MTH6115 Cryptography Exercises 6

Hand in to BLUE BOX on SECOND FLOOR of math sci building before 4:30pm on Friday 27/3/09.
Remember: *The work you hand in should be your OWN work. If you work in groups make sure you YOURSELF understand the answers that have been obtained, and write up your answers YOURSELF. I take a dim view of copied answers, and will penalise them severely when I detect them.*

Q1 Bob and Alice are using the RSA cipher system to communicate and Bob's public key is $(N_B = 77, e_B = 23)$.

(a) Suppose you are Alice. Encrypt the binary plaintext 1001000 as a ciphertext for sending to Bob (your solution should be a binary sequence of length seven). Give a full explanation of how you do this. [20]

(b) Suppose you are Eve. You intercept the binary ciphertext 0100011 which has been sent to Bob. Determine the original binary plaintext, giving a full explanation of how you deciphered the message. Why is it easy for you to do this? [25]

Q2 You are told that 3589 is a product of two primes and that $\lambda(3589) = 288$. Use this information to factorise 3589. [15]

Q3 Suppose that $n \geq 2$ is an integer and that $x, y \in \mathbb{Z}_n$ are coprime to n. Suppose further that x and y have orders s and t, respectively, in $\mathbb{Z}_n$.

(a) Prove that if $\gcd(s, t) = 1$ then xy has order st in $\mathbb{Z}_n$.

(b) Use (a) to deduce that if $\gcd(s, t) = d$ then $x^d y$ has order st/d in $\mathbb{Z}_n$.

(c) Use (b) to deduce that if y is chosen to have maximum order in $\mathbb{Z}_n$ then s divides t.

(d) Use (c) to deduce that $\mathbb{Z}_n$ has an element of order $\lambda(n)$. [30]

Q4 Bob uses the Miller-Rabin primality test to generate two large numbers p_B, q_B which are likely to be prime. He then uses them to construct his public and secret keys for the RSA cipher system. How would it affect the implementation of the cipher system if p_B turned out not to be prime? [10]