深空® RSA 加密和签名软件

SkyDeep® RSA Encrypt&Signing Software

Version 2.x 使用指南

" 计算机安全深度防御 "

更新日期: 2017-07

最新信息: http://www.sky-deep.com

目录

第一章 欢迎使用

" 深空® RSA 加密和签名软件 "

" 深空 RSA 加密和签名软件 "（原“深空数字签名软件”/“深空公钥加密系统”）是基于 **RSA 公钥加密体系**的集成电子签章（数字签名）与文件加密的类似 **PGP(Pretty Good Privacy)**的软件 ,提供比 **PGP** 更加傻瓜化的操作方式，用于保障电子信息的**保密性**、**真实性**和**完整性**以及签名人的**不可否认性。**

【广泛应用于】:文件加密、文件夹前后比较、文章作者投稿、杂志社收稿、教学成绩提交、电子合同、电子签章、检测网站文件篡改、产品发布、产品文件完整性和来源唯一性检测等场合。

【特别说明】为方便阅读，除非特别说明，否则后文所述的**“文件”**一词都包括**“文件夹 “**。本产品分为**“标准版”**、**“企业版”**、**“旗舰版”**这三种版本，为方便阅读，除非特别说明，否则后文所述所有功能和特性都涵盖这三种版本。

【产品主功能】数字签名、数字验签、文件加密、解密，清除磁盘上已删除数据、彻底删除文件。

数字签名、验签：使用 RSA512 位-RSA8192 位（**此表述为“RSA512 位、RSA1024 位、RSA2048 位、RSA4096 位、RSA8192 位”的简写，下同**）不等的公钥算法对文件进行数字签名或验签。

文件加密、解密：提供 AES256（对称密钥算法），AES256_RSA512 位-RSA8192 位（混合算法），RSA512 位-RSA8192 位（纯公钥算法）这 3 种类型的加密解密算法，对文件进行加密或解密。

清除磁盘上已删除数据：使用**美国国防部 DOD5220.22-M 标准，**对已删除的数据进行 3 次完全覆盖写入：第一次写入 0xFF（全 1），第二次写入 0x00（全 0），**如果是企业版和旗舰版，还将进行第三次写入 0xXX（随机数据）**，达到对磁盘上已删除的数据区域进行彻底清除，防止数据恢复的目的。

彻底删除文件：执行**美国国防部 DOD5220.22-M 标准，**对要删除的文件进行 3 次完全覆盖写入：第一次写入 0xFF（全 1），第二次写入 0x00（全 0），**如果是企业版和旗舰版，还将进行第三次写入 0xXX（随机数据），如果是旗舰版，还会执行 26 次重命名（文件名重命名为全 a、全 b、全 c...全 z）**，达到彻底删除文件，防止数据恢复的目的。

第二章 系统需求、安装、原理

一、 系统需求

1. 计算机硬件性能需求：

处理器： Intel Pentium III 以上

内存： 128MB 以上

硬盘： 剩余空间在 100MB 以上

2. 操作系统支持（32 位和 64 位)

	标准版	企业版	旗舰版
Windows XP/Server 2003	**不支持**	**不支持**	支持
Windows Vista/Server 2008	**不支持**	支持	支持
Windows 7/Server 2008R2	支持	支持	支持
Windows 8/Server 2012	支持	支持	支持
Windows 8.1/Server 2012R2	支持	支持	支持
Windows 10	支持	支持	支持

二、 安装

为防止被篡改、破解、绑定木马病毒等危害，本软件所有 PE 可执行文件（包括 exe 文件和 dll 文件等）都自带第三方权威数字证书颁发机构颁发

的正规的数字签名属性，并且任何可联入互联网的 Windows 计算机都能验证通过该数字签名属性。**如果无法验证通过该数字签名属性，则表明程序已被篡改或来源不可信，用户应立即停止使用。**本软件为绿色软件，无需安装，双击运行即可使用。此外，支持将主要功能添加到鼠标右键菜单，包括**“RSA 签名”、“RSA 加密”、“彻底删除”、“RSA 解密”、“RSA 验签”**等，详细操作请参考 “添加文件关联”。

三、 算法原理

本软件使用 AES256 位进行加密、使用 RSA512 位-RSA8192 位公钥进行验签和加密，使用 AES256 位进行解密、使用 RSA512 位-RSA8192 位私钥进行签名和解密。

