OLD DOMINION UNIVERSITY
CS 463

Homework 11

Madelene McFarlane

11/17/2023

#01096496

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 (hexadecimal) and Key = 6D; then LC=A $\oplus$ D = 1010 $\oplus$ 1101 = 0111 = 7 (hexadecimal); and RC = 7 $\oplus$ 6 = 0111 $\oplus$ 0110 = 0001 = 1 (hexadecimal); so Ciphertext = 71 (hexadecimal). 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:$\mathbf{k_A}$ = **A6 (hexadecimal)**	KEK:$\mathbf{k_A}$ = **A6 (hexadecimal)** KEK:$\mathbf{k_B}$ = **D8 (hexadecimal)**	KEK:$\mathbf{k_B}$ = **D8 (hexadecimal)**
Alice sends a message to KDC requesting a session key between Alice and Bob		
	Generate a random session key: $\mathbf{k_{ses}}$ = **7B (hexadecimal)**	
	$y_A = e_{kA}(kses) = ??$	
	$y_B = e_{kB}(kses) = ??$	
KDC sends $y_A = ??$ to Alice		
	KDC sends $y_B = ??$ to Bob	
Decrypt y_A to derive k_{scs} using k_A =		Decrypt y_B to derive k_{scs} using k_B =
Message to send, m = 45 (hexadecimal)		
Encrypyt m using session key, y = $e_{kscs}(m)$		
Alice sends y to Bob		
		Decrypt y using session key to get m =
		Verify that this is the message sent by Alice

CS 463
HW11

Madelene McFarlane

bold = answer

Block: LB||RB
Key: LK||RK
CT: LC||RC

Decrypt:
LB = LC ⊕ RK
RB = RC ⊕ LK

LC = LB ⊕ RK
RC = RB ⊕ LK

Alice	KDC	Bob
K_a = AC = 1010 0110	K_a = AC = 1010 0110 K_b = DB = 1101 1000	K_b = DB = 1101 1000
	K_{ses} = 7B = 0111 1011	
	Y_A = 0001 0001	
	Y_B = 1111 0110	
$K_{ses} = d_{K_A}(Y_A)$ 0111 1011		$K_{ses} = d_{K_B}(Y_B)$ 0111 1011
M = 45 = 0100 0101		
Y = 1111 0010		
		M = 0100 0101

$Y_A = e_{1010\ 0110}(0111\ 1011)$
LB: 0111
RB: 1011
LK: 1010
RK: 0110
LC: 0111 ⊕ 0110 = 0001
RC: 1011 ⊕ 1010 = 0001
Y_A = 0001 0001

$Y_B = e_{1101\ 1000}(0111\ 1011)$
LB: 0111
RB: 1011
LK: 1101
RK: 1000
LC: 0111 ⊕ 1000 = 1111
RC: 1011 ⊕ 1101 = 0110
Y_B = 1111 0110

$K_{ses} = d_{1010\ 0110}(0001\ 0001)$
LC: 0001
RC: 0001
LK: 1010
RK: 0110
LB: 0001 ⊕ 0110 = 0111
RB: 0001 ⊕ 1010 = 1011
K_{ses} = 0111 1011

$K_{ses} = d_{1101\ 1000}(1111\ 0110)$
LC: 1111
RC: 0110
LK: 1101
RK: 1000
LB: 1111 ⊕ 1000 = 0111
RB: 0110 ⊕ 1101 = 1011
K_{ses} = 0111 1011

$Y = e_{0111\ 1011}(0100\ 0101)$
LB: 0100
RB: 0101
LK: 0111
RK: 1011
LC: 0100 ⊕ 1011 = 1111
RC: 0101 ⊕ 0111 = 0010
Y = 1111 0010

$M = d_{0111\ 1011}(1111\ 0010)$
LC: 1111
RC: 0010
LK: 0111
RK: 1011
LB: 1111 ⊕ 1011 = 0100
RB: 0010 ⊕ 0111 = 0101
M = 0100 0101

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

Alice	**Carol (Intruder)**	**Bob**
$\rho = 17$ and $\alpha = 4$ are known to all		
Choose $\mathbf{k_{pri,A}} = \mathbf{a} = \mathbf{7}$		Choose $\mathbf{k_{pri,B}} = \mathbf{b} = \mathbf{8}$
Alice's public key: $\mathbf{k_{pub,A}} = \mathbf{A} = \alpha^a \bmod \rho =$		Bob's public key: $\mathbf{k_{pub,B}} = \mathbf{B} = \alpha^b \bmod \rho =$
Send A to Bob; intercepted by Carol		
	Send B to Alice; intercepted by Carol	
	Carol chooses c=6; computes $\mathbf{A'} = \mathbf{B'} = \alpha^c \bmod \rho$	
	Carol sends $\mathbf{A'}$ to Bob as if it is A from Alice	
Carol sends $\mathbf{B'}$ to Alice as if it is B from Bob		
Alice derives the shared secret key as K1 = $\mathbf{B'} \bmod \rho$	Carol derives the shared secret key as K1 = $\mathbf{B'} \bmod \rho$ K2 = $\mathbf{A'} \bmod \rho$	Bob derives the shared secret key as K2= $\mathbf{A'} \bmod \rho$
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	

CS 463
HW11

Madelene McFarlane

= answer

Alice	Carol (Intruder)	Bob
$p = 17$ $\alpha = 4$		
$k_{priv,A} = a = 7$		$k_{priv,B} = b = 8$
$k_{pub,A} = A = 13$		$k_{pub,B} = B = 1$
	$c = 6$ $A' = B' = 16$	
$K1 = 16$	$K1 =$ $K2 =$	$K2 = 16$

$k_{pub,A} = 4^7 \bmod 17$

$A = 13$

$k_{pub,B} = 4^8 \bmod 17$

$B = 1$

$A' = B' = 16$

$= 4^6 \bmod 17$

$K1 = 16 \bmod 17$

16

$k2 = 16 \bmod 17$

16