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.)

Using Chinese Remainder Theorem with moduli \( n_B \) and \( n_D \), and values \( c_B \) and \( c_D \), compute the unique value \( c \), \( 0 \leq c < n_B n_D \) such that \( c \equiv c_B \mod n_B \) and \( c \equiv c_D \mod n_D \). Recall that \( m^2 \equiv c_B \mod n_B \) and \( m^2 \equiv c_D \mod n_D \). Note that because \( m < n_B \) and \( m < n_D \), \( 0 \leq m^2 < n_B n_D \). Thus, \( m^2 \) satisfies the same three conditions as \( c \). But CRT says that there is only one integer satisfying these three conditions. Hence, \( m^2 = c \) as integers. Hence, to find \( m \), simply compute the positive integer square root of \( c \) (positive because we know that \( m \) was positive to begin with—it was a square).

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, \( m'_p \not\equiv m_p \), while the other modular exponentiation computes the correct \( m_q \), thus causing the output to be some \( m' \not\equiv m \). Show how to factor \( n \) given \( c \) and \( m' \) and \( (n, e) \). 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 \( (n, e) \).)

Let \( CRT : \mathbb{N} \times \mathbb{N} \rightarrow \{0, \ldots, n-1\} \) denote the function for which \( CRT(x, y) = z \) if and only if \( x \equiv z \mod p \) and \( y \equiv z \mod q \). By the Chinese Remainder Theorem, we know such a function exists. We are given \( c, m' = CRT(m'_p, m_q), n \) and \( e \). Let \( m = CRT(m_p, m_q) = c^d \mod n \). From the Chinese Remainder Theorem it follows that \( m' \not\equiv m \). In particular \( m' \not\equiv m \mod p \), but \( m' \equiv m \mod q \). Obviously, \( m'e \equiv me \equiv c \mod q \). But also \( m'e \not\equiv me \mod c \). Finally we have \( m'e - c \equiv 0 \mod q \) and so \( \gcd(m'e - c, n) = q \), and since this is efficiently computable, we can factor \( n \).