AES 算法详见附录一。

RSA 算法详见附录二。

四、 产品原理

- RSA 签名

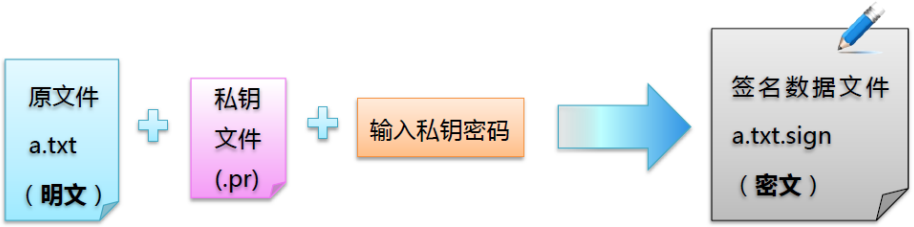


图 3 RSA 签名

➢ RSA 验证签名

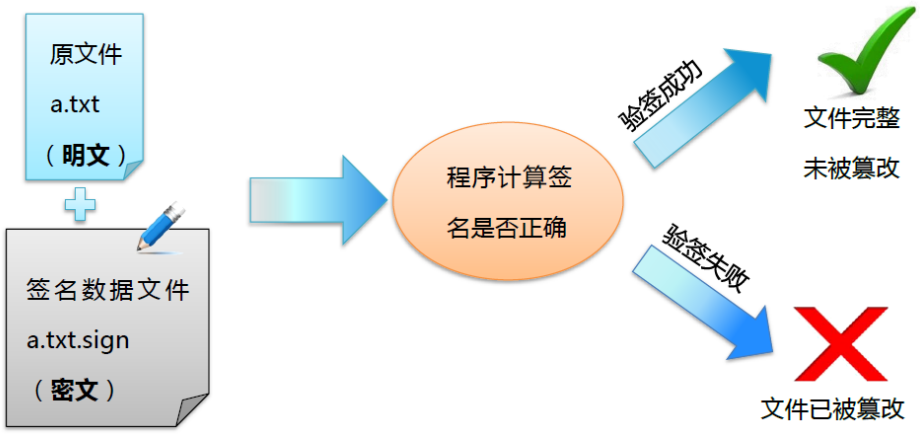


图 4　RSA 验证签名

➢ 传统加密（对称密钥，AES256 算法）

图 1　传统加密

➢ 传统解密（对称密钥，AES256 算法）

图 2　传统解密

- RSA 公钥加密

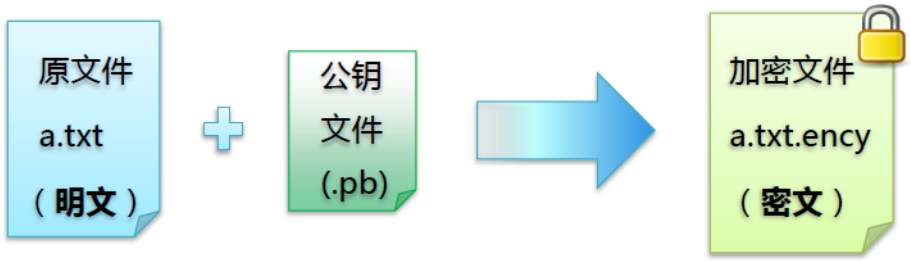


图 5　RSA 公钥加密

- RSA 私钥解密

图 6　RSA 私钥解密

第三章 产品使用

【提示】由于软件产品的特殊性，用户获取到的最新产品在细节上可能会与本说明中的有差异，请以实际为准。

一、 【初始化】添加文件关联

【提示】本软件为绿色软件，无需安装，双击即可使用。

【建议】为能更方便地使用本软件，建议用户将本程序添加文件关联，操作如下：双击本软件，选择“*功能 9：添加/删除文件关联*”，随后按提示点击。

添加成功后，软件会在安装目录下自动释放一个免费的私钥文件和配对的公钥文件（**后文将详解这两个文件**）。添加文件关联后，下面 4 类文件可显示图标：

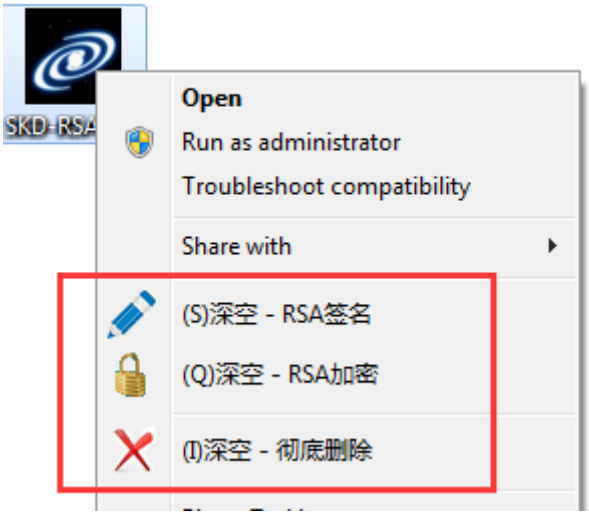
加密后的文件(**.ency**) 

签名数据文件**(.sign)**

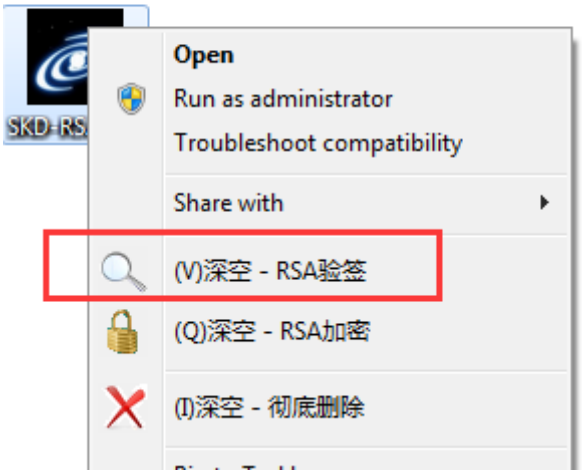
公钥文件**(.pb)**

私钥文件**(.pr)**

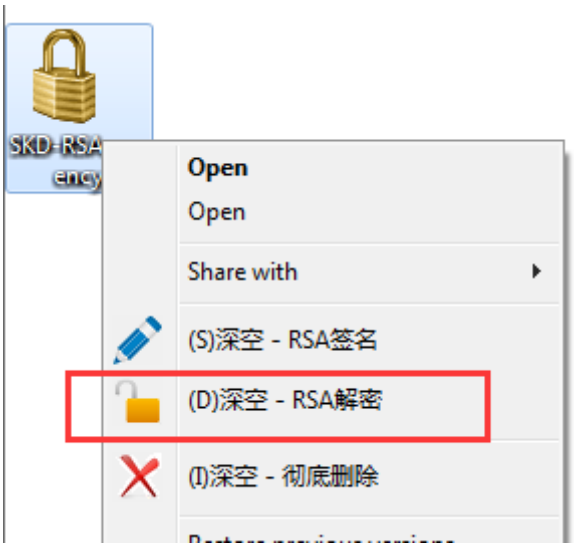
用户对任意一个文件点击鼠标右键，可看到相关新增菜单，如下图所示：



如果鼠标右键所点击文件的同目录下含有对应的签名文件，则右键菜单中会出现“RSA 验签”菜单，如下图所示：



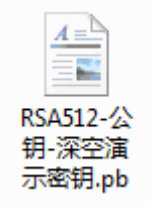
如果鼠标右键所点击文件是已被本软件加密的**.ency** 拓展名文件，则右键菜单中会出现 “RSA 解密”菜单，如下图所示：



二、 公钥和私钥文件

【公钥文件】含公钥数据的一个拓展名为**.pb** 的文件。用户可以随意存储、公开发布公钥文件。在软件使用过程中，需要公钥文件参与数字验签或者文件加密操作。公钥文件由**产品制造商**颁发给用户。软件在安装目录下已自带一个免费的公

钥文件（前面已提及），如下图所示。



双击该公钥文件，可以显示该公钥的相关信息，包括：**密钥版本号、密钥算法、密钥颁发时间、密钥授权期、密钥全球唯一 ID、密钥所有者名字、密钥所有者网址、密钥所有者电子邮件地址、密钥所有者物理地址、密钥所有者备注、密钥所有者头像、密钥当前状态等信息**，如下图所示：

【私钥文件】含私钥数据的一个拓展名为**.pr** 的文件。用户必须严格妥善保管私钥文件，建议只在固定的、较为安全的计算机中存储。在软件使用过程中，需要私钥文件参与数字签名或者文件解密操作。私钥文件由**产品制造商**颁发给用户。软件在安装目录下已自带一个免费的私钥文件（前面已提及），如下图所示。

双击该私钥文件，可以显示该私钥的相关信息，包括：**密钥版本号、密钥算法、密钥颁发时间、密钥授权期、密钥全球唯一 ID、密钥所有者名字、密钥所有者网址、密钥所有者电子邮件地址、密钥所有者物理地址、密钥所有者备注、密钥所有者头像、密钥当前状态等信息**，如下图所示：

【提示】产品制造商提供的上述免费公、私钥文件（后文分别简称**演示公钥**、**演示私钥**）是配对的：

用**演示公钥**加密的文件，可以被**演示私钥**解密；

用**演示私钥**签名的文件，可以被**演示公钥**验签；

演示公钥和演示私钥是用于产品演示使用，是公开的任何人都可以免费获取到，所以**对保密或敏感数据（进行加密或签名），**用户**不应使用这对演示密钥。**

【建议】用户向**产品制造商**申请不公开的、专属自己的、私有定制的私钥文件和配对公钥文件。

三、 数字签名

【作用】数字签名有两种功效，一是能确定消息确实是由发送方签名并发出来的，因为别人假冒不了发送方的签名，二是数字签名能确定消息的完整性。

当本产品作用于文件时，可以“记住”一个文件的内容状态，当内容有任何改动，比如新增或者删除任意字节，都能发现。当作用于文件夹时（如网站目录文件夹），可以记录下整个文件夹的状态（包括子文件、子文件夹的分布情况，子文件的内容状态，子文件夹的结构），当文件夹有任何改动，比如删除一个子文件或子文件夹，重命名一个文件或文件夹，新增一个文件或文件夹，修改子文件的内容，都能发现，并报告给用户。广泛应用于文件加密、文件夹前后比较、文章作者投稿、杂志社收稿、教学成绩提交、电子合同、电子签章、检测网站文件篡改、产品发布、产品文件完整性和来源唯一性检测等场合。

【使用方法】双击本软件程序，弹出如下对话框，选中“数字签名”功能：

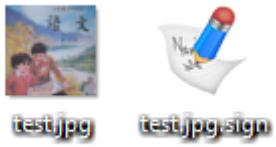
然后拖拽文件到列表框中（可一次选择多个文件进行批量操作），若要自定义签名数据文件输出路径，点击右边的“输出路径...“。最后点击第三步的“开始”,并按提示将私钥文件拖拽进去：

