Chamblandes 2009 — Problème 3

1. Pour décrypter le message codé c, il faut calculer $c^d \mod n$.
   Utilisons l'algorithme d'exponentiation modulaire pour calculer $322^{13} \mod 493$:

x	reste r	n	$3^{2^n} \mod 493$	contribution (si $r = 1$)
13	1	0	322	322
6	0	1	$322^2 \equiv 154$	
3	1	2	$154^2 \equiv 52$	52
1	1	3	$52^2 \equiv 239$	239

   $322^{13} \equiv \underbrace{322 \cdot 52}_{\equiv -18} \cdot 239 \equiv -18 \cdot 239 \equiv 135 \mod 493$

   On a obtenu $m = 135$: l'armée bordure posséderait 135 canons.

2. Il reste à présent à s'assurer de l'authenticité du message, c'est-à-dire qu'il provient bien de l'espion Éon.

   Commençons par décrypter la signature en calculant $287^{13} \mod 493$:

x	reste r	n	$3^{2^n} \mod 493$	contribution (si $r = 1$)
13	1	0	287	287
6	0	1	$287^2 \equiv 38$	
3	1	2	$38^2 \equiv -35$	-35
1	1	3	$(-35)^2 \equiv 239$	239

   $287^{13} \equiv \underbrace{287 \cdot (-35)}_{\equiv -185} \cdot 239 \equiv -185 \cdot 239 \equiv 155 \mod 493$

   L'auteur du message a donc envoyé la signature $s = 155$.

   Il reste à encoder la signature reçue avec la clé publique d'Éon pour s'assurer qu'elle correspond bien au message reçu, c'est-à-dire calculer $155^7 \mod 437$:

x	reste r	n	$3^{2^n} \mod 493$	contribution (si $r = 1$)
7	1	0	155	155
3	1	1	$155^2 \equiv -10$	-10
1	1	2	$(-10)^2 \equiv 100$	100

   $155^7 \equiv \underbrace{155 \cdot (-10)}_{\equiv 198} \cdot 100 \equiv 135 \mod 437$

   Comme le résultat 135 est conforme au message reçu, l'authenticité du message ne fait plus de doute et l'on est désormais certain que l'armée bordure possède 135 canons.