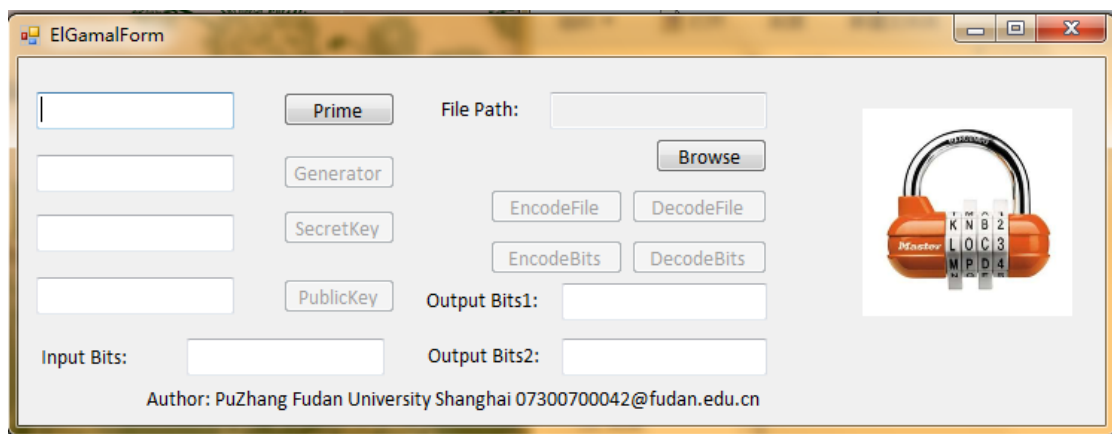


# ElGamal 程序文档说明

本程序我采用的 C#编程语言，编程环境是 Visual Studio 2010。如果要运行本程序，建议您的电脑首先安装 .net Framework 4.0 及以上版本。程序采用图形化界面，操作简单。先对程序的功能说明如下。程序的面板如下图所示。Prime 按钮用来生成一个 60 位的安全素数，Generator 按钮用来生成一个在  $Z_p^*$  中的生成元，SecretKey 从  $Z_p^*$  中随机选择一个数用来作为其密钥，PublicKey 用来根据 SecretKey 和 Generator 生成相应的公钥，所有生成的结果都显示在左边的文本框中。当然，用户也可以在文本框中手动输入各项数字，不过输入的数字要通过检验，符合要求，否则会报错。

并不是所有的按钮都是随时可用的，有些按钮只有当条件满足了才会可用，比如说，当且仅当输入的素数是 60 位的安全素数时，Generator 生成元按钮才可用。Browse 用来选择文件对话框选择要加密或者解密的文件，文件的路径显示在 File Path 对应的文本框中。

另外，我的程序还可以对二进制串进行加密或者解密，用户可以再 Input Bits 文本框中输入二进制串，然后点击 EncodeBits 或者 DecodeBits 来加密或者解密二进制串。结果会显示在 Output Bits1 和 Output Bits2 中。同样解密的话也是输入相应的数，然后再进行解密运算。



ElGamal 实现主要的难点在于密钥的产生。我在生成密钥的时候采用了 Miller-Rabin 检验法，随机选择一个 60 位的整数，然后对其进行 100 次检验，可以保证错误率小于  $4^{(-100)}$ 。当然，在进一步操作的时候，我还进行了优化，比如每次检验的时候首先用小于 256 的小素数进行“试除法”来检验，之后采用 Miller-Rabin 检验法。

另外，在寻找  $Z_p^*$  的生成元的时候，我利用了性质， $Z_p^*$  中的元素的阶应该都是  $p-1$  的因子。而这样的因子只有两个 2 和  $(p-1)/2$ ，这是因为在  $p$  是满足要求的安全素数。所以我只需要随机选取  $Z_p^*$  中的一个元素，然后检验其 2 和  $(p-1)/2$  次幂是否是 1 即可。如果不是，那么这个数就是符合要求的生成元。

在加密和解密的时候，要求明文映射到  $Z_p^*$  上，另外，每次操作的时候都必须是以  $p$  为单位（读/写）。我采用了如下的编码方法，首先把待加密的文件(file1)复制一份(file2)，然后在这份文件(file2)的末尾添加足够数量的 0，以保证文件(file2)的大小是 64bits 的整数倍。如果原来就是 64bits 的整数倍也要添加 0，然后再添加一个 64bits 的文件长度。这个过程成为 padding。这个时候可以对文件(file2)以 64bits 的单位读写了，不过不能保证是在  $Z_p^*$  上，我采

用如下的方法，读取一个 64bits 的数  $m$ ，然后写入另一个文件  $(file3)m/p+1$  和  $m\%p+1$ ，这样可以保证文件  $(file3)$  中的数字都是在 1 到  $p-1$  之间。然后就可以顺次读取一个 64bits 的数，然后对其进行加密，输出到目标文件  $(file4)$  中，而  $file4$  就是加密完成的文件。解密过程与此类似。

一个小的问题，就是 C# 没有可以生成 Long 型的随机类。我采用了首先生成一个 0 到 1 的随机 double 型数字  $factor$ ，然后再用公式  $factor(high-low)+low$ ，就可以得到 low 到 high 之间的一个随机数。我仔细分析了 double 型数据的精度范围，发现这样做的话，不会导致精度的降低，而且如果原来的 double 型随机数发生器足够的好的话，可以认为用这样方法生成的随机数也是均匀分布在 low 到 high 的区间中的。

由于大部分运算都发生在 60 位的整数和 60 位的整数之间,所以,乘法会导致溢出,我没有使用乘法,而是把乘法转换用加法和移位来做。具体来说，要计算  $A*B$ ，那么如果  $B$  是奇数，结果加  $A$ ，然后  $B$  减 1，然后  $A$  左移一位， $B$  右移一位。循环知道  $B$  为 0 为止，然后把最终的  $A$  加入到结果中，就是  $A*B$ ，每一步如果发现可能会溢出，立即取模运算。这样可以保证结果的正确性。

由于程序中没有采用多线程机制，所以在加密和解密大型文件的时候，会暂时失去相应。

07300700042 张璞  
复旦大学计算机科学技术学院  
计算机科学技术系 2008 级  
2010/11/13