OLD DOMINION UNIVERSITY
CS 463

Homework 5

Madelene McFarlane

9/29/2023

#01096496

CS-463/563 Crytography for Cyber Security
Fall 2023
Homework Assignment #5

August 9, 2023

Points: 20

Consider a simple system with 8-bit block size. Assume the encryption (and decryption) to be as follows: If plaintext is LT||RT and the key is LK||RK, where LC, RC, LT, and RT are each 4 bits, then ciphertext= LC||RC where LC=LK XOR RT; and RC = RK XOR LT; Plaintext and ciphertext are each 8 bits. Similarly, to decrypt ciphertext, we perform exactly the reverse operation where LT=RC XOR RK and RT = LC XOR LK. You are given the following 16-bit input D7F1 (in Hexa). You are provided IV as: A9 (hexadecimal).

For CTR assume the stream of bits to be used for counter to be starting from 0001 and incremented by 1 every time; so the stream would be 0001 0010 0011 0100 0101 0110 0111 1000 1001 1010 1011 1100 1101 1110 1111 0000 0001 0010 0011 0100 0101 0110 0111 1000 1001 1010 1011 1100 1101 1110 1111 ...

The 8-bit key to be used (where appropriate) is C5 (hexadecimal).

Compute the encrypted output with (i) ECB, (ii) CBC, (iii) OFB, (iv) CFB, and (v) CTR (with IV=0101_2).

Express the output as 4 hexadecimal characters so it is easy to read

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

CS 463
HW 5

Madelene McFarlane

** = answer

ECB)

D	7	F	1
1101	0111	1111	0001

11000101 = C5

$Y_1 = e(x_1) = e(11010111)$

LT = 1101
RT = 0111
LK = 1100
RK = 0101

LC = 1100 XOR 0111 = 1011
RC = 0101 XOR 1101 = 1000

LC || RC = 10111000 = BB

$Y_2 = e_x(X_2) = e(11110001)$

LT = 1111
RT = 0001
LK = 1100
RK = 0101

LC = 1100 XOR 0001 = 1101
RC = 0001 XOR 1111 = 1010

LC || RC = 11011010 = DA

BB DA

CS 463
HW 5

Madelene McFarlane

** = answer

CBC)

$Y_1 = e_{11000101}(11010111 \text{ XOR } 10101001)$

$Y_1 = e_{11000101}(01111110)$

LT = 0111
RT = 1110
LK = 1100
RK = 0101

LC = 1100 XOR 1110 = 0010
RC = 0101 XOR 0111 = 0010

LC || RC = 0010 0010 = **22**

$Y_2 = e_{\cdot}(1111\,0001 \text{ XOR } 00100010) \rightarrow$ 1111 0001 / 0010 0010 **1101 0011**

↳ 1101 0011

LT = 1101
RT = 0011
LK = 1100
RK = 0101

LC = 1111
RC = 1000

LC || RC = 1111 1000 = F8

1100 XOR 0011 = 1111
1100

0101 XOR 1101 = 1000
0101

22F8

CS 463 HW 5

Madelene McFarlane

** = answer

(10101001)

OFB)

$S_1 = e_{11000101}$

LT = 1010 LC = 1100 xor 1001 = 0101

RT = 1001 RC = 0101 XOR 1010 = 1111

LK = 1100

RK = 0101

LC || RC = 01011111

01011111 XOR 11010111

↳ 10001000 = 88

88C1

$S_2 = e_{11000101}$ (01011111)

LT = 0101 LC = 11001011

RT = 1111 RC = 01011011

LK = 1100

RK = 0101

LC || RC = 00110000

xor

11110001

11000001 C1

CFB)

$S_2 = e_{11000101}$ (10001000)

LT = 1000 LC = 1100 XOR 1000 = 0100

RT = 1000 RC = 0101 xor 1000 = 1101

LK = 1100

RK = 0101

LC || RC = 0100 1101

xor

1111 0001 = 1011 1100 BC

88BC

CS 463 Madelene McFarlane

HW 5

CTR)

bold = answer

$Y_1 = e_a(0101\,0001)$

LT = 0101 LK = 1100 LC = 1100 XOR 0001 = 1101

RT = 0001 RK = 0101 RC = 0101 XOR 0101 = 0000

$LC \| RC = 1101\,0000$ xor $1101\,0111 = 0000\,0111$

07

$Y_2 = e_a(0101\,0010)$

LT = 0101 LK = 1100 LC = 1100 XOR 0010 = 1110

RT = 0010 RK = 0101 RC = 0101 XOR 0101 = 0000

$LC \| RC = 1110\,0000$

$1111\,0001$

$0001\,0001 =$ **11**

0711