Міністерство освіти та науки України

Національній технічний універсиет України

«Київський політехнічний інститут»

Лабораторна робота № 7

**УЗГОДЖЕННЯ СЕАНСОВОГО КЛЮЧА ПО ПРОТОКОЛУ ДІФФІ-**

**ХЕЛЛМАНА**

Виконав:

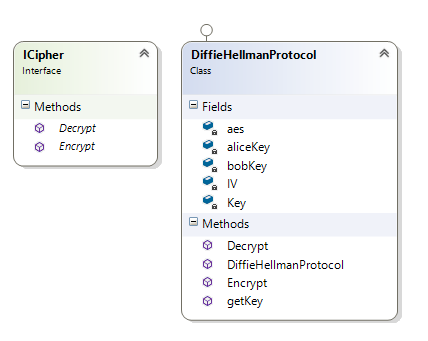
студент 3-го курсу

ТЕФ, групи ТР-21

Самойленко Дмитро

Київ – 2015

Діаграма класів:



Сеансовий ключ узгоджений за протоколом Діффі-Хелмана, шифрування здійснено за допомогою алгоритма AES(Advanced Encryption Standard).

Фрагмент функціонального коду:

public string Encrypt(string text)

        {

            byte[] plaintextbytes = System.Text.UnicodeEncoding.Unicode.GetBytes(text);

            ICryptoTransform crypto = aes.CreateEncryptor(aes.Key, aes.IV);

            byte[] encrypted = crypto.TransformFinalBlock(plaintextbytes, 0, plaintextbytes.Length);

            crypto.Dispose();

            return Convert.ToBase64String(encrypted);

        }

        public string Decrypt(string encrypted)

        {

            byte[] encryptedbytes = Convert.FromBase64String(encrypted);

            ICryptoTransform crypto = aes.CreateDecryptor(aes.Key, aes.IV);

            byte[] secret = crypto.TransformFinalBlock(encryptedbytes, 0, encryptedbytes.Length);

            crypto.Dispose();

            return System.Text.UnicodeEncoding.Unicode.GetString(secret);

        }

Конструктор класу:

public DiffieHellmanProtocol()

        {

            ECDiffieHellmanCng alice = new ECDiffieHellmanCng();

            alice.KeyDerivationFunction = ECDiffieHellmanKeyDerivationFunction.Hash;

            alice.HashAlgorithm = CngAlgorithm.Sha256;

            ECDiffieHellmanCng bob = new ECDiffieHellmanCng();

            bob.KeyDerivationFunction = ECDiffieHellmanKeyDerivationFunction.Hash;

            bob.HashAlgorithm = CngAlgorithm.Sha256;

            byte[] bobKey = bob.DeriveKeyMaterial(alice.PublicKey);

            byte[] aliceKey = alice.DeriveKeyMaterial(bob.PublicKey);

            aes.BlockSize = 128;

            aes.KeySize = 256;

            aes.IV = System.Text.UnicodeEncoding.Unicode.GetBytes(IV);

            aes.Padding = PaddingMode.PKCS7;

            aes.Mode = CipherMode.CBC;

            foreach (var keyPart in aliceKey)

            {

                Key += Convert.ToString(keyPart);

            };

            var keyForAES = "";

            for (int i = 0; i < 16; i++)

            {

                keyForAES += Key[i];

            }

            aes.Key = System.Text.UnicodeEncoding.Unicode.GetBytes(keyForAES);

        }