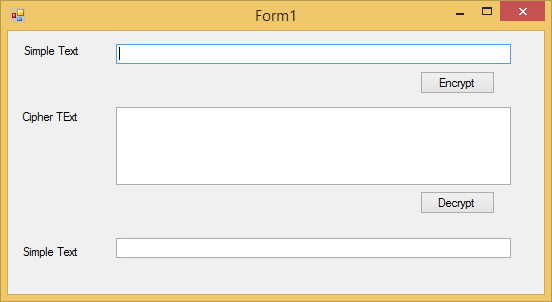
Lecture # 27:

Objective:

* Encryption / Decryption using 3DES



using System;

using System.Collections.Generic; using System.ComponentModel; using System.Data;

using System.Drawing; using System.Linq; using System.Text;

using System.Windows.Forms;

using System.Security.Cryptography;

namespace encryptionDecruption

{

public partial class Form1 : Form

{

public Form1()

{

InitializeComponent();

}

private void button1\_Click(object sender, EventArgs e)

{

byte[] keyArray;

byte[] etext = UTF8Encoding.UTF8.GetBytes(textBox1.Text);

string key = "aaaaaaav";

//keyArray=UTF8Encoding.UTF8.GetBytes(key);

MD5CryptoServiceProvider hashmd5 = new MD5CryptoServiceProvider();

keyArray = hashmd5.ComputeHash(UTF8Encoding.UTF8.GetBytes(key));

hashmd5.Clear();

TripleDESCryptoServiceProvider tdes = new TripleDESCryptoServiceProvider();

tdes.Key = keyArray; tdes.Mode = CipherMode.ECB;

tdes.Padding = PaddingMode.PKCS7;

ICryptoTransform iTransform = tdes.CreateEncryptor(); byte[] resultArray= iTransform.TransformFinalBlock(etext, 0,

etext.Length);

textBox2.Text = Convert.ToBase64String(resultArray);

}

private void button2\_Click(object sender, EventArgs e)

{

byte[] keyArray;

byte[] etext = Convert.FromBase64String(textBox2.Text);

string key = "aaaaaaav";

//keyArray = UTF8Encoding.UTF8.GetBytes(key);

MD5CryptoServiceProvider hashmd5 = new MD5CryptoServiceProvider();

keyArray = hashmd5.ComputeHash(UTF8Encoding.UTF8.GetBytes(key));

hashmd5.Clear();

TripleDESCryptoServiceProvider tdes = new TripleDESCryptoServiceProvider();

tdes.Key = keyArray; tdes.Mode = CipherMode.ECB;

tdes.Padding = PaddingMode.PKCS7;

ICryptoTransform iTransform = tdes.CreateDecryptor();

byte[] resultArray = iTransform.TransformFinalBlock(etext, 0, etext.Length);

textBox3.Text = UTF8Encoding.UTF8.GetString(resultArray);

}

}

}