【ABO(All By One)模式说明】

如果启用 ABO 模式：当签名一个文件夹时，对该文件夹下的每个子文件只生成统一的一个签名数据文件；

如果不启用 ABO 模式：当签名一个文件夹时，对该文件夹下的每个子文件都生成各自独立的签名数据文件。

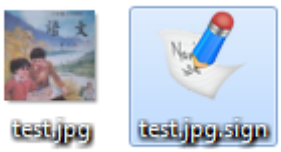
最后点击“**开始数字签名**”，执行完毕后，将生成一个拓展名为**.sign**的签名数据文件，如下图所示：



四、 数字验签

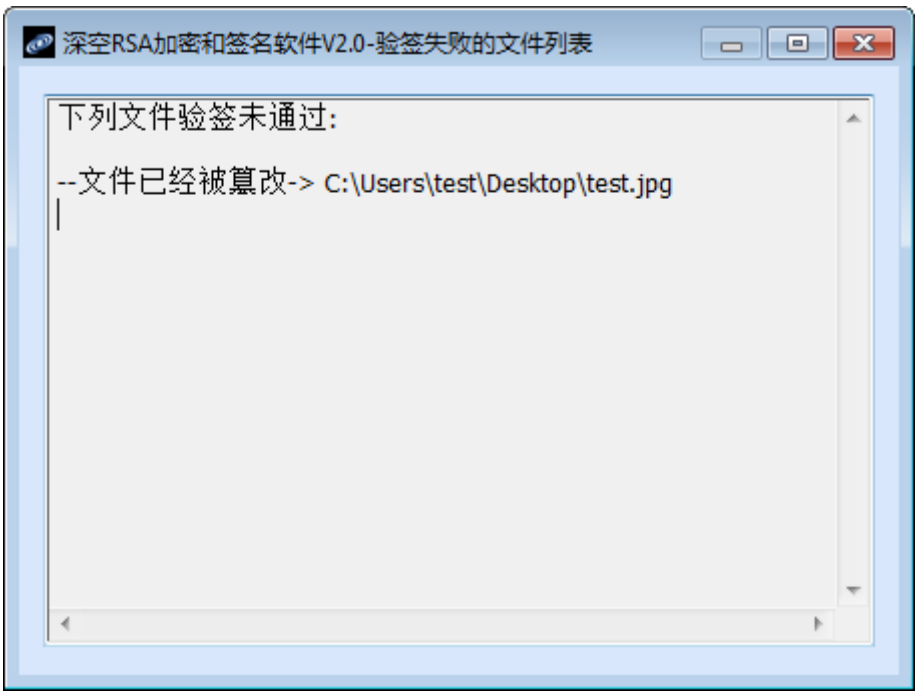
【作用】：使用数字验签，可以检查一个文件是否被篡改，并且识别签名人。当验签文件夹时，检查文件夹是否被篡改，如有则列出详细篡改清单。

【使用方法】双击签名数据文件(.sign 文件)（可一次选择多个文件进行批量操作）：

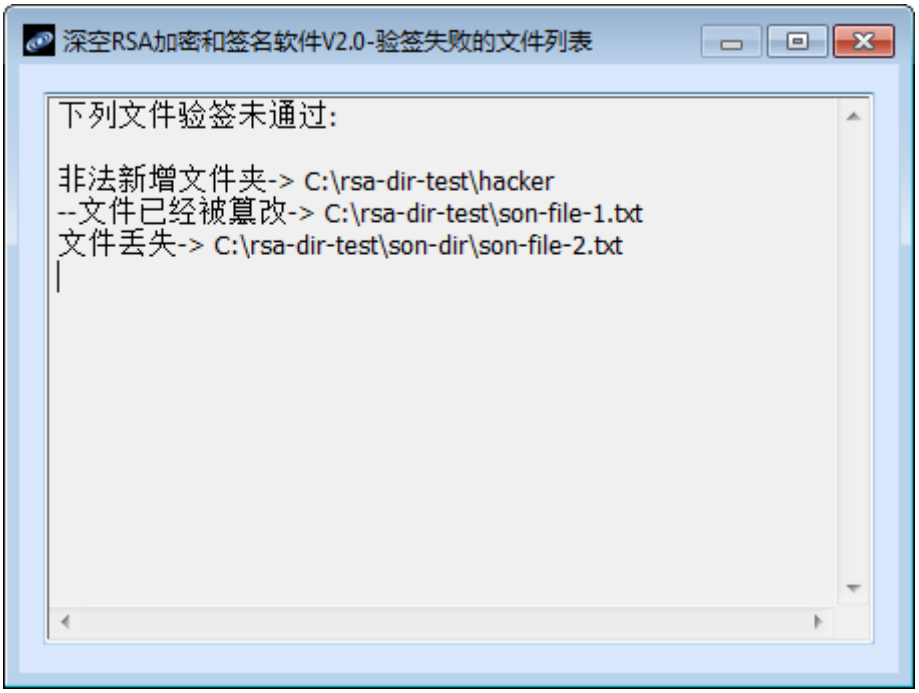


弹出签名者信息：

如果文件被篡改，则弹窗提示应类似下图：



如果验签对象是文件夹，而且文件夹中的子文件对象产生了变化，则验签弹窗提示类似下图：



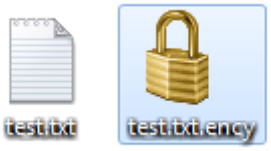
五、 加密

对要加密的文件右键（可一次选择多个文件进行批量操作），选中“加密”功能：

弹出提示输入公钥对话框，将公钥文件拖拽进去：

【加密“高级”选项提示】本程序默认使用 AES256_RSAx 算法加密文件（x 由公钥文件的密钥位数决定）。用户可以点击上图中的“**高级**”来更改加密算法，有关“**高级**”选项的详细介绍，请参考这里。

