Homework #12

1. Shared session key establishment using a Key Distribution Center (KDC). Using the following table, illustrate how Alice can initiate a secure session with Bob with the help of KDC.

Alice	KDC	Bob
Kek: ka = A6 = 1010 0110	Ka = A6 = 1010 0110 Kb = D8 = 1101 1000	Kb = D8 = 1101 1000
	Alice sends a message to KDC requesting between Alice and Bob	
	Kses 7B = 0111 1011	
	ya → ekA (kses)= 1010 0110(0111 1011) LC = 1010 xor 1011 = 0001 RC = 0110 xor 0111 = 0001 ya = 00010001 = 11 (hexa)	
	yb →ekB (kses)= 1101 1000(0111 1011) LC = 1101 xor 1011 = 0110 RC = 1000 xor 0111 = 1111 yb = 01101111 6F (hexa)	
KDC send ya = 11 to alice		
	KDC send yb = 6F to bob	
Decrupt Ka LB = 0001 xor 1011 = 1010 RB = 0001 xor 0111 = 0110 kA = 10100110 A6 (hexa)		Kb LB = LC xor RK LB = 0110 xor 1011= 1101 RB = RC xor LK RB = 1111 xor 0111 = 1000 kB= 1101 1000= D8
m=45→ 0100 0101		
y= ekses(m) LC = LB xor RK LC = 0100 xor 1011 = 1111 RC = 0101 xor 0111 = 0010 y= 11110010 F2 (hexa)		
Alice send y = F2 to bob		
		m= C =LC || RC

		F2 = 1111 0010 LB = 1111 xor 0010 = 0100 RB = 0010 xor 0111 = 0101 m= 0100 0101 is 45
		Verify, yes m=45

2. Man-in-the-middle attack when Alice and Bob employ Diffie-Hellman key exchange

Alice	Carol	Bob
	P = 17 and α = 4	
Choose a = 7		b=8
Alice's public key: kpub,A = A = α^ a mod p = 4^7 mod 17 = 13	Send A to Bob intercepted by carol	Bob's public key: k pub,B = B = α ^b mod p = 4^8 mod 17 = 1
	Send B Alice	
	Carol chooses c =6 α ^c mod p= 4^6 mod 17 = 16	
		Carol sends A to Bob as if it is A from Alice
Carol send B' to alice as if is from bob		
Alice derives the shared secret key as K1 = B'^a mod p K1 = 16^7 mod 17 =16	Carol derives K1 = A^c mod p, K1= 13^6 mod 17 =16 K2 = B^c mod p K2 = 1^6 mod 17 = 1	Bob derives the shared secret key as K2 = A'^b mod p= 16 ^8 mod 17 = 1
	Verify that alice and carol have derived the same key K1, yes they have the same key K1 = 16	
		Verify that carol and bob have derived the same key K2 = 1 yes they have the same key