Ibrahim Abou Zahr

**Lab 3**

*ID: 202300976*

Exercise 1:

1. 10100001 10110010 11000011 11010100 11100101 11110110 00000111 10001001
2. 10111111 00111100 00110011 00100110 01100111 10001000 00001010

1. C0: 1011111 1001111 0000110 0110010

D0: 0110011 0011110 0010000 0001010

1. Round 1:

C1: 0111111 0011110 0001100 1100101

D1: 1100110 0111100 0100000 0010100

Round 2:

C2: 1111110 0111100 0011001 1001010

D2: 1001100 1111000 1000000 0101001

Round 3:

C3: 1111001 1110000 1100110 0101011

D3: 0110011 1100010 0000001 0100110

Round 4:

C4: 1100111 1000011 0011001 0101111

D4: 1001111 0001000 0000101 0011001

Round 5:

C5: 0011110 0001100 1100101 0111111

D5: 0111100 0100000 0010100 1100110

Round 6:

C6: 1111000 0110011 0010101 1111100

D6: 1110001 0000000 1010011 0011001

Round 7:

C7: 1100001 1001100 1010111 1110011

D7: 1000100 0000010 1001100 1100111

Round 8:

C8: 0000110 0110010 1011111 1001111

D8: 0010000 0001010 0110011 0011110

Round 9:

C9: 0001100 1100101 0111111 0011110

D9: 0100000 0010100 1100110 0111100

Round 10:

C10: 0110011 0010101 1111100 1111000

D10: 0000000 1010011 0011001 1110001

Round 11:

C11: 1001100 1010111 1110011 1100001

D11: 0000010 1001100 1100111 1000100

Round 12:

C12: 0110010 1011111 1001111 0000110

D12: 0001010 0110011 0011110 0010000

Round 13:

C13: 1001010 1111110 0111100 0011001

D13: 0101001 1001100 1111000 1000000

Round 14:

C14: 0101011 1111001 1110000 1100110

D14: 0100110 0110011 1100010 0000001

Round 15:

C15: 0101111 1100111 1000011 0011001

D15: 0011001 1001111 0001000 0000101

Round 16:

C16: 1011111 1001111 0000110 0110010

D16: 0110011 0011110 0010000 0001010

**Keys:**

Key0: 101111 100100 111101 101111 010100 111000 001011 000000

Key1: 001001 110101 111110 010011 010100 110010 101010 000010

Key2: 011011 100111 001100 001001 000100 001010 001101 000111

Key3: 000010 111001 110101 111101 101101 101000 010010 000100

Key4: 110011 010110 100011 011011 010010 000010 011111 000011

Key5: 001101 111110 111110 101000 001111 101110 000000 001001

Key6: 110110 100011 110110 000011 011000 100101 010101 000010

Key7: 011110 011010 111001 011101 100011 001010 000100 101010

Key8: 010001 011111 010010 001110 111001 000101 111001 000000

Key9: 110101 000010 011111 101100 010010 111001 100001 000000

Key10: 110100 101101 111000 110001 110000 001100 010100 111100

Key11: 110011 011011 101101 100110 000010 010001 111010 001100

Key12: 101000 101111 011011 001111 110110 000101 000010 110001

Key13: 011110 010101 011101 100010 000000 110100 101000 101101

Key14: 111000 001101 100111 111001 100100 100011 100110 010000

Key15: 100101 011110 001101 010111 101000 010000 001100 110101

Key16: 101111 100100 111101 011110 101001 110100 001011 000000

**Exercise 2**:

1. 0011 0010 0001 0000 1010 0101 0110 1101 1000 1001 0100 1011 1100 0111 1110 1111
2. 1110100000000011110011001111110011010100100011011011100011100001
3. L0: 1110 1000 0000 0011 1100 1100 1111 1100  
   R0: 1101 0100 1000 1101 1011 1000 1110 0001

Round1:

L1: 1101 0100 1000 1101 1011 1000 1110 0001

K1=001001 110101 111110 010011 010100 110010 101010 000010

sbox = 1011 0101 0111 0000 1000 1111 1000 0001

f (R0, K1) = 0001 0101 1010 0001 0110 1010 0001 1111

R1🡪 L0 ⊕ f (R0, K1) = 1111 1101 1010 0010 1010 0110 1110 0011

Round2:

L2: 1111 1101 1010 0010 1010 0110 1110 0011

K2=011011 100111 001100 001001 000100 001010 001101 000111

sbox = 1110 0101 0101 1001 1000 0010 1110 1101

f (R1, K2) = 1000 1101 1011 0001 1100 1110 0111 0001

R2🡪L1 ⊕ f (R1, K2) = 0101 1001 0011 1100 0111 0110 1001 0000

Round3:

L3: 0101 1001 0011 1100 0111 0110 1001 0000

K3=000010 111001 110101 111101 101101 101000 010010 000100

sbox = 1110 0010 1101 1011 1000 0100 0100 0100

f (R2, K3) = 1100 0101 1101 0001 1000 0011 0110 1000

R3🡪 L2 ⊕ f (R2, K3) = 0011 1000 0111 0011 0010 0101 1000 1011

Round4:

