КІТ-м120Б

Богомаз Олекссій

Лабораторна робота №3

Тема: Time-based One Time Password

Мета роботи: Дослідити і реалізувати механізм генерації одноразових паролів TOTP.

Завдання:

Дослідити алгоритм Time-based One Time Password. Створити програму, що реалізує механізм генерації одноразових паролів TOTP.

Виконання роботи.

Для виконання роботи використаємо на наш розсуд найбільш простий варіант побудови віконної програми - C#.

Код програми генерації одноразових паролів TOTP C# :

Program.cs

using System;

using System.Collections.Generic;

using System.Linq;

using System.Threading.Tasks;

using System.Windows.Forms;

namespace lab7

{

static class Program

{

/// <summary>

/// Главная точка входа для приложения.

/// </summary>

[STAThread]

static void Main()

{

Application.EnableVisualStyles();

Application.SetCompatibleTextRenderingDefault(false);

Application.Run(new Form2());

}

}

}

Form2.cs

using System;

using System.Collections.Generic;

using System.ComponentModel;

using System.Data;

using System.Drawing;

using System.Linq;

using System.Text;

using System.Threading.Tasks;

using System.Windows.Forms;

using System.Security.Cryptography;

namespace lab7

{

public partial class Form2 : Form

{

//byte[] easyC = { 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 109, 113, 127, 131, 137, 139, 149, 151, 157, 163, 167, 173, 179, 181, 191, 193, 197, 199, 211, 223, 227, 229, 233, 239, 241, 251 }; // Каждый раз считать алгоритмом не имеет смысла, а так Решето Эратосфена поможет

public Form2()

{

InitializeComponent();

textBox2.Text = "";

textBox1.Text = "";

}

private void heshGen()

{

TimeSpan timeSpan = DateTime.UtcNow - new DateTime(1970, 1, 1, 0, 0, 0);

double curT\_T0 = timeSpan.TotalSeconds;

Random rd = new Random();

int x = 30;

long t = (long)curT\_T0 / x;

String k = textBox1.Text;

//String a = "1";

var enc = Encoding.ASCII;

HMACSHA1 hmac = new HMACSHA1(enc.GetBytes(k));

hmac.Initialize();

byte[] buffer = enc.GetBytes(t.ToString());

String key20 = BitConverter.ToString(hmac.ComputeHash(buffer)).Replace("-", "").ToLower();

byte[] barr = Encoding.ASCII.GetBytes(key20);

String key4 = barr[2].ToString() + barr[4].ToString() + barr[1].ToString() + barr[0].ToString();

textBox2.Text = key4;

}

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

{

heshGen();

/\*for (int i = 0; i < 8; i++)

{

p[i] = easyC[rd.Next(0, 54)];

q[i] = easyC[rd.Next(0, 54)];

n[i] = p[i] \* q[i];

f[i] = (p[i] - 1) \* (q[i] - 1);

do

{

prime = true;

k[i] = rd.Next(2, 6);

cou = k[i] \* f[i] + 1;

for (int j = 2; j <= Math.Sqrt(cou); j++)

{

if (cou % j == 0)

{

prime = false;

break;

}

}

em[i] = rd.Next(3, 230);

} while (prime);

do

{

em[i]--;

if (em[i] < 2)

{

em[i] = rd.Next(2, 255);

}

}

while (((k[i] \* f[i] + 1) % em[i]) != 0);

d[i] = (k[i] \* f[i] + 1) / em[i];

}

for (int i = 0; i < 8; i++)

{

textBox2.Text += em[i].ToString("X3");

textBox2.Text += ":";

textBox1.Text += d[i].ToString("X3");

textBox1.Text += ":";

}

textBox2.Text = textBox2.Text.Remove(textBox2.Text.Length - 1, 1);

textBox1.Text = textBox1.Text.Remove(textBox1.Text.Length - 1, 1);

textBox2.Text += "-";

textBox1.Text += "-";

for (int i = 0; i < 8; i++)

{

textBox2.Text += n[i].ToString("X4");

textBox2.Text += ":";

textBox1.Text += n[i].ToString("X4");

textBox1.Text += ":";

}

textBox2.Text = textBox2.Text.Remove(textBox2.Text.Length - 1, 1);

textBox1.Text = textBox1.Text.Remove(textBox1.Text.Length - 1, 1);

\*/

}

private void textBox2\_TextChanged(object sender, EventArgs e)

{

}

private void textBox1\_TextChanged(object sender, EventArgs e)

{

}

}

}

Код основної програми на паролі TOTP C# :

Program.cs

using System;

using System.Collections.Generic;

using System.Linq;

using System.Threading.Tasks;

using System.Windows.Forms;

namespace PassV2

{

public class GlobalVars

{

public static String adlogin;

public static String adpass;

public static bool autoriz;

}

static class Program

{

/// <summary>

/// Главная точка входа для приложения.

