|  |
| --- |
| **Практическое занятие №8** |
| **Тема «Изучение стандартных средств для реализации приложений, использующих симметричное и ассиметричное шифрование с использованием библиотеки** [**System.Security.Cryptography**](https://docs.microsoft.com/ru-ru/dotnet/api/system.security.cryptography)**»** |
| Цель: Изучить модель криптографии .NET Framework, основные классы и структуры данных, разработать приложение для шифрования файлов использующих симметричные и ассиметричные алгоритмы шифрования |
| **Теоретические сведения** |

**Криптография в .Net**

В .Net Framework присутствует пространство имён для выполнения криптографических операций под названием System.Security.Cryptography. Данное пространство имён предоставляет криптографические службы, включающие безопасное кодирование и декодирование данных, а также другие операции, такие как хеширование сообщений, генерация случайных чисел и проверка подлинности сообщений. Данная библиотека предоставляет доступ для использования различных реализаций алгоритмов в основном это программные интерфейсы CryptoApi (CAPI) и Cryptography Next Generation API (CNG API) помимо этого для некоторых алгоритмов возможно использование реализаций на основе OpenSsl.

CryptoAPI — интерфейс программирования приложений, который обеспечивает разработчиков Windows-приложений стандартным набором функций для работы с криптопровайдером. Входит в состав операционных систем Microsoft. Большинство функций CryptoAPI поддерживается, начиная с Windows 2000.

Cryptography Next Generation стала долгосрочной заменой CAPI. Данный набор интерфейсов поддерживает все алгоритмы предлагаемые CAPI а также другие алгоритмы перечисленные в своде правил Suite B Агентства национальной безопасности США [1]. Данный интерфейс поддерживает следующие длины ключей или размерность хеша.

* RSA 512 бит to 16384 бит, с шагом 64 бит
* DH 512 бит to 16384 бит, с шагом 64 бит
* DSA 512 бит to 1024 бит, с шагом 64 бит
* ECDSA P-256, P-384, P-521 (NIST Curves)
* ECDH P-256, P-384, P-521 (NIST Curves)
* MD2 128 бит
* MD4 128 бит
* MD5 128 бит
* SHA-1 160 бит
* SHA-256 256 бит
* SHA-384 384 бит
* SHA-512 512 бит

Рассматривая структуру наследования для симметричных алгоритмов в .Net стоит упомянуть что SymmetricAlgorithm является абстрактным классом, от который наследуют абстрактные классы для реализаций каждого из алгоритмов. В свою очередь каждая из реализации алгоритма является производной от абстрактного класса алгоритма. Ниже представлена структура наследования.

SymmetricAlgorithm

Aes

AesCng

AesManeged

AesCryptoServiceProvider

Des

DesCng

DesManeged

DesCryptoServiceProvider

TripleDes

TripleDesCng

TripleDesManeged

TripleDesCryptoServiceProvider

Данная структура наследования повторяется для каждого из трех типов поддерживаемых криптографических операций: SymmetricAlgorithm, AsymmetricAlgorithm, HashAlgorithm.

Рассмотрим часть кода для шифрования сообщения используя алгоритм Aes. Как представлено ниже мы создаём объект шифратор на основе созданного экземпляра криптографического объекта aesAlg. Далее мы создаём потоки для шифрования. Стоит отметить CryptoStream который определяет поток, связывающий потоки данный с криптографическим преобразованием.

ICryptoTransform encryptor = aesAlg.CreateEncryptor(aesAlg.Key, aesAlg.IV);

// создание потоков используемого для шифрования

using (MemoryStream msEncrypt = new MemoryStream())

{

using (CryptoStream csEncrypt = new CryptoStream(msEncrypt, encryptor, CryptoStreamMode.Write))

//1-используемый поток, 2 - криптографические преобразование, 3 тип доступа

{

using (StreamWriter swEncrypt = new StreamWriter(csEncrypt))

{

swEncrypt.Write(plainText);

}

encrypted = msEncrypt.ToArray();

}

}

}

Дешифрование выполняется аналогично за исключением изменения типа доступа CryptoStream и изменения потока с записи на чтение.