最后点击“开始加密”，加密完成后生成一个**.ency** 的文件：



【提示】用户可以选择加密后自动彻底删除原文件，只需勾选“删除原文件”即可，如下图所示：

六、 解密

双击**.ency** 拓展名的加密文件，弹出类似下图所示对话框：

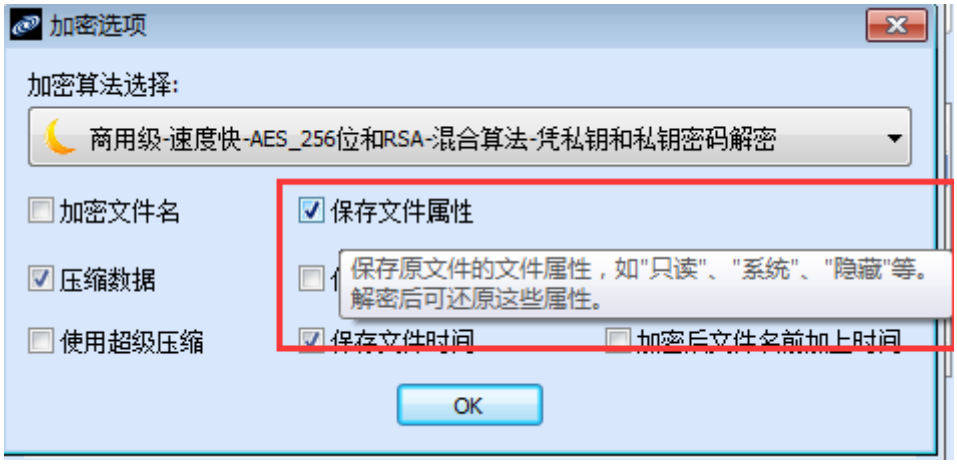
拖拽私钥文件到上图对话框，最后点击“**开始解密**”。

【提示】可一次选择多个文件进行批量操作。

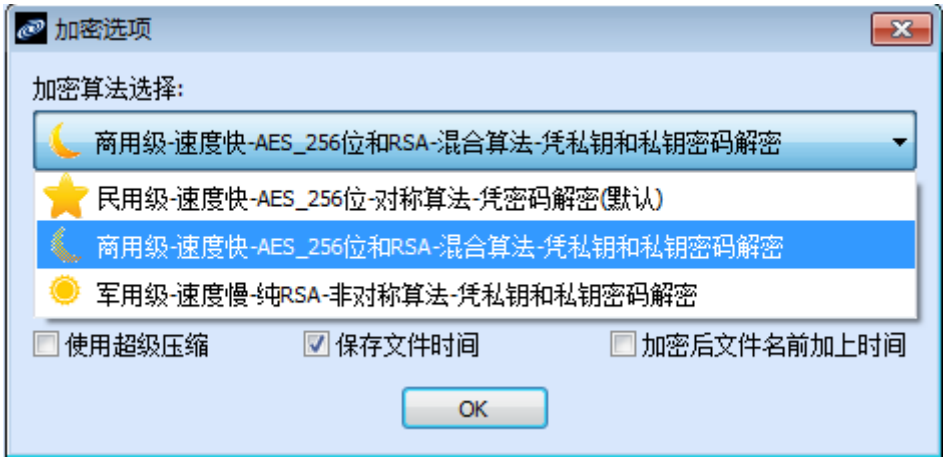
七、 加密操作 - 高级选项

用户进行加密操作时，还可以自由设置其它参数。在输入公钥文件或设置密码的对话框中，点击“**高级**”，出现多个选项，包括**“加密文件名”**（加密保存原文件的文件名，同时用随机值作为加密文件的文件名，解密后可还原回原文件名）、**“保存文件属性”**（解密时自动还原）、**“压缩数据”**（解密时自动解压）、**“保存文件安全属性”**（解密时自动还原）、**“加密打包成一个文件”**、**“使用超级压缩”**（解密时自动解压）、**“保存文件时间”**（包括创建时间和最后一次修改时间，解密时自动还原）、**“加密后文件名前加上时间”**，如下所示窗口：

并且每个选项在鼠标滑过时会有详细的提示，如下图所示：



用户还可以选择加密算法类型，本产品提供 3 种加密级别的算法。



适合**民用场合**的是 **AES256 加密算法**，属于对称算法。使用用户输入密码来加密文件，解密时输入解密密码即可。优点是简单易用，易于理解，**速度快。**

适合**商用场合**的是 **AES256 + RSAx 加密算法**（x 由公钥文件的密钥位数决定），属于混合算法，文件内容采用 AES256 加密，AES256 的加解密密钥采用 RSAx 加密后存储在加密文件中，优点是速度快，AES 密钥被公钥加密保护，当 x 的位数不小于 2048 时，**密钥的安全性高，本产品 x 的位数支持 512 位-8192 位。**

适合**高安全场合（如军用场合）**的是 **RSAx 纯公钥加密算法**（x 由公钥文件的密钥位数决定），属于公钥算法，文件内容采用 RSAx 加密，解密私钥文件由用户自己保存，不存储在加密文件中，优点是使用了纯 RSAx 算法，当 x 的位数不小于 2048 时，提供了**高安全性，本产品 x 的位数支持 512 位-8192 位。**

八、 清除磁盘上已删除数据

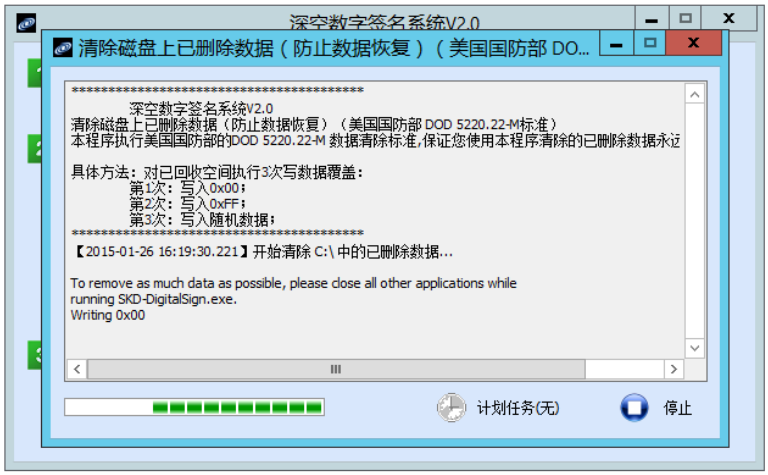
磁盘上已删除的数据如果未经特殊处理，那么非法人员可以通过技术手段进行恢复。本程序提供彻底清除磁盘上已删除数据的功能，使得已删除数据永远无法恢复（**美国国防部 DOD5220.22-M 标准**）。本功能是基于磁盘分区的操作，如果要彻底删除现有文件，请参考**彻底删除文件**。

【具体实现细节】对要删除的文件进行 2-3 次完全覆盖写入：第一次写入 0xFF（全 1），第二次写入 0x00（全 0），**如果是企业版和旗舰版，还将进行第三次写入 0xXX（随机数据）**，达到彻底删除文件，防止数据恢复的目的。

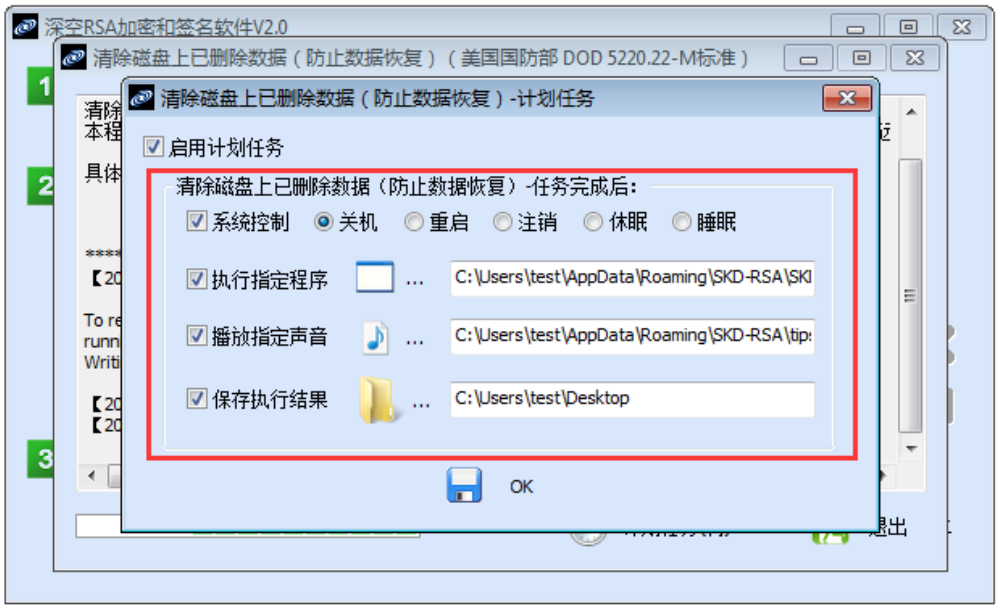
在任意空白处，单击鼠标右键，点击本软件菜单：

然后选择“*功能 5：清除磁盘上已删除数据*”，如下图所示：

下图是正在执行清除操作时的界面：



上图 “**计划任务**”可设置清除完成后的动作，包括“**关机**”、“**重启**”、“**注销**”、“**休眠**”、“**睡眠**”、“**执行指定程序**”、“**播放指定声音**”、“**保存执行结果**”（将执行结果保存到一个指定的文件夹），如下图所示：



