

**7.10** On factorise facilement la clé publique :  $n = 35 = 5 \cdot 7$ .

Par conséquent,  $\varphi(n) = (5 - 1)(7 - 1) = 24$ .

L'exposant de décryptage  $d$  satisfait la congruence  $5d \equiv 1 \pmod{24}$ .

Cette congruence se résout facilement :  $5 \cdot 5 \equiv 25 \equiv 1 \pmod{24}$ .

C'est pourquoi  $d = 5$ .

Pour décrypter le code 10, il faut calculer  $10^5 \pmod{35}$  :

$x$	reste $r$	$n$	$10^{2^n} \pmod{35}$	contribution (si $r = 1$ )
5	1	0	10	10
2	0	1	$10^2 \equiv -5$	
1	1	2	$(-5)^2 \equiv -10$	-10

$$10^5 \equiv 10 \cdot (-10) \equiv 5 \pmod{35}$$

On conclut que le message en clair est  $m = 5$ .