aardio 范例: RSA 加密解密

```
//RSA 加密解密
import win.ui;
/*DSG{{*/
var winform = win.form(text="RSA加密、解密";right=794;bottom=553)
winform.add(
btnDecrypt={cls="button";text="解密(使用私钥)";left=585;top=501;right=719;bottom=537;db=1;dr=1;z=9};
btnEncrypt={cls="button";text="加密(使用公钥)";left=434;top=501;right=568;bottom=537;db=1;dr=1;z=8};
btnExportPrivatePkcs1Raw={cls="button";text="导出 PKCS#1 私钥";left=29;top=198;right=166;bottom=234;dl=1;dt=1;z=5};
btnExportPrivatePkcs8={cls="button";text="导出 PKCS#8 私钥";left=29;top=84;right=166;bottom=120;dl=1;dt=1;z=4};
btnExportPublicPkcs1Raw={cls="button";text="导出 PKCS#1 公钥";left=29;top=141;right=166;bottom=177;dl=1;dt=1;z=3};
btnExportPublicX509={cls="button";text="导出 SPKI 公钥";left=29;top=28;right=166;bottom=64;dl=1;dt=1;z=2};
btnImportKey={cls="button";text="导入公钥或私钥(自动识别)";left=417;top=255;right=767;bottom=291;db=1;dr=1;z=6};
editKey={cls="richedit";left=189;top=18;right=769;bottom=249;db=1;dl=1;dr=1;dt=1;edge=1;font=LOGFONT(name='NSimSun');hscroll=1;multiline=1;vscroll=1;z=1};
editText={cls="richedit";text="测试数据( UTF-8 编码)";left=29;top=299;right=771;bottom=498;db=1;dl=1;dr=1;edge=1;hscroll=1;multiline=1;vscroll=1;z=7}
)
/*}}*/

import crypt.rsa;
var rsa = crypt.rsa();
rsa.genKey();

winform.btnExportPublicX509.oncommand = function(id,event){
    //导出通用的 SPKI (Subject Public Key Info) 格式公钥
    winform.editKey.text = rsa.exportPublicKeyX509ToPem();
}

winform.btnExportPublicPkcs1Raw.oncommand = function(id,event){
    winform.editKey.text = rsa.exportPublicKeyPkcs1RawToPem();
}

winform.btnExportPrivatePkcs8.oncommand = function(id,event){
    winform.editKey.text = rsa.exportPrivateKeyPkcs8ToPem();
}

winform.btnExportPrivatePkcs1Raw.oncommand = function(id,event){
    winform.editKey.text = rsa.exportPrivateKeyPkcs1RawToPem();
}

winform.btnImportKey.oncommand = function(id,event){
    var header = rsa.importPemKey(winform.editKey.text);
    if(header) winform.msgbox("已导入: " + header);
    else winform.msgboxErr("错误的密钥格式")
}

winform.btnEncrypt.oncommand = function(id,event){
    var plaintext = winform.editText.text;
    var ciphertext = rsa.encryptReverse(plaintext);
    if(ciphertext){
        winform.editText.text = crypt.encodeBin(ciphertext);
    }
    else {
        winform.msgboxErr("加密失败,请检查是否导入了正确的公钥")
    }
}

winform.btnDecrypt.oncommand = function(id,event){
    var ciphertext = crypt.decodeBin(winform.editText.text);
    if(!ciphertext){
        winform.msgboxErr("解密失败,请检查是否输入了 Base64 编码的密文");
        return;
    }

    //与其他编程语言互通必须使用 rsa.decryptReverse() 而非 rsa.decrypt() 函数
    var plaintext = rsa.decryptReverse(ciphertext);
    if(plaintext){
        winform.editText.text = plaintext;
    }
    else {
        winform.msgboxErr("解密失败,请检查是否导入了正确的私钥")
    }
}

winform.show()
win.loopMessage();
```

Markdown 格式