DES 加密、解密

1.DES 加密 Java 语言 示例

```
public class DESEncrypt{
    String key;
    public DESEncrypt(){
    }
    public DESEncrypt(String key){
        this.key = key;
    }
    public byte[] desEncrypt(byte[] plainText) throws Exception {
        SecureRandom sr = new SecureRandom();
        DESKeySpec dks = new DESKeySpec(key.getBytes());
        SecretKeyFactory keyFactory = SecretKeyFactory.getInstance("DES");
        SecretKey key = keyFactory.generateSecret(dks);
        Cipher cipher = Cipher.getInstance("DES");
        cipher.init(Cipher.ENCRYPT_MODE, key, sr);
        byte data[] = plainText;
        byte encryptedData[] = cipher.doFinal(data);
        return encryptedData;
    }

    public byte[] desDecrypt(byte[] encryptText) throws Exception {
        SecureRandom sr = new SecureRandom();
        DESKeySpec dks = new DESKeySpec(key.getBytes());
        SecretKeyFactory keyFactory = SecretKeyFactory.getInstance("DES");
        SecretKey key = keyFactory.generateSecret(dks);
        Cipher cipher = Cipher.getInstance("DES");
        cipher.init(Cipher.DECRYPT_MODE, key, sr);
        byte encryptedData[] = encryptText;
        byte decryptedData[] = cipher.doFinal(encryptedData);
        return decryptedData;
    }

    public String encrypt(String input) throws Exception {
        return base64Encode(desEncrypt(input.getBytes())).replaceAll("\\s*", "");
    }

    public String decrypt(String input) throws Exception {
        byte[]
```

```
            result = base64Decode(input);
            return new String(desDecrypt(result));
        }
        public String base64Encode(byte[] s) {
            if (s == null)
                return null;
            BASE64Encoder b = new sun.misc.BASE64Encoder();
            return b.encode(s);
        }

        public byte[] base64Decode(String s) throws IOException {
            if (s == null) {
                return null;
            }
            BASE64Decoder decoder = new BASE64Decoder();
            byte[] b = decoder.decodeBuffer(s);
            return b;
        }

        public static void main(String args[]) {
            try {
                DESEncrypt d = new DESEncrypt("abcdefgh");
                String
                p = d.encrypt("agent=test&username=test ");
                System.out.println("密文:" + p);
            }
            catch (Exception e) {
                e.printStackTrace();
            }
        }

        public String getKey() {
            return key;
        }
        public void setKey(String key) {
            this.key = key;
        }
}
```

2. DES 加密 php 语言示例

```
<?php
class DES
{
```

```
    var $key;
    var $iv; //偏移量

    function DES( $key, $iv=0 ) {
    //key 长度 8 例如:1234abcd
        $this->key = $key;
        if( $iv == 0 ) {
            $this->iv = $key; //默认以$key 作为 iv
        } else {
            $this->iv = $iv; //mcrypt_create_iv ( mcrypt_get_block_size (MCRYPT_DES, MCRYPT_MODE_CBC), MCRYPT_DEV_RANDOM );
        }
    }

    function encrypt($str) {
    //加密，返回大写十六进制字符串
        $size = mcrypt_get_block_size ( MCRYPT_DES, MCRYPT_MODE_CBC );
        $str = $this->pkcs5Pad ( $str, $size );
        return strtoupper( bin2hex( mcrypt_cbc(MCRYPT_DES, $this->key, $str, MCRYPT_ENCRYPT, $this->iv ) ) );
    }

    function decrypt($str) {
    //解密
        $strBin = $this->hex2bin( strtolower( $str ) );
        $str = mcrypt_cbc( MCRYPT_DES, $this->key, $strBin, MCRYPT_DECRYPT, $this->iv );
        $str = $this->pkcs5Unpad( $str );
        return $str;
    }

    function hex2bin($hexData) {
        $binData = "";
        for($i = 0; $i < strlen ( $hexData ); $i += 2) {
            $binData .= chr ( hexdec ( substr ( $hexData, $i, 2 ) ) );
        }
        return $binData;
    }

    function pkcs5Pad($text, $blocksize) {
        $pad = $blocksize - (strlen ( $text ) % $blocksize);
        return $text . str_repeat ( chr ( $pad ), $pad );
    }
```

```
    function pkcs5Unpad($text) {
        $pad = ord ( $text {strlen ( $text ) - 1} );
        if ($pad > strlen ( $text ))
            return false;
        if (strspn ( $text, chr ( $pad ), strlen ( $text ) - $pad ) != $pad)
            return false;
        return substr ( $text, 0, - 1 * $pad );
    }

}
?>
```

