Assignment 4

1a. Differentiate between a one-way function and a trap door one-way function.

b. Write the RSA algorithm. Given p=3, q=13, e=5 and message M=10 perform encryption and decryption using RSA algorithm.

2a. Explain the four possible approaches for attacking the RSA algorithm.

b. Write the Diffie-Hellman key exchange algorithm. Explain its strengths and weaknesses.

3a. What are the applications of cryptographic hash functions?

b. Consider the following hash function. Messages are in the form of a sequence of decimal numbers, M = (a_1, a_2, ... a_t). The hash value h is calculated as h = $(5+\Sigma^t_{i=1} (a_i))$ mod n. Given M = (89, 32, 90, 22, 49, 73) and n=898. Find the hash value.

4a. Along with a neat diagram explain HMAC structure. How can it be made more efficient?

b. What are the security requirements for a cryptographic hash function?

5a. Along with neat diagrams explain the SHA-512 algorithm.

b. What is blinding?

6a. What is the need for error control during message authentication? Along with neat diagrams distinguish between internal error control and external error control.

b. Explain any four situations in which a MAC is used.