ICryptoTransform decryptor = aesAlg.CreateDecryptor(aesAlg.Key, aesAlg.IV);

using (MemoryStream msDecrypt = new MemoryStream(cipherText))

{

using (CryptoStream csDecrypt = new CryptoStream(msDecrypt, decryptor, CryptoStreamMode.Read))

{

using (StreamReader srDecrypt = new StreamReader(csDecrypt))

{

plaintext = srDecrypt.ReadToEnd();

}

}

}

Также стоит упомянуть что сложность большинства алгоритмов шифрование имеет сильную зависимость от длины ключа. Изменение длины ключа возможно в большинстве алгоритмов как симметричного, так и ассиметричного шифрования. Для того что бы изменить размер ключа после инициализации алгоритма необходимо изменить свойство KeySize, что представлено в листинге ниже.

using (TripleDES myDes = TripleDES.Create())

{

myDes.KeySize = 128;

EncryptStringToFile\_DES(route, "2 keys usedE.txt", myDes.Key, myDes.IV);

DecryptStringToFile\_DES("2 keys usedE.txt", "2 key deceypted.txt", myDes.Key, myDes.IV);

}

Что касается ассиметричных алгоритмов то они представлены в данной структуре наследования.

AsymmetricAlgorithm

Rsa

RsaCng

RsaOpenSsl

RsaCryptoServiceProvider

Dsa

DsaCng

DsaOpenSsl

DsaCryptoServiceProvider

ECDiffieHellman

ECDiffieHellmanCng

ECDiffieHellmanOpenSsl

Шифрование и дешифрование для асимметричных алгоритмов выполняется проще из за встроенных функций Encrypt и Decrypt. Так же стоит помнить, что Rsa является блочным алгоритмов и если длина данных не совпадает с длиной блока, то данные нужно дополнить до длины блока. Для этого в данном пространстве имён можно использовать разные режимы заполнения.

using (RSA myRsa = RSA.Create())

{

string publickey = myRsa.ToXmlString(false); //получим открытый ключ

string privatekey = myRsa.ToXmlString(true);//получим закрытый ключ

byte[] encrypted = myRsa.Encrypt(data, RSAEncryptionPadding.Pkcs1);

byte[] decrypted = myRsa.Decrypt(encrypted, RSAEncryptionPadding.Pkcs1);

Console.WriteLine("До шифрования: {0}", original);

Console.WriteLine("Зашифрованное: {0}", System.Text.Encoding.UTF8.GetString(encrypted));

Console.WriteLine("После дешифровки: {0}", System.Text.Encoding.UTF8.GetString(decrypted));

}

Как представлено в коде выше после создания экземпляра Rsa возможна сразу же зашифровать и дешифровать данные использую автоматически сгенерированные ключи. Также код представленный выше содержит пример для получения открытого и закрытого ключа в виде строки в формате Xml.

<RSAKeyValue>

<Modulus>6yEjtrItcUq1hoA01xc63EW5/P99kstIobXsxPCUfUODRn2dazzcyhJ5Quhw1oHodlOMvtDN3xJdOTWDbH3xdQ==

</Modulus>

<Exponent>AQAB

</Exponent>

</RSAKeyValue>

Пример сохранённого в файл открытого ключа

<RSAKeyValue>

<Modulus>6yEjtrItcUq1hoA01xc63EW5/P99kstIobXsxPCUfUODRn2dazzcyhJ5Quhw1oHodlOMvtDN3xJdOTWDbH3xdQ==

</Modulus>

<Exponent>AQAB

</Exponent>

<P>9TsbWvgvA2OqPZxUZ96PomUG8rJk2T0SiH6chz65zkc=

</P>

<Q>9XR41YP8/CUoajovRPKWQZou3J23n3usp1acC3v9dGM=

</Q>

<DP>lnjHJ0GD72t3KUjETdu1fKrK4Z5u3RFpTtGJkD7/2b8=

</DP>

<DQ>9Qv2ppNCuigOlR7JmjflslDPgAklDN9XmyhoWT7L5qk=

</DQ>

<InverseQ>gSJ6G275fGFrEMqwSdgJYvmUQhnpCTcX0T3imIVQwOE=

</InverseQ>

<D>z0gMwu+6zehNtP/rFT9eXXd+qgHWAwYAxsapr0hjrzSXv1qS9QJJ+062YbdHc24WZagrKqABfOLQ3hfLXP3JdQ==

</D></RSAKeyValue>

Пример сохранённого в файл открытого ключа

Как видно на представленных выше файлах открытого и закрытого ключа объём ключей отличается, но также совпадают modulus (n) и Exponent (e). Остальные параметры в закрытом ключе совпадают с общепринятыми обозначениями кроме DP=d mod (p-1), DQ=d mode (q-1) и D обозначающего r или закрытый показатель степени.

