算法测试向量要求

算法设计团队应提供分组长度/密钥长度为128/128、128/256、256/256三种版本的分组算法的测试向量。验证数据应满足以下要求：

（**1**）**ECB**模式测试向量文件

10组测试样本分别放在10个文件夹中，文件夹用数字

1、2……10分别命名。每组测试样本包含3个十六进制数据文件，分别为明文（文件命名为p.dat）、密钥（文件命名为key.dat）和密文（文件命名为c.dat）。选择随机数据作为明文、密钥，10组明文输入长度应不同。

（**2**）**CBC**模式测试向量文件

10组测试样本分别放在10个文件夹中，文件夹用数字1、2……10分别命名。每组测试样本包含3个十六进制数据文件，分别为明文（文件命名为p.dat）、密钥（文件命名为key.dat）和密文（文件命名为c.dat）。选择随机数据作为明文、密钥，10组明文输入长度应不同。

（3）蒙特卡洛测试向量文件

分别选择随机数作为明文、密钥，用同一密钥对明文或上一次的密文结果进行加密，输出1次、100次、10000次加密后的密文结果。相关数据以txt文件形式提供。