L4: 0011 1000 0111 0011 0010 0101 1000 1011

K4=110011 010110 100011 011011 010010 000010 011111 000011

sbox = 0110 1011 1000 0010 0101 0111 1110 0110

f (R3, K4) = 0110 0000 0111 1110 1110 0111 0010 1001

R4🡪 L3 ⊕ f (R3, K4) = 0011 1001 0100 0010 1001 0001 1011 1001

Round5:

L5: 0011 1001 0100 0010 1001 0001 1011 1001

K5=001101 111110 111110 101000 001111 101110 000000 001001

sbox = 0110 0011 0111 1101 1000 1001 1111 0101

f (R4, K5) = 1101 0111 0001 0001 1111 1110 0110 0101

R5🡪 L4 ⊕ f (R4, K5) = 1110 1111 0110 0010 1101 1011 1110 1110

Round6:

L6: 1110 1111 0110 0010 1101 1011 1110 1110

K6=110110 100011 110110 000011 011000 100101 010101 000010

sbox = 1001 1110 0100 0011 1011 1101 1100 0010

f (R5, K6) = 1111 0001 1101 1011 0010 0000 1001 1011

R6🡪L5 ⊕ f (R5, K6) = 1100 1000 1001 1001 1011 0001 0010 0010

Round7:

L7: 1100 1000 1001 1001 1011 0001 0010 0010

K7=011110 011010 111001 011101 100011 001010 000100 101010

sbox = 0100 0010 1111 1101 1111 0010 0001 1101

f (R6, K7) = 1110 1111 0010 0101 1001 1001 1110 0100

R7🡪 L6 ⊕ f (R6, K7) = 0000 0000 0100 0111 0100 0010 0000 1010

Round8:

L8: 0000 0000 0100 0111 0100 0010 0000 1010

K8=010001 011111 010010 001110 111001 000101 111001 000000

sbox = 0011 0101 0100 0111 0101 1010 0000 0011

f (R7, K8) = 1011 0000 0110 0111 0101 1010 0001 0010

R8🡪 L7 ⊕ f (R7, K8) = 0111 1000 1111 1110 1110 1011 0011 0000

Round 9:

L9: 0111 1000 1111 1110 1110 1011 0011 0000

K9=110101 000010 011111 101100 010010 111001 100001 000000

sbox = 1010 0110 1010 0100 0001 1010 0111 0111

f (R8, K9) = 0111 0010 1011 0010 0001 1111 0011 0100

R9🡪L8 ⊕ f (R8, K9) = 0111 0010 1111 0101 0101 1101 0011 1110

Round10:

L10: 0111 0010 1111 0101 0101 1101 0011 1110

K10=110100 101101 111000 110001 110000 001100 010100 111100

sbox = 1010 0110 1001 1010 1001 1010 0101 1101

f (R9, K10) = 0111 1111 1111 0000 0000 1011 0111 0000

R10🡪L9 ⊕ f (R9, K10) = 0000 0111 0000 1110 1110 0000 0100 0000

Round11:

L11: 0000 0111 0000 1110 1110 0000 0100 0000

K11=110011 011011 101101 100110 000010 010001 111010 001100

sbox = 1011 0001 1111 0111 1001 0110 1111 1011

f (R10, K11) = 1010 1111 1111 0011 0101 1111 0000 1111

R11🡪 L10 ⊕ f (R10, K11) = 1101 1101 0000 0110 0000 0010 0011 0001

Round12:

L12: 1101 1101 0000 0110 0000 0010 0011 0001

K12=101000 101111 011011 001111 110110 000101 000010 110001

sbox = 0110 0001 0101 1000 0101 1010 0010 1001

f (R11, K12) = 0011 1100 0010 0101 1100 1110 0100 0000

R1🡪L11 ⊕ f (R11, K12) = 0011 1011 0010 1011 0010 1110 0000 0000

Round13:

L13: 0011 1011 0010 1011 0010 1110 0000 0000

K13=011110 010101 011101 100010 000000 110100 101000 101101

sbox = 1001 1000 0101 0011 1100 0010 1100 1000

f (R12, K13) = 1000 1101 1111 1101 0000 0000 0000 0011

R13🡪 L12 ⊕ f (R12, K13) = 0101 0000 1111 1011 0000 0010 0011 0010

Round14:

L14: 0101 0000 1111 1011 0000 0010 0011 0010

K14=111000 001101 100111 111001 100100 100011 100110 010000

sbox = 1100 1101 0101 0011 0100 1100 0001 1010

f (R13, K14) = 1001 1110 1100 1111 1100 0000 0001 1000

R14🡪 L13 ⊕ f (R13, K14) = 1010 0101 1110 0100 1110 1110 0001 1000

Round15:

L15: 1010 0101 1110 0100 1110 1110 0001 1000

K15 = 100101 011110 001101 010111 101000 010000 001100 110101

sbox = 0101 0001 0100 1111 0000 0110 1010 1000

f (R14, K15) = 1000 1000 0110 0001 1101 0100 0100 1011

R15 🡪L14 ⊕ f (R14, K15) = 1101 1000 1001 1010 1101 0110 0111 1001

Round16:

L16: 1101 1000 1001 1010 1101 0110 0111 1001

K16:101111 100100 111101 011110 101001 110100 001011 000000

sbox = 0110 0001 0000 0001 1111 1110 0010 1100

f (R15, K16) = 1011 1001 0010 0100 1100 0110 1010 1000

R16 🡪L15 ⊕ f (R15, K16) = 0001 1100 1100 0000 0010 1000 1011 0000