Exercice 1.

a) Trouver l'ordre de 2 modulo 3 ; l'ordre de 2 modulo 5 ; l'ordre de 7 modulo 10 ; l'ordre de 9 modulo 10.

b) Montrer qu'il n'existe aucun entier k tel que $2^k \equiv 1 \pmod{10}$. Expliquer.

Exercice 2.

1. Soit n dont l'écriture en base 10 est donnée par $n = \sum_{i=0}^{k} b_i 10^i$. Donner une expression de $n \bmod 11$ et en déduire que la valeur de $n \bmod 11$ est la somme alternée des chiffres de n, par exemple $1234 \bmod 11 = 4 - 3 + 2 - 1 = 2$.
2. Vérifier que 101 est un nombre premier et trouver un procédé similaire pour calculer le reste d'un entier modulo 101. Calculer $1234 \bmod 101$.
3. Calculer $2^{11} \bmod 101$ et $18^{23} \bmod 101$.

Exercice 3.

1. Vérifier que 2 est un générateur du groupe multiplicatif $(\mathbb{F}_{11}^*, \times)$.
2. Trouver le logarithme discret de 6 en base 2 modulo 11.
3. Quel est le secret commun qu'établissent deux correspondants A et B qui utilisent le protocole de Diffie-Hellmann avec $p = 11$, $g = 2$ et s'ils choisissent respectivement $X_A = 7$ et $X_B = 8$ comme paramètre privé.

Exercice 4.

1. Vérifier que 2 est un générateur du groupe multiplicatif $(\mathbb{F}_{101}^*, \times)$ (n'effectuer que deux exponentiations).
2. Deux correspondants A et B qui utilisent le chiffrement ElGamal avec $p = 101$, $g = 2$.
   La clé privée de A est $X_A = 17$. Quelle est sa clé publique ?
   La clé privée de B est $X_B = 25$. Quelle est sa clé publique ?
3. A tire au hasard la valeur $k = 41$. Quel est l'entête du message que A transmettra à B. Quelle est la valeur de la clé de session ?

Exercice 5. (méthode de Pohlig-Hellman)

Dans cet exercice, les entiers sont considérés modulo $p = 31$. L'ordre du groupe multiplicatif $(\mathbb{F}_{31}^*, \times)$ est $31 - 1 = 30 = 2 \times 3 \times 5$.

1. Vérifier que 3 est un élément générateur du groupe multiplicatif $(\mathbb{Z}/31\mathbb{Z}^*, \times)$.
2. Montrer que $\alpha_1 = 3^{15}$ est d'ordre 2, que $\alpha_2 = 3^{10}$ est d'ordre 3 et que $\alpha_3 = 3^6$ est d'ordre 5
3. On veut déterminer x, le logarithme discret de $y = 17$ en base 3. Calculer $y_1 = 17^{15}$, $y_2 = 17^{10}$ et $y_3 = 17^6$.
   Trouver x_1 tel que $y_1 = \alpha_1^{x_1}$, x_2 tel que $y_2 = \alpha_2^{x_2}$ et x_3 tel que $y_3 = \alpha_3^{x_3}$.
   Combien d'opérations au maximum sont-elles nécessaires pour trouver les x_i ?
   vérifier que $\begin{cases} x \equiv x_1 \pmod 2 \\ x \equiv x_2 \pmod 3 \\ x \equiv x_3 \pmod 5 \end{cases}$
   En déduire la valeur de x.
4. Quelle condition doit satisfaire le nombre premier p pour que cette méthode ne soit pas applicable ?