SOEN 321

Prob. 1
Suppose that users Alice and Bob carry out the Diffie-Hellman key agreement protocol with p = 101 and g = 17. Suppose that Alice chooses x = 19 and Bob chooses y = 13. Show the computations performed by both Alice and Bob, and determine the key that they will share.

Ans.
Alice -> Bob g^x mod p=6
Bob -> Alice g^y mod p=65
Shared key = g^(xy) mod p=14

Prob. 2

Suppose that users Alice and Bob carry out the 3-pass Diffie-Hellman protocol with p = 101. Suppose that Alice chooses a_1 = 19 and Bob chooses b_1 = 13. If Alice wants to send the secret message m=5 to Bob, show all the messages exchanged between Alice and Bob

Ans.
a_2=a_1 ^ (-1) mod (p-1) =79
b2=77
Alice -> Bob m^a_1 mod p =37
Bob -> Alice 80
Alice to Bob 56
Bob obtains m by evaluating 56^b2 mod p =5

Prob. 3
Consider an RSA system where the public key of three users (i.e., (n,e) are given by: (319,3), (697,3) and (1081,3). If the same message was sent to the three users. Show how the attacker can recover m by observing the ciphertexts c1=128, c2=34 and c3=589.

Ans. This is an example of the low exponent attack. The attacker uses the Chinese remainder theorem to solve for m^3 mod (n1 n2 n3). Just denote m^3 by x. Then this is equivalent to solving for x that satisfies x=128 mod 319, x=34 mod 697 and x=589 mod 1081. Using CRT we get x=4913 -> m=4913^(1/3)=17