# 国密算法工具使用帮助

1. 使用前的环境准备

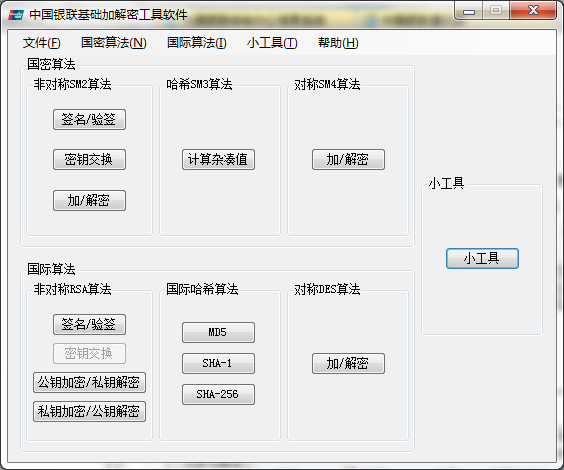
本程序在windows上运行，需用.NET Framework v2.0支持。

如果您的系统是XP，可能需要安装.NET运行环境，请先尝试打开程序，如果可正常运行则无需安装；如果无法正常打开，请[点击这里](http://www.onlinedown.net/softdown/38669_2.htm)下载.NET Framework，然后安装。

如果您的系统是Vista或者Win7，则可直接运行本程序。

1. 主界面

请双击打开与本说明文件同目录下的名为UP\_Crypt\_APP、图标为的应用程序。成功打开后显示的界面如下：

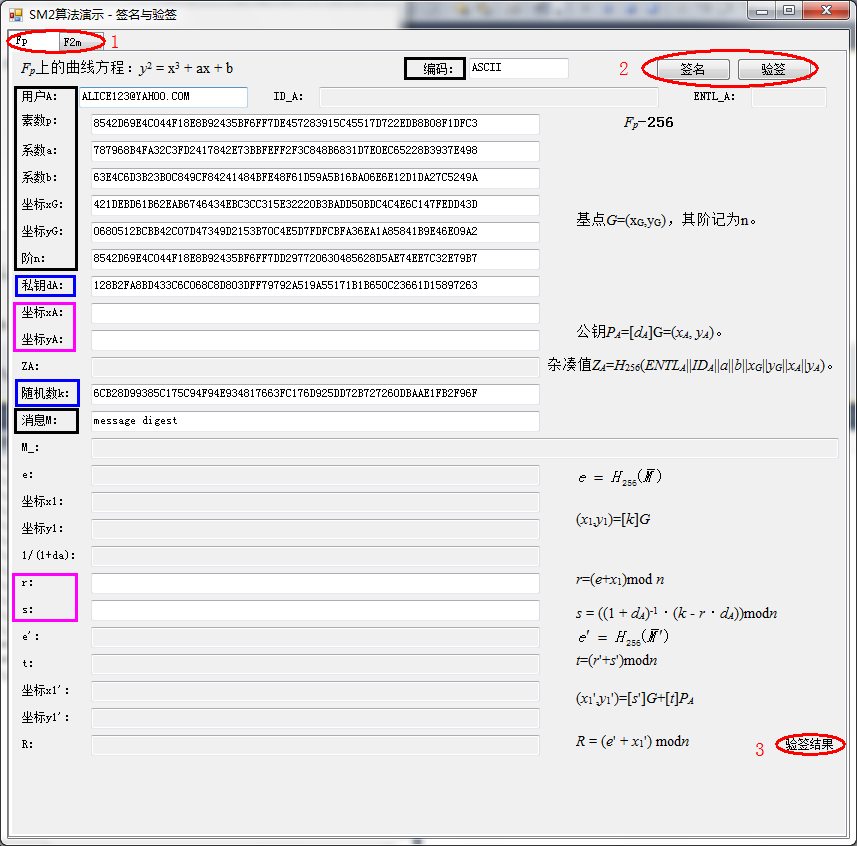


本程序支持国密算法中的SM2，SM3和SMS4三种算法，其中SM2算法分为三种应用：签名/验签、加/解密和密钥交换，同时，提供的小工具中包含XOR计算功能和字符串与16进制串互转的功能。单击相应的按钮即可打开相应的功能。本程序内置了国密局文档中所给的示例，且程序对于所有16进制串输入都会自动忽略其中插入的空格。

