جامـــــعة المـــــستقبل
AL MUSTAQBAL UNIVERSITY

قســـم الامـــــن الـــــــــسيبرانـــــــــي

Department of Cyber Security

Subject:

F-function in DES

Class:

Second

Lecturer:

Asst. lect. Mustafa Ameer Awadh

Lecture: (3Pr)

Introduction

Here's a **Visual Basic .NET** program that implements the **F-function** in the **Data Encryption Standard (DES)**. This function takes a 32-bit right half of the data and a 48-bit subkey, expands the right half to 48 bits, performs an XOR with the subkey, applies S-boxes to reduce it back to 32 bits, and then permutes the result.

Key Features of This Program:

- Expands the 32-bit input to 48-bit using the expansion table.
- Performs XOR with a 48-bit subkey.
- Uses S-boxes to compress it back to 32-bit.
- Applies the P-box permutation

```
Module DES_FFunction
    ' Expansion Table (E)
    Dim E As Integer() = { _
        32, 1, 2, 3, 4, 5, 4, 5, 6, 7, 8, 9, _
        8, 9, 10, 11, 12, 13, 12, 13, 14, 15, 16, 17, _
        16, 17, 18, 19, 20, 21, 20, 21, 22, 23, 24, 25, _
        24, 25, 26, 27, 28, 29, 28, 29, 30, 31, 32, 1 _
    }

    ' P-Box Permutation Table
    Dim P As Integer() = { _
        16, 7, 20, 21, 29, 12, 28, 17, _
        1, 15, 23, 26, 5, 18, 31, 10, _
        2, 8, 24, 14, 32, 27, 3, 9, _
        19, 13, 30, 6, 22, 11, 4, 25 _
    }

    ' S-Boxes (S1 to S8)
    Dim S(,) As Integer = { _
        {14, 4, 13, 1, 2, 15, 11, 8, 3, 10, 6, 12, 5, 9, 0, 7}, _
        {0, 15, 7, 4, 14, 2, 13, 1, 10, 6, 12, 11, 9, 5, 3, 8}, _
        {4, 1, 14, 8, 13, 6, 2, 11, 15, 12, 9, 7, 3, 10, 5, 0}, _
        {15, 12, 8, 2, 4, 9, 1, 7, 5, 11, 3, 14, 10, 0, 6, 13} _
    }
```

```
' Function to apply the P-Box permutation
Function PBoxPermutation(ByVal input32 As UInteger) As UInteger
    Dim permuted As UInteger = 0
    For i As Integer = 0 To 31
        permuted = (permuted << 1) Or ((input32 >> (32 - P(i))) And 1)
    Next
    Return permuted
End Function

' Function to apply the Expansion table (E)
Function ExpandRightHalf(ByVal rightHalf As UInteger) As ULong
    Dim expanded As ULong = 0
    For i As Integer = 0 To 47
        expanded = (expanded << 1) Or ((rightHalf >> (32 - E(i))) And 1)
    Next
    Return expanded
End Function

' Function to apply S-Box transformation
Function SBoxSubstitution(ByVal input48 As ULong) As UInteger
    Dim output32 As UInteger = 0
    For i As Integer = 0 To 7
        Dim chunk As Integer = CInt((input48 >> (42 - i * 6)) And &H3F)
        Dim row As Integer = ((chunk And &H20) >> 4) Or (chunk And 1)
        Dim col As Integer = (chunk >> 1) And &HF
        output32 = (output32 << 4) Or S(row, col)
    Next
    Return output32
End Function
```

```
' Function to apply the P-Box permutation
Function PBoxPermutation(ByVal input32 As UInteger) As UInteger
    Dim permuted As UInteger = 0
    For i As Integer = 0 To 31
        permuted = (permuted << 1) Or ((input32 >> (32 - P(i))) And 1)
    Next
    Return permuted
End Function

' Main F-function of DES
Function FFunction(ByVal rightHalf As UInteger, ByVal subKey As ULong) As UInteger
    Dim expanded As ULong = ExpandRightHalf(rightHalf)
    Dim xored As ULong = expanded Xor subKey
    Dim sBoxOutput As UInteger = SBoxSubstitution(xored)
    Return PBoxPermutation(sBoxOutput)
End Function
```

```
' Main entry point for testing

Sub Main() Dim rightHalf As UInteger = &H12345678

Dim subKey As ULong = &H1A2B3C4D5E6F

Console.WriteLine("Original Right Half: " &
Convert.ToString(rightHalf, 2).PadLeft(32, "0"c))

Dim result As UInteger = FFunction(rightHalf, subKey)

Console.WriteLine("Output of F-Function: " &
Convert.ToString(result, 2).PadLeft(32, "0"c))

Console.ReadLine()

End Sub
Module
```

Explanation of the Code:

1. **Expansion (E-Table)**: Expands the 32-bit input to 48-bit.
2. **XOR with Subkey**: Combines the expanded input with a 48-bit round key.
3. **S-Box Substitution**: Uses S-boxes to compress the 48-bit value into 32-bit.
4. **P-Box Permutation**: Applies a final permutation to rearrange bits.

Sample Output:

```
Original Right Half: 00010010000110100010101100111100 0
Output of F-Function: 11010010101001100001101000110100
```