1. (10’) What is the frame size of STS-256? What is the date rate? What is the percentage of the data (excluding section, line and path overhead) in a frame?

2. (10’) When a user using cellular networks moves out of the home MSC he/she registers, what is the process for the call from someone else to be directed/connected to the user? What is difference between FDD and TDD in WiMAX?

3. (10’) What are the differences between a Supervisory Control and Data Acquisition (SCADA) system and a Distributed Control System (DCS)?

4. (10’) The Common Information Model (CIM) uses the class concept of the Unified Modeling Language (UML) to represent components in power systems. What relationships can exist between classes? Describe them in some detail.

5. (10’) To understand the DES algorithm, we can simplify it with the following changes:
   
   1) Remove the initial and final permutation; and
   2) Reduce the number of rounds from 16 to 3.

   Answer the following questions:
   
   a. Assume that function \( f \) is implemented as \( f(R_{I-1}, K_I) = R_{I-1} \) in each round. What bits in the final result will be affected by the 40th bit in the original input? What is the mapping from the input to the output implemented by the algorithm?

   b. Suppose function \( f(R_{I-1}, K_I) \) only permutes \( R_{I-1} \) according to the straight permutation table, i.e., put the 1st bit at the 9th bit position, put the 2nd bit at the 17th position, put the 3rd bit at the 23rd position, etc. What bits in the final result will be affected by the 40th bit in the original input?

6. (10’) Generate a public key and private key pair by using the key generation method for RSA described on the slides by choosing \( p = 5 \) and \( q = 11 \). To verify the correctness of your keys, use the public key to encrypt message 2 and then use the private key to decrypt it. Show the process.

7. (10’) When adding padding bits to the original message in SHA1, we add all 0’s so that the total length is multiple of 512 bits. We do not append the length field at the end. What is the problem with this modified algorithm? You may use some examples to explain it.