Xеширования в .Net выполняется проще остальных операций из за отсутствия необходимости в обратном преобразовании. В данном пространстве имён поддерживаются следующие алгоритмы:

* MD5
* SHA256
* SHA384
* SHA512

Пример кода представлен ниже.

byte[] hashValue = new byte[256];

using (SHA256 mysha256 = SHA256.Create())

{

hashValue = mysha256.ComputeHash(File.ReadAllBytes("sha.txt"));

File.WriteAllBytes("hash.txt", hashValue);

}

Как видно из представленного кода после инициализации экземпляра для шифрования нужно вызвать только один метод ComputeHash который выполнит хеширование данных.

Пример захешированных данных представлен ниже

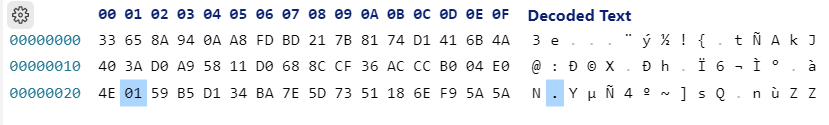


Рисунок 1

Список литературы:

[1] https://apps.nsa.gov/iaarchive/programs/iad-initiatives/cnsa-suite.cfm

|  |
| --- |
| **Ответить на следующие вопросы:**   1. Основное назначение библиотеки System.Security.Cryptography? 2. Что из себя представляет интерфейс CryptoApi? 3. Что такое Cryptography Next Generation? |
| **Выполнить практическое задание:**  *Оформить отчет по ПЗ следующим образом:*   1. Титульный лист с указанием дисциплины, темы занятия, сведений о студенте и преподавателе, вариант задания (если есть). 2. Цель занятия и краткие теоретические сведения по изученному материалу (если они не охвачены ответами на вопросы). 3. Условие задания. 4. Исполнительская часть. 5. Использованные источники (нормативные документы, сайты, учебники и т.п.) |
| **Задание для выполнения:**   1. Ознакомиться с созданием криптографического приложения; 2. Выполнить шифрование, дешифрование и хеширование своей фамилии по указанным алгоритмам. Используя функции работы с файлами сохранить ключи шифрования, результаты шифрования и хеширования. 3. Для выше указанных алгоритмов используя Hex-редактор продемонстрировать ключи шифрования, зашифрованные и захешированные данные.   \*Реализовать проверку сообщения (фамилии) и хеша по примеру ЭЦП. Также продемонстрировать что будет если будет изменен хеш или сообщение. Пример того что нужно реализовать представлен ниже. |

**Варианты индивидуальных заданий**

|  |  |  |
| --- | --- | --- |
| № | Алгоритм шифрования(размер ключа) | Алгоритм хеширования |
| 1 | AES (128bit) | SHA256 |
| 2 | DES | SHA1 |
| 3 | TripleDes (128bit) | SHA384 |
| 4 | RSA (512bit) | MD5 |
| 5 | AES (192bit) | SHA1 |
| 6 | DES | SHA256 |
| 7 | TripleDes (192bit) | SHA384 |
| 8 | RSA (1024bit) | SHA256 |
| 9 | AES (256bit) | SHA512 |
| 10 | DES | SHA384 |
| 11 | TripleDes (128bit) | SHA1 |
| 12 | RSA (640bit) | SHA384 |
| 13 | AES (128bit) | SHA384 |
| 14 | DES | SHA512 |
| 15 | TripleDes (128bit) | SHA1 |
| 16 | RSA (2048bit) | SHA512 |
| 17 | AES (192bit) | SHA1 |
| 18 | DES | MD5 |
| 19 | TripleDes (192bit) | SHA256 |
| 20 | RSA (4096bit) | MD5 |
| 21 | AES (256bit) | MD5 |
| 22 | DES | SHA1 |
| 23 | TripleDes (128bit) | SHA256 |
| 24 | RSA (576bit) | SHA1 |
| 25 | AES (128bit) | SHA1 |
| 26 | DES | SHA256 |
| 27 | TripleDes (128bit) | MD5 |
| 28 | RSA (1088bit) | SHA512 |
| 29 | AES (192bit) | SHA384 |
| 30 | RSA (1536bit) | SHA256 |

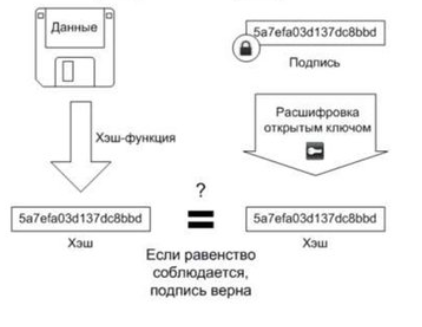


Рисунок 2