Hamza Shahid
20P-0117

Information Security
Assignment #02

SE-7A

Plaintext = 1101 0111 0010 1000
Key = 0100 1010 1111 0101

w_0 = 0100 1010
w_1 = 1111 0101
w_2 = w_0 XOR 10000000 XOR SubNib(0101 1111)
= 1101 1101

w_3 = w_2 XOR w_1
= 1101 1101 XOR 1111 0101
= 0010 1000

w_4 = w_2 XOR 0011 0000 XOR SubNib(1000 0010)
= 1000 0111

w_5 = w_4 XOR w_3
= 1010 1111

key_0 = $w_0 w_1$
= 0100 1010 1111 0101

key_1 = $w_2 w_3$
= 1101 1101 0010 1000

key_2 = $w_4 w_5$
= 1000 0111 1010 1111

Encryption:

Add Round 0 key

= Plain text XoR key$_0$

= 1001 1101 1101 1101

Round 1:

Nibble sub S-box

= 0010 1110 1110 1110

Shift rows

swap 2nd & 4th

= 0010 1110 1110 1110

Mix columns

$$= \begin{bmatrix} 0010 & 1110 \\ 1110 & 1110 \end{bmatrix} \begin{bmatrix} 1 & 4 \\ 4 & 1 \end{bmatrix}$$

S_{00} = 0010 XoR (4×1110)

= 1111

S_{10} = (4×0010) XoR (1110)

= 0110

S_{01} = 1110 XoR (4×1110)

= 0011

S_{11} = (4×1110) XoR (1110)

= 0011

Output = S_{00} S_{10} S_{01} S_{11}

= 1111 0110 0011 0011

Add Round key 1

= 0010 1011 0001 1011

Final round

Nibble sub

= 1010 0011 0100 0011

swap 2nd & 4th

= 1010 0011 0100 0011

Add Round key 2

cipher = 0010 0100 1110 1100

Decryption

Add Round key 2

= 1010 0011 0100 0011

Inverse shift rows

= 1010 0011 0100 0011

Inverse nibble sub

= 0010 1011 0001 1011

Add Round key 1

= 1111 0110 0011 0011

Inverse Mix Col

= 1111 0011

0110 0011

S_{00} = (9x1111) XoR(2x0110)

= 0010

S_{10} = (2x1111) XoR (9x0110)

= 1110

S_{01} = (9x0011) XoR (2x0011)

= 1110

S_{11} = (2x0011) XoR (9x0011)

= 1110

= 0010 1110 1110 1110

Inverse shift rows

= 0010 1110 1110 1110

Inverse Nibble Sub

= 1001 1101 1101 1101

Add Round key 0

= 1101 0111 0010 1000

which is original text