Plaintext P : 1101011100101000

Key k : 0100101011110101

w_0 = 01001010

w_1 = 11110101

w_2 = w_0 XOR 10000000 XOR SubNib(RotNib(w_1))

= 01001010 XOR 10000000 XOR SubNib(01011111)

= 11001010 XOR SubNib(01011111)

= 1101 1101

w_3 = w_2 XOR w_1

= 1101 1101 XOR 11110101

= 00101000

w_4 = w_2 XOR 0011 0000 XOR SubNib(RotNib(w_3))

= 1101 1101 XOR 0011 0000 XOR SubNib(10000010)

= 10000111

w_5 = w_4 XOR w_3

= 10000111 XOR 00101000

= 10101111

Now the subkey are :

key 0 = $w_0 w_1$

= 0100101011110101

key 1 = $w_2 w_3$

= 1101 1101 0010 1000

key 2 = $w_4 w_5$

= 10000111 10101111

Encryption

Plaintext XOR keys

1101 0111 0010 1000

0100 1010 1111 0101

⊕ 10011101 1101 1101

Round 1:

Input = 1001 1101 1101 1101

output = 0010 1110 1110 1110

= 0010 1110 1110 1110

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

1110 1110 S_{10} S_{11}

S = Me x S

S_{00} = 0010 ⊕ (4 x 1110)

= 0010 ⊕ (4 x E)

= 0010 ⊕ 1101

= 1111

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

= 1000 XOR 1110

= 0110

S_{01} = 1110 ⊕ (4 x 1110)

= 1110 ⊕ (4 x E)

= 0011

$S_{11} = (4 \times 1110) \oplus 1110$

$= 1101 \oplus 1110$

$= 0011$

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

1111 0110 0011 0011

Add round 1 key:

= 1111 0110 0011 0011

1101 1101 0010 1000

$\oplus$ 0010 1011 0001 1011

Final round:

Nibble substitution (s-boxes)

= 1010 0011 0100 0011

Shift row (2nd and 4th)

= 1010 0011 0100 0011

Add Round 2 key:

1010 0011 0100 0011

$\oplus$ 1000 0111 1010 1111

= 0010 0100 1110 1100

Now we can the final cipher text

ciphertext = 0010 0100 1110 1100

Decryption

Add Rand 2 key

0010 0100 1110 1100

⊕ 1000 0111 1016 1111

= 1010 0011 0100 0011

Inverse shift row (same as normal)

= 1010 0011 01000011

Inverse Nibble Sub (use the inverse of decryption)

= 0016 1011 0001 1011

Add Round 1 key

= 0010 1011 0001 1011

⊕ 1101 1101 0010 0000

1111 0110 0011 0011

Inverse wix Culovrs

$S = \begin{matrix} S_{00} & S_{01} \\ S_{10} & S_{11} \end{matrix}$

= 1111 0011

0110 0011

$S' = \begin{matrix} S_{00}' & S_{01}' \\ S_{10}' & S_{11}' \end{matrix}$

$= \begin{matrix} 9 \times S_{00} \text{ XOR } 2 \times S_{00} & 9 \times S_{01} \text{ XOR } 2 \times S_{11} \\ 2 \times S_{00} \text{ XOR } 9 \times S_{10} & 2 \times S_{01} \text{ XOR } 9 \times S_{1} \end{matrix}$

$S_{00}' = (9 \times 1111) \text{ XOR } (2 \times 0110)$

$= 9 \times F \text{ XOR } 2 \times 6$

$= E \text{ XOR } ($

$= 1110 \oplus 1106$

$= 0010$

$S_{10}' = 2 \times 1111 \text{ XOR } 9 \times 0110$

$= 2 \times F \text{ XOR } 9 \times 6$

$= b \text{ XOR } 3$

$= 1101 \text{ XOR } 0011$

$= 1110$

$S_{01}' = 9 \times 0011 \text{ XOR } 2 \times 0011$

$= 9 \times 3 \text{ XOR } 2 \times 3$

$= 8 \text{ XOR } 6$

$= 1000 \text{ XOR } 0110$

$= 1110$

$S_{11}' = 2 \times 0011 \text{ XOR } 9 \times 0011$

$= 1110$

output = 0010 1110 1110 1110

Inverse shift row

$= 0010\ 1110\ 1110\ 1110$

Inverse Nibble Sub

$= 1001\ 1101\ 1101\ 1101$

Add Round ① key:

$= 1001\ 1101\ 1101\ 1101$

$\oplus\ 0100\ 1010\ 1111\ 0101$

$= 1101\ 0111\ 0010\ 1000$

Plaintext = 1101 0111 0010 1000

original = 1101 0111 0010 1000

The decryption worked