisé précédemment avec le chiffrement affine et la clé $(a, b) = (15, 8)$.
4. On considère l'entier $a = 15$. Calculer $pgcd(15, 26)$ et déterminer deux entiers u et u tels que $15u+26v = pgcd(15, 26)$. En déduire l'inverse de 15 mod 26.
5. Calculer la fonction de déchiffrement pour le chiffrement affine qui utilise la clé $(15, 8)$
6. Déchiffrer le message $C = (16, 17, 24, 18, 10, 21, 18)$ qui a été chiffré avec la clé $(15, 8)$. On donnera le message avec des lettres.

Exercice 2 : Calculer la fonction indicatrice d'Euler $\varphi(n)$ dans chacun des cas suivants :
1. $n = 33$
2. $n = 34$
3. $n = 35$
4. $n = 36$

Exercice 3 : Calculer s'il existe les inverses suivants :
1. $x = 5^{-1} \mod 10$
2. $x = 5^{-1} \mod 12$
3. $x = 6^{-1} \mod 13$
4. $x = 4^{-1} \mod 5$

Exercice 4 : Le mercredi 7 Février, 3 étudiants décident de fixer un jour pour faire une partie de cartes. Le premier est occupé tous les jours sauf le jeudi. Le deuxième pourrait le vendredi 9 Février et ensuite tous les 8 jours. Le troisième aurait pu le mercredi 7 Février et ensuite tous les 5 jours. On suppose que le mois de Février compte 28 jours. Quand vont-ils pouvoir jouer aux cartes ? Quel jour de la semaine sera-t-on ?

Exercice 5 :
1. Rappeler la définition du cryptosystème RSA : les paramètres publics et privés, le lien entre les clés publiques et privées, les fonctions de chiffrement et de déchiffrement.
2. Soit le cryptosystème RSA pour lequel l'exposant public $e = 9$ est connu.
   (a) On considère les paires $(253, 9)$ et $(221, 9)$. Laquelle de ces paires donne une clé publique valide ?
   (b) Déterminer la clé secrète associée à la clé publique choisie à la question précédente ?
   (c) Avec le cryptosystème ainsi déterminé, si le message chiffré est $C = 2$, quel est le message clair M ?