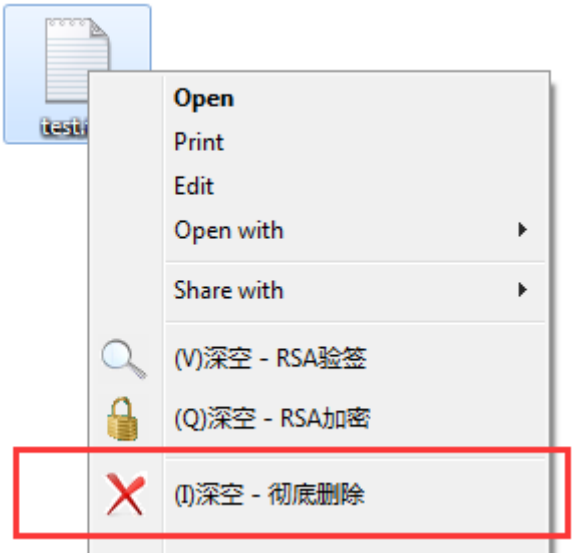
九、 彻底删除文件

本功能是基于现有文件的操作，如果要彻底清除磁盘分区上之前删除的数据，请参考**清除磁盘上已删除数据**。

传统的删除文件，实际上只是在磁盘上标记文件已删除，并未真正擦除文件在磁盘上的记录，因此可以通过技术手段进行恢复。本程序提供彻底删除文件的功能，使得文件永远无法恢复（**美国国防部 DOD5220.22-M 标准**）。

【具体实现细节】对要删除的文件进行 2-3 次完全覆盖写入：第一次写入 0xFF（全 1），第二次写入 0x00（全 0），**如果是企业版和旗舰版，还将进行第三次写入 0xXX（随机数据），如果是旗舰版，还会执行 26 次重命名（文件名重命名为全 a、全 b、全 c...全 z）**，达到彻底删除文件，防止数据恢复的目的。

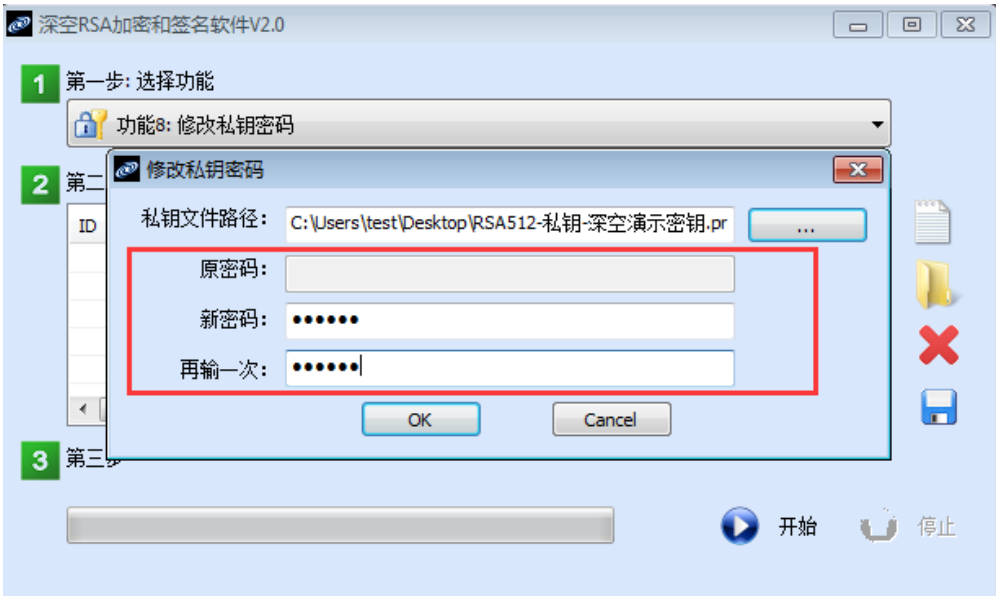
鼠标右键选中要彻底删除的文件，然后点击“**彻底删除**”，如下图所示：



十、 修改私钥密码

产品制造商颁发私钥文件给用户时，私钥文件具有默认的保护密码，如果用户未修改默认密码，则私钥文件在使用时（比如签名操作或解密操作）无需用户输入私钥密码即可使用。

【建议】用户获取到私钥文件后，第一时间修改私钥文件保护密码。选择“修改私钥密码”功能，如下图所示：



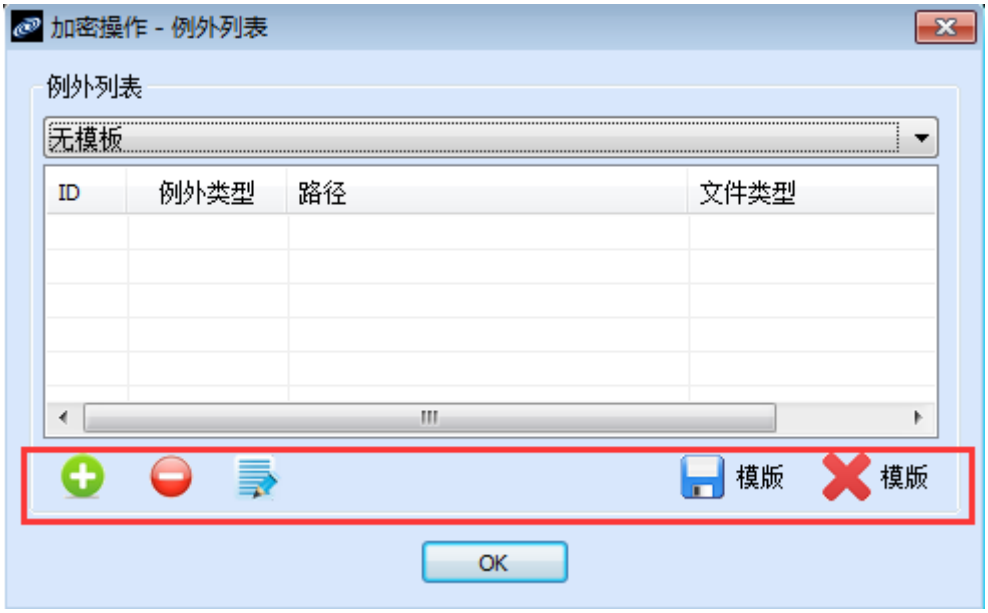
十一、 恢复默认配置操作

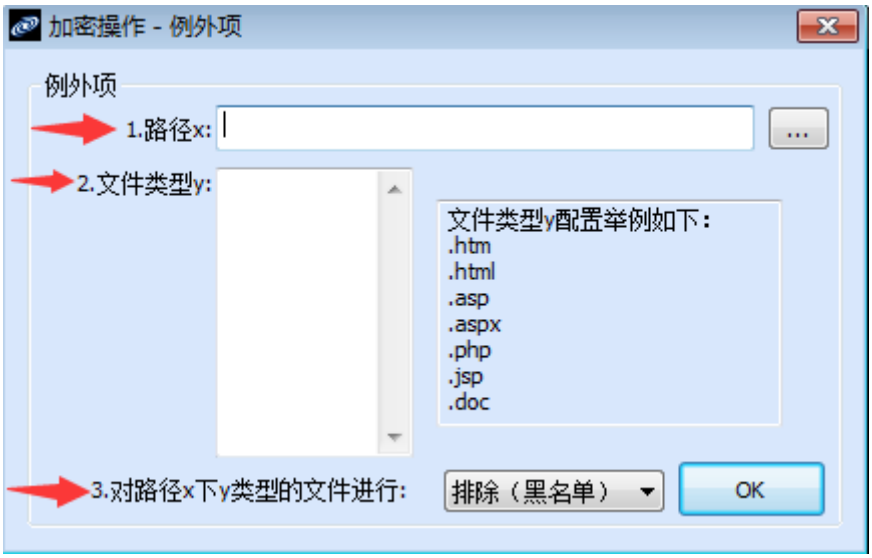
若要恢复默认配置，可在第一步的功能选择中选择“恢复默认配置 “。

十二、 加密或签名时设置例外项

用户在进行加密或签名操作时，可以设置例外项。这里以加密操作为例做介绍（签名操作中的例外项设置和加密操作的完全一致）。在进行加密操作时，点击**“例外...”** ，如下图所示：

