This exam has four questions, each question has two parts. Answer all questions.

1. (25 pts)
   (a) Describe what is triple DES? Why is it more secure than single key DES?
   (b) Alice has selected the public key \((n = 33; e = 3)\). Using this key, Bob sends plaintext \(X\) to Alice which encrypts as ciphertext \(10\). What is the plaintext \(X\)?

2. (25 pts)
   (a) Explain why most cryptographic hash functions generate at least a 128 bit hash? Why not a 64 bit hash?
   (b) What is a Message Authentication Code (MAC)? Show one way how you could build a 128 bit MAC using DES.

3. (25 pts)
   (a) In the Diffie-Helman protocol, the common modulus is chosen as \(n = 19\) and the generator \(g\) is chosen to be 2. Suppose Alice and Bob choose the numbers 6 and 10 privately. What will be the public values they transmit and what would be the final secret computed?
   (b) Consider the following protocol for sending an encrypted message from Alice to Bob in the presence of a Key Distribution Center (KDC).
      - Alice sends to KDC \(\{Alice, Bob, E_{K_{DC}}(R)\}\). That is, her identity, Bob’s identity and also a random session key encrypted with the KDC’s public key (of which it has a trusted copy).
      - The KDC decrypts the random session key \(R\) and then encrypts the same with Bob’s public key (of which it has a trusted copy) and sends to Alice \(\{E_{Bob}(R)\}\).
      - Alice sends to Bob \(E_R(M)\), that is the message \(M\) encrypted with the random session key \(R\) and also \(\{E_{Bob}(R)\}\) which it received from the KDC.
      - Bob decrypts \(E_{Bob}(R)\) to get \(R\) and then \(E_R(M)\) to get \(M\).
   
   Show why the above protocol is not secure and show how you could fix it. Hint: Oscar can listen to the message in step 1 and sends to the KDC a similar message but indicating that Alice wants to talk to him ...

4. (25 pts)
   (a) Explain the terms Screening router, Application gateway, NAT, DMZ and Bastion host.
   (b) State three advantages and disadvantages of screening routers (packet filters) and Application gateways.