|  |  |  |
| --- | --- | --- |
| Министерство науки и высшего образования  Российской Федерации | | |
| Федеральное государственное бюджетное  образовательное учреждение высшего образования | | |
| «Новосибирский государственный технический университет» | | |
|  | | |
| Прикладной математики | | |
|  | | |
| Практическая работа № 4 | | |
| по дисциплине «Основы криптографии» | | |
|  | | |
| **Симметричные криптографические алгоритмы** | | |
|  | | |
|  | Факультет: | ПМИ |
| Группа: | ПМ-81 |
| Вариант: | 1 |
| Студент: | Ефремов Артур |
| Преподаватель: | Ступаков Илья Михайлович |
|
|  |  |
| Новосибирск | | |
| 2020 | | |

1. **Цель работы**  
   Научится использовать готовые криптографические примитивы для шифрования данных.
2. **Задание**  
   **Обязательная часть (15 баллов)**

Сделать программу которая шифрует и дешифрует некоторый файл с помощью алгоритма AES. В качестве ключа использовать хеш (с возможностью выбора алгоритма) от вводимого пользователем пароля. Сам ключ в итоге нигде сохраняться не должен. Использовать режим CBC и в качестве IV взять ключ (такой подход считается плохим, подумайте почему).

Сделать селфи бригады (можно по отдельности и составить коллаж), зашифровать и выложить на общий диск. Изображение и пароль добавить в отчет.

**Доп. Задания**

**(5 баллов)** Сделать чтобы шифровалась только часть файла отвечающая за данные, т.е. после шифрования файл должен остаться валидным изображением и корректно открываться. Привести зашифрованное изображение в отчете. Зашифровать и привести изображение используя режим ECB.

1. **Текст программы**

using System;

using System.Linq;

using System.IO;

using System.Security.Cryptography;

using System.Text;

using System.Drawing;

using System.Collections.Generic;

namespace CryptLab4

{

class Program

{

static public string path = "../../../files/";

static void Main(string[] args)

{

bool repeat = true;

while (repeat)

{

Console.WriteLine("Выберете опцию:");

Console.WriteLine("<1> Зашифровать файл");

Console.WriteLine("<2> Дешифровать файл");

Console.WriteLine("<3> Зашифровать только пиксели файла");

Console.WriteLine("<4> Дешифровать только пиксели файла");

Console.WriteLine("<0> Выйти(");

string choice = Console.ReadLine();

switch (choice)

{

case "1":

{

Console.WriteLine("Введите название файла для шифрования:");

string inFileName = Console.ReadLine();

byte[] toEncrypt;

try

{

toEncrypt = File.ReadAllBytes(path + inFileName);

}

catch (Exception)

{

Console.WriteLine("Нет такого файла!");

break;

}

Console.WriteLine("Введите название файла для вывода:");

string outFileName = Console.ReadLine();

Console.WriteLine("Введите пароль для шифрования:");

byte[] password = Encoding.UTF8.GetBytes(Console.ReadLine());

File.WriteAllBytes(path + outFileName, Encrypt(toEncrypt, password, GetHashAlgorithm(), CipherMode.CBC));

Console.WriteLine("Шифрование прошло успешно!");

break;

}

case "2":

{

Console.WriteLine("Введите название файла для дешифровки:");

string inFileName = Console.ReadLine();

byte[] toDecrypt;

try

{

toDecrypt = File.ReadAllBytes(path + inFileName);

}

catch (Exception)

{

Console.WriteLine("Нет такого файла!");

break;

}

Console.WriteLine("Введите название файла для вывода:");

string outFileName = Console.ReadLine();

Console.WriteLine("Введите пароль для дешифровки:");

byte[] password = Encoding.UTF8.GetBytes(Console.ReadLine());

try

{

File.WriteAllBytes(path + outFileName, Decrypt(toDecrypt, password, GetHashAlgorithm(), CipherMode.CBC));

}

catch (Exception)

{

Console.WriteLine("Неверный пароль или алгоритм генерации хеша!");

break;

