

## Re: MD5

**Source:**

<http://www.derkeiler.com/Newsgroups/microsoft.public.dotnet.framework.aspnet.security/2005-11/0239.html>

---

**From:** Marre (*news\_at\_supremelink.se*)

**Date:** 11/22/05

Date: Tue, 22 Nov 2005 15:25:04 +0100

Hi Dominick!

Thanks for your answer. Now I get a string, but I can't get that string equal with the string I receive :) I have to try it a little bit more. My code looks like this:

```
private string checkMD5sum(string inputvalue)
{
    // Perform a hash operation using the phrase. This will
    // generate a unique 32 character value to be used as the key.
    byte[] bytePhrase = Encoding.Default.GetBytes(inputvalue);
    MD5 md5 = new MD5CryptoServiceProvider();

    md5.ComputeHash(bytePhrase);
    byte[] result = md5.Hash;

    // Build the final string by converting each byte
    // into hex and appending it to a StringBuilder
    StringBuilder sb = new StringBuilder();
    for (int i=0;i<result.Length;i++)
    {
        sb.Append(result[i].ToString("X2"));
    }

    // And return it
    return sb.ToString();
}
```

Best regards

Marre

"Dominick Baier [DevelopMentor]" <[dbaier@pleasepleasenosspamdevelop.com](mailto:dbaier@pleasepleasenosspamdevelop.com)>  
wrote in message <news:4580be631481398c7bd799da46c07@news.microsoft.com>...

> Hello Marre,

>

> this uses SHA1 for something similar – should be enough to get you

> started...

Re: MD5

```
>
> // Hash = H(salt, H(password))
> static void lengthExtensionHash2()
> {
> Console.WriteLine("Hash with anti length extension attack 2");
>
> string password = "secret";
> byte[] passwordBytes = Encoding.Unicode.GetBytes(password);
> byte[] salt = new byte[32];
>
> new RNGCryptoServiceProvider().GetBytes(salt);
>
> SHA1Managed sha = new SHA1Managed();
>
> byte[] hashedPasswordBytes = sha.ComputeHash(passwordBytes);
>
> CryptoStream cs = new CryptoStream(Stream.Null, sha,
> CryptoStreamMode.Write);
> cs.Write(salt, 0, salt.Length);
> cs.Write(hashedPasswordBytes, 0, hashedPasswordBytes.Length);
> cs.FlushFinalBlock();
>
> byte[] hash = sha.Hash;
>
> string hashString = Convert.ToBase64String(hash);
> string saltString = Convert.ToBase64String(salt);
>
> Console.WriteLine("Hash: " + hashString);
> Console.WriteLine("Salt: " + saltString);
> }
>
> -----
> Dominick Baier – DevelopMentor
> http://www.leastprivilege.com
>
>> Hi all!
>>
>> I have a md5 question.
>> I receive a md5 string created with Message–Digest algorithm and I
>> want to
>> create the same string in my webapplication.
>> I have this values to go on:
>>
>> myMD5String = MD5(mySecretValue2 + MD5(mySecretValue1 + "some
>> string"))
>>
>> myMD5String should of course be the same as the md5 string i receive.
>>
>> I have no idea if I have told you enough about my problem, but someone
>> might be able to point me to right direction :)
>>
```

microsoft.public.dotnet.framework.aspnet.security: Re: MD5

>> *Best regards*

>> *Marre*

>

>