1.DES 加密 java 语言 示例

==========

```
public class PHPDESEncrypt {
    String key;

    public PHPDESEncrypt() {

    }

    public PHPDESEncrypt(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 {

			PHPDESEncrypt d = new PHPDESEncrypt("abcdefgh");
			String
p=d.encrypt("cagent=XXXXXX/\\\\/loginname=ptest98/\\\\/method=ice");
			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 DES1 {
	var $key;
	function	DES1($key) {
		$this->key = $key;
	 }
	function encrypt($input) {
		$size = mcrypt_get_block_size('des', 'ecb');
		$input = $this->pkcs5_pad($input, $size);
		$key = $this->key;
		$td = mcrypt_module_open('des', '', 'ecb', '');
		$iv = @mcrypt_create_iv (mcrypt_enc_get_iv_size($td), MCRYPT_RAND);
		 @mcrypt_generic_init($td, $key, $iv);
		$data = mcrypt_generic($td, $input);
		 mcrypt_generic_deinit($td);
		 mcrypt_module_close($td);
		$data = base64_encode($data);
		return preg_replace("/\s*/", '',$data);
	 }
	function decrypt($encrypted) {
		$encrypted = base64_decode($encrypted);
		$key =$this->key;
		$td = mcrypt_module_open('des','','ecb','');
```

```
            //使用 MCRYPT_DES 算法,cbc 模式
            $iv = @mcrypt_create_iv(mcrypt_enc_get_iv_size($td), MCRYPT_RAND);
            $ks = mcrypt_enc_get_key_size($td);
              @mcrypt_generic_init($td, $key, $iv);
            //初始处理
            $decrypted = mdecrypt_generic($td, $encrypted);
            //解密
              mcrypt_generic_deinit($td);
            //结束
              mcrypt_module_close($td);
            $y=$this->pkcs5_unpad($decrypted);
            return $y;
        }
    function pkcs5_pad ($text, $blocksize) {
            $pad = $blocksize - (strlen($text) % $blocksize);
            return $text . str_repeat(chr($pad), $pad);
        }
    function pkcs5_unpad($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);
        }
}
            $key = "abcdefgh";
            $input = "cagent=AG01/\\\\/method=tc";
            $crypt = new DES1($key);
            echo "Encode:".$crypt->encrypt($input)."<br/>";
            echo "Decode:".$crypt->decrypt($crypt->encrypt($input));
?>
```

==========

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
```

==========1.DES 加密 java 语言 示例

==========

```
public class PHPDESEncrypt {
    String key;

    public PHPDESEncrypt() {
```

```
}

public PHPDESEncrypt(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 {

            PHPDESEncrypt d = new PHPDESEncrypt("abcdefgh");
            String
p=d.encrypt("cagent=XXXXXX/\\\\/loginname=ptest98/\\\\/method=ice");
            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 DES1 {
    var $key;
    function        DES1($key) {
        $this->key = $key;
     }
    function encrypt($input) {
        $size = mcrypt_get_block_size('des', 'ecb');
        $input = $this->pkcs5_pad($input, $size);
        $key = $this->key;
        $td = mcrypt_module_open('des', '', 'ecb', '');
        $iv = @mcrypt_create_iv (mcrypt_enc_get_iv_size($td), MCRYPT_RAND);
          @mcrypt_generic_init($td, $key, $iv);
        $data = mcrypt_generic($td, $input);
          mcrypt_generic_deinit($td);
          mcrypt_module_close($td);
        $data = base64_encode($data);
        return preg_replace("/\s*/", '',$data);
     }
    function decrypt($encrypted) {
        $encrypted = base64_decode($encrypted);
        $key =$this->key;
        $td = mcrypt_module_open('des','','ecb','');
        //使用 MCRYPT_DES 算法,cbc 模式
        $iv = @mcrypt_create_iv(mcrypt_enc_get_iv_size($td), MCRYPT_RAND);
        $ks = mcrypt_enc_get_key_size($td);
          @mcrypt_generic_init($td, $key, $iv);
        //初始处理
        $decrypted = mdecrypt_generic($td, $encrypted);
        //解密
```

```
            mcrypt_generic_deinit($td);
            //结束
            mcrypt_module_close($td);
            $y=$this->pkcs5_unpad($decrypted);
            return $y;
        }
    function pkcs5_pad ($text, $blocksize) {
            $pad = $blocksize - (strlen($text) % $blocksize);
            return $text . str_repeat(chr($pad), $pad);
        }
    function pkcs5_unpad($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);
        }
}
            $key = "abcdefgh";
            $input = "cagent=AG01/\\\\/method=tc";
            $crypt = new DES1($key);
            echo "Encode:".$crypt->encrypt($input)."<br/>";
            echo "Decode:".$crypt->decrypt($crypt->encrypt($input));
?>
```

==========

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
```

==========