弹出例外项配置对话框，用户可以通过界面上提供的相关按钮完成**“添加”**、**“修改”**、**“删除”**功能，同时可以把当前配置的例外项信息保存为一个模板，供日后重复操作使用，如下图所示：





例外项的添加规则遵从下面的公式：

什么路径+什么文件类型+要怎么处理（是排除还是筛选）

【举例 1】对 c:\rsa-test 文件夹进行加密操作，此时用户配置的例外项信息如下：

路径： c:\rsa-test\uploads\

文件类型： .tmp

处理方式： 排除（黑名单）

表明：用户希望程序对 c:\rsa-test\uploads\ 文件夹下的所有 .tmp 拓展名的文件一律跳过，无需加密。

【举例 2】对 c:\rsa-test 文件夹进行加密操作，此时用户配置的例外项信息如下：

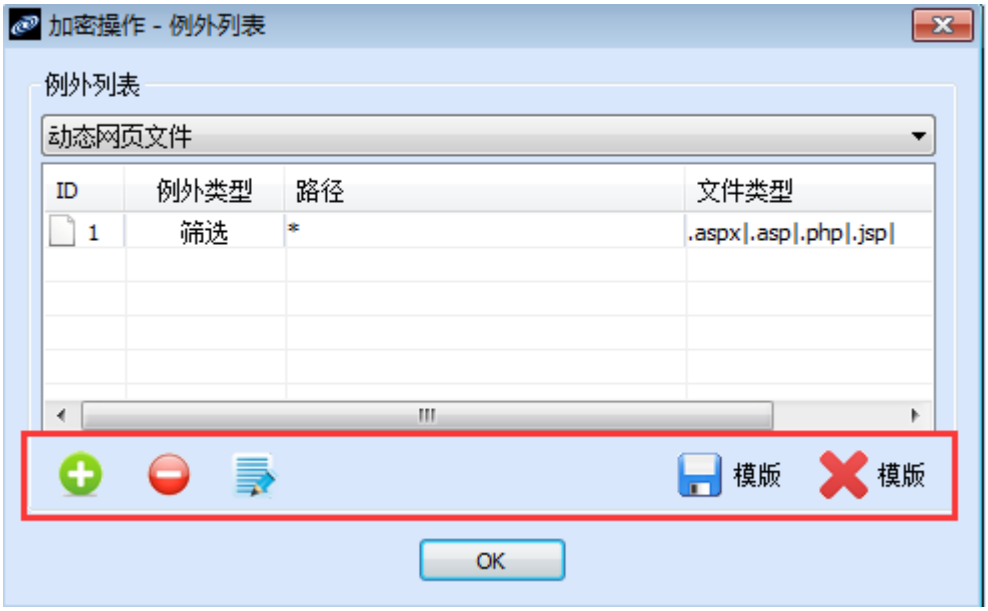
路径： *

文件类型： .aspx、.asp、.php、.jsp

处理方式： 过滤（白名单）

表明：用户希望程序只对 c:\rsa-test\ 文件夹下的所有 .aspx、.asp、.php、.jsp 拓展名的文件进行加密，其它类型的文件一律跳过无需加密。

下面为配置完毕并保存为模板的效果图：



点击上图“**OK**”后生效。

第四章 技术支持及联系方式

用户在使用 **深空 RSA 加密和签名软件** 过程中遇到任何技术问题，可以通过下列方式与本产品制造商 **福建深空信息技术有限公司**（FuJian SkyDeep Information Technology Co.,Ltd)取得联系。

■统一客服热线:400-0300-630 ■传真: 0591-22856511

■电子邮件: sales@sky-deep.com ■统一客服 QQ: 652500285

■公司网址：www.sky-deep.com ■邮编: 350002

■公司地址:福建省 福州市 晋安区 儒江西路 东方名城 华郡 25 号楼 01-02 单元 2502 室

第五章 附录

附录一 高级加密标准（Advanced Encryption Standard，AES）

AES 在密码学中又称 Rijndael 加密法，是美国联邦政府采用的一种区块加密标准。这个标准用来替代原先的 DES，已经被多方分析且广为全世界所使用。经过五年的甄选流程，高级加密标准由美国国家标准与技术研究院（NIST）于 2001 年 11 月 26 日发布于 FIPS PUB 197，并在 2002 年 5 月 26 日成为有效的标准。2006 年，高级加密标准已然成为对称密钥加密中最流行的算法之一。

该算法为比利时密码学家 Joan Daemen 和 Vincent Rijmen 所设计，结合两位作者的名字，以 Rijndael 为名投稿高级加密标准的甄选流程。（Rijndael 的发音近于 "Rhine doll"）

严格地说，AES 和 Rijndael 加密法并不完全一样（虽然在实际应用中二者可以互换），因为 Rijndael 加密法可以支持更大范围的区块和密钥长度：AES 的区块长度固定为 128 比特，密钥长度则可以是 128，192 或 256 比特；而 Rijndael 使用的密钥和区块长度可以是 32 位的整数倍，以 128 位为下限，256 比特为上限。加密过程中使用的密钥是由 Rijndael 密钥生成方案产生。

➢ AES 算法描述

大多数 AES 计算是在一个特别的有限域完成的。

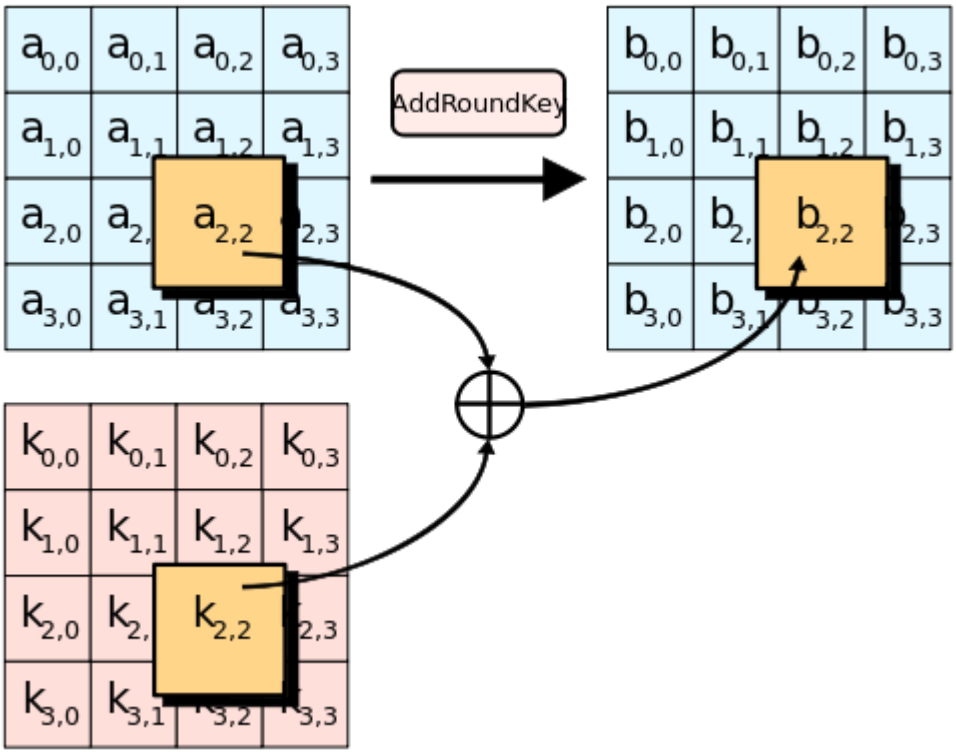
AES 加密过程是在一个 4×4 的字节矩阵上运作，这个矩阵又称为“体（state）”，其初值就是一个明文区块（矩阵中一个元素大小就是明文区块中的一个 Byte）。加密时，各轮 AES 加密循环（除最后一轮外）均包含 4 个步骤：

