عنوان مقاله : MD5 چیست ؟ موضوع : برنامه نویسی ویندوز تاریخ انتشار: تابستان ۸۷

چکیده:

MD5 یک الگوریتم است که از رشته ورودی خود یک رشته منحصر بفرد با طول ۱۲۸ بیت می سازد. کاربرد آن در رمزنگاری و مقایسه صحت انتقال داده می باشد. MD5 معمولا با ۳۲ بایت نمایش داده میشود.

اگر الگوریتم MD5 را روی یک فایل یا یک رشته اجرا کنیم آنچه به ما می دهد به نحوی شبیه یک checksum منحصر بفرد است. به نحو خوشبینانه اگر یک فایل داشته باشیم و MD5 آنرا محاسبه نماییم و یک بیت از آن فایل تغییر کند، آنگاه MD5 فایل نیز تغییر خواهد کرد. لذا در انتقال داده ها میتوانیم در مبدا MD5 را محاسبه کرده و با MD5 بدست امده در مقصد مقایسه کنیم در صورت تفاوت درخواست انتقال مجدد نماییم.

شکل یک اجرای MD5 در محیط لینوکس

کاربرد:

الگوریتم MD5 در رمز نگاری و در حفظ صحت داده ها کاربرد دارد. مورد دوم بیشتر در انتقال داده ها مورد توجه است. همانطور که ذکر شد در مبدا و مقصد MD5 محاسبه شده و با هم مقیسه میشوند و در صورت تفاوت درخواست انتقال مجدد داده میشود. احتمال آنکه دو فایل متفاوت دارای MD5 یکسان باشند بسیار کم است و احتمال آنکه دو فایل شبیه به هم که فقط در چند بیت با هم اختلاف دارند دارای MD5 برابر باشند بسیار کمتر است. لذا اگر در اثر نویز چند بیت از یک فایل عوض شود MD5 آن کاملا متفاوت خواهد بود.

در مواردی که میخواهیم «کنترل نگارش» انجام دهیم نیز می توانیم از این روش استفاده کنیم. به عنوان یک مثال در برنامه ای از پایگاه داده محلی روی فایل سیستم کاربر استفاده شده بود. قبل از استفاده از آن MD5 از مرکز دریافت می گردید و با MD5 محلی مقایسه می شد در صورت مغایرت برنامه اجرا نمیشد.

طرح مسئله:

می خواهیم یک برنامه بنویسیم که دو فایل را دریافت کرده و پس از محاسبه، MD5 آنها را نشان دهد و مشخص کند که آیا فایلها برابرند یا خیر.

کد برنامه:

```
private void btnFile1_Click(object sender, EventArgs e)
{
    if (openFileDialog1.ShowDialog() == DialogResult.OK)
    {
        txtFile1.Text = openFileDialog1.FileName;
```

```
        }


    }


    private void btnFile2_Click(object sender, EventArgs e)
    {
        if (openFileDialog1.ShowDialog() == DialogResult.OK)
        {
            txtFile2.Text = openFileDialog1.FileName;
        }
    }


    private void btnCompare_Click(object sender, EventArgs e)
    {
        if ((txtFile1.Text != "") & (txtFile2.Text != ""))
        {
            try
            {
                txtMd51.Text = cMd5.GetMD5Hash(txtFile1.Text);
                txtMd52.Text = cMd5.GetMD5Hash(txtFile2.Text);
                if (txtMd51.Text == txtMd52.Text)
                {
```

```
                txtResult.Text = "برابر";
                txtResult.BackColor = System.Drawing.Color.FromArgb(102,255,204);
            }
            else
            {
                txtResult.Text = "نابرابر";
                txtResult.BackColor = System.Drawing.Color.FromArgb(255, 102, 153);
            }
        }
        catch
        {
            MessageBox.Show("خطا یک ", "ورودی نامعتبر", MessageBoxButtons.OK, MessageBoxIcon.Error);
        }

    }
    else
    {
        MessageBox.Show("خطای دو ", "ورودی تهی", MessageBoxButtons.OK, MessageBoxIcon.Error);
    }
}
```

```
public static string GetMD5Hash(string pathName) // کد آقای تصدیقی
{
    string strResult = "";
    string strHashData = "";

    byte[] arrbytHashValue;
    System.IO.FileStream oFileStream = null;

    System.Security.Cryptography.MD5CryptoServiceProvider oMD5Hasher =
            new System.Security.Cryptography.MD5CryptoServiceProvider();

    try
    {
        oFileStream = GetFileStream(pathName);
        arrbytHashValue = oMD5Hasher.ComputeHash(oFileStream);
        oFileStream.Close();

        strHashData = System.BitConverter.ToString(arrbytHashValue);
        strHashData = strHashData.Replace("-", "");
        strResult = strHashData;
    }
    catch (System.Exception ex)
```

```
        {
            System.Windows.Forms.MessageBox.Show(ex.Message, "Error!",
                        System.Windows.Forms.MessageBoxButtons.OK,
                        System.Windows.Forms.MessageBoxIcon.Error,
                        System.Windows.Forms.MessageBoxDefaultButton.Button1);
        }

        return (strResult);
    }
```

نکته مهم:

در این مقاله از کد آقای داریوش تصدیقی و مقاله ایشان در code project استفاده شده.