

```
using System;
using System.IO;
using System.Runtime.InteropServices;

class AESInterop
{
    [DllImport("kernel32", SetLastError = true)]
    private static extern bool SetDllDirectory(string lpPathName);

    const int AES_KEY_SIZE = 16;
    const int AES_IV_SIZE = 16;

    [DllImport(@"D:\CryptoLibrary\AES.dll", CallingConvention =
CallingConvention.Cdecl)]
    public static extern void GenerateAESKeyIV(byte[] key, byte[] iv);

    [DllImport(@"D:\CryptoLibrary\AES.dll", CallingConvention =
CallingConvention.Cdecl)]
    public static extern void SaveKeyToFile(string filename, byte[] key,
byte[] iv);

    [DllImport(@"D:\CryptoLibrary\AES.dll", CallingConvention =
CallingConvention.Cdecl)]
    public static extern void LoadKeyFromFile(string filename, byte[] key,
byte[] iv);

    [DllImport(@"D:\CryptoLibrary\AES.dll", CallingConvention =
CallingConvention.Cdecl)]
    public static extern void AESEncryptFile(byte[] key, byte[] iv, string
infile, string outfile);

    [DllImport(@"D:\CryptoLibrary\AES.dll", CallingConvention =
CallingConvention.Cdecl)]
    public static extern void AESDecryptFile(byte[] key, byte[] iv, string
infile, string outfile);

    static void Main(string[] args)
    {
        SetDllDirectory(@"C:\msys64\mingw64\bin");

        if (args.Length == 0)
        {
            Console.WriteLine("Usage:");
        }
    }
}
```

```

        Console.WriteLine("    generate          -> Generate and save AES
key/IV");
        Console.WriteLine("    show              -> Show key/IV from
saved file");
        Console.WriteLine("    encrypt <in> <out> -> Encrypt file");
        Console.WriteLine("    decrypt <in> <out> -> Decrypt file");
        return;
    }

    string command = args[0].ToLower();

    byte[] key = new byte[AES_KEY_SIZE];
    byte[] iv = new byte[AES_IV_SIZE];

    switch (command)
    {
        case "generate":
            if (args.Length != 2)
            {
                Console.WriteLine("Wrong arguments: generate
<keyfile>");
                break;
            }
            GenerateAESKeyIV(key, iv);
            SaveKeyToFile(args[1].ToString(), key, iv);
            Console.WriteLine("Generated and saved AES key/IV to
keyfile.bin.");
            break;

        case "show":
            if (args.Length != 2)
            {
                Console.WriteLine("Wrong arguments: show <key>");
                break;
            }
            if (!File.Exists(args[1].ToString()))
            {
                Console.WriteLine("Key file not found.");
                break;
            }
            LoadKeyFromFile(args[1].ToString(), key, iv);
            Console.WriteLine("Key: " +
BitConverter.ToString(key).Replace("-", " "));
            Console.WriteLine("IV : " +
BitConverter.ToString(iv).Replace("-", " "));

```

```

        break;

    case "encrypt":
        if (args.Length != 4)
        {
            Console.WriteLine("Wrong arguments: encrypt <key>
<input> <output>");
            break;
        }
        LoadKeyFromFile(args[1].ToString(), key, iv);
        AESEncryptFile(key, iv, args[2], args[3]);
        Console.WriteLine("File encrypted.");
        break;

    case "decrypt":
        if (args.Length != 4)
        {
            Console.WriteLine("Missing arguments: decrypt <input>
<output>");
            break;
        }
        LoadKeyFromFile(args[1].ToString(), key, iv);
        AESDecryptFile(key, iv, args[2], args[3]);
        Console.WriteLine("File decrypted.");
        break;

    default:
        Console.WriteLine("Unknown command.");
        break;
    }
}
}

```

```
x64 Native Tools Command P...
D:\CryptoLibrary>csc. AES.cs
Microsoft (R) Visual C# Compiler version 4.13.0-3.25126.2 (44ee46ab)
Copyright (C) Microsoft Corporation. All rights reserved..

D:\CryptoLibrary>AES.exe
Usage:
    generate      -> Generate and save AES key/IV
    show         -> Show key/IV from saved file
    encrypt <in> <out> -> Encrypt file
    decrypt <in> <out> -> Decrypt file

D:\CryptoLibrary>AES.exe generate
Wrong arguments: generate <keyfile>

D:\CryptoLibrary>AES.exe generate key.bin
Generated and saved AES key/IV to keyfile.bin.

D:\CryptoLibrary>AES.exe show key.bin
Key: 0F431C25EB2B404A15C3ADE782572239
IV : C179A6256CBF5944DF5B51F201AE96B1

D:\CryptoLibrary>AES.exe encrypt hihi.txt hehe.txt
Wrong arguments: encrypt <key> <input> <output>

D:\CryptoLibrary>AES.exe encrypt key.bin hihi.txt hehe.txt
File encrypted.

D:\CryptoLibrary>AES.exe decrypt key.bin hehe.txt huhu.txt
File decrypted.

D:\CryptoLibrary>cat hihi.txt
ngvanhung.sun
D:\CryptoLibrary>cat hehe.txt
F6D4C1D1CD49E82E3022FE57B724C8B9
D:\CryptoLibrary>cat huhu.txt
ngvanhung.sun
```