Звіт до Практичної роботи (3-4)

Тема: «Хеш-функції та перевірка цілісності інформації»

Студента Ремеза Максима

Завдання 1

using System;

using System.Security.Cryptography;

using System.Text;

namespace Task1

{

class Program

{

public static byte[] ComputeHashSha1(byte[] toBeHashed)

{

using (var sha1 = SHA1.Create())

{

return sha1.ComputeHash(toBeHashed);

}

}

public static byte[] ComputeHashSha256(byte[] toBeHashed)

{

using (var sha256 = SHA256.Create())

{

return sha256.ComputeHash(toBeHashed);

}

}

public static byte[] ComputeHashSha384(byte[] toBeHashed)

{

using (var sha384 = SHA384.Create())

{

return sha384.ComputeHash(toBeHashed);

}

}

public static byte[] ComputeHashSha512(byte[] toBeHashed)

{

using (var sha512 = SHA512.Create())

{

return sha512.ComputeHash(toBeHashed);

}

}

static byte[] ComputeHashMd5(byte[] dataForHash)

{

using (var md5 = MD5.Create())

{

return md5.ComputeHash(dataForHash);

}

}

static void Main(string[] args)

{

const string strForHash1 = "Hi there!!";

const string strForHash2 = "Hello World!!";

var md5ForStr1 = ComputeHashMd5(Encoding.Unicode.GetBytes(strForHash1));

var md5ForStr2 = ComputeHashMd5(Encoding.Unicode.GetBytes(strForHash2));

Console.WriteLine("Алгоритм MD5:");

Console.WriteLine(strForHash1);

Console.WriteLine(strForHash2);

Console.WriteLine(Convert.ToBase64String(md5ForStr1));

Console.WriteLine(Convert.ToBase64String(md5ForStr2));

var sha1ForStr1 = ComputeHashSha1(Encoding.Unicode.GetBytes(strForHash1));

var sha1ForStr2 = ComputeHashSha1(Encoding.Unicode.GetBytes(strForHash2));

Console.WriteLine("Алгоритм SHA1:");

Console.WriteLine(strForHash1);

Console.WriteLine(strForHash2);

Console.WriteLine(Convert.ToBase64String(sha1ForStr1));

Console.WriteLine(Convert.ToBase64String(sha1ForStr2));

var sha256ForStr1 = ComputeHashSha256(Encoding.Unicode.GetBytes(strForHash1));

var sha256ForStr2 = ComputeHashSha256(Encoding.Unicode.GetBytes(strForHash2));

Console.WriteLine("Алгоритм SHA256:");

Console.WriteLine(strForHash1);

Console.WriteLine(strForHash2);

Console.WriteLine(Convert.ToBase64String(sha256ForStr1));

Console.WriteLine(Convert.ToBase64String(sha256ForStr2));

var sha384ForStr1 = ComputeHashSha384(Encoding.Unicode.GetBytes(strForHash1));

var sha384ForStr2 = ComputeHashSha384(Encoding.Unicode.GetBytes(strForHash2));

Console.WriteLine("Алгоритм SHA384:");

Console.WriteLine(strForHash1);

Console.WriteLine(strForHash2);

Console.WriteLine(Convert.ToBase64String(sha384ForStr1));

Console.WriteLine(Convert.ToBase64String(sha384ForStr2));

var sha512ForStr1 = ComputeHashSha512(Encoding.Unicode.GetBytes(strForHash1));

var sha512ForStr2 = ComputeHashSha512(Encoding.Unicode.GetBytes(strForHash2));

Console.WriteLine("Алгоритм SHA512:");

Console.WriteLine(strForHash1);

Console.WriteLine(strForHash2);

Console.WriteLine(Convert.ToBase64String(sha512ForStr1));

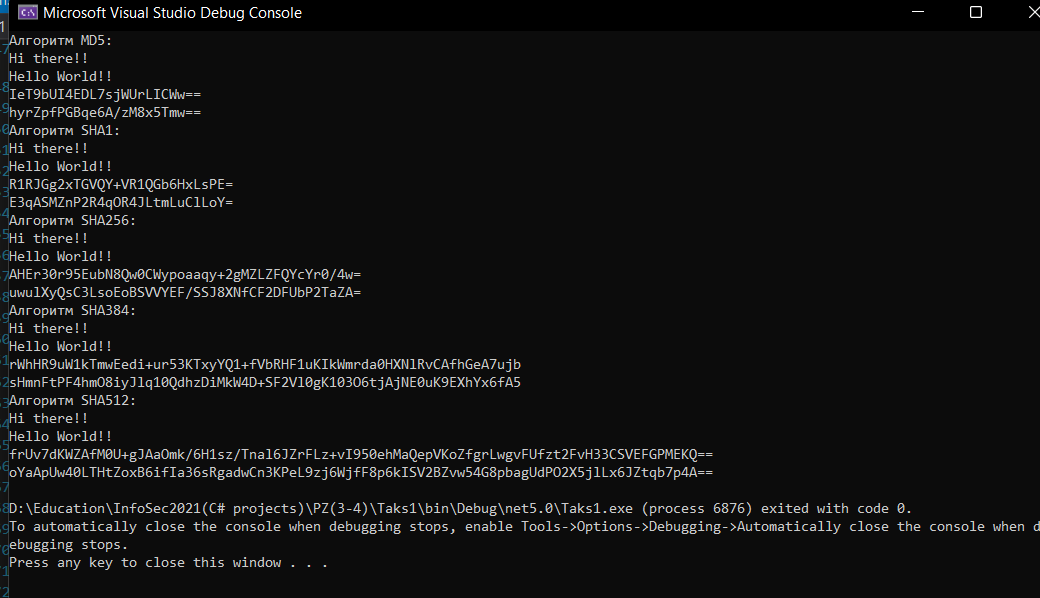
Console.WriteLine(Convert.ToBase64String(sha512ForStr2));

}

}

}

У консолі:



Завдання 2

using System;

using System.Security.Cryptography;

using System.Text;

namespace Task2

{

class Program

{

static byte[] ComputeHashMd5(byte[] dataForHash)

{

using (var md5 = MD5.Create())

{

return md5.ComputeHash(dataForHash);

}

}

static void Main(string[] args)

{

string hash = "po1MVkAE7IjUUwu61XxgNg==";

for (int i = 100000000; i <= 189999999; i++)

//Основна конвертація

{

var returnedHash = Convert.ToBase64String(ComputeHashMd5(Encoding.Unicode.GetBytes(i.ToString().Substring(1, 8))));

if (returnedHash == hash)

{

Console.WriteLine($"User's password is {i.ToString().Substring(1, 8)}");

}

}

}

}

}

У консолі:

