Tutorial-VIII (Digital Signature)

1. (i)Alice chooses p = 3119, e1 = 2, d = 127 and calculates e2 = 2127 mod 3119 = 1702. She also chooses r to be 307. She announces e1, e2, and p publicly; she keeps d secret. Show how Alice can sign a message.

   (ii) Now imagine that Alice wants to send another message, M = 3000, to Ted. She chooses a new r,107. Alice sends M, S1, and S2 to Ted. Ted uses the public keys to calculate V1 and V2. Show signature generation and verification process for this case also.

2. Suppose that Alice chooses p = 823 and q = 953, The value of $\varphi(n)$ is 782544. Now she chooses e = 313 and calculates d = 160009. At this point key generation is complete. Now imagine that Alice wants to send a message with the value of M = 19070 to Bob. Show the signature generation and verification process.