TD de cryptographie

1. $2Z$ est-il un sous groupe additif de Z? Déterminer le coset de $2Z$ dans Z contenant 1. Déterminer $Z/2Z$.
2. $(Z_6, +, 0)$ est-il isomorphe à $(Z_{12}^*, ., 1)$? Trouver un groupe isomorphe à $(Z_{14}^*, ., 1)$.
3. Trouver un groupe multiplicatif isomorphe à $(Z_6, +, 0)$
4. Soit $\phi : G_1 \to G_2$ un morphisme de groupes (finis). Montrer que $Im(\phi)$ est un sous-groupe de G_2.
5. Montrer que $C_x = \{y \in G |\ xy = yx\},\ x \in G$, est un groupe de G (G étant un groupe fini).
6. Calculer $\phi(35)$ et $\phi(28)$.
7. Calculer $51 * 25 \mod 91$, $25^{71} \mod 91$.
8. Calculer $\phi(85)$, $\phi(1024)$, $\phi(759)$, $\phi(105)$, $\phi(1155)$, $\phi(48)$.
9. Une bande de 17 pirates s'est emparée d'un butin composé de pièces d'or d'égale valeur. Ils décident de se les partager également, et de donner le reste au cuisinier chinois. Celui-ci reçoit alors 3 pièces. Mais les pirates se querellent, et 6 d'entre eux sont tués. Après un nouveau partage du même butin, le cuisinier reçoit 4 pièces. Dans un naufrage ultérieur, seuls le butin, 6 pirates et le cuisinier sont sauvés, et le partage donne alors 5 pièces d'or à ce dernier. Quelle est la fortune minimale que peut espérer le cuisinier s'il décide d'empoisonner les derniers pirates?
10. Calculer $8^{11} \mod 11$, $7^{11} \mod 11$, $5^8 \mod 7$, $14^{16} \mod 17$, $67^{258} \mod 68$, $3^{45} \mod 5$, $7^{31} \mod 11$, $4^{25} \mod 35$, $7^8 \mod 30$.

Les calculs se font avec le logiciel Xcas (présent sur vos machines)

1. Déterminer p et q, deux entiers premiers d'au plus 1024 bits. Calculer $n := p * q$ puis $phi := (p-1) * (q-1)$. Que remarquez-vous? Comment expliquez-vous ce que vous remarquez?
2. Calculer la taille en bits de p, q, et n.

Le chiffrement RSA

1. Ecrivez l'énoncé du théorème d'Euler.
2. Décrivez le protocole RSA.
3. Soit $(p, q) = (5953, 7253)$, le message à chiffrer est $m = 1794$ et $e = 5$.
   Déterminez le chiffré mc
4. Essayez de déchiffrer mc pour retrouver le message clair.
5. Essayez maintenant d'utiliser le théorème des restes Chinois dans le calcul du déchiffrement.