جامـــــعة المـــــستـقبـل
AL MUSTAQBAL UNIVERSITY

قســـم الامـــــن الـــــــسيبرانـــــــي

Department of Cyber Security

Subject:

S-Boxes

Class:

Second

Lecturer:

Asst. lect. Mustafa Ameer Awadh

Lecture: (2Pr)

Creating an S-Box for DES in Visual Basic (VB.NET)

Introduction

The Data Encryption Standard (DES) is a symmetric-key algorithm that uses **S-Boxes (Substitution Boxes)** to introduce non-linearity into the encryption process. In this lecture, we will learn how to create an S-Box using **Visual Studio** with **VB.NET**.

Steps to Create an S-Box in VB.NET

1. Setting Up the Project in Visual Studio

1. Open **Visual Studio** and create a **New Project**.
2. Select **Windows Forms App (.NET Framework)**.
3. Name the project **"DES_SBox_Generator"**.
4. Click **Create**.

---

2. Designing the User Interface (UI)

1. Add a **Button** (`btnGenerateSBox`) for generating the S-Box.
2. Add a **TextBox** (`txtSBoxOutput`) for displaying the S-Box.
3. Add a **Label** (`lblTitle`) to describe the application.
4. Adjust layout and properties for readability.

---

3. Writing the Code for S-Box Generation

3.1 Defining the S-Box Table

DES uses **8 S-Boxes**, each mapping **6-bit input to a 4-bit output**. Below is an example S-Box in VB.NET:

```
Public Class Form1
    ' Define a sample S-Box (S1)
    Dim SBox(,) 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}
    }
    ' Button Click Event to Display S-Box
    Private Sub btnGenerateSBox_Click(sender As Object, e As EventArgs) Handles
btnGenerateSBox.Click
        Dim output As String = ""
        For i As Integer = 0 To 3
            For j As Integer = 0 To 15
                output &= SBox(i, j).ToString("D2") & " "
            Next
            output &= Environment.NewLine
        Next
        txtSBoxOutput.Text = output
    End Sub
End Class
```

Understanding the Code

1. **Define the S-Box:**
   - The **SBox(,)** array stores substitution values.
   - It contains **4 rows × 16 columns**, representing part of an S-Box in DES.
2. **Generate Output on Button Click:**
   - The `btnGenerateSBox_Click` method loops through the array and prints values.
   - The output is displayed in the `txtSBoxOutput` textbox.
3. **Displaying the S-Box:**
   - The numbers are formatted to be **easily readable**.
   - Each row is printed in a new line.

---

5. Running and Testing the Program

1. Click the **Start (▶) button** in Visual Studio.
2. Click the **Generate S-Box** button.
3. The predefined S-Box values will appear in the **textbox**.

---

6. Expanding the Project

- Allow users to **input different S-Boxes**.
- Implement **all 8 S-Boxes** of DES.
- Add a function to **simulate S-Box substitution** for a given 6-bit input.