本次大作业包含三个部分：分组密码、序列密码、Hash函数

1. 编程实现DES、AES-128、SM4三个算法的加解密运算。使用CBC模式，加密一段16K的明文(随机产生)。密钥、IV随机生成。
   1. 编程实现RC4算法，生成16K的密钥流。初始密钥（128字节）。
   2. 使用B-M算法，生成一段序列最短LFSR(生成10个比特长度的序列)
2. 编码实现SHA-2、SM3、SHA-3算法，压缩16K左右的随机数据

要求：

1. 正确性
2. 算法实现效率要大于等于100Mbps
3. 上述问题中16K的随机数据保持一致，相关的随机密钥、IV和代码、结果一起给出。