1. (对称密码分析)阅读论文On the security of 2-key triple DES[1], 看懂并简述the van Oorschot-Wiener attack以及本文的分析方法。包括算法攻击思路，攻击的时间和数据复杂度以及如何利用部分明文信息进行攻击。
2. （对称密码算法实现）实现分组密码AES128-CBC以及哈希算法SHA3-256。

要求：1.AES-CBC 写出加密和解密算法。IV随机选取，加密1M或更长数据。

2.SHA3-256压缩1M或更长数据。3.保证正确性 4.要求算法效率大于100Mbps