密码算法实现报告

一、 对称密码部分

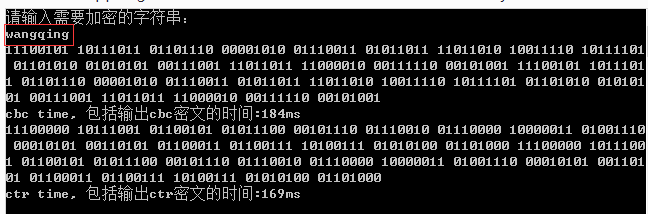
1. AES-128的实现，要求:

(1) 密钥为0x 00000001 00000001 00000001 00000001;

(2) 加密明文填充后的分组数大于等于2； 使用CBC和CTR两种模式分别加密，IV值均为0。

(3) 提交明密文以及对应的C语言代码。

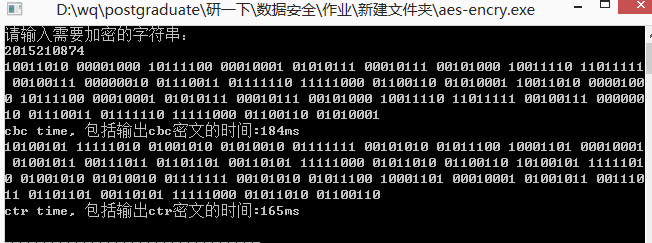
(4) 测试加密的算法软件效率。



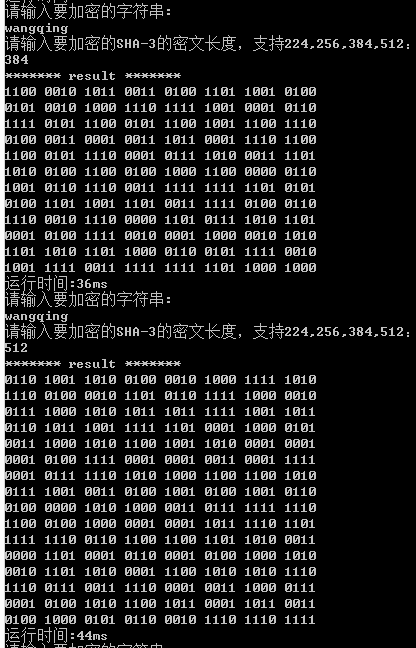
填充规则为：PKCS7

CTR的计数器：从0开始，包括0，每次加1.

State和Key都是4\*4的矩阵，按列读入。



２．**Keccak（SHA-3)算法实现：输入消息为每位同学姓名的ASCII表示，输出为杂凑值以及加密速度。**





**３. 公钥密码部分**

**RSA算法的实现：(1)为必做题，(2),(3),(3)为选做题。**

**(1) 产生两个512位的随机数p1, p2，检测其是否为素数。计算n=p1\*p2;**

**(2) 产生一个私钥ｅ，利用欧几里德算法计算公钥ｄ.**

**(3) 计算密文Ｃ＝Ｍｄｍｏｄｎ．**

**(4) 解密明文　Ｍ＝Ｃｅｍｏｄｎ．**

确定底数a和n的Miller-Rabin算法正确,曾经输出3000以内的素数进行验证，结果非常理想。截图如下：

50为输入的随机数种子值：





当随机数种子为233424，可以看到随机结果不相同：

