Exercice1 *Chiffrement RSA (5 points)* **C.R_2015**

Alice et Bob, deux interlocuteurs à travers un réseau non sécurisé. La clé publique de Bob est $(e_B = 3, N_B = 55)$ *et* $N_B = p_B \times q_B$, *avec* $p_B = 11$. *La clé privé d'Alice est* $(d_A = 7, N_A = 33)$ *et* $N_A = p_A \times q_A$, *avec* $p_A = 11$.

1. *Pour assurer la confidentialité de ses messages, Bob chiffre un message m1 et envoi son chiffré c1= 12 à Alice. Quel est la valeur du message m1 après son déchiffrement par Alice.*
2. *Pour assurer l'authenticité de ses messages, Alice signe un message m2* avec sa clé RSA et chiffre le résultat avec la clé RSA de Bob. Bob reçoit ainsi le message 23. Quelle est le message m2 correspondant ?

Exercice 3 Exponentiation modulaire *(3 points)* **C.R_2015**

Calculer par la méthode basée sur la décomposition de l'exposant en décimale, l'exponentiation suivante : $15^{1573} mod\ 311$.
Détaillez vos réponses