E4.44 Network Security : Problem Sheet 2

1. What properties should a good message digest function have? The following schemes are proposed as efficient Message Digest functions. Determine whether they would make good message digest functions.

(i) In order to compress a message prior to computing an RSA signature it is proposed by sign the message mod n.
(ii) In order to improve on the performance of MD5 which provides a 128-bit MD is proposed to divide the message into 128-bit chunks and + all the chunks together to get a 128-bit result on which MD5 would be applied.

2. Why does SHA-1 require padding of messages that are already a multiple of 512 bits?
3. What are the minimal and maximal amounts of padding required in SHA-1?
4. What applications does Euclid's algorithm have in cryptography? By reference to Euclid's algorithm or otherwise prove the following:

(i) If m and n are two positive integers, show that m/gcd(m,n) and n/gcd(m,n) are relatively prime.
(ii) If a and b are relatively prime, and bc is a multiple of a, show that c is a multiple of a.

5. For what type of number is Φ (n) largest (relative to n)?

6. For what type of number is Φ (n) smallest (relative to n)?

7. Is it possible for Φ (n) to be bigger than n?

8. In RSA what is the probability that something to be encrypted will not be in Z_n^* ?

9. In mod n arithmetic why does x have a multiplicative inverse if and only if x is relatively prime to n?

10. In Diffie-Hellman one method of protection is to encrypt the Diffie-Hellman value with the other side's public key. Why is this the case given that an attacker has the capability to encrypt any value with known public keys?

11. What is the probability that a randomly chosen number would not be relatively prime to some particular RSA modulus n? What threat would finding such a number pose?

12. In RSA is it possible for more that one d to work with a given e, p and q?