Exercise 1: Factorization

Ici on a $n1 = p^2$, donc il est très facile de retrouver la valeur de p, et donc celle de $\varphi(n1)$. Attention tout de même, $\varphi(p^2) = p^2 - p \neq (p-1) * (p-1)$.

À partir de là, on retrouve a valeur `d = inverse_mod(e,` $\varphi(p^2)$), ce qui permet de déchiffrer le message.

Exercice 2 : Decryption oracle

On ne peut pas demander de déchiffrer c directement, mais on peut envoyer $c' = 2^e \times c \bmod n$.
Le serveur répond alors par $m' = c'^d \bmod n = (2^e \times c)^d \bmod n = 2 * m \bmod n$. Il suffit alors de multiplier m' par l'inverse de 2 modulo n pour trouver le résultat.