1. What are the two countermeasures against timing attacks one needs to consider?  
   +10 pnts

2. Why El Gamal better than RSA?  
   +10 pnts

3. What are the two important properties of cryptographically strong pseudorandom generators (in two words please)?  
   +5 pnts

   Explain either of the pseudorandom generators in detail, one using 3 EDE of DES, or the other Blum Blum Shub generators.  
   +15 pnts

4. Why not use double DES, explain the possible attack mechanism in detail against which?  
   +20 pnts

5. Encrypt the following message by using Playfair Cipher, whose key is set to “AUSTRALIAN TIGER” tiger recovery of Extinction”? Message: “UNDER THE GIVEN CONDITIONS THE MAXIMUM NUMBER OF SPECIES MUST BE ENTROPY BOUNDED, THEREFORE ONCE EXTINCT SPECIES ARE LIKELY TO REAPPEAR”.  
   +20 pnts

6. Calculate required elements of RSA, and then perform encryption and decryption of PT =2, \( p = 17, \phi(n) = 480; K_e = 7. \)  
   +20 pnts