Основи інформаційної безпеки

ПЗ №8

“ Обмін зашифрованими повідомленнями”

Підготував:

Студент групи МІТ-21

Міхальський Владислав

Завдання №1

using System;

using System.IO;

using System.Linq;

using System.Security.Cryptography;

using System.Text;

namespace lab7.\_2

{

class RSAWithRSAParameterKey

{

public void AssignNewKey(string publicKeyPath, string

privateKeyPath)

{

using (var rsa = new RSACryptoServiceProvider(2048))

{

rsa.PersistKeyInCsp = false;

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

File.WriteAllText(privateKeyPath, rsa.ToXmlString(true));

}

}

public byte[] EncryptData(string publicKeyPath, byte[] dataToEncrypt)

{

byte[] cypherbytes;

using (var rsa = new RSACryptoServiceProvider(2048))

{

rsa.PersistKeyInCsp = false;

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

cypherbytes = rsa.Encrypt(dataToEncrypt, true);

}

return cypherbytes;

}

public byte[] DecryptData(string privateKeyPath, byte[] dataToDecrypt)

{

byte[] plainText;

using (var rsa = new RSACryptoServiceProvider(2048))

{

rsa.PersistKeyInCsp = false;

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

plainText = rsa.Decrypt(dataToDecrypt, true);

}

return plainText;

}

}

class Program

{

static void Main(string[] args)

{

var rsaParams = new RSAWithRSAParameterKey();

Console.WriteLine("Choose what you want to do: generate new public and private keys, encrypt message or decrypt message (g/e/d):");

string action = Convert.ToString(Console.ReadLine());

if (action == "g")

{

Console.WriteLine("Enter desired path to newly generated public key: ");

string publicKeyPath = Convert.ToString(Console.ReadLine());

Console.WriteLine("Enter desired path to newly generated private key: ");

string privateKeyPath = Convert.ToString(Console.ReadLine());

rsaParams.AssignNewKey(publicKeyPath, privateKeyPath);

Console.WriteLine("Done! Check your newly generated keys in folder");

} else if (action == "e")

{

Console.WriteLine("Enter path to public key which we will use to encrypt data: ");

string publicKeyPath = Convert.ToString(Console.ReadLine());

Console.WriteLine("Enter message to encrypt: ");

string message = Convert.ToString(Console.ReadLine());

Console.WriteLine("Enter desired path to encrypted message (.dat format):");

string messagePath = Convert.ToString(Console.ReadLine());

var encData = rsaParams.EncryptData(publicKeyPath, Encoding.Unicode.GetBytes(message));

Console.WriteLine("Encrypted Text: " + Convert.ToBase64String(encData));

File.WriteAllBytes(messagePath, encData);

Console.WriteLine("Encrypted message was saved");

} else if (action == "d")

{

Console.WriteLine("Enter path to private key which we will use to decrypt data: ");

string privateKeyPath = Convert.ToString(Console.ReadLine());

Console.WriteLine("Enter path to message to decrypt: ");

string messagePath = Convert.ToString(Console.ReadLine());

byte[] newEncData = File.ReadAllBytes(messagePath).ToArray();

var decrypted = rsaParams.DecryptData(privateKeyPath, newEncData);

Console.WriteLine("Decrypted Text: " + Encoding.Default.GetString(decrypted));

} else

{

Console.WriteLine("Invalid command, try again");

}

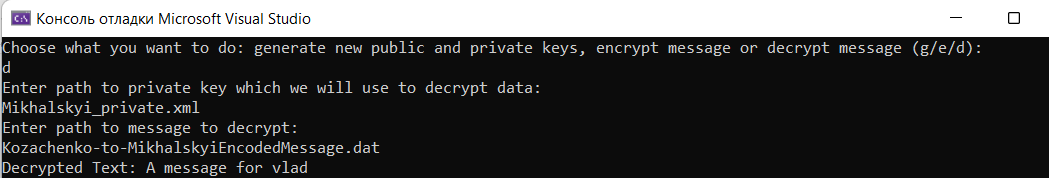
}

}

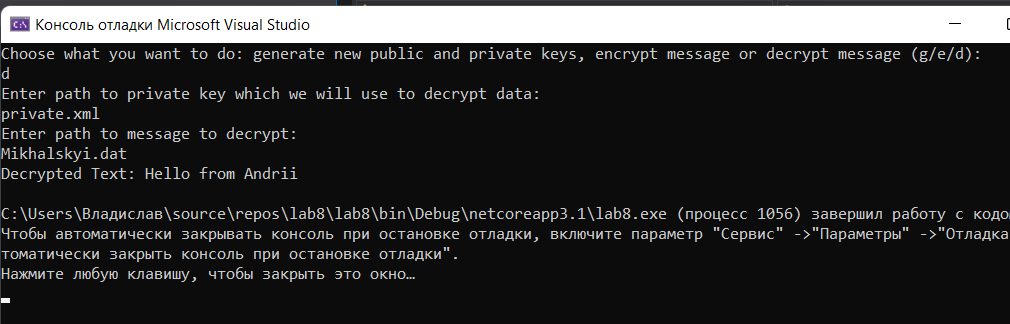
}

Результат: у ході виконання програми, користувач може обрати, що він хоче зробити, а саме: згенерувати нову пару публічного та приватного ключа, розшифрувати зашифроване повідомлення, та зашифрувати повідомлення. Я обмінявся своїм публічним ключем з двома одногрупниками й вони зашифрували для мене два повідомлення, я його розшифрував і от що в мене вийшло:

Це повідомлення від Олесі Козаченко

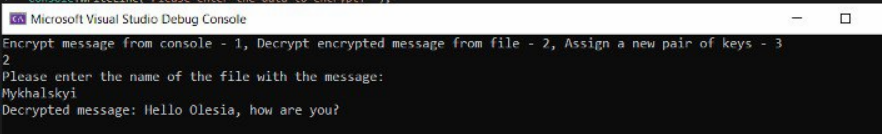


Це повідомлення від Андрія Мірошника

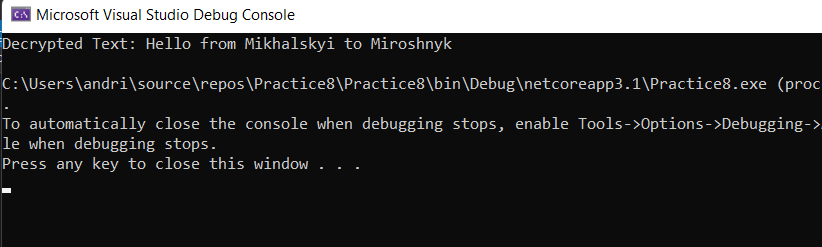


Також за допомогою публічних ключів одногрупників я зашифрував для них також два повідомлення, от що в мене вийшло:

Розшифроване повідомлення від Олесі Козаченко



Розшифроване повідомлення від Андрія Мірошника



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

Висновок: у ході лабораторної роботи я навчився, обмінюватись зашифрованими повідомленнями та публічними ключами з одногрупниками. Розшифровувати повідомлення, за допомогою приватного ключа й зашифровувати повідомлення, за допомогою публічного ключа.