1 Tutorial 5

1. Some proposals suggest making the RSA modulus a product of three primes, $n = pqr$ of equal size. Describe the RSA system in this case. That is, explain how e and d are chosen.

2. Show how you can construct a permutation from a one-way function. Think about how DES does the same thing! In particular, show how you can construct a block cipher using SHA1 (you can pattern it after how DES does it). What is the block length of your cipher? What is its key length? How does the block cipher encrypt and decrypt?

3. Suppose that a cryptanalyst discovers a message P that is not relatively prime to the enciphering modulus $n = pq$ used in a RSA cipher. Show that the cryptanalyst can factor n.

4. For a hypothetical 5-DES encryption scheme with 5 independent keys used as E-E-E-D-D, what is the effective key length for a KPA (known plain-text attack), CPA (chosen plain-text attack) given that storage is not a consideration.