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 ⊕ RK; and
RC=RB ⊕ LK;

For example, if plaintext=A7 (Hexa) and Key = 6D; then LC=A ⊕ D = 1010 ⊕ 1101 = 0111 = 7 (Hexa); and RC = 7 ⊕ 6 = 0111 ⊕ 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 ⊕ RK and RB = RC ⊕ 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);**	
	$y_A = e_{kA}(k_{ses})$ = ?? 11	
	$y_B = e_{kB}(k_{ses})$ = ?? 6F	
KDC sends y_A = ?? **to Alice** 11		
	KDC send y_B = ?? **to Bob** 6F	
Decrypt y_A **to derive** k_{ses} **using** k_A = ?? 7B		Decrypt y_B **to derive** k_{ses} **using** k_B = ?? 7B
Message to send, m = 45 (Hexa)		
Encrypyt m using session key, $y = e_{kses}(m)$		
Alice sends y = ?? to Bob AF		
		Decrypt y using session key to get m = ?? 45
		Verify that this is the message sent by Alice