

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 RSA\_ORA

{

public partial class Form1 : Form

{

public Form1()

{

InitializeComponent();

}

RSAParameters rsaParametratJoPrivat; //Pjesa publike modulus dhe exponent të nevojshme për kriptim

RSAParameters rsaParametrat; //RSA parametrat pubik dhe privat per dekriptim

byte[] BajtatEKriptuar; //Variblat për komunikim mes kriptimit dhe dekriptimit

private void GjeneroRSAParametra()

{

RSACryptoServiceProvider rsa = new RSACryptoServiceProvider();

rsaParametrat = rsa.ExportParameters(true); //true = përfshi edhe parametrat privat

rsaParametratJoPrivat = rsa.ExportParameters(false); //false = mos përfshi parametrat privat

StringBuilder sb = new StringBuilder();

for (int i = 0; i < rsaParametrat.P.Length; i++)

{

sb.Append(String.Format("{0,2:X2} ", rsaParametrat.P[i]));

}

txtp.Text = sb.ToString();

sb = new StringBuilder();

for (int i = 0; i < rsaParametrat.Q.Length; i++)

{

sb.Append(String.Format("{0,2:X2} ", rsaParametrat.Q[i]));

}

txtq.Text = sb.ToString();

sb = new StringBuilder();

for (int i = 0; i < rsaParametrat.Exponent.Length; i++)

{

sb.Append(String.Format("{0,2:X2} ", rsaParametrat.Exponent[i]));

}

txte.Text = sb.ToString();

sb = new StringBuilder();

for (int i = 0; i < rsaParametrat.D.Length; i++)

{

sb.Append(String.Format("{0,2:X2} ", rsaParametrat.D[i]));

}

txtd.Text = sb.ToString();

btnKripto.Enabled = true;

}

private void FshiTekstet()

{

txtTekstiKriptuar.Text = "";

txtTekstiKriptuarByteArray.Text = "";

txtTekstiDekriptuar.Text = "";

}

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

{

GjeneroRSAParametra();

}

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

{

FshiTekstet();

RSACryptoServiceProvider rsa = new RSACryptoServiceProvider();

rsa.ImportParameters(rsaParametratJoPrivat); //Importimi pjeses publike te RSA parameterave per enkriptim

byte[] plainbytes = Encoding.UTF8.GetBytes(txtTekstiPerKriptim.Text); //Lexmi i mesazhit të paenkriptuar

BajtatEKriptuar = rsa.Encrypt(plainbytes, false); //Enkriptimi

txtTekstiKriptuar.Text = Encoding.UTF8.GetString(BajtatEKriptuar); //Paraqitja e tekstiti te kriptuar si string

StringBuilder sb = new StringBuilder(); //paraqitja e tekstit te kriptuar ne byte array ne foramtin hex

for (int i = 0; i < BajtatEKriptuar.Length; i++)

{

sb.Append(String.Format("{0,2:X2} ", BajtatEKriptuar[i]));

}

txtTekstiKriptuarByteArray.Text = sb.ToString();

btnParamRSATeRi.Enabled = false;

btnKripto.Enabled = false;

btnDekripto.Enabled = true;

txtTekstiPerKriptim.Enabled = false;

btnDekripto.Select();

}

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

{

RSACryptoServiceProvider rsa = new RSACryptoServiceProvider();

rsa.ImportParameters(rsaParametrat); //Importimi i RSA parametrave privat dhe publik

byte[] BajtatEPakriptuar = rsa.Decrypt(BajtatEKriptuar, false); //Leximi i tekstit te kriptuar dhe dekriptimi i tij

txtTekstiDekriptuar.Text = Encoding.UTF8.GetString(BajtatEPakriptuar); //Paraqitja e tekstit te dekriptuar

btnParamRSATeRi.Enabled = true;

btnDekripto.Enabled = false;

txtTekstiPerKriptim.Enabled = true;

btnMbyll.Enabled = true;

btnKripto.Select();

}

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

{

Close();

}

}

}

p: name: txtp

q: name: txtq

e: name: txte

d: name: txtd

Teksti per enkriptim: text: Algoritmi RSA, name: txtTekstiPerKriptim, window

Teksti I kriptuar: name: txtTekstiKriptuar

Teksti I kriptuar (byte array): name: txtTekstiKriptuarByteArray

Teksti I dekriptuar: name: txtTekstiDekriptuar

Button1: text: Gjenero parametra te ri, name: btnParamRSATeRi

Button2: text: text: &Kripto, name: btnKripto

Button3: text: &Dekripto, name: btnDekripto

Button4: text: Mbyll,name: btnMbyll