1. SM2算法

1 ) 签名与验签

在主界面点击SM2框内的“签名/验签”按钮，打开如下所示的界面：



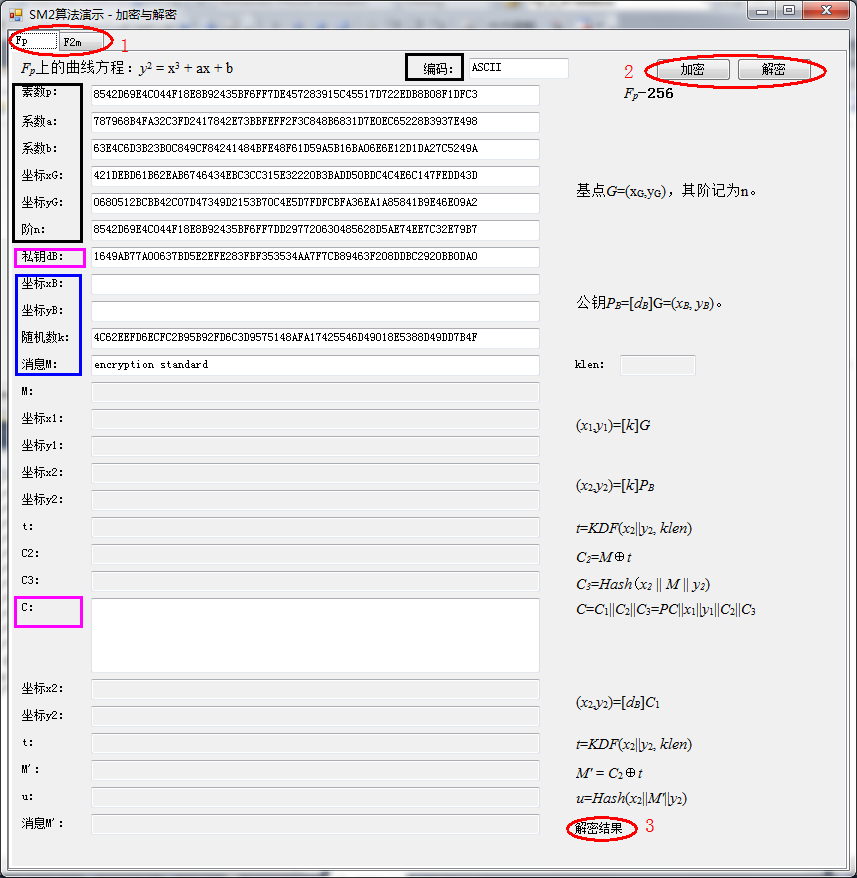
界面上方有两个选项卡（标记为1的位置），可根据需要选择计算*Fp*或F2m上的椭圆曲线数字签名。

签名所需的参数为图中黑色和蓝色圈出的内容，输入完毕后点击“签名”按钮（标记为2的位置）计算签名，签名的结果（即r和s）和中间计算过程会在相应的文本框中呈现。之后可继续点击“验签”按钮（标记为2的位置）对签名进行验证。验签的中间计算过程会在相应的文本框中呈现，最终结果会在标记位置为3的地方显示。

