**7.12** Pour vérifier l'authenticité du message, c'est-à-dire que le message a bien été envoyé par Alice, Bob doit contrôler que $m = s^{e_A} \mod n_A$.
En l'occurrence, Bob doit s'assurer que $341076^{251} \equiv 11911 \mod 638611$.

| $x$ | reste $r$ | $n$ | $341076^{2^n} \mod 638611$ | contribution (si $r = 1$) |
|---|---|---|---|---|
| 251 | 1 | 0 | 341076 | 341076 |
| 125 | 1 | 1 | $341076^2 \equiv 264961$ | 264961 |
| 62 | 0 | 2 | $264961^2 \equiv -91542$ | |
| 31 | 1 | 3 | $(-91542)^2 \equiv 84222$ | 84222 |
| 15 | 1 | 4 | $84222^2 \equiv 292907$ | 292907 |
| 7 | 1 | 5 | $292907^2 \equiv 315854$ | 315854 |
| 3 | 1 | 6 | $315854^2 \equiv -61104$ | $-61104$ |
| 1 | 1 | 7 | $(-61104)^2 \equiv -259701$ | $-259701$ |

$$
\begin{aligned}
341076^{251} &\equiv \underbrace{341076 \cdot 264961}_{\equiv 79593} \cdot \underbrace{84222 \cdot 292907}_{\equiv 309035} \cdot 315854 \cdot \underbrace{(-61104) \cdot (-259701)}_{\equiv -74835} \\
&\equiv \underbrace{79593 \cdot 309035}_{\equiv 281479} \cdot \underbrace{315854 \cdot (-74835)}_{\equiv -25147} \\
&\equiv 281479 \cdot (-25147) \\
&\equiv 11911
\end{aligned}
$$

Bob en conclut que le message est bien valide.