1. AddRoundKey — 矩阵中的每一个字节都与该次回合密钥（round key）做 XOR 运算；每个子密钥由密钥生成方案产生。
2. SubBytes — 通过一个非线性的替换函数，用查找表的方式把每个字节替换成对应的字节。
3. ShiftRows — 将矩阵中的每个横列进行循环式移位。
4. MixColumns — 为了充分混合矩阵中各个直行的操作。这个步骤使用线性转换来混合每内联的四个字节。

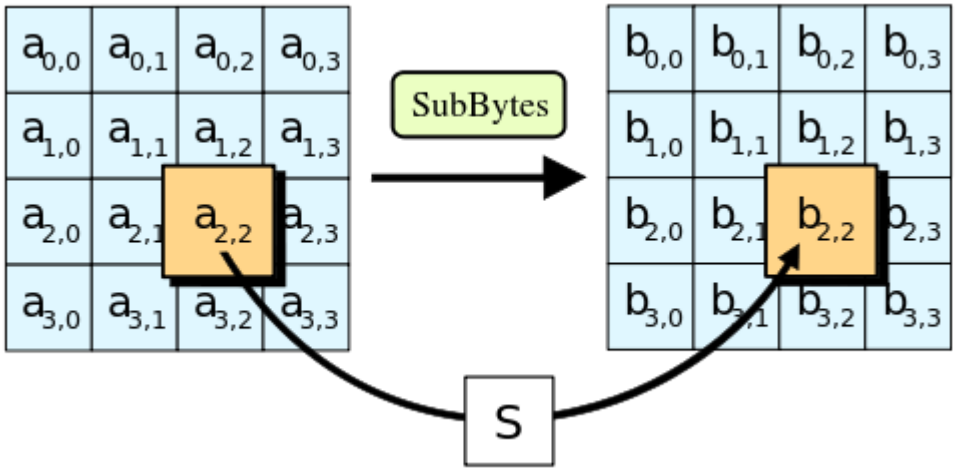
最后一个加密循环中省略 MixColumns 步骤，而以另一个 AddRoundKey 取代。

- **具体步骤**

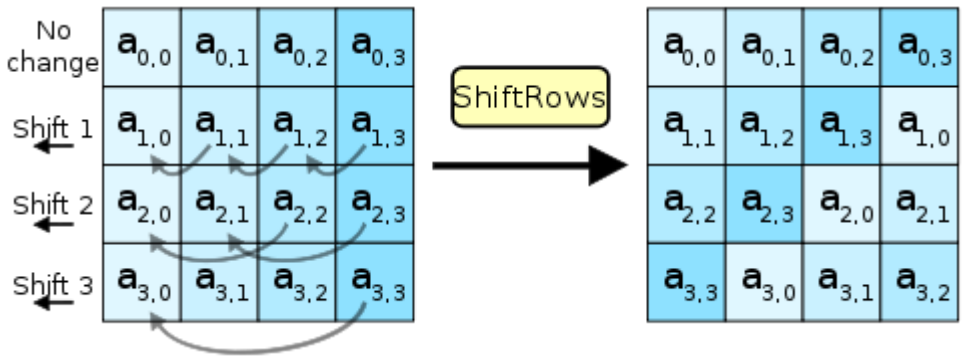
AddRoundKey 步骤：回合密钥将会与原矩阵合并。在每次的加密循环中，都会由主密钥产生一把回合密钥（通过 Rijndael 密钥生成方案产生），这把密钥大小会跟原矩阵一样，以与原矩阵中每个对应的字节作异或（⊕）加法。



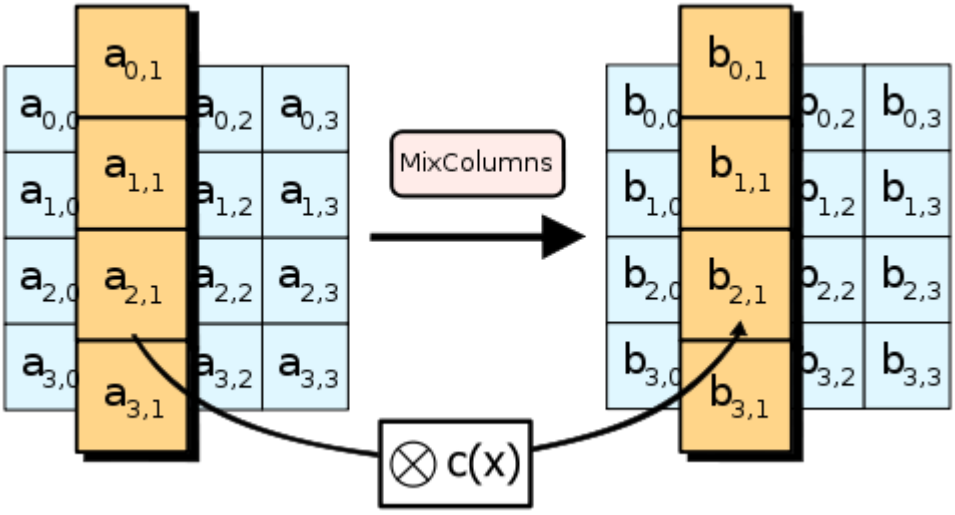
SubBytes 步骤：在 SubBytes 步骤中，矩阵中的各字节通过一个 8 位的 S-box 进行转换。这个步骤提供了加密法非线性的变换能力。S-box 与 **GF**(*2*^{8}) 上的乘法反元素有关，已知具有良好的非线性特性。为了避免简单代数性质的攻击，S-box 结合了乘法反元素及一个可逆的仿射变换矩阵建构而成。 此外在建构 S-box 时，刻意避开了固定点与反固定点，即以 S-box 替换字节的结果会相当于错排的结果。



ShiftRows 步骤：ShiftRows 是针对矩阵的每一个横列操作的步骤。 在此步骤中，每一行都向左循环位移某个偏移量。在 AES 中（区块大小 128 位），第一行维持不变，第二行里的每个字节都向左循环移动一格。同理，第三行及第四行向左循环位移的偏移量就分别是 2 和 3。128 位和 192 比特的区块在此步骤的循环位移的模式相同。经过 ShiftRows 之后，矩阵中每一竖列，都是由输入矩阵中的每个不同列中的元素组成。Rijndael 算法的版本中，偏移量和 AES 有少许不同；对于长度 256 比特的区块，第一行仍然维持不变，第二行、第三行、第四行的偏移量分别是 1 字节、3 字节、4 位组。除此之外，ShiftRows 操作步骤在 Rijndael 和 AES 中完全相同。

