PMAT 329 Introduction to Cryptography

ADDENDUM to ASSIGNMENT 3

Problem 1:

In part (c), note that $\gcd(C, n) > 1$. Normally, this means that if a cryptanalyst received this ciphertext, he could factor n and break this system; in fact, the message corresponding to ciphertext C was not coprime to n in the first place. However, this is not really relevant here as you've already factored n and broken the scheme in part (b).

You can still decrypt C, i.e. compute $C^d \pmod{n}$, which is what you are asked to do here. In fact, by Problem 13, pp. 160-161, of the Trapp/Washington book, RSA will still work even if $\gcd(M, n) > 1$; that is, you still have $M^{ed} \equiv M \pmod{n}$.

Problem 3:

The formula $\left(\frac{q+p}{2}\right)^2 = n - \left(\frac{q-p}{2}\right)^2$ should read $\left(\frac{q+p}{2}\right)^2 = n + \left(\frac{q-p}{2}\right)^2$. However, this makes no difference in the solution to this problem.

Problem 4:

Actually, $e = 2$ is an impossible choice for an RSA encryption exponent because $\gcd(e, \phi(n)) > 1$ always. However, you can still use exponent 2 for a cryptosystem; in fact, that's a special case of the Rabin system given in Problem 5 (with $b = 0$). Here, encryption of a message M is accomplished via modular squaring, i.e. $C \equiv M^2 \pmod{n}$. (Note that encryption is *extremely* fast!)

In Problem 5, you show that if $p + 1$ and $q + 1$ are both divisible by 4, then decryption is possible. Essentially, what is happening here is that you compute square roots of C modulo p and modulo q and combine them to a square root modulo n which gives you M. Even if $p + 1$ (or $q + 1$) is not divisible by 4, there exists a fast probabilistic algorithm that computes square roots modulo p (or modulo q), so decryption is possible.

In any case, here is what this problem asks you to do:

Scenario (a): Two people send the same message M to two different receivers. A different modulus is used for each transmission, but $e = 2$ for both.

This means that an adversary is in possession of two ciphertexts C and C' where $C \equiv M^2 \pmod{n}$, $C' \equiv M^2 \pmod{n'}$, and n, n' are the respective moduli of the two users (which of course are also known to the adversary). Prove that from this information, the adversary can obtain M *without* having to factor n or n'.

Scenario (b): Two different messages which differ by only a few characters (the adversary can deduce the position of these characters) are sent under the same key. Here, $e = 2$ and n is the same for both messages.

This means that an adversary is in possession of two ciphertexts C and C' where $C \equiv M^2 \pmod{n}$, $C' \equiv (M')^2 \pmod{n}$, M and M' differ in only a few characters (the adversary knows the position of these characters, and n is the common modulus (which is also known to the adversary). Prove that from this information, the adversary can obtain M and M' *without* having to factor n.

Problem 5:

There is a typo in Hint 2: "$p \equiv 1 \pmod{4}$" should read "$p \equiv -1 \pmod{4}$".