Question 2. [Points 10] Man-in-the-middle attack when Alice and Bob employ Diffie-Hellman key exchange.

9.5

Alice	Carol (Intruder)	Bob
P =17 and α = 4 are known to all		
Choose $\mathbf{k_{pri,A}}$ =**a = 7**		Choose $\mathbf{k_{pri,B}}$ **= b = 8**
Alice's public key: $\mathbf{k_{pub,A} = A = \alpha^a}$ **mod p =** 13		Bob's public key: $\mathbf{k_{pub,B} = B = \alpha^b}$ **mod p =** 1
Send A to Bob; intercepted by Carol		
	Send B to Alice; intercepted by Carol	
	Carol chooses c=6; computes A' = B' = $\mathbf{\alpha^c}$ **mod p** 16	
	Carol sends A' to Bob as if it is A from Alice	
Carol sends B' to Alice as if it is from Bob		
Alice derives the shared secret key as K1 = $\mathbf{B'^a}$ **mod p** 1	Carol derives K1 = $\mathbf{A^c}$ **mod p,** **K2 =** $\mathbf{B^c}$ **mod p,** 1, 16	Bob derives the shared secret key as K2 = $\mathbf{A'^b}$ **mod p** 16
Session 1 established with key K1: verify that Alice and Carol have derived the same key K1 ✓		
	Session 2 established with key K2; verify that Carol and Bob have derived the same key K2	