IS Assignment 2

Name:- Ashhad Khan
Enrollment:- 01-134221-109
Class:- BS-CS 8-A

Q.

Ans Initial Key Derivation (K_0)

Key Components

First four letters (ASHH): A → 41, S → 53, H → 48, H → 48
Hex Bytes: 41 53 48 48

Last four digits (2109): 2 → 02, 1 → 01, 0 → 00, 9 → 09
Hex Bytes: 02 01 00 09

Initial Key

K_0 = 41534848 02010009 41534848 02010009
(W_0 W_1 W_2 W_3)

	B_0	B_1	B_2	B_3
W_0	41	53	48	48
W_1	02	01	00	09
W_2	41	53	48	48
W_3	02	01	00	09

CamScanner

AES Key Expansion (Round 1 Key)

a. Calculate $W_4 = W_0 \oplus \bar{T}(W_3)$

$W_3 = 02010009$

Operation	Input (Hex)	Output (Hex)
~~RotWord (W_3)~~		
RotWord (W_3)	02010009	01000902
SubWord	01 -> C7	C7637C7B
	00 -> 63	
	09 -> 84	
	02 -> 7B	
Rcon ($Rcon_1$)	C763847B	C6637C7B
$\bar{T}(W_3)$		C6637C7B
XOR ($W_0 \oplus \bar{T}(W_3)$)	41 53 48 48	8730CC33
	$\oplus$ C6 63 84 7B	

41 $\oplus$ C6 = 87

53 $\oplus$ 63 = 30

48 $\oplus$ 84 = CC

48 $\oplus$ 7B = 33

$W_4 = 8730CC33$

b) Calculate $W_5 = W_1 \oplus W_4$

$W_5 = 02010009 \oplus 8730CC33 = 8531CC3A$

c) Calculate $W_6 = W_2 \oplus W_5$

$W_6 = 41534848 \oplus 8531CC3A = C4628472$

d) Calculate $W_7 = W_3 \oplus W_6$

$W_7 = 02010009 \oplus C4628472 = C663847B$

Round 1 key (K_1)

	B_0	B_1	B_2	B_3
W_4	87	30	CC	33
W_5	85	31	~~84~~ CC	3A
W_6	C4	62	84	72
W_7	C6	63	84	7B

CamScanner

AES Key Expansion (Round 2 Key)

Operation	Input (Hex)	Output (Hex)
RotWord (W_7)	C6 63 84 7B	63 84 7B C6
SubWord	63 → 7F	7F 02 01 F0
	84 → 02	
	7B → 01	
	C6 → F0	
Rcon (Rcon$_2$)	7F 02 01 F0	7D 02 01 F0 ⊕ 02 00 00 00
$T(W_7)$		7D 02 01 F0
XOR ($W_1 \oplus T(W_7)$)	87 30 CC 33 ⊕ 7D 02 01 F0	FE 32 CD C3

$87 \oplus 7D = FE$

$30 \oplus 02 = 32$

$CC \oplus 01 = CD$

$33 \oplus F0 = C3$

$W_8 = FE32CDC3$

b. Calculate $W_9 = W_5 \oplus W_8$

$W_9 = 8531CC3A \oplus FE32CDC3 = 7B030109$

c. Calculate $W_{10} = W_6 \oplus W_9$

$W_{10} = C4628472 \oplus 7B030109 = BFF1857B$

d. Calculate $W_{11} = W_7 \oplus W_{10}$

$W_{11} = C6638478 \oplus BFF1857B = 0DB20100$

Round 2 Key (K_2)

	B_0	B_1	B_2	B_3
W_8	FE	32	CD	C3
W_9	7B	03	01	09
W_{10}	BF	F1	85	7B
W_{11}	0D	B2	01	00

CamScanner