

Лабораторна робота №2

Тема: Password storing

Мета роботи: Дослідити і порівняти існуючі механізми зберігання паролів.

Завдання:

Дослідити існуючі механізми зберігання паролів. Зробити порівняльну характеристику кожного механізму. Реалізувати механізм зберігання паролів та продемонструвати процес аутентифікації. Довести що даний метод оптимальний.

Виконання роботи.

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

Код програми аутентифікації 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.authoriz = 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
    {
        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();
            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 myNKey = softwareKey.OpenSubKey("Kovalenko", true);
            RegistryKey myKey = myNKey.OpenSubKey("Lab2", 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();
            myNKey.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 != 5)
    //{
    //    MessageBox.Show("Неверный пароль");
    //    textBox2.Text = "";
    //}
    else
    {
        if (GlobalVars.adpass == heshGen(textBox2.Text))
        {
            GlobalVars.authoriz = true;
            this.Close();
        }
        else
        {
            MessageBox.Show("Неверный пароль");
            textBox2.Text = "";
        }
    }
}

}

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 + "?";
}

private String heshGen(String pass)
{
    //String a = "1";

    var enc = Encoding.ASCII;
    HMACSHA1 hmac = new HMACSHA1(enc.GetBytes(pass));
    hmac.Initialize();
}

```

```

        byte[] buffer = enc.GetBytes(pass);
        String key20 = BitConverter.ToString(hmac.ComputeHash(buffer)).Replace("-",
""").ToLower();

        return key20;
        //textBox2.Text = key20;
    }
}

```

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
            }
            //GlobalVars.adpass = "123";
        }

        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.Security.Cryptography;
using System.Text;
using System.Threading.Tasks;
using System.Windows.Forms;
using Microsoft.Win32;

namespace PassV2
{
    public partial class Form3 : Form
    {
        String oldpass;
        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 textBox3_TextChanged(object sender, EventArgs e)
            {
                oldpass = textBox3.Text;
            }

            private void button1_Click(object sender, EventArgs e)
            {
                RegistryKey currentUserKey = Registry.CurrentUser;
                RegistryKey softwareKey = currentUserKey.OpenSubKey("Software", true);
                RegistryKey myNKey = softwareKey.OpenSubKey("Kovalenko", true);
                RegistryKey myKey = myNKey.OpenSubKey("Lab2", true);

                oldpass = heshGen(oldpass);

                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 (oldpass == myKey.GetValue("password").ToString() && (newpass ==
newpass2))
                {
                    MessageBox.Show("Пароль изменен!");
                    newpass = heshGen(newpass);
                    GlobalVars.adpass = newpass;
                    myKey.SetValue("password", newpass);
                    this.Close();
                }
                else
                {
                    MessageBox.Show("Не подходит старый пароль!");
                }
            }
        }
    }
}

```

```

    }
    myKey.Close();
    myNKey.Close();
    softwareKey.Close();
}

private String heshGen(String pass)
{
    //String a = "1";

    var enc = Encoding.ASCII;
    HMACSHA1 hmac = new HMACSHA1(enc.GetBytes(pass));
    hmac.Initialize();

    byte[] buffer = enc.GetBytes(pass);
    String key20 = BitConverter.ToString(hmac.ComputeHash(buffer)).Replace("-",
""").ToLower();

    return key20;
    //textBox2.Text = key20;
}
}
}

```

Результат:

Вводимо логін і код(рис. 1):

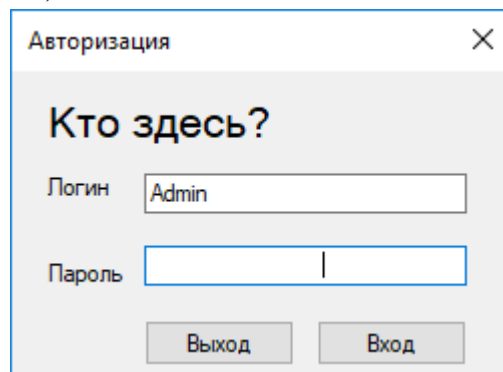


Рисунок 1

Успішно входимо в програму(рис. 2):

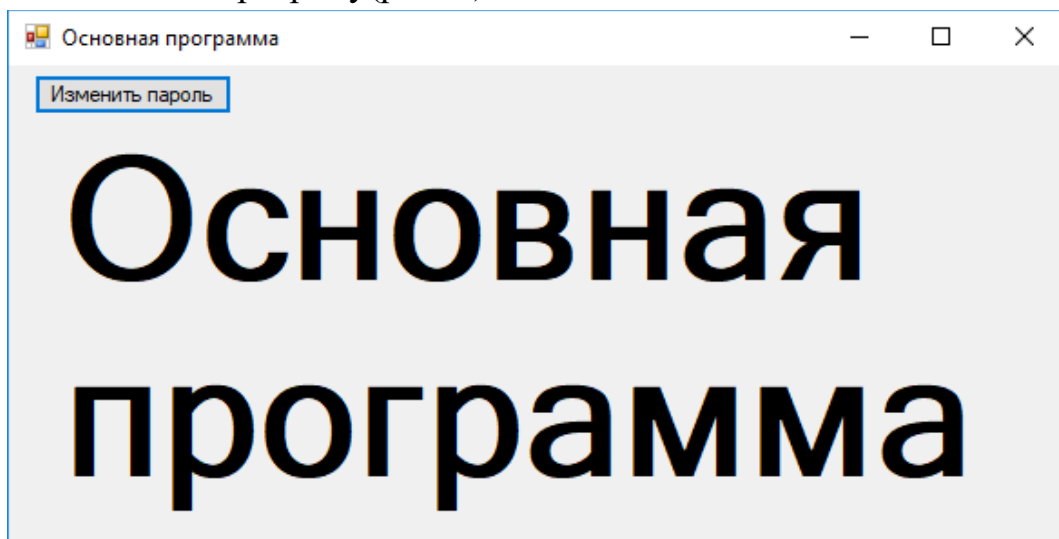


Рисунок 2

Висновок: у ході лабораторної роботи дослідили і порівняли існуючі механізми зберігання паролів з використанням мови C#.