## Authentification SRP6 en CSharp

**Mithrandir**

# SRP6 en CSharp

Bien le bonjour, ayant commencé mon site en C# j'ai décidé de vous partager l'authentification SRP6 qui m'a demandé quelques jours de travailles.

```
using System;
using System.Globalization;
using System.Linq;
using System.Numerics;
using System.Security.Cryptography;
using System.Text;

namespace your_models.Utils
{
    public static class SRP6Hash
    {
        public static byte[] Verifier(string username, string passsword, byte[] salt)
        {
            var sha1 = SHA1.Create();
            //INIT
            BigInteger g = 7;
            //00 in order to make the number positive !
            BigInteger N = BigInteger.Parse("00894B645E89E1535BBDAD5B8B290650530801B18EBFBF5E8FAB3C82872A3E9BB7",NumberSty
            byte[] h1 = sha1.ComputeHash(Encoding.UTF8.GetBytes(username.ToUpper() + ":" + passsword.ToUpper()));
            byte[] h2 = sha1.ComputeHash(salt.Concat(h1).ToArray());

            if (!BitConverter.IsLittleEndian)
                h2 = h2.Reverse().ToArray();

            BigInteger _h2 = new BigInteger(h2,true);
            // BigInteger _n = N;
            byte[] v = BigInteger.ModPow(g, _h2, N).ToByteArray(false, false);
            return v;
        }
    }
}
```