

aardio 范例: des

```
//DES
import console;
import crypt.des;

var des = crypt.des();

//修改工作模式为 工作模式 ECB （ECB 不使用向量 IV ）
//aes.setKeyParamMode(2/* _CRYPT_MODE_ECB*/);

/*
根据密钥长度自动选择算法。
小于等于 8 字节使用 DES 算法。
小于等于 16 字节使用 2DES 算法。
小于等于 24 字节使用 3DES 算法。
如果遇到 32 字节密钥，通常只要用 string.left 函数取最前面的算法对应长度字节就可以。
*/
des.setPassword("abcd1234" )

//加密
var ciphertext = des.encrypt("测试字符串");

//解密
var plaintext = des.decrypt(ciphertext);

console.log( plaintext, ciphertext )
console.pause(true);

/*
不同编程语言中DES加解密结果要保持一致要注意以下一些要点：

1、工作模式CBC，填充模式 PKCS5（兼容 PKCS7 ），不同语言要保持一致。
2、向量要一致，默认使用'\x12\x34\x56\x78\x90\xAB\xCD\xEF'
3、密钥要一致，DES密钥为8位，3DES可以使用24位密钥
4、使用的文本编码要一致，同一个字符串，使用UTF8或GBK编码在内存中存储的实际数据可能是不一样的。在aardio中使用 string.fromto进行转换。
5、如果加密后返回的密文用了BASE64或16进制编码，那么在解密时同样也先做对应的逆向解码。

DES加密算法不同编程语言通用写法(aardio,php,c#,java等)
http://bbs.aardio.com/forum.php?mod=viewthread&tid=13148
*/
```