Name Sharif Ali
Roll P20-0130
Date: Day:
Section 7A

AES example

16-Bit plain text P: 1101011100101000
16-Bit key K: 0100101011110101
Key 1 Generation

$w_0 = 01001010$
$w_1 = 1111\,0101$
$w_2 = w_0$ XOR 10000000 XOR SubNib(RotNib(w_1))
= 01001010 XOR 10000000 XOR SubNib(01011111
= 11001010 XOR 00010111
= 11011101
$w_3 = w_2$ XOR w_1
= 11011101 XOR 1111 0101
= 00101000
$w_4 = w_2$ XOR 00110000 XOR SubNib(RotNib(w_3
$w_5 = w_4$ XOR w_3
= 10000111 XOR 00101000
= 10101111

$K_0 = w_0 w_1$ 0100101011110101
key1 = $w_2 w_3$ 1101110100101000
key2 = $w_4 w_5$ 1000011110101111
plain text XOR key1
= 1101011100101000 XOR 0100101011110101
= 1001110111011101

Scanned with CamScanner

Round L:

input = 100 1110 1 11 0 1110 1

^{ut}opueot = 0010 1110 111 0 110 0

= 0010 111·0 111 0 111 0

Me = 1 4

4 1

S_0 = 0010 1110 = S_{00} S_{01}

1110 1110 S_{10} S_{11}

S_{00} = 0010 XOR (4 x 1101)

S_{10} = (4 x 0010) XOR (1110)

S_{01} = 1010 XOR (4 x 1110)

S_{11} = 1110 XOR (4 x E)

output = S_{00}' S_{10}' S_{01}' S_{11}

1111 0110 0011 0011

final round 00100100 11101100.

Decryption

0010 0100 1110 1100 XOR 10000 11110101111

add round L key = 0010101100011011 XOR

1101 1101 0010 1000

inverse

S_{00} S_{01}

S_{10} S_{11}

S_{11} 2 x 0011 XOR 9 x 00 11

= 11 00 p.T.O

-1

Date: ____________ Day: ____________

output = 0010 1110 111 0111 0

Inverse Srft Row 0010 1110 111 0 1110

Add Round key = 100 111 0 111 0 111 01

=> 1101 0111 0010 1000

plaih text = 1101 0111 0010 1000

orginal = 1101 0111 0010 1000.

✓