$p = 131, q = 137$

$n = p \cdot q = 17947$

$\phi = (p-1)(q-1) = 17680$

i) TEST: $e_1 = 343$

$17680 = 51 \cdot 343 + 187$

$343 = 1 \cdot 187 + 156$

$187 = 1 \cdot 156 + 31$

$156 = 5 \cdot 31 + 1$

$31 = 31 \cdot 1 + 0$ ok!

$1 = 156 - 5(187 - 1 \cdot 156)$

$\Rightarrow 1 = 156 - 5 \cdot 31$

$= 6 \cdot 156 - 5 \cdot 187$

$= 6(343 - 1 \cdot 187) - 5 \cdot 187$

$= 6 \cdot 343 - 11 \cdot 187$

$= 6 \cdot 343 - 11(17680 - 51 \cdot 343)$

$= 567 \cdot 343 - 11 \cdot 17680$

ALLTSÅ $1 = 567 \cdot 343 - 11 \cdot 17680$

$= 567 \cdot 343 \bmod \phi$

$d_1 = e^{-1} \bmod \phi$

$= 567$

(och därmed har vi också svar på b)

TEST $e_2 = 351$

$17680 = 50 \cdot 351 + 130$

$351 = 2 \cdot 130 + 91$

$130 = 1 \cdot 91 + 39$

$91 = 2 \cdot 39 + 13$

$39 = 3 \cdot 13 + 0$ ej ok.

BARA $e_1$ fungerar som RSA exponent.

c) $4^e \bmod n$

$4^{343} = 4 \cdot 4^{342} = 4(4^{171})^2$

$4^{171} = 4 \, 4^{170} = 4(4^{85})^2$

$4^{85} = 4(4^{84}) = 4(4^{42})^2$

$4^{42} = (4^{21})^2$

$4^{21} = 4(4^{10})^2$

$4^{10} = (4^5)^2 = (1024)^2 \bmod n = 7650$

$= 4 \cdot (7650)^2 \bmod n = 7279$

$= (7279)^2 \bmod n = 4297$

$= 4(4297)^2 \bmod n = 4931$

$= 4(4931)^2 \bmod n = 4251$

$= 4 \cdot (4251) \bmod n = 11435$