4. En un sistema criptogràfic RSA amb $p = 7$ i $q = 11$, troba la clau pública (N, c) i la clau privada (N, d) apropiades.

Seguim els passos de les transparencies.

1. $p=7$ i $q=11$

2. Compute $N = p \cdot q \Rightarrow N = 7 \cdot 11 = 77$

3. Compute $\phi(N) = (p-1)\cdot(q-1) \Rightarrow \phi(N) = (6)\cdot(10) = 60$

4. Choose $c \in \mathbb{Z}^*_{\phi(N)} \Rightarrow c = 7$

5. Compute d such that $cd \equiv 1 \bmod 60$

Utilitzem EXT-EUC per trobar d. Podem trobar x, y en que

$60x + 7y = 1 \Rightarrow x = 2$ e $y = -17$

$y = -17 + 60 = \boxed{43} \Rightarrow$ perquè sigui positiu. $\boxed{d=43}$

La clau publica es $Pb(77, 7)$, $Sb(77, 43)$.

2. **2EXP modular**. Doneu un algorisme de temps polinòmic que amb entrada els enters a, b, c i un nombre primer p computi $a^{b^c} \mod p$.

Resolem el problema per el teorema del petit Fermat.

$$a^{b^c} \bmod p \equiv a^{b^c \bmod (p-1)} \bmod p.$$

1. Primer computem $(b \bmod (p-1))$ en temps $O(\log b \log p)$

2. Computem $(b^c \bmod (p-1))$ utilitzant la exponenciació binaria. Això consisteix en $O(\log c)$ multiplicacions de tamany com a molt p. Cada multiplicació consisteix en $O(\log^2 p)$ de temps, per tant el cost total $O(\log c \log^2 p)$.

3. Computem $a \bmod p$ en temps $O(\log a \log p)$

4. Tornem a utilitzar la exponenciació binaria per computar $a^{b^c} \bmod p$ al seu cost $O(\log p \log^2 p) = O(\log^3 p)$.

El cost total es la suma de cost de tots els apartats. El cost te una cota superior de $O(n^3)$ on n es el tamany de l'entrada que en aquest cas es $[\log a + \log b + \log c + \log p = n]$