Homework 3 - Due Monday November 2, by 5pm - in my mailbox

Problem 1
This problem gives an example of what's wrong with deterministic encryption. Suppose Bob and David have two independent Rabin public keys $n_B$ and $n_D$, respectively. Suppose Alice has a single message $m$ to send to both of them, and $m$ is a square in both $\mathbb{Z}_{n_B}^*$ and $\mathbb{Z}_{n_D}^*$. She encrypts it with plain Rabin twice to get $c_B = m^2 \mod n_B$ and $c_D = m^2 \mod n_D$. Show how an eavesdropper Eve who intercepts $c_B$ and $c_D$ can recover $m$.

(Hint: if Rabin public keys are generated independently, then they are relatively prime with all but negligible probability. You can use the fact that Chinese remainder theorem applies not only to primes, but to any pair of relatively prime integers.)

Problem 2
Suppose you have a device (smart card, computer, etc.) that is performing an RSA secret key operation (computing $m = c^d \mod n$ for some $c$) using CRT: separately computing $m_p = c^d \mod p$ and $m_q = c^d \mod q$ and then combining. Suppose you can hit the device with just enough radiation to cause exactly one of the two modular exponentiations to compute an incorrect value, $m_p' \neq m_p$, while the other modular exponentiation computes the correct $m_q$, thus causing the output to be some $m' \neq m$. Show how to factor $n$ given $c$ and $m'$ (and, of course, the RSA public key $(n, e)$). This is an actual attack that can be carried out on certain smart cards. (Hint: it may be easier to first figure out first how to factor $n$ given $m, m'$, and the public key $(n, e)$.)