CS 463/563: Cryptography for Cybersecurity
Spring 2024
Homework # 12
Points: 20

Question 1. [Points 10] 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. Here, KEKs are the long-term key establishment keys used to transport the session keys across the network securely. Assume the encryption process to be as follows:

Block (LB || RB) is 8 bits;
Encryption Key (LK||RK) is 8 bits;
Ciphertext = LC|| RC where LC=LB $\oplus$ RK; and
RC=RB $\oplus$ LK;

For example, if plaintext=A7 (Hexa) and Key = 6D; then LC=A $\oplus$ D = 1010 $\oplus$ 1101 = 0111 = 7 (Hexa); and RC = 7 $\oplus$ 6 = 0111 $\oplus$ 0110 = 0001 = 1 (Hexa); so Ciphertext = 71 (Hexa).

To decrypt, it does the reverse operation: Given ciphertext of C=LC||RC, it finds plaintext B=LB||RB, by finding LB=LC $\oplus$ RK and RB = RC $\oplus$ LK.

Alice	KDC	Bob
KEK: **k_A = A6 (hexa)**	KEK: **k_A = A6 (hexa); k_B = D8(hexa);**	KEK: **k_B = D8 (hexa);**
Alice sends a message to KDC requesting a session key between Alice and Bob		
	Generate a random session key: **k_{ses} = 7B (hexa);**	
	$y_A = e_{kA}(k_{ses})$ = ??	
	$y_B = e_{kB}(k_{ses})$ = ??	
KDC sends **y_A = ?? to Alice**		
	KDC send **y_B = ?? to Bob**	
Decrypt **y_A to derive k_{ses} using k_A = ??**		Decrypt **y_B to derive k_{ses} using k_B = ??**
Message to send, m = 45 (Hexa)		
Encrypyt m using session key, y = **$e_{kses}(m)$**		
Alice sends y = **??** to Bob		
		Decrypt y using session key to get m = **??**
		Verify that this is the message sent by Alice

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

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 =** $\boldsymbol{\alpha^a}$ **mod p =**		Bob's public key: $\mathbf{k_{pub,B}}$ **= B =** $\boldsymbol{\alpha^b}$ **mod p =**
Send A to Bob; intercepted by Carol		
	Send B to Alice; intercepted by Carol	
	Carol chooses c=6; computes A' = B' = $\boldsymbol{\alpha^c}$ **mod p**	
	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**	Carol derives K1 = $\mathbf{A^c}$ **mod p, K2 =** $\mathbf{B^c}$ **mod p,**	Bob derives the shared secret key as K2 = $\mathbf{A'^b}$ **mod p**
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	

What to submit? Submit a pdf file with your answers via Canvas. Show your work