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。

2.1 编程实现 RC4 算法，生成 16K 的密钥流。初始密钥（128 字节）。

2.2 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)

3、 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。