}

Console.WriteLine("Дешифровка прошла успешно!");

break;

}

case "3":

{

Console.WriteLine("Введите название файла для шифрования:");

string inFileName = Console.ReadLine();

Bitmap img;

try

{

img = new Bitmap(path + inFileName);

}

catch (Exception)

{

Console.WriteLine("Нет такого файла!");

break;

}

byte[] toEncrypt = PixelsToBytes(img);

Console.WriteLine("Введите название файла для вывода:");

string outFileName = Console.ReadLine();

Console.WriteLine("Введите пароль для шифрования:");

byte[] password = Encoding.UTF8.GetBytes(Console.ReadLine());

byte[] encData = Encrypt(toEncrypt.ToArray(), password, GetHashAlgorithm(), CipherMode.ECB);

SetPixels(img, encData);

img.Save(path + outFileName, System.Drawing.Imaging.ImageFormat.Png);

Console.WriteLine("Шифрование прошло успешно!");

break;

}

case "4":

{

Console.WriteLine("Введите название файла для дешифровки:");

string inFileName = Console.ReadLine();

Bitmap img;

try

{

img = new Bitmap(path + inFileName);

}

catch (Exception)

{

Console.WriteLine("Нет такого файла!");

break;

}

byte[] toDecrypt = PixelsToBytes(img);

Console.WriteLine("Введите название файла для вывода:");

string outFileName = Console.ReadLine();

Console.WriteLine("Введите пароль для дешифровки:");

byte[] password = Encoding.UTF8.GetBytes(Console.ReadLine());

byte[] decData = Decrypt(toDecrypt.ToArray(), password, GetHashAlgorithm(), CipherMode.ECB);

SetPixels(img, decData);

img.Save(path + outFileName, System.Drawing.Imaging.ImageFormat.Png);

Console.WriteLine("Дешифровка прошла успешно!");

break;

}

case "0":

{

repeat = false;

break;

}

default:

{

Console.WriteLine("Неверный выбор!");

break;

}

}

}

}

public static HashAlgorithm GetHashAlgorithm()

{

bool repeat = true;

HashAlgorithm res = HashAlgorithm.Create("SHA-256");

while (repeat)

{

repeat = false;

Console.WriteLine("Выберете алгоритм генерации хеша:");

Console.WriteLine("<1> SHA-256");

Console.WriteLine("<2> MD5");

Console.WriteLine("<3> SHA-512");

string hashChoice = Console.ReadLine();

switch (hashChoice)

{

case "1":

{

res = HashAlgorithm.Create("SHA-256");

break;

}

case "2":

{

res = HashAlgorithm.Create("MD5");

break;

}

case "3":

{

res = HashAlgorithm.Create("SHA-512");

break;

}

default:

{

repeat = true;

Console.WriteLine("Неверный выбор!");

break;

}

}

}

return res;

}

public static byte[] Encrypt(byte[] dataToEncrypt, byte[] password, HashAlgorithm hashAlg, CipherMode cipherMode)

{

using (var aes = Aes.Create())

{

aes.Mode = cipherMode;

aes.Key = hashAlg.ComputeHash(password).ToList().Take(32).ToArray();

aes.IV = aes.Key.ToList().Take(16).ToArray();

aes.Padding = PaddingMode.Zeros;

return PerformCrypt(aes.CreateEncryptor(), dataToEncrypt);

}

}

public static byte[] Decrypt(byte[] dataToDecrypt, byte[] password, HashAlgorithm hashAlg, CipherMode cipherMode)

{

using (var aes = Aes.Create())

{

aes.Mode = cipherMode;

aes.Key = hashAlg.ComputeHash(password).ToList().Take(32).ToArray();

aes.IV = aes.Key.ToList().Take(16).ToArray();

aes.Padding = PaddingMode.Zeros;

var decryptor = aes.CreateDecryptor();

return PerformCrypt(aes.CreateDecryptor(), dataToDecrypt);

