

Forum:[Hack Forums](#)

Thread: [\[Source\] AES Encryption \[C#\]](#)

zek0 - September 17, 2010, 10:41 am

Here is source of AES encryption algorithm written in C#

How to use this class

- string plainText - string you want encrypt
- chiperText - string you want decrypt
- passPharse - what ever password you want
- saltValue - can be any string, act like secon password
- hashAlgorithm - can be SHA1, MD5, SHA512 etc...
- passwordIterations - any number
- initVector - must be "@1B2c3D4e5F6g7H8";
- keySize - can be 128,192,256

```
Code using System;
using System.IO;
using System.Text;
using System.Security.Cryptography;
```

```
namespace Encryption
{
    public class AES
    {
        public static string Encrypt(string plainText,
                                     string passPhrase,
                                     string saltValue,
                                     string hashAlgorithm,
                                     int passwordIterations,
                                     string initVector,
                                     int keySize)
        {
            byte[] initVectorBytes = Encoding.ASCII.GetBytes(initVector);
            byte[] saltValueBytes = Encoding.ASCII.GetBytes(saltValue);
            byte[] plainTextBytes = Encoding.UTF8.GetBytes(plainText);

            PasswordDeriveBytes password = new PasswordDeriveBytes(
                passPhrase,
                saltValueBytes,
                hashAlgorithm,
                passwordIterations);

            byte[] keyBytes = password.GetBytes(keySize / 8);

            RijndaelManaged symmetricKey = new RijndaelManaged();
```

```

symmetricKey.Mode = CipherMode.CBC;
ICryptoTransform encryptor = symmetricKey.CreateEncryptor(
    keyBytes,
    initVectorBytes);
MemoryStream memoryStream = new MemoryStream();

CryptoStream cryptoStream = new CryptoStream(memoryStream,
    encryptor,
    CryptoStreamMode.Write);

cryptoStream.Write(plainTextBytes, 0, plainTextBytes.Length);
cryptoStream.FlushFinalBlock();

byte[] cipherTextBytes = memoryStream.ToArray();

memoryStream.Close();
cryptoStream.Close();

string cipherText = Convert.ToBase64String(cipherTextBytes);

return cipherText;
}

public static string Decrypt(string cipherText,
    string passPhrase,
    string saltValue,
    string hashAlgorithm,
    int passwordIterations,
    string initVector,
    int keySize)
{
    byte[] initVectorBytes = Encoding.ASCII.GetBytes(initVector);
    byte[] saltValueBytes = Encoding.ASCII.GetBytes(saltValue);

    byte[] cipherTextBytes = Convert.FromBase64String(cipherText);

    PasswordDeriveBytes password = new PasswordDeriveBytes(
        passPhrase,
        saltValueBytes,
        hashAlgorithm,
        passwordIterations);

    byte[] keyBytes = password.GetBytes(keySize / 8);

    RijndaelManaged symmetricKey = new RijndaelManaged();

    symmetricKey.Mode = CipherMode.CBC;

    ICryptoTransform decryptor = symmetricKey.CreateDecryptor(
        keyBytes,
        initVectorBytes);

```

```

MemoryStream memoryStream = new MemoryStream(cipherTextBytes);

CryptoStream cryptoStream = new CryptoStream(memoryStream,
                                              decryptor,
                                              CryptoStreamMode.Read);

byte[] plainTextBytes = new byte[cipherTextBytes.Length];

int decryptedByteCount = cryptoStream.Read(plainTextBytes,
                                           0,
                                           plainTextBytes.Length);

memoryStream.Close();
cryptoStream.Close();

string plainText = Encoding.UTF8.GetString(plainTextBytes,
                                           0,
                                           decryptedByteCount);

return plainText;
}
}
}

```

Download link: <http://www.multiupload.com/9IMBEJETR6>

pr3fix - September 17, 2010, 10:44 am

Good job, if you made this....

zek0 - September 17, 2010, 10:48 am

(Sep 17, 2010 10:44 AM)pr3fix Wrote: [\[CITE\]](#) Good job, if you made this....

Thanks...!

?

(too short message)

zek0 - September 20, 2010, 11:53 am

Just to refresh this thread.

BUMP!

killerdoob420 - September 20, 2010, 11:56 am

<http://www.discussweb.com/other-web-programming-languages/2091-uses-symmetric-key-algorithm-rijndael-encrypt-decrypt-data.html>

at least give credits if your gonna leech...

newbie223 - September 20, 2010, 11:57 am

yea bro give credits man

shorty msg

zek0 - September 20, 2010, 11:59 am

Credits to: H2o

Can't update first post!

