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

Examen du 23 Avril 2007

Exercice 1 :

1. Donner la définition du chiffrement affine
2. A quelle condition, l'opération de déchiffrement est-elle possible ?
3. En utilisant un chiffrement affine avec $a = 3$ et $b = 5$, chiffrer le texte suivant :
   "RENDEZ VOUS AU METRO".
   (On considérera que les 26 lettres de l'alphabet sont représentées par les chiffres 0 à 25 et on donnera le message chiffré avec des lettres)

Exercice 2 : L'armée de César comptait plus de 1000 hommes et moins de 3000. Lorsqu'il voulut la dénombrer par groupes de 11, il n'en resta pas ; par groupe de 9, il en resta 5 ; par groupe de 13, il en resta 8. Combien y avait-il de soldats dans cette armée ?
(On énonera de façon précise le théorème utilisé)

Exercice 3 :

1. Ecrire 103 en base 2.
2. Décomposer 143 en facteurs premiers.
3. Calculer $\varphi(143)$. Combien y a-t-il de nombres compris entre 1 et 142 qui ne sont pas inversibles modulo 143 ?
4. Enoncer le théorème d'Euler-Fermat. En déduire $x^{120} \mod 143$ pour x premier avec 143.
5. Calculer $103^{-1} \mod 120$.
6. Calculer $27^{103} \mod 143$.
7. Alice et Bob ont lu dans la revue "Pour la science" un article sur le principe de cryptographie RSA. Ils décident de le tester sur un exemple simple pour vérifier qu'ils ont compris. Pour cela, Alice choisit la clé publique ($n = 143$ et $e = 7$). Bob choisit alors un entier, compris entre 0 et 142, puis le code avant de transmettre le résultat à Alice : 27. Pouvez-vous aider Alice à retrouver l'entier choisi par Bob ? Justifiez soigneusement votre réponse ; en particulier, rappelez le principe du codage et du décodage, et calculez la clé secrète qui permet le décodage. (On peut utiliser les résultats des questions précédentes.)