}

}

public static byte[] PerformCrypt(ICryptoTransform transform, byte[] data)

{

using (var msDecrypt = new MemoryStream())

{

using (var csEncrypt = new CryptoStream(msDecrypt, transform, CryptoStreamMode.Write))

{

csEncrypt.Write(data);

csEncrypt.FlushFinalBlock();

return msDecrypt.ToArray();

}

}

}

public static byte[] PixelsToBytes(Bitmap img)

{

int w = img.Width;

int h = img.Height;

byte[] res = new byte[h \* w \* 4];

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

for (int j = 0; j < w; j++)

{

Color pixel = img.GetPixel(j, i);

res[(i \* w + j) \* 4 + 0] = pixel.A;

res[(i \* w + j) \* 4 + 1] = pixel.R;

res[(i \* w + j) \* 4 + 2] = pixel.G;

res[(i \* w + j) \* 4 + 3] = pixel.B;

}

return res;

}

public static void SetPixels(Bitmap img, byte[] bytes)

{

int w = img.Width;

int h = img.Height;

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

for (int j = 0; j < w; j++)

{

byte A = bytes[(i \* w + j) \* 4 + 0];

byte R = bytes[(i \* w + j) \* 4 + 1];

byte G = bytes[(i \* w + j) \* 4 + 2];

byte B = bytes[(i \* w + j) \* 4 + 3];

img.SetPixel(j, i, Color.FromArgb(A, R, G, B));

