

Re: one way password encryption

Source:

<http://www.tech-archive.net/Archive/DotNet/microsoft.public.dotnet.languages.vb/2004-10/5534.html>

From: Jim Hughes (NOSPAMJ3033_at_Hotmail.com)

Date: 10/24/04

Date: Sun, 24 Oct 2004 09:06:45 -0700

User supplies initial password

You create and store hash based on that password, you don't store the original password and have no need to know what it actually was.

User tries to login and supplies password again.

You recreate hash using same function as before and compare hash to the one you stored previously.

No key is required because you use the same hash function each time.

Keys are only necessary when you need to encrypt and then decrypt.

<http://aspnet.4guysfromrolla.com/articles/112002-1.aspx> has a good article on password management with salt values.

"PJones" <pjones@hotmail.com> wrote in message

news:uPzL0FeuEHA.3788@TK2MSFTNGP09.phx.gbl...

>I am looking for the best way to one way encrypt a password for storage in
>a database using (asp.net / vb.net)

> basically I need some functions or examples that I can freely use in a
> commercial project

>

> anyone got any good functions or links I can look at ?

>

> I was looking at MD5 hash .. the examples I saw confused me as I didn't
> see a key ?

> Does MD5 not used a key ?

>

> I was also looking into SHA-1

>

> I figure if I am going to do this I might as well make it a good as
> possible within reason

>

> any help or pointers is appreciated

>