如果需要单独执行验签则需要输入图中黑色和紫红色圈出的内容，输入完毕后点击“验签”按钮（标记为2的位置），结果会在标记位置为3的地方显示。

2 ) 加密与解密

在主界面点击SM2框内的“加/解密”按钮，打开如下所示的界面：



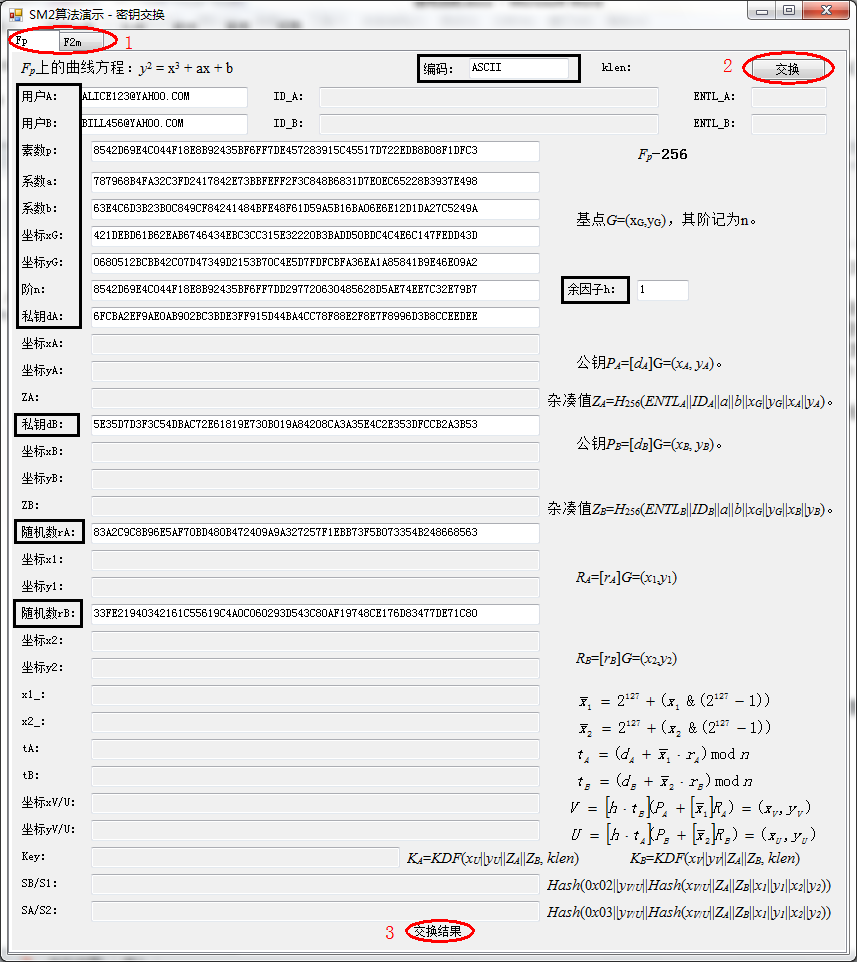
界面上方有两个选项卡（标记为1的位置），可根据需要选择使用*Fp*或F2m上的椭圆曲线公钥加密。

加密所需的参数为图中黑色和蓝色圈出的内容，输入完毕后点击“加密”按钮（标记为2的位置）计算密文，加密的结果（即C）和中间计算过程会在相应的文本框中呈现。之后可继续点击“解密”按钮（标记为2的位置）对密文进行解密。解密的中间计算过程会在相应的文本框中呈现，解密出的明文即消息M’，对解密结果的验证会在标记位置为3的地方显示。

