Основи інформаційної безпеки

ПЗ №9-10

“Електронно цифровий підпис”

Підготував:

Студент групи МІТ-21

Міхальський Владислав

Завдання №1

using System;

using System.IO;

using System.Security.Cryptography;

using System.Text;

namespace lab9

{

class Program

{

private readonly static string CspContainerName = "RsaContainer";

public static void AssignNewKey(string publicKeyPath)

{

CspParameters cspParams = new CspParameters(1)

{

KeyContainerName = CspContainerName,

ProviderName = "Microsoft Strong Cryptographic Provider"

};

var rsa = new RSACryptoServiceProvider(cspParams)

{

PersistKeyInCsp = true

};

File.WriteAllText(publicKeyPath, rsa.ToXmlString(false));

}

public static byte[] SignData(byte[] dataToSign)

{

var cspParams = new CspParameters

{

KeyContainerName = CspContainerName

};

using (var rsa = new RSACryptoServiceProvider(cspParams))

{

rsa.PersistKeyInCsp = true;

var rsaFormatter = new RSAPKCS1SignatureFormatter(rsa);

rsaFormatter.SetHashAlgorithm(nameof(SHA512));

byte[] hashData;

using (var sha512 = SHA512.Create())

{

hashData = sha512.ComputeHash(dataToSign);

}

return rsaFormatter.CreateSignature(hashData);

}

}

public static bool Verify(string publicKeyPath, byte[] data, byte[] signature)

{

using (var rsa = new RSACryptoServiceProvider())

{

rsa.PersistKeyInCsp = false;

rsa.FromXmlString(File.ReadAllText(publicKeyPath));

var rsaDeformatter = new RSAPKCS1SignatureDeformatter(rsa);

rsaDeformatter.SetHashAlgorithm(nameof(SHA512));

byte[] hashData;

using (var sha512 = SHA512.Create())

{

hashData = sha512.ComputeHash(data);

}

return rsaDeformatter.VerifySignature(hashData, signature);

}

}

static void Main(string[] args)

{

string publicKeyPath = "Mikhalskyi\_public\_lab9.xml";

string data = "Hello";

Console.WriteLine(data);

byte[] byteData = Encoding.UTF8.GetBytes(data);

AssignNewKey(publicKeyPath);

var signedbyteData = SignData(byteData);

var verSignedByteData = Verify(publicKeyPath, byteData, signedbyteData);

Console.WriteLine (Convert.ToBase64String(signedbyteData));

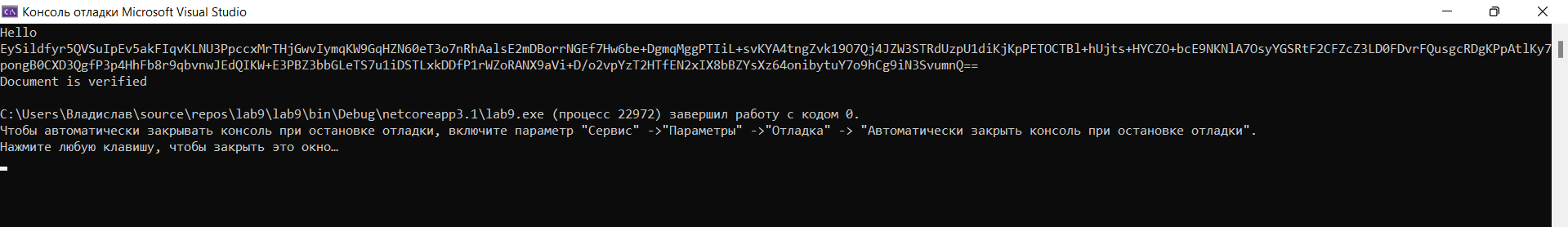
Console.WriteLine(verSignedByteData ? "Document is verified" : "Document is not verified");

}

}

}

Результат:



Посилання на гітхаб репозиторій: https://github.com/vmikhalskyi/Security-basics-2021.git

Висновок: у ході лабораторної роботи я дізнався, що таке електронно цифровий підпис та як він працює. Зрозумів, що ЕЦП – це невід'ємна частина нашого життя та дуже зручна технологія. Також, навчився підписувати повідомлення, спочатку хешуючи його, а потім накладаючи секретний ключ шифрування. А потім, звіряти хеші, щоб розуміти, що повідомлення не було спотворено.