/// </summary>

[STAThread]

static void Main()

{

GlobalVars.adlogin = "Admin";

GlobalVars.adpass = "admin";

GlobalVars.autoriz = false;

Application.EnableVisualStyles();

Application.SetCompatibleTextRenderingDefault(false);

Application.Run(new Form2());

}

}

}

Form1.cs

using System;

using System.Collections.Generic;

using System.ComponentModel;

using System.Data;

using System.Drawing;

using System.Linq;

using System.Text;

using System.Threading.Tasks;

using System.Windows.Forms;

using System.Runtime.InteropServices;

using Microsoft.Win32;

using System.Security.Cryptography;

namespace PassV2

{

public partial class Form1 : Form

{

private Form3 form3;

String pass;

Random rnd = new Random();

int[] mquest = new int[5];

int[] passarr = new int[5];

[DllImport("user32.dll", EntryPoint = "GetSystemMetrics")]

public static extern int GetSystemMetrics(int nIndex);

String patch;

int mouse = GetSystemMetrics(43);

public Form1()

{

InitializeComponent();

form3 = new Form3();

AutoCompleteStringCollection source = new AutoCompleteStringCollection()

{

"Admin"

};

textBox1.AutoCompleteCustomSource = source;

textBox1.AutoCompleteMode = AutoCompleteMode.SuggestAppend;

textBox1.AutoCompleteSource = AutoCompleteSource.CustomSource;

RegistryKey currentUserKey = Registry.CurrentUser;

RegistryKey softwareKey = currentUserKey.OpenSubKey("Software", true);

RegistryKey myKey = softwareKey.OpenSubKey("Kovalenko", true);

GlobalVars.adlogin = myKey.GetValue("login").ToString();

GlobalVars.adpass = myKey.GetValue("password").ToString();

if (myKey.GetValue("user").ToString() != SystemInformation.UserName &&

myKey.GetValue("pcName").ToString() != Environment.MachineName &&

myKey.GetValue("mouseKey").ToString() != mouse.ToString() &&

myKey.GetValue("display").ToString() != SystemInformation.PrimaryMonitorSize.ToString())

{

MessageBox.Show("Не тот ПК");

Application.Exit(); // Завершить приложение

myKey.Close();

softwareKey.Close();

}

myKey.Close();

softwareKey.Close();

}

private void label1\_Click(object sender, EventArgs e)

{

}

private void textBox1\_TextChanged(object sender, EventArgs e)

{

}

private void textBox2\_TextChanged(object sender, EventArgs e)

{

pass = textBox2.Text;

}

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

{

MessageBox.Show("А зачем тогда было приходить?");

Application.Exit(); // Завершить приложение

}

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

{

if (textBox1.Text == "")

{

MessageBox.Show("Ну хоть что-то введите");

}

else if (!(GlobalVars.adlogin == textBox1.Text))

{

MessageBox.Show("Мы таких не знаем");

}

else if (pass == "")

{

MessageBox.Show("А пароль?");

}

//else if (pass.Length != 16)

//{

// MessageBox.Show("Неверный пароль");

// textBox2.Text = "";

//}

else

{

if (heshGen() == pass)

{

GlobalVars.autoriz = true;

this.Close();

}

else

{

MessageBox.Show("Неверный пароль");

textBox2.Text = "";

}

}

}

private void button3\_Click(object sender, EventArgs e)

{

form3.ShowDialog();

}

private string heshGen()

{

TimeSpan timeSpan = DateTime.UtcNow - new DateTime(1970, 1, 1, 0, 0, 0);

double curT\_T0 = timeSpan.TotalSeconds;

Random rd = new Random();

int x = 30;

long t = (long)curT\_T0 / x;

String k = GlobalVars.adpass;

var enc = Encoding.ASCII;

HMACSHA1 hmac = new HMACSHA1(enc.GetBytes(k));

hmac.Initialize();

byte[] buffer = enc.GetBytes(t.ToString());

String key20 = BitConverter.ToString(hmac.ComputeHash(buffer)).Replace("-", "").ToLower();

byte[] barr = Encoding.ASCII.GetBytes(key20);