如果需要单独执行解密则需要输入图中黑色和紫红色圈出的内容，输入完毕后点击“解密”按钮（标记为2的位置）即可。

3 ) 密钥交换

在主界面点击SM2框内的“密钥交换”按钮，打开如下所示的界面：

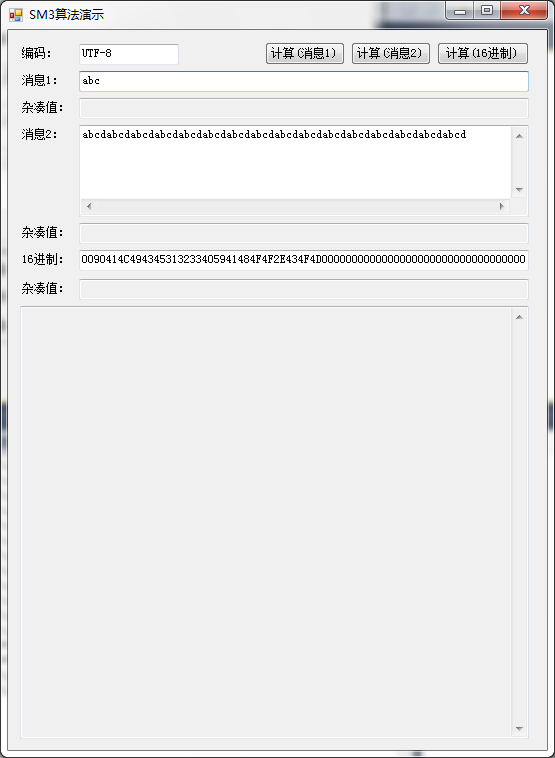


界面上方有两个选项卡（标记为1的位置），可根据需要选择使用*Fp*或F2m上的椭圆曲线密钥交换。

密钥交换所需的参数为图中黑色圈出的内容，输入完毕后点击“交换”按钮（标记为2的位置），交换的结果（即Key）和中间计算过程会在相应的文本框中呈现。对交换结果的验证会在标记位置为3的地方显示。

1. SM3算法

在主界面点击SM3框内的“计算杂凑值”按钮，打开如下所示的界面：

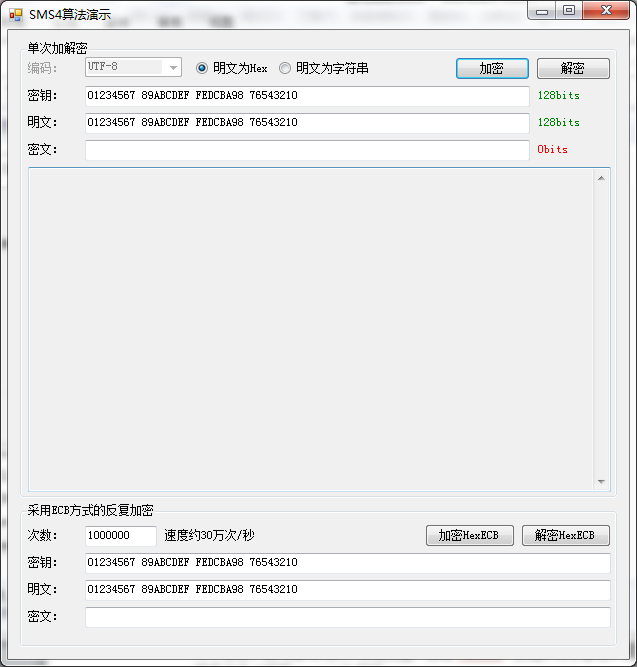


如果需要对一个文本消息字符串直接计算杂凑值，首先应指定编码（默认为UTF-8，也可改成GB2312或其他系统支持的编码格式），然后将待计算的消息填入消息1（不支持多行消息）或消息2（支持多行消息）中，然后点击相应的计算按即可。杂凑值会在消息下方显示，窗口最下方将显示计算过程。

如果需要对一个已经编码为16进制的消息进行杂凑值计算，需要将16进制消息填入“16进制”文本框中，然后点击“计算(16进制)”按钮即可。杂凑值会在消息下方显示，窗口最下方将显示计算过程。

1. SMS4算法

在主界面点击SMS4框内的“加/解密”按钮，打开如下所示的界面：



窗口上部分为采用ECB方式的单次加/解密的演示，下部分为为采用ECB方式使用一个密钥，对一个明文反复加密多次的演示。本算法中，规定密钥必须为128bits，明文和密文均为128bits的整数倍。

1. 采用ECB方式单次加解密

密钥必须使用16进制表示，且必须输入。

如果需要对一个文本形式的明文字符串加密，首先应选中“明文为字符串”的单选框，再指定编码（默认为UTF-8，也可改成GB2312或其他系统支持的编码格式），然后将待加密的消息填入“明文”文本框中，最后点击“加密”按钮即可。密文会以16进制的形式显示在密文文本框中，窗口中间的大文本框将显示计算过程。

如果需要对一个已经编码为16进制的消息进行加密，首先应选中“明文为Hex”的单选框，再将16进制消息直接填入“明文”文本框中，然后点击“加密”按钮即可。密文会以16进制的形式显示在密文文本框中，窗口中间的大文本框将显示计算过程。