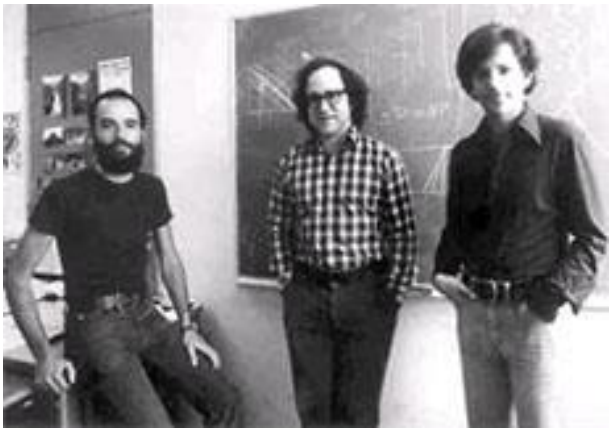


MixColumns 步骤：在 MixColumns 步骤，每一直行的四个字节通过线性变换互相结合。每一直行的四个元素分别当作$1, x, x^2, x^3$的系数，合并即为 **GF**(*2*⁸) 中的一个多项式，接着将此多项式和一个固定的多项式 $c(x) = 3x^3 + x^2 + x + 2$ 在 modulo $x^4 + 1$ 下相乘。此步骤亦可视为 Rijndael 有限域之下的矩阵乘法。MixColumns 函数接受 4 个字节的输入，输出 4 个字节，每一个输入的字节都会对输出的四个字节造成影响。因此 ShiftRows 和 MixColumns 两步骤为这个密码系统提供了扩散性。



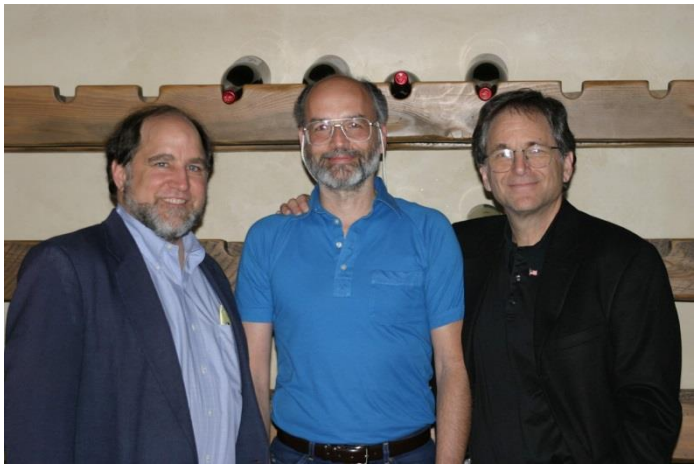
附录二　RSA 公钥加密算法

RSA 是第一个比较完善的公开密钥算法，它既能用于加密，也能用于数字签名。RSA 以它的三个发明者 Ron Rivest, Adi Shamir, Leonard Adleman 的名字首字母命名，这个算法经受住了多年深入的密码分析，虽然密码分析者既不能证明也不能否定 RSA 的安全性，但这恰恰说明该算法有一定的可信性，目前它已经成为最流行的公开密钥算法。



图为 RSA 公开密钥算法的发明人,从左到右 Adi Shamir, Ron Rivest, Leonard Adleman.

照片摄于 1978 年.



从左到右 Ron Rivest, Adi Shamir, Leonard Adleman.

RSA 的安全基于大数分解的难度。其公钥和私钥是一对大素数（100 到 200 位十进制数或更大）的函数。从一个公钥和密文恢复出明文的难度，等价于分解两个大素数之积（这是公认的数学难题）。 RSA 的公钥、私钥的组成，以及加密、解密的公式可见于下表：

公钥 KU	n: 两素数 p 和 q 的乘积（p 和 q 必须保密） e: 与（p-1）（q-1）互质
私钥 KR	d: e^{-1} (mod(p-1)(q-1)) n:
加密	$C \equiv m^e \bmod n$
解密	$m \equiv c^d \bmod n$

RSA 公钥密码学算法详细介绍如下:

➢ RSA 算法描述

RSA 公钥密码体制的基本原理：**根据数论，寻求两个大素数比较简单，而将他们的乘积分解开则极为困难。**

欧拉函数Φ(n)：Φ(n)表示小于 n 且与 n 互素的正整数个数。显然，对于任一素数 p，有Φ(p) = p-1。

求欧拉函数值:对两个不同的素数 p 和 q ,如果 n=pq ,则Φ(n) = Φ(p)×Φ(q) = (p-1)×(q-1)

➢ RSA 算法密钥计算过程

用户秘密选取两个大素数 p 和 q，计算 n=pq，n 称为 RSA 算法的模数，公开。

计算出 n 的欧拉函数Φ(n) = (p-1)×(q-1)，保密。

从(1, Φ(n))中随机地选择一个与Φ(n)互素的数 e 作为加密密钥，公开。

计算出满足下式的 d 作为解密密钥，保密。

$$ed=1 \bmod \Phi(n)$$

RSA 算法密钥：

加密密钥 PK = |e, n|　　公开

解密密钥 SK = |d, n|　　保密

举例：选择两个素数 p=7 以及 q=17 。

计算：n=pq=7×17=119，$\Phi(n)=(p-1)(q-1)=96$ 。

选择小于$\Phi(n)$且与$\Phi(n)$互素的 e ，这里取 e=5 。

根据式： $ed=1 \bmod \Phi(n)$ 计算 d ：

代入已知值：5d = k×96 + 1，求得 d = 77

➢ RSA 算法加密解密过程

RSA 算法属于分组密码，明文在加密前要进行分组，分组的值 m 要满足：0 < m < n

加密算法：$C = E(m) \equiv m^e \bmod n$

解密算法：$m = D(c) \equiv c^d \bmod n$

证明加密和解密是一对逆运算：

欧拉定理：对任何互素的整数 a 和 n，有：

$$a\Phi(n) \equiv 1 \bmod n \rightarrow a\Phi(n)+1 \equiv a \bmod n$$

欧拉定理推论：给定两个素数 p 和 q，以及整数 n=pq 和 m，其中 $0 < m < n$ ，则下列关系成立：

$$m\Phi(n)+1 \equiv m \bmod n \rightarrow m\Phi(n) \equiv 1 \bmod n$$

$$\rightarrow [\, m\Phi(n) \,]k \equiv 1 \bmod n \rightarrow mk\Phi(n) \equiv 1 \bmod n$$

证明：因为 $ed = 1 \bmod \Phi(n)$，所以存在 k 使得

$ed = k\Phi(n)+1$，k 为不小于 1 的整数。

$$D(c) = cd \bmod n \equiv (me)d \bmod n$$

$$\equiv mk\Phi(n)+1 \bmod n \equiv m \bmod n = m$$

➢ RSA 算法的几点说明

对于 RSA 算法，相同的明文映射出相同的密文。

RSA 算法的密钥长度：是指模数 n 的长度，即 n 的二进制位数，而不是 e 或 d 的长度。

RSA 的保密性基于大数进行因式分解很花时间，因此，进行 RSA 加密时，应选足够长的密钥。512bit 已被证明不安全，1024bit 也不保险。

RSA 最快情况也比 DES 慢 100 倍，仅适合少量数据的加密。公钥 e 取较小值的方案不安全。

- **RSA 算法的实现**

大素数的生成(p,q)：采用先随机生成大奇数，然后检验其是否为素数。Rabin Miller 算法。

幂运算和大数除法：加解密运算。

- **RSA 算法参数的选择**

模数 n 与素数 p,q，加密密钥 e 和解密密钥 d。