}

}

}

}

1. **Тестирование**

|  |  |  |  |
| --- | --- | --- | --- |
| **№** | **Тест** | **Назначение** | **Результат** |
| **1** | Выберете опцию:  <1> Зашифровать файл  <2> Дешифровать файл  <3> Зашифровать только пиксели файла  <4> Дешифровать только пиксели файла  <0> Выйти(  1  Введите название файла для шифрования:  Arthur.png  Введите название файла для вывода:  Arthur\_encrypted1.png  Введите пароль для шифрования:  crypt4  Выберете алгоритм генерации хэша:  <1> SHA-256  <2> MD5  <3> SHA-512  1  Шифрование прошло успешно! | Шифрование файла целиком. | Файл открывается, но изображение не отображается. |
| **2** | Выберете опцию:  <1> Зашифровать файл  <2> Дешифровать файл  <3> Зашифровать только пиксели файла  <4> Дешифровать только пиксели файла  <0> Выйти(  2  Введите название файла для дешифровки:  Arthur\_encrypted1.png  Введите название файла для вывода:  Arthur\_decrypted1.png  Введите пароль для дешифровки:  crypt4  Выберете алгоритм генерации хэша:  <1> SHA-256  <2> MD5  <3> SHA-512  1  Дешифровка прошла успешно! | Дешифровка файла правильным паролем. | C:\Users\Артур\AppData\Local\Microsoft\Windows\INetCache\Content.Word\Arthur_decrypted1.png  Все нормально. |
| **3** | Выберете опцию:  <1> Зашифровать файл  <2> Дешифровать файл  <3> Зашифровать только пиксели файла  <4> Дешифровать только пиксели файла  <0> Выйти(  2  Введите название файла для дешифровки:  Arthur\_encrypted1.png  Введите название файла для вывода:  Arthur\_decrypted2.png  Введите пароль для дешифровки:  random\_password  Выберете алгоритм генерации хэша:  <1> SHA-256  <2> MD5  <3> SHA-512  1  Неверный пароль или алгоритм генерации хеша! | Дешифровка файла неправильным паролем. | Получаем соответствующее сообщение. |
| **4** | Выберете опцию:  <1> Зашифровать файл  <2> Дешифровать файл  <3> Зашифровать только пиксели файла  <4> Дешифровать только пиксели файла  <0> Выйти(  2  Введите название файла для дешифровки:  Arthur\_encrypted1.png  Введите название файла для вывода:  Arthur\_decrypted3.png  Введите пароль для дешифровки:  crypt4  Выберете алгоритм генерации хэша:  <1> SHA-256  <2> MD5  <3> SHA-512  2  Неверный пароль или алгоритм генерации хеша! | Дешифровка файла неправильным алгоритмом генерации хеша. | Получаем соответствующее сообщение. |
| **5** | Выберете опцию:  <1> Зашифровать файл  <2> Дешифровать файл  <3> Зашифровать только пиксели файла  <4> Дешифровать только пиксели файла  <0> Выйти(  3  Введите название файла для шифрования:  Arthur.png  Введите название файла для вывода:  Arthur\_encrypted2.png  Введите пароль для шифрования:  crypt4  Выберете алгоритм генерации хеша:  <1> SHA-256  <2> MD5  <3> SHA-512  1  Шифрование прошло успешно! | Шифрование только пикселей изображения. | **C:\Users\Артур\AppData\Local\Microsoft\Windows\INetCache\Content.Word\Arthur_encrypted2.png**  **Arthur\_encrypted2.png**  Видим черты исходного изображения, так как использовали режим шифрования ECB. |
| **6** | Выберете опцию:  <1> Зашифровать файл  <2> Дешифровать файл  <3> Зашифровать только пиксели файла  <4> Дешифровать только пиксели файла  <0> Выйти(  4  Введите название файла для дешифровки:  Arthur\_encrypted2.png  Введите название файла для вывода:  Arthur\_decrypted2.png  Введите пароль для дешифровки:  crypt4  Выберете алгоритм генерации хеша:  <1> SHA-256  <2> MD5  <3> SHA-512  1  Дешифровка прошла успешно! | Расшифровка только пикселей изображения. | **E:\Мнё\Биба\Крипта\CryptLab4\CryptLab4\files\Arthur_decrypted2.png**  **Arthur\_decrypted2.png**  Пиксели изображения успешно расшифровались. |
| **7** | Выберете опцию:  <1> Зашифровать файл  <2> Дешифровать файл  <3> Зашифровать только пиксели файла  <4> Дешифровать только пиксели файла  <0> Выйти(  3  Введите название файла для шифрования:  Arthur.png  Введите название файла для вывода:  Arthur\_encrypted3.png  Введите пароль для шифрования:  crypt4  Выберете алгоритм генерации хеша:  <1> SHA-256  <2> MD5  <3> SHA-512  3  Шифрование прошло успешно! | Шифрование с использованием алгоритма генерации хеша длины >32 байт. | C:\Users\Артур\AppData\Local\Microsoft\Windows\INetCache\Content.Word\Arthur_encrypted3.png  **Arthur\_encrypted3.png** |
| **8** | Выберете опцию:  <1> Зашифровать файл  <2> Дешифровать файл  <3> Зашифровать только пиксели файла  <4> Дешифровать только пиксели файла  <0> Выйти(  4  Введите название файла для дешифровки:  Arthur\_encrypted3.png  Введите название файла для вывода:  Arthur\_decrypted3.png  Введите пароль для дешифровки:  crypt4  Выберете алгоритм генерации хеша:  <1> SHA-256  <2> MD5  <3> SHA-512  3  Дешифровка прошла успешно! | Дешифрование с использованием алгоритма генерации хеша длины >32 байт. | **C:\Users\Артур\AppData\Local\Microsoft\Windows\INetCache\Content.Word\Arthur_decrypted3.png**  **Arthur\_decrypted3.png** |

1. **Данные**

|  |  |  |
| --- | --- | --- |
| **№** | **Содержание** | **Назначение** |
| **1** |  | Исходное изображение Arthur.png |
| **2** | C:\Users\Артур\AppData\Local\Microsoft\Windows\INetCache\Content.Word\Arthur_encrypted2.png | Изображение Arthur\_encrypted2, с шифрованием только пикселей. |
| **3** | E:\Мнё\Биба\Крипта\CryptLab4\CryptLab4\files\Arthur_decrypted2.png | Изображение Arthur\_decrypted2, успешно расшифрованное. |
| **4** | crypt4 | Пароль |