如果需要将密文解密成一个文本形式的明文字符串，首先应选中“明文为字符串”的单选框，再指定编码（默认为UTF-8，也可改成GB2312或其他系统支持的编码格式），然后将16进制的密文填入“密文”文本框中，最后点击“解密”按钮即可。文本形式的明文会显示在“明文”文本框中，，窗口中间的大文本框将显示计算过程。

如果需要将密文解密成一个16进制表示的消息，首先应选中“明文为Hex”的单选框，再将16进制的密文填入“密文”文本框中，然后点击“解密”按钮即可。16进制明文会显示在“明文”文本框中，，窗口中间的大文本框将显示计算过程。

1. 采用ECB方式反复加密

密钥、明文和密文均以16进制的形式表示。使用时需先指定加密或解密的次数，对于加密，需先填写明文和密钥，然后点击“加密HexECB”按钮；对于解密，需先填写密文和密钥，然后点击“解密HexECB”按钮。

1. 联机MAC计算

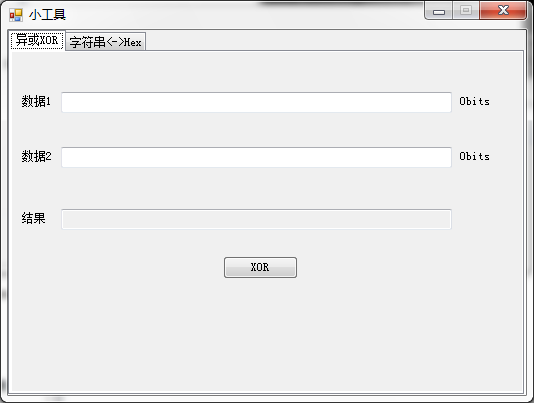
在主界面点击SMS4算法框内的“联机MAC”按钮，打开如下所示的界面：



首先输入128bits的密钥，然后输入已组好的MAB，最后点击“计算”按钮，算出的MAC会显示在“MAC”文本框内，计算的中间过程值将显示在“过程”文本框中。本窗口中，密钥和MAC是16进制串，MAB可以选择以16进制串或是文本字符串的形式输入，当指定MAB为文本字符串时，需要选择合适的编码，默认为ASCII，也可人工选择其他系统支持的编码。

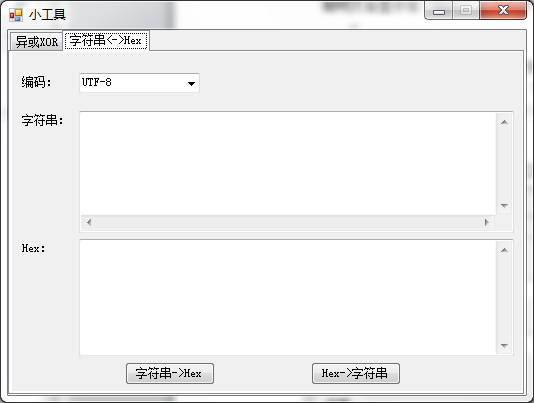
1. 小工具

在主界面点击小工具框内的“小工具”按钮，打开如下所示的界面：



点击“异或XOR”选项卡，显示的界面如上图所示，在“数据1”和“数据2”文本框内填入等长的16进制串，然后点击“XOR”按钮，在“结果”文本框中就会呈现异或结果。

点击“字符串<->Hex”选项卡，显示的界面如下图所示：



首先选择字符串的编码（默认为UTF-8，也可改成GB2312或其他系统支持的编码格式），如需要将文本字符串编码为16进制串，则在“字符串”文本框内输入，然后点击“字符串->Hex”按钮；如需将16进制串解码为文本，则在“Hex”框内输入，然后点击“Hex->字符串”按钮。

1. 联系方式

如果在使用中遇到其他问题，请与我联系，联系方式为：

杨 阳

中国银联 电子支付研究院

手 机：138 1748 8587

电 话：021-50360137

邮 箱：yangyang3@unionpay.com

地 址：上海浦东新区顾唐路1899号培训中心408室

邮 编: 201201