Exercice 1. a) 2 ; b) 4 ; c) 4 ; d) 2 ;
e) 2^k est pair, il ne peut pas se terminer par 1. En fait, 2 n'est pas inversible en Modulo 10 puisque 2 et 10 ne sont pas premiers entre eux. Pas suite 2 n'appartient pas au groupe multiplicatif des elements inversibles Modulo 10 , c'est à dire au groupe mulitplicatif $(\mathbb{Z}/10\mathbb{Z})^*$. L'ordre de 2 modulo 10 n'a pas de sens !!(et donc n'existe pas).

Exercice 2.
1. $10 = 11 - 1$ donc $10 \equiv -1 \bmod 11$. Modulo 11, $n = \sum_{i=0}^{k} b_i 10^i = \sum_{i=0}^{k} b_i (-1)^i$.
2. *Idem* avec $100 = 101 - 1$, donc $100 \equiv -1 \bmod 101$. Prendre la somme alternée des chiffres deux par deux modulo 100. $1234 \equiv 34 - 12 \equiv 22 \pmod{101}$.
3. $2^{11} = 2048 \equiv 48 - 20 \equiv 28 \pmod{101}$
   Comme $23 = 16 + 4 + 2 + 1$, $18^{23} = 18^{16} \times 18^4 \times 18^2 \times 18$. $18^2 = 324 \equiv 24 - 3 \equiv 21 \pmod{101}$. $18^4 \equiv 21^2 \equiv 441 \equiv 41 - 4 \equiv 37 \pmod{101}$. $18^8 \equiv 37^2 \equiv 1\,369 \equiv 69 - 13 \equiv 56 \pmod{101}$. $18^{16} \equiv 56^2 \equiv 3\,136 \equiv 36 - 31 \equiv 5 \pmod{101}$. $18^{23} \equiv 5 \times 37 \times 21 \times 18 \equiv 69\,930 \equiv 30 - 99 + 6 \equiv -63 \equiv 38 \pmod{101}$.

Exercice 3.
1. Les puissances successives de 2 modulo 11 sont $(1, 2, 4, 8, 5, 10, 9, 7, 3, 6, 1, \ldots)$.
2. $2^9 \equiv 6 \pmod{11}$ donc $\log_2(6) = 9 \bmod 11$.
3. $K = 2^{7\times 8} \equiv 2^{56} \equiv 2^6 \equiv 64 \equiv 4 - 6 \equiv 9 \pmod{11}$.

Exercice 4.
1. Les diviseurs premier de 100 sont 2 et 5. L'ordre de 2 modulo 101 est nécessairement un diviseur de 100. Il suffit de vérifier que $2^{100/2}$ et $2^{100/5}$ ne sont pas égaux à 1. C'est bien le cas, car d'une part $2^{50} = (2^2 5)^2$ et $2^{25} = 33\,554\,432 \equiv 32 - 44 + 55 - 33 \equiv 10 \pmod{101}$ donc $2^{50} \equiv 10^2 \equiv 100 \equiv -1 \pmod{101}$, et d'autre part $2^{20} = 1\,048\,576 \equiv 76 - 85 + 4 - 1 \equiv -6 \equiv 95 \pmod{101}$. L'ordre de 2 est donc 100 modulo 101.
2. Clé publique de A : $2^{17} \equiv 131\,072 \equiv 72 - 10 + 13 \equiv 75 \pmod{101}$
   Clé publique de B : $2^{25} \equiv 10 \pmod{101}$
3. Entête : $2^{41} = 2 \times (2^{10})^4$; $2^{10} \equiv 1024 \equiv 24 - 10 \equiv 14 \pmod{101}$. $14^4 \equiv 38\,416 \equiv 16 - 84 + 3 \equiv -65 \equiv 36 \pmod{101}$. $2^{41} \equiv 2 \times 36 \equiv 72 \pmod{101}$.
   Clé de session :$10^{41} = 10^4 0.10 = (10^2)^2 0.10 \equiv (-1)^2 0.10 \equiv 10 \pmod{101}$

Exercice 5.
1. Dans $\mathbb{Z}/31\mathbb{Z}$, on a $3^{30/2} = 30$, $3^{30/3} = 25$ et $3^{30/5} = 16$.
   N.B. 2 n'est pas générateur car $2^{30/2} = 1$.
2. Si α est d'ordre r pour tout diviseur d de r, l'ordre de $\beta = \alpha^{r/d}$ est d, car $\beta^d = \alpha^r = 1$ et d est minimal, sinon r ne le serait pas. $\alpha_1 = 30$, $\alpha_2 = 25$ et $\alpha_3 = 16$.
3. $y_1 = 30$, $y_2 = 25$ et $y_3 = 8$.
   $x_1 = 1$, $x_2 = 1$ et $x_3 = 2$. Il faut au plus respectivement 2, 3 et 5 multiplications pour tester toutes les possibilités. En utilisant un algorithme plus élaboré (Pas-de-bébé-pas-de-géant par exemple) on peut encore réduire cette complexité.
   On a $\alpha_1^{x_1} = \alpha^x$. Comme α_1 est d'ordre 2, on a $x \equiv x_1 \bmod 2$, *idem* pour les deux autres cas.
   En résolvant le système, on trouve $x = 7$
4. Pour que cette méthode soit difficile, il ne faut pas pouvoir factoriser $p - 1$ avec uniquement des petits facteurs premiers.