String key4 = barr[2].ToString() + barr[4].ToString() + barr[1].ToString() + barr[0].ToString();

return key4;

}

private void label4\_Click(object sender, EventArgs e)

{

}

private void Form1\_Load(object sender, EventArgs e)

{

//for (int i = 0; i < 5; i++)

//{

// mquest[i] = rnd.Next(0, GlobalVars.adpass.Length);

// label4.Text = label4.Text + mquest[i].ToString() + ",";

//}

//label4.Text = label4.Text + "?";

}

}

}

Form2.cs

using System;

using System.Collections.Generic;

using System.ComponentModel;

using System.Data;

using System.Drawing;

using System.Linq;

using System.Text;

using System.Threading.Tasks;

using System.Windows.Forms;

namespace PassV2

{

public partial class Form2 : Form

{

private Form1 form1;

private Form3 form3;

public Form2()

{

InitializeComponent();

form1 = new Form1();

form3 = new Form3();

}

private void label1\_Click(object sender, EventArgs e)

{

}

private void Form2\_Load(object sender, EventArgs e)

{

form1.ShowDialog();

if (!GlobalVars.autoriz)

{

Application.Exit(); // Завершить приложение

}

}

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

{

form3.ShowDialog();

}

}

}

Form3.cs

using System;

using System.Collections.Generic;

using System.ComponentModel;

using System.Data;

using System.Drawing;

using System.Linq;

using System.Text;

using System.Threading.Tasks;

using System.Windows.Forms;

using Microsoft.Win32;

namespace PassV2

{

public partial class Form3 : Form

{

String newpass;

String newpass2;

public Form3()

{

InitializeComponent();

}

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

{

this.Close();

}

private void textBox1\_TextChanged(object sender, EventArgs e)

{

newpass = textBox1.Text;

}

private void textBox2\_TextChanged(object sender, EventArgs e)

{

newpass2 = textBox2.Text;

}

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

{

if (newpass == null || newpass2 == null)

{

MessageBox.Show("Ну хоть что-то введите");

newpass = " ";

newpass2 = " ";

}

else if (!(newpass == newpass2))

{

MessageBox.Show("Пароли не совпадают!");

}

else if(newpass == newpass2)

{

MessageBox.Show("Пароль изменен!");

GlobalVars.adpass = newpass;

RegistryKey currentUserKey = Registry.CurrentUser;

RegistryKey softwareKey = currentUserKey.OpenSubKey("Software", true);

RegistryKey myKey = softwareKey.OpenSubKey("Kovalenko", true);

myKey.SetValue("password", newpass);

myKey.Close();

softwareKey.Close();

this.Close();

}

else

{

MessageBox.Show("Не подходит старый пароль!");

}

}

}

}

Результат:

Генерація TOTP ключа на 30с(рис. 1):

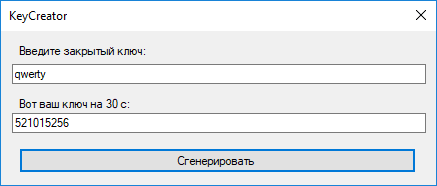


Рисунок 1

В основну програму вводимо ключ синхронізації(Він зберігається і після закриття програми)(рис. 2):

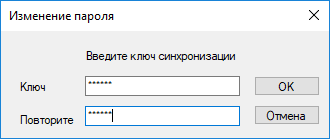


Рисунок 2

Вводимо логін і TOTP код(рис. 3):

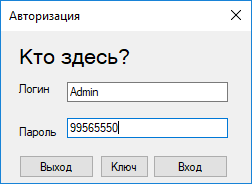


Рисунок 3

Успішно входимо в програму(рис. 4):

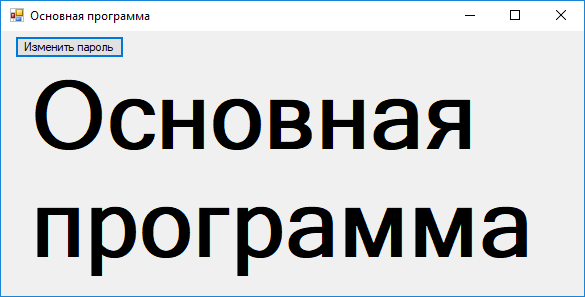


Рисунок 4

**Висновок:** у ході лабораторної роботи дослідили і реалізували механізм генерації одноразових паролів TOTP з використанням мови C#.