NETWORK SECURITY Sample Questions for MIDTERM

1). Discuss the different types of security attacks (passive/attack) in detail

2). What are the different security principles? Explain in detail

3). Applications of e-commerce security and computer forensics

4). What do you mean by stenography? Explain with a suitable example

5). Discuss the following in brief:

i]. Digital Signatures

ii]. Kerberos v4

6). Differentiate between block cipher and string cipher algorithms

7). What do you mean by feistel/feizel block cipher?

8). Differentiate between confusion and diffusion in block cipher

9). What is the purpose of s-boxes in DES algorithm?

10). Explain the working of IDEA algorithm. How do we generate the keys in different rounds?

11). Explain the following modes of operations:

i]. ECB (Electronic Code Block)

ii]. CBC (Cipher Block Chaining)

iii]. OFB (Output Feedback Mode)

iii]. CFB (Cipher Feedback Mode)