3. DES 加密 C#语言 示例

```
using System;
using System.Collections.Generic;
using System.ComponentModel;
using System.Data;
using System.Drawing;
using System.Text;
using System.Windows.Forms;
using System.Security.Cryptography;
using System.Configuration;
using System.Web;
using System.IO;
public class DES
{
    private string DES_Key = "abcdefgh";

    #region DESEnCode DES 加密
    public string DESEncode(string pToEncrypt)
    {
        DESCryptoServiceProvider des = new DESCryptoServiceProvider();
        byte[] inputByteArray = Encoding.GetEncoding("UTF-
        8").GetBytes(pToEncrypt);
        des.Key = ASCIIEncoding.ASCII.GetBytes(DES_Key);
        des.IV = ASCIIEncoding.ASCII.GetBytes(DES_Key);
        MemoryStream ms = new MemoryStream();
        CryptoStream cs = new CryptoStream(ms, des.CreateEncryptor(),
            CryptoStreamMode.Write);
        cs.Write(inputByteArray, 0, inputByteArray.Length);
        cs.FlushFinalBlock();
        StringBuilder ret = new StringBuilder();
        foreach (byte b in ms.ToArray())
```

```
            {
                ret.AppendFormat("{0:X2}", b);
            }
            ret.ToString();
            return ret.ToString();
        }
        #endregion

        #region DESDeCode DES 解密
        public string DESDecode(string pToDecrypt)
        {
            DESCryptoServiceProvider des = new DESCryptoServiceProvider();
            byte[] inputByteArray = new byte[pToDecrypt.Length / 2];
            for (int x = 0; x < pToDecrypt.Length / 2; x++)
            {
                int i = (Convert.ToInt32(pToDecrypt.Substring(x * 2, 2), 16));
                inputByteArray[x] = (byte)i;
            }
            des.Key = ASCIIEncoding.ASCII.GetBytes(DES_Key);
            des.IV = ASCIIEncoding.ASCII.GetBytes(DES_Key);
            MemoryStream ms = new MemoryStream();
            CryptoStream cs = new CryptoStream(ms, des.CreateDecryptor(),
                CryptoStreamMode.Write);
            cs.Write(inputByteArray, 0, inputByteArray.Length);
            cs.FlushFinalBlock();
            StringBuilder ret = new StringBuilder();
            return System.Text.Encoding.UTF8.GetString(ms.ToArray());
        }
        #endregion
}
```

4. DES 加密 VB 语言 示例

```
Public Shared Function Encrypt(ByVal pToEncrypt As String, ByVal sKey As String) As String
    Dim des As New System.Security.Cryptography.DESCryptoServiceProvider()
    Dim inputByteArray() As Byte
    inputByteArray = Encoding.GetEncoding("GBK").GetBytes(pToEncrypt)
    des.Key = System.Text.ASCIIEncoding.ASCII.GetBytes(sKey)
    des.IV = System.Text.ASCIIEncoding.ASCII.GetBytes(sKey)
    Dim ms As New System.IO.MemoryStream()
    Dim cs As New System.Security.Cryptography.CryptoStream(ms,
    des.CreateEncryptor, System.Security.Cryptography.CryptoStreamMode.Write)
    cs.Write(inputByteArray, 0, inputByteArray.Length)
    cs.FlushFinalBlock()
```

```
    Dim ret As New System.Text.StringBuilder()
    Dim b As Byte
    For Each b In ms.ToArray()
      ret.AppendFormat("{0:X2}", b)
    Next
    Return ret.ToString()
End Function
```